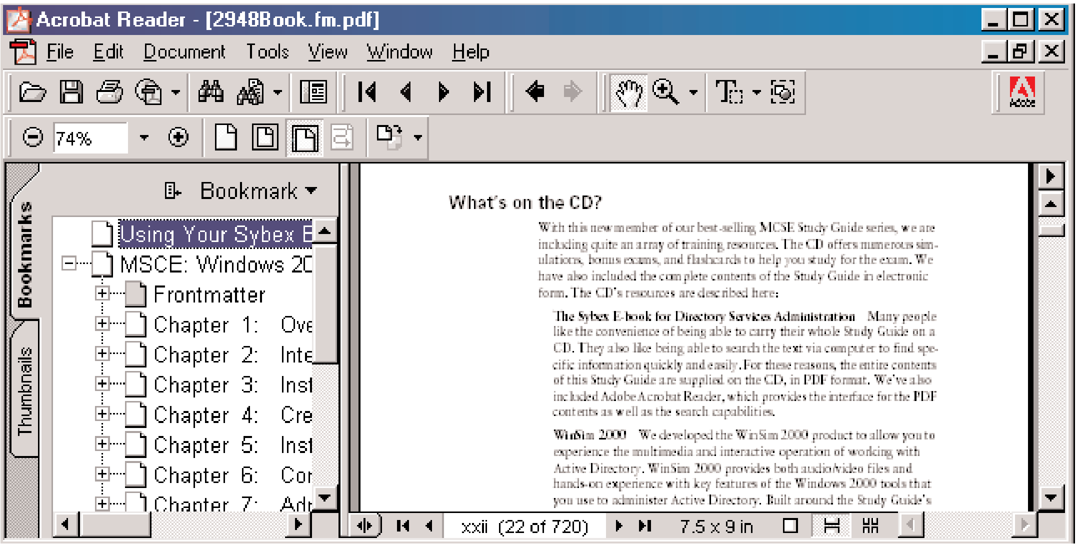
# Using Your Sybex Electronic Book

To realize the full potential of this Sybex electronic book, you must have Adobe Acrobat Reader with Search installed on your computer. To find out if you have the correct version of Acrobat Reader, click on the Edit menu—Search should be an option within this menu file. If Search is not an option in the Edit menu, please exit this application and install Adobe Acrobat Reader with Search from this CD (double-click rp500enu.exe in the Adobe folder).

## Navigation

Navigate through the book by clicking on the headings that appear in the left panel; the corresponding page from the book displays in the right panel.



What's on the CD?

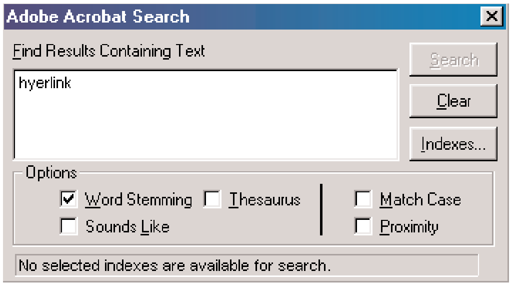
With this new member of our best-selling MCSE Study Guide series, we are including quite an array of training resources. The CD offers numerous simulations, bonus exams, and flashcards to help you study for the exam. We have also included the complete contents of the Study Guide in electronic form. The CD's resources are described here:

**The Sybex E-book for Directory Services Administration** Many people like the convenience of being able to carry their whole Study Guide on a CD. They also like being able to search the text via computer to find specific information quickly and easily. For these reasons, the entire contents of this Study Guide are supplied on the CD, in PDF format. We've also included Adobe Acrobat Reader, which provides the interface for the PDF contents as well as the search capabilities.

**WinSim 2000** We developed the WinSim 2000 product to allow you to experience the multimedia and interactive operation of working with Active Directory. WinSim 2000 provides both audio/video files and hands-on experience with key features of the Windows 2000 tools that you use to administer Active Directory. Built around the Study Guide's

xxii (22 of 720) 7.5 x 9 in

## Search



Find Results Containing Text: hyerlink

☑ Word Stemming ☐ Thesaurus ☐ Match Case
☐ Sounds Like ☐ Proximity

No selected indexes are available for search.

To search, click the Search Query button on the toolbar or choose Edit >Search > Query to open the Search window. In the Adobe Acrobat Search dialog's text field, type the text you want to find and click Search.

Use the Search Next button (Control+U) and Search Previous button (Control+Y) to go to other matches in the book. The Search command also has powerful tools for limiting and expanding the definition of the term you are searching for. Refer to Acrobat's online Help (Help > Plug-In Help > Using Acrobat Search) for more information.

# CCA:
# Citrix® MetaFrame XP™ 1.0 Administration
## Study Guide

Brad Price
John Price

San Francisco • London

Associate Publisher: Neil Edde
Acquisitions and Developmental Editor: Elizabeth Hurley
Editor: Linda Recktenwald
Production Editor: Mae Lum
Technical Editors: Hai Hilvitz, Scott Warmbrand
Graphic Illustrator: Tony Jonick
Electronic Publishing Specialists: Stacey Loomis, Bill Clark, Interactive Composition Corporation
Proofreaders: Emily Hsuan, Nelson Kim, David Nash, Laurie O'Connell, Yariv Rabinovitch, Nancy Riddiough
Indexer: Nancy Guenther
CD Coordinator: Dan Mummert
CD Technician: Kevin Ly
Book Designer: Bill Gibson
Cover Designer: Archer Design
Cover Photographer: John Wang, PhotoDisc

Library of Congress Card Number: 2001096989

ISBN: 0-7821-4057-2

SYBEX is an independent entity from Citrix Systems, Inc., and not affiliated with Citrix Systems, Inc. in any manner. This publication may be used in assisting students to prepare for a Citrix Certified Administrator Exam. Neither Citrix Systems, its designated review company, nor SYBEX warrants that use of this publication will ensure passing the relevant exam. Citrix is either a registered trademark or trademark of Citrix Systems, Inc. in the United States and/or other countries.

TRADEMARKS: SYBEX has attempted throughout this book to distinguish proprietary trademarks from descriptive terms by following the capitalization style used by the manufacturer.

The author and publisher have made their best efforts to prepare this book, and the content is based upon final release software whenever possible. Portions of the manuscript may be based upon pre-release versions supplied by software manufacturer(s). The author and the publisher make no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accept no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this book.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

SYBEX

To Our Valued Readers:

In a CertCities.com article dated December 15, 2001, Citrix Systems' CCA certification was ranked #8 in a list of the "10 Hottest Certifications for 2002." This shouldn't come as a surprise, especially when you consider the success Citrix has seen with their flagship product, MetaFrame XP, since its release last year. Citrix continues to expand its dominance in the application services market, and as companies begin integrating Citrix products into their multi-platform IT infrastructures, you can be assured of high demand for professionals with the CCA certification.

Sybex is proud to have helped thousands of IT professionals prepare for certification exams over the years, and we are excited about the opportunity to continue to provide professionals like you with the skills needed to succeed in the highly competitive IT industry.

Our authors and editors have worked hard to ensure that the *CCA: Citrix MetaFrame XP 1.0 Study Guide* you hold in your hand is comprehensive, in-depth, and pedagogically sound. We're confident that this book will meet and exceed the demanding standards of the certification marketplace and help you, the Citrix certification candidate, succeed in your endeavors.

As always, your feedback is important to us. Please send your comments, questions, or suggestions to support@sybex.com.

Good luck in pursuit of your Citrix certification!

Neil Edde
Associate Publisher—Certification
Sybex, Inc.

## Software License Agreement: Terms and Conditions

The media and/or any online materials accompanying this book that are available now or in the future contain programs and/or text files (the “Software”) to be used in connection with the book. SYBEX hereby grants to you a license to use the Software, subject to the terms that follow. Your purchase, acceptance, or use of the Software will constitute your acceptance of such terms.

The Software compilation is the property of SYBEX unless otherwise indicated and is protected by copyright to SYBEX or other copyright owner(s) as indicated in the media files (the “Owner(s)”). You are hereby granted a single-user license to use the Software for your personal, noncommercial use only. You may not reproduce, sell, distribute, publish, circulate, or commercially exploit the Software, or any portion thereof, without the written consent of SYBEX and the specific copyright owner(s) of any component software included on this media.

In the event that the Software or components include specific license requirements or end-user agreements, statements of condition, disclaimers, limitations or warranties (“End-User License”), those End-User Licenses supersede the terms and conditions herein as to that particular Software component. Your purchase, acceptance, or use of the Software will constitute your acceptance of such End-User Licenses.

By purchase, use or acceptance of the Software you further agree to comply with all export laws and regulations of the United States as such laws and regulations may exist from time to time.

### Software Support

Components of the supplemental Software and any offers associated with them may be supported by the specific Owner(s) of that material, but they are not supported by SYBEX. Information regarding any available support may be obtained from the Owner(s) using the information provided in the appropriate read.me files or listed elsewhere on the media.

Should the manufacturer(s) or other Owner(s) cease to offer support or decline to honor any offer, SYBEX bears no responsibility. This notice concerning support for the Software is provided for your information only. SYBEX is not the agent or principal of the Owner(s), and SYBEX is in no way responsible for providing any support for the Software, nor is it liable or responsible for any support provided, or not provided, by the Owner(s).

### Warranty

SYBEX warrants the enclosed media to be free of physical defects for a period of ninety (90) days after purchase. The Software is not available from SYBEX in any other form or media than that enclosed herein or posted to `www.sybex.com`. If you discover a defect in the media during this warranty period, you may obtain a replacement of identical format at no charge by sending the defective media, postage prepaid, with proof of purchase to:

SYBEX Inc.
Product Support Department
1151 Marina Village Parkway
Alameda, CA 94501
Web: `http://www.sybex.com`

After the 90-day period, you can obtain replacement media of identical format by sending us the defective disk, proof of purchase, and a check or money order for $10, payable to SYBEX.

### Disclaimer

SYBEX makes no warranty or representation, either expressed or implied, with respect to the Software or its contents, quality, performance, merchantability, or fitness for a particular purpose. In no event will SYBEX, its distributors, or dealers be liable to you or any other party for direct, indirect, special, incidental, consequential, or other damages arising out of the use of or inability to use the Software or its contents even if advised of the possibility of such damage. In the event that the Software includes an online update feature, SYBEX further disclaims any obligation to provide this feature for any specific duration other than the initial posting.

The exclusion of implied warranties is not permitted by some states. Therefore, the above exclusion may not apply to you. This warranty provides you with specific legal rights; there may be other rights that you may have that vary from state to state. The pricing of the book with the Software by SYBEX reflects the allocation of risk and limitations on liability contained in this agreement of Terms and Conditions.

### Shareware Distribution

This Software may contain various programs that are distributed as shareware. Copyright laws apply to both shareware and ordinary commercial software, and the copyright Owner(s) retains all rights. If you try a shareware program and continue using it, you are expected to register it. Individual programs differ on details of trial periods, registration, and payment. Please observe the requirements stated in appropriate files.

### Copy Protection

The Software in whole or in part may or may not be copy-protected or encrypted. However, in all cases, reselling or redistributing these files without authorization is expressly forbidden except as specifically provided for by the Owner(s) therein.

*For Bill Burkhardt*

*For all the lives you have touched and all the guidance you have given, thank you for everything you have brought to so many.*

*In loving memory of Pearl, Imogene, and Mary*

# Acknowledgments

We want to thank everyone who supported us and guided us to this point in our lives. Without all of the people who make up our family and friends, we could not have accomplished this task. Know that you are in our hearts forever.

I must start out these acknowledgments with a huge heartfelt thank-you to my family. To my wife, DeAnn: You have traveled along this rocky road with me for many years, and you never seem to tire of the hairpin turns I take along the way. Thank you for all of your support; I could never have done this without you. You may never know how much your understanding meant to me when things got crazy and I was lost in my own little world while I wrote. You truly are my soul mate and my very best friend. And to my daughters, Jami and Becca: The two of you were great throughout this process, just as you have been with everything that comes along. Thank you for understanding what this meant to me and for supporting me. I know that I didn't get to do everything we wanted to do as deadlines loomed in front of me, but you never became discouraged or upset. The three of you are my life, and I couldn't imagine my world without you in it. I cannot say "thank you" enough. I love you with all of my heart.

To my parents: I have so much to thank you for. To Dad: Thank you for the work ethic you instilled in me. And thank you for showing me how to do so many things—car repair, woodworking, and home improvements. It is from your teachings that I built the troubleshooting skills that have helped me throughout my computer career. To Mom: Thank you for all of the insight you gave me and the patience you showed as I went through every phase of my life. Your world is a magical place full of love for everyone you meet. While I may be obsessive at times when it comes to all of this crazy computer stuff, you two allowed me to see what is important in life: family, friends, and a good hearty laugh!

To the rest of my family and all of the friends with whom I have not been able to spend much time while writing this book: This process made me a hermit; thank you for understanding what it meant to me. I have always dreamt of having my name attached to a book—I just never thought it would really happen. Your support made it much easier when I was trying to pull those words out of the deep, dark recesses of my over-caffeinated brain!

I also need to thank everyone along my career path who helped me hone my talents, but especially Bruce Hall, Bill Burkhardt, Gary McDowell, Mike

Lampson, Chuck Sneddon, Wendy Johnson, and Dan McCain. Thank you for all of your help, guidance, and friendships.

And to John: For all you have done for me and for being my best friend, thank you. I can't wait for our next project!

—Brad

First, I would like to thank my wife, Julie, for her support and encouragement throughout the writing of this book. Thank you for being there for me, as you always are, each and every step of the way. Without your love, support, and patience, I don't think I could have made it through the late nights and long weekends. All the white roses in the world could not convey how much I love you, my best friend.

Thank you, Mom and Dad. Thank you, Mom, for reminding me to take time to enjoy sunsets. Thank you, Dad, for giving me the courage to jump into a job and not be afraid to figure things out for myself. Thanks for letting Brad and me talk about the book at family get-togethers and dinners. At the next family outing, we will play a full game of wiffleball, and I promise we will not utter one word about work. Thank you, Captain Milo, for talking me into buying your Commodore SX-64 instead of a Betamax VCR. You not only started me on this road, but you also helped me map a route and warned me of potholes. I would not be where I am today without your help, advice, and guidance.

Professionally, I would like to thank everyone I have ever worked for or with. I have learned something valuable from each and every one of you. Thanks to the following people, whose advice and help have been a great influence on me: Bruce Hall, Dan Edwards, Jeff Koenke, Chuck Wallbaum, Doug Buttry, Dave VanDerHeyden, Greg Bachman, and Ernest Riggen.

—John

There is no way this book could have come to fruition without the assistance, guidance, and support that we received. Every book is the culmination of much talent, and this one is no exception. The two of us would like to give credit where credit is due.

To the talented Sybex staff who assisted us: Julie Sakaue, thank you for getting the ball rolling on this one. You were a gem to work with. We missed you throughout the last part of the book and want to wish you the very best in everything you do. Elizabeth Hurley, are you tired of the calls yet? Seriously, we can't think of anyone who could have done as excellent a job after this project was dumped into your lap. Mae Lum, how you coordinated all this with all of the parties involved and still didn't go insane, we will never know. Thanks for your perseverance when things got a little crazy! Neil Edde, your leadership helped keep everyone sane through the trying times. It was a privilege to have the opportunity to work for you. Linda Recktenwald, you made our words sound good! Thank you for repairing the broken English and catching all of the little things. Hai Hilvitz, through Citrix we met, but through your sincerity and kindness we became friends. Thanks for finding all the things we missed. Scott Warmbrand, to be brought in at the end of the process and to go through the entire manuscript at one time is never an easy task. Thank you for catching all the missteps on our journey. Stacey Loomis and Bill Clark, without you, the book would not appear nearly as professional. Thank you for adding your special touches to it and making us look all that much better.

We also thank proofreaders Emily Hsuan, Nelson Kim, David Nash, Laurie O'Connell, Yariv Rabinovitch, and Nancy Riddiough, and indexer Nancy Guenther.

# Introduction

If you are preparing to take the Citrix Certified Administrator (CCA) exam, you will undoubtedly want to find as much information as you can concerning MetaFrame XP. The more information you have at your disposal and the more hands-on experience you gain, the better off you will be when attempting the exam. This study guide was written with that in mind. We have attempted to dispense as much information as we can about MetaFrame XP administration. The key was to provide enough information so that you will be prepared for the exam but not too much so that you will be overloaded. Using the Citrix Certified Administrator Exam Guide found on the Citrix website, we have arranged this book into chapters that represent the exam objectives. If you need to concentrate on a particular objective, you will find everything you need within the chapter on which the objective is based.

This book presents the material at an intermediate technical level. Experience with, and understanding of, the two Microsoft operating systems on which MetaFrame XP can be installed, Windows 2000 Server and Windows NT Server 4.0, Terminal Server Edition, is essential. We do not have enough room within this text to include a primer on the finer points of Windows administration and configuration. While you do not have to be Microsoft certified to successfully complete the CCA exam, it does help. Of course, if you are going to be administering and supporting MetaFrame XP, you will need those skills anyway.

We've included review questions at the end of each chapter to give you a taste of what it's like to take the exam. If you're already administering and supporting MetaFrame XP, we recommend that you check out these questions first to gauge your level of expertise. You can then use the book mainly to fill in the gaps in your current knowledge. You may find, as many administrators have, that working on a daily basis with MetaFrame XP may not allow you to actually take advantage of all the functionality of the product. Using this study guide will help you round out your knowledge base before tackling the exam.

If you can answer 80 percent or more of the review questions correctly for a given chapter, you can probably feel safe moving on to the next chapter. If you're unable to answer that many correctly, reread the chapter and try the questions again. Your score should improve.

WARNING

*Don't* just study the questions and answers—the questions on the actual exam will be different from the practice ones included in this book and on the CD. The exam is designed to test your knowledge of a concept or objective, so use this book to learn the objective *behind* the question.

## What Is the Citrix MetaFrame Certification?

After gaining acceptance in the computer industry for providing an enterprise-level solution for terminal services, Citrix Systems decided that they needed a way of identifying individuals who have become proficient at administering MetaFrame and WinFrame. Hence the Citrix Certified Administrator certification was born. The exam concentrates on the administration and management of a MetaFrame or WinFrame server and does not overlap the Microsoft arena. Questions are geared to test the user's knowledge of Citrix technologies and leave the operating and networking fields to the Microsoft Certified Professional exams. The CCA exam is actually the jumping-on point for Citrix certification. Although it is a stand-alone exam and will grant you CCA credentials, it is used as the first exam of the Citrix Certified Enterprise Administrator (CCEA) certification, which includes four other exams.

The exam itself is aimed toward those administrators who will be working with MetaFrame on a daily basis and need to understand the basic building blocks. Topics such as Resource Manager, Network Manager, and NFuse are touched upon in this exam but not in great detail. Those topics are reserved for the CCEA exams. Institutions that hire individuals based not only on experience but also on credentials can be assured that an individual with CCEA certification has the knowledge needed to administer a Citrix-based network. Those administrators who successfully complete the exam can be assured that their certification is respected in the computer industry.

## Why Become CCA Certified?

There are a number of reasons for becoming CCA certified:

- It demonstrates proof of professional achievement.
- It increases your marketability.

- It provides greater opportunity for advancement in your field.
- It is increasingly found as a requirement for some types of advanced training.
- It raises customer confidence in you and your company's services.

Let's explore each reason in detail.

## Provides Proof of Professional Achievement

Specialized certifications are the best way to stand out from the crowd. In this age of technology certifications, you will find hundreds of thousands of administrators who have successfully completed the Microsoft and Novell certification tracks. To set yourself apart from the crowd, you need a little bit more. The Citrix Certified Administrator exam is the starting point for the Citrix Certified Enterprise Administrator certification and will give you the recognition you deserve.

## Increases Your Marketability

Almost anyone can bluff their way through an interview. Once you have certified on a product such as MetaFrame XP, you will have the credentials to prove your competency. And certifications are not something that can be taken from you when you change jobs. Once certified, you can take that certification with you to any of the positions you accept.

## Provides Opportunity for Advancement

Those individuals who prove themselves as competent and dedicated are the ones who will most likely be promoted. Becoming certified is a great way to prove your skill level and shows your employers that you are committed to improving your skill set. Look around you at those who are certified. They are probably the ones who receive good pay raises and promotions when they come up.

## Fulfills Training Requirements

Many companies have set training requirements for their staff so that they stay up-to-date on the latest technologies. Having a certification program for the Citrix family of products provides administrators another certification path to follow when they have exhausted some of the other industry-standard certifications.

### Raises Customer Confidence

As companies discover the Citrix advantage, they will undoubtedly require qualified staff to implement this technology. Many companies outsource the work to consulting firms with experience working with MetaFrame XP. Those firms that have certified staff have a definite advantage over other firms that do not.

## How to Become a Citrix Certified Administrator

As this book goes to press, the only exam provider is Prometric, a division of Thomson Learning. To register for a Citrix Certified Administrator exam, contact Prometric at 1-800-481-EXAM or visit their website at `www.2test.com`. When you register for the exam, you will be asked for the exam number, 1Y0-220. Payment of $100 will be requested at that time, and you will have one year in which to take the exam. Exams can be scheduled up to six weeks out or as early as the next day.

When you schedule the exam, you will receive instructions regarding appointment and cancellation procedures, ID requirements, and information about the testing center location. In addition, you will receive a registration and payment confirmation letter from Prometric.

The exam consists of 40 questions, and you will be given one hour to complete it. Make sure you use your time wisely. Follow the guidelines later in this introduction on how to take the exam.

NOTE

In addition to reading the book, you might consider downloading and reading the white papers that Citrix has provided on their website.

## Who Should Buy This Book?

If you want to acquire a solid foundation in Citrix MetaFrame XP administration, and your goal is to prepare for the exam by learning how to use and manage MetaFrame XP, this book is for you. You'll find clear explanations of the concepts you need to grasp and plenty of help to achieve the high level of professional competency you need in order to succeed in your chosen field.

If you want to become certified as a Citrix Certified Administrator, this book is definitely for you. However, if you just want to attempt to pass the exam without really understanding MetaFrame XP, this study guide is not for you. It is written for people who want to acquire hands-on skills and in-depth knowledge of MetaFrame XP.

## How to Use This Book and the CD-ROM

We've included several testing features both in the book and on the CD-ROM bound in the book. These tools will help you retain vital exam content as well as prepare to sit for the actual exam. Using our custom test engine on the CD-ROM, you can identify weak areas up front and then develop a solid studying strategy using each of these robust testing features. Our thorough readme file on the CD-ROM will walk you through the quick and easy installation process.

**Before You Begin** At the beginning of the book (right after this introduction, in fact) is an assessment test that you can use to check your readiness for the actual exam. Take this test before you start reading the book. It will help you determine the areas you may need to brush up on. The answers to each assessment test appear on a separate page after the last question of the test. Each answer also includes an explanation and a note telling you in which chapter this material appears.

**Chapter Review Questions** To test your knowledge as you progress through the book, there are review questions at the end of each chapter. As you finish each chapter, answer the review questions and then check to see if your answers are right—the correct answers appear on the page following the last review question. You can go back to reread the section that deals with each question you got wrong to ensure that you get the answer correct the next time you are tested on the material.

**Electronic "Flashcards"** You'll also find 150 flashcard questions for on-the-go review. Download them right onto your Palm device for quick and convenient reviewing.

**Test Engine** In addition to the assessment test and the chapter review tests, you'll find two sample exams on the CD-ROM. Take these practice exams just as if you were taking the actual exam (i.e., without any reference material). When you have finished the first exam, move onto the next one to solidify your test-taking skills. If you get more than

90 percent of the answers correct, you're ready to go ahead and take the certification exam.

**Full Text of the Book in PDF** Also, if you have to travel but still need to study for the Citrix MetaFrame exam and you have a laptop with a CD-ROM drive, you can carry this entire book with you just by taking along the CD-ROM. The CD-ROM contains this book in PDF (Adobe Acrobat) format so it can be easily read on any computer.

## Exam Objectives

Behind every computer industry exam you are sure to find exam objectives—the broad topics on which the exam developers want to ensure your competency. The official Citrix Certified Administrator exam objectives are listed here.

NOTE Exam objectives are subject to change at any time without prior notice and at Citrix's sole discretion. Please visit the Training and Certification page of Citrix's website at `http://www.citrix.com/training/testing.asp#cert` for the most current listing of exam objectives.

1. Introduction to MetaFrame XP
   - a. Identify the Key Benefits of Deploying MetaFrame
   - b. Understanding Digital Independence
   - c. Identify the Benefits of MetaFrame Interoperability
2. MetaFrame Installation process
   - a. Identify the Software and Hardware requirements for MetaFrame XP
   - b. Perform Server Planning and Sizing Issues
   - c. Installing MetaFrame and various setup options
3. Using Citrix Technologies
   - a. Identify the components of the ICA Packet
   - b. List the benefits of SpeedScreen Technology
   - c. Discuss the features of Independent Management Architecture
   - d. Recognizing Listener Ports, Idle Sessions, ICA Sessions and Client Device Licensing

4. MetaFrame XP Administration
   - a. Administering using the Citrix Management Console
   - b. Identify Published Application, Server and Citrix Administrator Properties
   - c. Understanding Citrix Management Console
5. Additional Management Tools
   - a. Identify features of Citrix Server Administration
   - b. Shadowing with the Shadow Taskbar
   - c. Creating connections with the Citrix Connection Configuration
   - d. Configure SpeedScreen Latency Reduction Manager
6. Load Management and Security
   - a. Analyzing Load with Load Manager
   - b. Identify Encryption Strengths and Performance
7. Applications
   - a. Installing, Uninstalling and Migrating Applications
   - b. Configuring Applications for use in a MetaFrame environment
8. Citrix ICA Client Software
   - a. Installing the Citrix ICA Client Software
9. Citrix Program Neighborhood
   - a. Customizing Program Neighborhood interface and recognizing the ICA Toolbar Icons
10. Web Connectivity
    - a. Recognizing Citrix Web Components
    - b. Identifying NFuse Features and Components
11. Printing
    - a. Creating Client, Network and local Printers
    - b. Replicating Print drivers and Importing Print Servers

12. Monitoring and Troubleshooting MetaFrame XP Servers
    a. Using Event Viewer and System Information
    b. Managing Resource and Citrix Network Manager and Troubleshooting Network Monitor

## Tips for Taking the Citrix Certified Administrator Exam

Here are some general tips for taking your exam successfully:

- Bring two forms of ID with you. One must be a photo ID, such as a driver's license. The other can be a major credit card or a passport. Both forms must contain a signature.
- Arrive early at the exam center so you can relax and review your study materials, particularly tables and lists of exam-related information.
- Read the questions carefully. Don't be tempted to jump to an early conclusion. Make sure you know exactly what the question is asking.
- Don't leave any unanswered questions. Unanswered questions are scored against you.
- There will be questions with multiple correct responses. When there is more than one correct answer, a message at the bottom of the screen will prompt you to "Choose all that apply." Be sure to read the messages displayed.
- When answering multiple-choice questions you're not sure about, use a process of elimination to get rid of the obviously incorrect answers first. This will improve your odds if you need to make an educated guess.
- On form-based tests, because the hard questions will eat up the most time, save them for last. You can move forward and backward through the exam. (When the exam becomes adaptive, this tip will not work.)
- For the latest pricing on the exams and updates to the registration procedures, call Prometric at (800) 481-EXAM (481-3926). If you have further questions about the scope of the exams or related Citrix certifications, refer to the Citrix website at `www.citrix.com/calc`.

## About the Authors

Brad Price is a Citrix Certified Instructor and Citrix Certified Administrator. He has his Windows 2000 MCSE, Windows NT 4.0 MCSE+I, MCT, and CAN certifications. Currently employed as a Technical Education Consultant, he specializes in Windows 2000, Exchange 5.5 and 2000, and Citrix Administration. You can e-mail him at `BPrice@zygort.com`.

John Price is a Citrix Certified Administrator. He is both MCSE and MCT certified. Currently he works as a trainer and a Network Engineer Consultant, specializing in Citrix enterprise implementations. John has been working with Citrix products since 1996. You can e-mail him at `JPrice@zygort.com`.

# Assessment Test

1. You want to take advantage of the new features of MetaFrame XP. Your server farm is in native mode and you want to utilize the XML service to look for published applications. Which protocol would you select for your clients to use?

   **A.** TCP/IP

   **B.** TCP/IP+HTTP

   **C.** HTTP

   **D.** NETBIOS

2. Which of the following database engines is not supported for use with the data store?

   **A.** Microsoft SQL

   **B.** Oracle

   **C.** Sybase

   **D.** Microsoft Access

3. When you grant access permissions, which of the following individual permissions are assigned when the Guest Access permission is used?

   **A.** Query Information

   **B.** Set Information

   **C.** Shadow

   **D.** Logon

   **E.** Logoff

   **F.** Message

   **G.** Connect

   **H.** Disconnect

**4.** On which of the following systems can you install the Win32 client? (Choose all that apply.)

**A.** Windows 2000 Professional, 64MB RAM

**B.** Windows NT Workstation 4.0, 64MB RAM

**C.** Windows Me, 96MB RAM

**D.** Windows for Workgroups version 3.11, 16MB RAM

**E.** DOS 6.20, 16MB RAM

**5.** When assigning evaluators to servers, where can you view all of the servers and the evaluators that are assigned to each?

**A.** Servers node, Contents tab

**B.** Servers node, Load Manager tab

**C.** Load Evaluators node, Contents tab

**D.** Load Evaluators node, Usage Reports tab

**6.** Within the Client Settings of the Connection Properties sheet, the (Inherit User Config) and By Default, Connect Only The Client's Main Printer options are selected. Within the user's profile, the options Connect Client Printers At Logon and Default To Main Client Printer are selected. When the user logs on to a session, what printers are available?

**A.** All of the client printers are auto-created and available, and the user's default printer is the default printer in the session.

**B.** All of the client printers are auto-created and available, and the server's default printer is the default printer in the session.

**C.** Only the user's default printer is auto-created and set as the default printer.

**D.** The user's default printer is auto-created along with the server printers. The server's default printer is made the default printer in the session.

**7.** Which of the following encryption levels are not subject to international export laws? (Choose all that apply.)

**A.** RC5 (128 bit) logon only

**B.** RC5 (40 bit)

**C.** RC5 (56 bit)

**D.** RC5 (128 bit)

**8.** What additional component is included in MetaFrame XPa that is not included in MetaFrame XPs?

**A.** Installation Manager

**B.** Load Manager

**C.** Network Manager

**D.** Resource Manager

**9.** If you take the default drive mappings as they appear within the setup program, what drive letter is the client's C: drive mapped to?

**A.** C:

**B.** F:

**C.** H:

**D.** M:

**E.** Z:

**10.** Which file is used to supply the substitution tags with information about an application?

**A.** HTML file

**B.** ICA file

**C.** Logon file

**D.** NFuse file

**11.** What is the name of the utility included with Windows 2000 that can be used to track informational, warning, and error messages from applications and the operating system?

**A.** Event Viewer

**B.** System Information

**C.** System Monitor

**D.** Task Manager

**12.** You want to keep users from running a published application but do not want to unpublish it. What is the easiest way to do this?

**A.** Use Add/Remove Programs.

**B.** Open the Properties sheet of the published application and remove all of the users from the Configured Users list.

**C.** Open the Properties sheet of the published application and remove all of the servers from the Configured Servers list.

**D.** Open the Properties sheet of the published application and click the Disable Application check box.

**13.** When installing MetaFrame XP on Windows NT Server 4.0, Terminal Server Edition, what is the minimum memory requirement for the operating system?

**A.** 32MB

**B.** 64MB

**C.** 128MB

**D.** 256MB

**14.** Servers that are configured with a product code for MetaFrame XPa are automatically enrolled in load management. Which load evaluator is automatically assigned to them?

**A.** Advanced evaluator

**B.** Basic evaluator

**C.** Default evaluator

**D.** XPa evaluator

15. If you accept the default drive mappings as they appear within the Setup program, to what drive letter is the client's C: drive mapped?

    A. C:

    B. F:

    C. H:

    D. V:

    E. Z:

16. Which of the Windows 2000 utilities provides a list of the resources and configuration options?

    A. Event Viewer

    B. System Information

    C. System Monitor

    D. Task Manager

17. When a user has the Logoff permission granted to them, what are they allowed to do?

    A. Log off a session they are currently running.

    B. Access the Logoff option from the Start menu.

    C. Log off other users from Citrix Management Console and Citrix Server Administration.

    D. Log off other users from Citrix Management Console only.

18. Which of the following is an example of an Incremental rule?

    A. CPU Utilization

    B. Server User Load

    C. Context Switches

    D. Scheduling

**19.** When installing MetaFrame XP on Windows 2000 Server, what is the minimum memory requirement for the operating system?

**A.** 32MB

**B.** 64MB

**C.** 128MB

**D.** 256MB

**20.** Which of the following can you *not* do with the Client Update Configuration utility?

**A.** Configure the properties of the database.

**B.** Add new ICA Clients to the database.

**C.** Set ICA Clients to be either enabled or disabled according to the time of day.

**D.** Create a new update database.

**21.** Which of the following options will start the Application Publishing Wizard? (Choose all that apply.)

**A.** Press the Insert key.

**B.** Click the Published Applications icon.

**C.** Right-click the Applications node and select Publish Applications.

**D.** Right-click the Contents tab of the Applications node and select Published Applications.

**22.** You are the administrator of a small office using MetaFrame XP. Currently, you have 25 users in one building who are using your MetaFrame XP server. There are no plans to allow remote access to the server via dial-in or VPN connections. Your main concern is fast, efficient processing of the sessions. Which level of encryption would you choose when configuring a published application?

A. None

B. Basic

C. RC5 (128 bit) logon only

D. RC5 (40 bit)

E. RC5 (56 bit)

F. RC5 (128 bit)

23. Rebecca has started a session that runs Microsoft Word in a seamless window. She starts another session running an application written by the software development team of her company. It too is a seamless window, but the application is started on a separate server. How many connection licenses does Rebecca use?

A. None

B. One

C. Two

D. Three

24. Which utility is used when installing an application in multiple user mode? (Choose all that apply.)

A. Add/Remove Programs

B. AppInstall

C. `chgusr /install`

D. `chgusr /execute`

25. You are installing the second MetaFrame XP server in your server farm. You want this server to access the data store. The SQL server is hosting the database for your data store. Since you do not want to have a single point of failure while accessing the data store, you want to use an ODBC connection from this server. Which of the following options should you use when configuring the server to access the data store?

**A.** Use A Local Database For The Data Store.

**B.** Use A Third Party Database For The Data Store.

**C.** Direct Data Store Connection.

**D.** Connect To Data Store Set Up Locally On Another Computer.

**26.** On which of the following products will MetaFrame XP install? (Choose all that apply.)

**A.** Windows NT Server 3.51

**B.** Windows NT Server 4.0

**C.** Windows NT Server 4.0, Terminal Server Edition

**D.** Windows 2000 Server

**27.** You have installed MetaFrame XP on a new server and entered your original licenses from MetaFrame 1.8 into the pool. You then add the connection migration licenses. The Connection tab of the Licenses node does not show any of these licenses being used. What is the most likely cause?

**A.** The licenses are not assigned to any servers.

**B.** Upgrade licenses should have been added instead.

**C.** The licenses are not activated.

**D.** The product code from the connection license was not added to a server.

**28.** Which of the following printers can be auto-created for a user when they start a session? (Choose all that apply.)

**A.** Local printers on the client device

**B.** Network printers on other client devices

**C.** Imported network print server printers

**D.** Printers connected directly to MetaFrame XP servers

**29.** You choose a drive with 15GB total drive space to use for your bitmap cache. If you use the default settings, how much drive space will be used for caching bitmaps?

**A.** 15MB

**B.** 150MB

**C.** 1.5GB

**D.** 15GB

**30.** You cannot start an ICA session on your MetaFrame XP server but you can start an RDP session. You look at the Connections tab on the Licenses node, and the licenses display as Expired. Why?

**A.** You have not activated the licenses.

**B.** The serial number was not entered correctly.

**C.** The data store cannot be accessed to gather license information.

**D.** The system time on your server has been changed to reflect a date five years or more off.

**31.** What option is not available from the Application Publishing Wizard that is available from the published application's Properties sheet?

**A.** Disable Application

**B.** Configure Servers

**C.** Configure Users

**D.** Schedule Install Time

**32.** From which configuration button on the Connection Properties dialog box can you control the amount of time before an idle session is terminated?

**A.** Advanced

**B.** Client Settings

**C.** Connection Settings

**D.** ICA Settings

33. Which file is used to generate a web page?

A. HTML file

B. ICA file

C. Logon file

D. NFuse file

34. When you view sessions within Citrix Management Console, in what state does a connection appear when a user is in the process of logging into a session?

A. Conn

B. ConnQ

C. Disc

D. Idle

35. What mode should the server farm be placed in if there are no MetaFrame 1.8 servers that need to interoperate with the MetaFrame XP server farm?

A. Integrated

B. Mixed

C. Native

D. Synchronized

# Answers to Assessment Test

1. B. TCP/IP+HTTP is the recommended network protocol for ICA connections with MetaFrame XP running in native mode. The connection will look to the data store for connection information to a published application or server. For more information, see Chapter 11.

2. C. Of the four, only Sybase is not supported by Citrix for use as the data store database. For more information, see Chapter 2.

3. D. A user with the Guest Access permission will only be able to start a session since the Logon permission is the only permission granted to them by default. For more information, see Chapter 6.

4. A, B, C. While all of these options are viable for use in a MetaFrame XP environment, only Windows 2000 Professional, Windows NT Workstation 4.0, and Windows Me can use the Win32 client. For more information, see Chapter 10.

5. D. Once you navigate to the Load Evaluators node, you can click the Usage Report tab and view all of the servers and the evaluators that are assigned to them by selecting the By Server radio button. For more information, see Chapter 7.

6. C. Even though the (Inherit User Config) option is selected, the only option that setting controls is which client printers are automatically created for the session. Since the connection controls whether or not the only printer that is created is the user's default, or main, printer, that setting overrides the creation of other printers. For more information, see Chapter 13.

7. A, B. Of those listed, RC5 (40 bit) and (128 bit) logon only are the only ones that are not restricted by the export laws. For all other levels, you should check before using them on servers and clients outside of the United States. For more information, see Chapter 8.

8. B. XPs, the standard version of MetaFrame ships with only the core MetaFrame product. XPa includes the Load Manager component. MetaFrame XPe provides all of the enterprise-level components including Installation Manager, Load Manager, Resource Manager, and Network Manager. For more information, see Chapter 1.

**9.** D. By default, the client's drives are mapped starting with V: and decreasing for every drive on the client system. The server drives are mapped starting with C: and increasing for every drive on the server. The administrator may modify this configuration during setup. For more information, see Chapter 4.

**10.** B. ICA files contain information that controls how the application is presented to the user. For more information, see Chapter 12.

**11.** A. As applications and the operating system process information, messages are sent to the logs that make up the Event Viewer database. You can save these logs for later use when trying to track trends or use them to monitor activities and possibly detect problems before they manifest themselves. For more information, see Chapter 14.

**12.** D. To keep users from accessing a published application without removing the application from Citrix Management Console, all you have to do is disable the application. You could remove all of the users or servers from the published application Properties sheet, but when you want to allow access again you will have to remember to reassign all of the users, groups, and servers that were previously configured. For more information, see Chapter 9.

**13.** A. The minimum RAM requirement to install Windows NT Server 4.0, Terminal Server Edition is 32MB. Additional memory should be installed for Citrix MetaFrame XP. For more information, see Chapter 3.

**14.** C. The Default evaluator is automatically assigned to all servers added to the server farm. For more information, see Chapter 7.

**15.** D. By default, the client's drives are mapped as V:, U:, and they decrease for every drive on the client system. The server drives are mapped as C:, D:, and they increase for every drive on the server. The administrator may modify this configuration during setup. For more information, see Chapter 4.

**16.** B. System Information provides a list of all the resources and tasks and the configuration information from each. For more information, see Chapter 14.

17. C. Once you grant the Logoff permission to a user, that user will have the ability to log off other users from Citrix Server Administration and Citrix Management Console. You will have to add them to the Citrix Administrators list in order for them to have access to the Citrix Management Console. For more information, see Chapter 6.

18. B. Incremental rules are based on an integer value that determines the maximum number that can be obtained for that rule. For more information, see Chapter 7.

19. D. The minimum RAM requirement to install Windows 2000 Server is 256MB. Additional memory should be installed for Citrix MetaFrame XP. For more information, see Chapter 3.

20. C. You can set the ICA Clients to be either enabled or disabled but you cannot schedule them to be enabled at certain times. For more information, see Chapter 10.

21. B, C. Both of these options will start the Application Publishing Wizard. Pressing the Insert key will open the Add License screen, and the last option does not exist. For more information, see Chapter 5.

22. B. Since encryption is not a concern but processing speed and efficiency are, you should select Basic for the application. None is not an option for an application; it is available only for connections. For more information, see Chapter 8.

23. B. When a user starts sessions within the server farm, only one connection license is consumed, regardless of the number of servers responsible for running the applications. For more information, see Chapter 2.

24. A, C. Both of these utilities will put the system in installation mode, which monitors the setup of the program and configures settings for applications used in multiple user mode. For more information, see Chapter 9.

25. C. When setting up the second server in the server farm, you will choose the Join An Existing Server Farm option. In doing so, you will be presented with the options Direct Data Store Connection and Connect to Data Store Set Up Locally On Another Computer. If you

want to connect to the SQL Server hosting the data store database, you would choose Direct Data Store Connection. If you want to connect to another MetaFrame XP server which will act as a data store proxy for your server, you would choose Connect To Data Store Set Up Locally On Another Computer. For more information, see Chapter 4.

**26.** C, D. MetaFrame XP is designed to run on Windows NT Server 4.0, Terminal Server Edition and the entire Windows 2000 Server family, which includes Server, Advanced Server, and Datacenter Server. Windows NT Server 3.51 and Windows NT Server 4.0 do not have terminal services available. For more information, see Chapter 1.

**27.** D. Until you add the product code from the connection migration license, the original legacy licenses are not available for use by a MetaFrame XP server. For more information, see Chapter 5.

**28.** A, B, C, D. All of these printers can be auto-created for a user when they initiate a session. This functionality allows you to configure a user so that they have access to all of the printers available on your network. For more information, see Chapter 13.

**29.** B. The default setting used for the bitmap cache on a client is configured as 1 percent of the total drive size. For more information, see Chapter 11.

**30.** A. Unless you activate a license set, the license will expire at the end of the grace period. For more information, see Chapter 5.

**31.** A. You can configure the servers that the application is published on and the users who have access to the application, but you cannot disable the application from the wizard. For more information, see Chapter 9.

**32.** A. The Advanced button brings up the settings for connection timeouts, autologon, security encryption level requirements, reconnection restrictions, shadowing, and user profiles. For more information, see Chapter 6.

**33.** A. The HTML file uses information passed to it from the ICA file to determine how the web page should be displayed. For more information, see Chapter 12.

**34.** A. When a user initiates a connection, the connection goes into a ConnQ state until the session is built. After the session is created and the user is prompted to log on, the connection goes into a Conn state. For more information, see Chapter 2.

**35.** C. Mixed mode allows the server farm to interoperate with MetaFrame 1.8 servers by using the IMA service as the Browser service for those systems. Native mode is used when no MetaFrame 1.8 servers are used. For more information, see Chapter 4.

Chapter 1

# Why Citrix MetaFrame XP?

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **1. Introduction to MetaFrame XP**

- 1a. Identify the Key Benefits of Deploying MetaFrame
- 1b. Understanding Digital Independence
- 1c. Identify the Benefits of MetaFrame Interoperability

Throughout this book, we will look at *Citrix MetaFrame XP* and review all of the tools an administrator needs to learn and know in order to fulfill the requirements of the *Citrix Certified Administrator* exam. Within this chapter, we want to introduce you to MetaFrame XP—the history, benefits, and the objectives we will be addressing between the covers of this tome. Let's start with the history of this fine product.

## The History

Before *terminal services* were available, users would have to execute every application on their local personal computer, and applications written for a particular operating system would not run on any other operating system. Microsoft Word compiled to run on Windows 2000 would not load or execute on an Apple Macintosh. If an organization utilized multiple operating systems, it had to support multiple versions of the same application or different applications that performed the same function.

Further complications arose when an application needed to be updated and the computer system did not have enough horsepower to run the new application. Historically, applications written to take advantage of new technologies tend to ignore slower legacy systems. It's very cost-prohibitive for companies to upgrade computer systems with the sole purpose of keeping up with software (sometimes referred to as "keeping up with the Gateses"). At the same time, running applications on a slow system reduces the user's productivity and increases the company's total cost of ownership. All of these complications mean that expensive computer systems become obsolete very quickly.

Terminal services provided a much-needed remedy for the issues just raised. The terminal services model, however, wasn't entirely new. It actually spawned from the mainframe model. In the mainframe model, one large computer system processes applications while the user employs an inexpensive terminal. This terminal simply displays information as the server processes it and sends keystrokes to the server as the client enters information. This model has existed for many years, but until just recently, it was not implemented in a personal computer platform. After all, PCs were known for their distributed processing, not centralized processing. Terminal services changed all that.

**Real World Scenario**

### Networking Your Donations

In a small community in Illinois, there is a public library system that periodically receives donations of older computer systems. These systems typically are slower 486 or early Pentium-based and run Microsoft Windows 95 as their operating system. Each of the donated computers works. It's just that the original owners had upgraded to take advantage of a newer system's speed and functionality. Not surprisingly, most of the applications purchased by the library for use by patrons will not run on these machines due to their limited speed and functionality. This situation is actually quite common. Many organizations like this public library system find that they cannot do much with the computers that are donated to them.

This library did find a unique use for the older systems. Instead of filing for a grant to purchase new desktop systems, they purchased a large server running Windows 2000 and Citrix MetaFrame. The operating systems were deleted from the donated computers, and a bare-bones Windows 95 operating system with the Citrix client software was loaded onto them.

System policies were created that turned the client computers into kiosks. Now when the computers start, the system starts a Citrix session. Most users do not realize they are running a session—it appears to them as though these 486-based computers are running Windows 2000. Web browsing and application execution are performed at the server, yet this is transparent to most users.

The library has been able to extend the life of the donated computers years longer than they would have been able to under normal circumstances. An added benefit is that the library was able to attach more computers to the network and take advantage of additional sessions. More patrons could use the systems for research, and the total cost of owning the server and operating system was averaged out over more client systems.

Today, patrons using the systems at the library do not think twice about the session they are starting. They access the card catalog, request book transfers, and perform research either on the Internet or from the online encyclopedias that are provided through the server's CD-ROM drives. And as more computer systems are donated, they are stored to be used in case one of the existing systems fails. It is the best of both worlds for the library system: They are able to take advantage of their patrons' generosity and centrally control their resources.

Many times over the past few years, as MetaFrame—and its predecessor WinFrame—has been introduced into companies, administrators have asked about MetaFrame's usefulness. That question arises especially now that Microsoft has introduced *Windows NT 4.0 Terminal Server Edition* and the *Windows 2000 Server* family. Both provide the basic functionality that allows a user's session to run on a server instead of the local computer. The key here is the word *basic*. An understanding of Citrix Systems history and its relationship with Microsoft will help to put this in perspective.

Terminal Services, as delivered through Microsoft, allows a client to run its session on a server and not tax the local resources of the desktop computer. As the user moves the mouse and types on the keyboard, the data is redirected to the server instead of the local computer processing the information. The server then processes the information it receives from the client and delivers screen updates for the user to see.

NOTE

Having the server process information sent from a client system is called *client/server technology* and is sometimes referred to as *thin client technology.*

As clients start sessions on the server running Terminal Services, the server reserves an area of memory for the session to run. This session is a complete user environment that includes the user's profile information. Each user's session is contained in a memory area on the server separate from all other users' sessions. All processing of applications and access to data is performed from the server session. These multiple sessions that are created on a server are made possible by a technology known as *MultiWin*.

Citrix is the company that is responsible for the MultiWin technology. Ed Iacobucci, the founder of Citrix Systems, developed the original concept behind MultiWin and the product that developed from it, MetaFrame. From 1978 until 1989, he was employed by IBM, working in their Personal Computer Division, designing operating systems. It was in this capacity that he envisioned an operating system that would act as a mainframe although based on the personal computer platform. When appointed head of the joint Microsoft/IBM project that was designing OS/2, he proposed adding the terminal services functionality to the new operating system. When it was decided that the project would not include this idea, he left IBM to start Citrix Systems.

Citrix Systems created a product called MultiView that would allow an OS/2 server to run multiple user sessions. OS/2 had not gained wide acceptance in the computer industry, and its future was not seen as very stable. Iacobucci needed to keep his company viable, so he entered into negotiations with Microsoft, which was trying to get their server operating system, Windows NT Server, off the ground. Microsoft saw the inclusion of a multiple-user session operating system as a way to improve the market position of their product. Microsoft licensed the NT kernel to Citrix and was so impressed with its technology that they bought 6 percent of the company.

In 1995, Citrix launched their vision, *Citrix WinFrame*. The product shipped as a stand-alone operating system that consisted of a redesigned *Windows NT Server 3.51* kernel. This kernel was known as MultiWin. Citrix enjoyed a great deal of success with WinFrame—so much so that they started working on a beta version of WinFrame 2.0 based on the Windows NT 4.0 kernel.

In February 1997, Microsoft informed Citrix that they would no longer license the Windows NT 4.0 kernel for use in WinFrame 2.0. Microsoft understood the impact that WinFrame had made and wanted to design and ship their own version of a multiuser operating system. Citrix's stock plummeted. Ed Iacobucci went on the offensive, and Citrix immediately went into negotiations with Microsoft. The outcome of those negotiations included the licensing of the MultiWin technology for use in future Microsoft products. Shortly after the agreement was finalized, Microsoft shipped Windows NT Server 4.0, Terminal Server Edition. This time, the product was also a completely independent operating system that separated itself from

Windows NT Server 4.0 because of the redesigned kernel, but Microsoft was responsible for the distribution and support. The licensing extended to the Windows 2000 Server family.

What Citrix did not license to Microsoft is what sets Citrix apart from the crowd. Since Citrix is not allowed to ship their own version of terminal services, they have specialized in providing enterprise-level functionality to the terminal services provided by Microsoft. Such technologies as *multi-vendor support*, *load balancing*, *installation management*, and many others are provided to ease an administrator's job. These services are packaged under the auspices of MetaFrame. The original version of MetaFrame shipped as an add-on to the Windows NT Server 4.0, Terminal Server Edition. The latest version of MetaFrame, MetaFrame XP, adds its enterprise functionality to both Windows NT Server 4.0, Terminal Server Edition and the Windows 2000 Server family running the Terminal Services service. When used with Windows 2000 Server, MetaFrame can take advantage of the new technologies Microsoft has implemented, such as the new domain structure and network security.

MetaFrame XP is marketed in three flavors: *XPs*, *XPa*, and *XPe*. The main difference among the three levels is the inclusion of various components. The size of the MetaFrame environment is usually the deciding factor for which product will be used.

The XPs version is the standard version of MetaFrame XP and is used in small MetaFrame environments. It ships with only the MetaFrame XP product—no additional pieces. Small organizations wanting to take advantage of the *Independent Computing Architecture (ICA)* protocol, additional client platform support, additional network protocol support, and seamless desktop features, yet do not have an immediate need for load balancing, utilize this version.

The XPa version ships with the Load Manager add-on. With this additional component, the MetaFrame servers in an organization can be load-balanced within the server farm. It's perfect for the medium-sized installation where the administrator wants centralized administrative control and ease of server load balancing.

The final product, XPe, includes all of the components for large enterprise-wide implementations of MetaFrame XP. These components include *Load Manager*, *Installation Manager*, *Resource Manager*, and *Network Manager*. Each of these tools provides additional functionality to the base MetaFrame XP product. We will examine them in greater detail during later chapters. In the meantime, let's move on to why MetaFrame is such a great product.

# The Benefits

With the release of WinFrame, and now MetaFrame, Citrix has given administrators the ability to start deploying a standardized set of applications across a variety of computing platforms. Users who run Unix or Macintosh as their operating system of choice can now run Windows-based applications. This standardization of applications helps to control the total cost of ownership by reducing the number of applications that administrators need to support. For the moment, let's take a look at the benefits of running Terminal Services, whether MetaFrame is used or not; then we will look at how MetaFrame augments these benefits.

## Benefits of Terminal Services and MetaFrame

Many discussions have arisen over the topic of Total Cost of Ownership (TCO). It's a telling gauge of how efficient and effective a product or course of action may be. Since the cost of owning computer systems can be very hard to quantify, we need to look at some of the areas that differ between a typical computer installation and Terminal Services or MetaFrame installation. By doing this, we'll gain a better grasp of how both Terminal Services and MetaFrame installations can positively affect the TCO of an organization.

### Direct and Indirect Costs

One of the main benefits of running terminal services is the ability to have a thin client. This means that the client has as little as possible loaded onto it. Most clients in a terminal services environment have nothing more than the operating system and terminal services client software loaded. This is true for a network running Windows 2000 Server Terminal Services as well as MetaFrame XP. The reduced administrative overhead needed to maintain applications on a user's system is a reduction in an area usually known as an indirect cost.

*Indirect costs* are those that have no true dollar amount that we can apply to the balance sheet and are not easily calculated. The amount of time an administrator spends working on systems is seen as a cost, but defining that cost is difficult. The actual dollar amount is hard to set since, among other things, the administrator may be doing more than one function at a time. Thus, as administrators' time is used in performing tasks, the company incurs the cost of payroll and benefits by employing them, and the TCO increases for every function they perform.

*Direct costs*, on the other hand, are easy to attribute a dollar amount. Consider the example of a school system that obtained a grant to purchase computer systems in 1996. At the time, they were able to purchase Pentium 166MHz-based systems. These systems were considered fast when they were purchased, but with the advances made by the software industry, these systems were barely able to run newer versions of Internet Explorer by the 2000–2001 school year. Other applications the school obtained during the 2000–2001 school year would not load onto these computers. The software's minimum system requirements exceeded the computer system's hardware.

After submitting another grant proposal, the school received another grant for additional hardware and software. The school system determined that it could either purchase new hardware to replace existing computer systems or purchase servers that would run terminal services and use the current computers as clients.

After receiving quotes on various servers, the school chose servers that were configured to host 40 users each. Although the servers needed to support only 25 users, the greater size was utilized so that just in case one server failed, all of the users could still function. The four servers were priced at $15,000 each, or $60,000 total. If the school had purchased 100 new computer systems at $1,800 each to replace all of the existing systems, they would have incurred a charge of $180,000. Thus, a direct savings of $120,000 in hardware costs alone could be attributed to terminal services. With this cost savings, the school was able to purchase MetaFrame XPe and implement load balancing to allow the 100 client computers to efficiently run sessions. If any one of the servers failed, the remaining servers could handle the additional load and all users could continue working.

## Application Savings

Application deployment is easier to perform since a single installation is all that is needed to allow all users access to the software. An administrator decides which applications need to be installed, performs the installation, and configures permissions for the users who need access to the application. When the users open their sessions, they have access to the application. Any updates or service packs that are required for the application need only be installed once on the server, and all users' sessions will have the upgrade.

The same holds true for the operating system. As hot fixes, service packs, and configuration changes are applied, they are applied for every user who accesses a session on the server. Instead of having to install the service pack or hot fix on all client systems in the organization, the administrator need only apply it once at the server level.

Since applications are not loaded on a user's computer in a terminal services environment, the user may not be able to make configuration changes to the application. When only an administrator is allowed to initiate application modifications, user error is nearly eliminated, thus reducing the amount of time a technician needs to work on the system and reducing indirect costs at the same time.

Another benefit of running applications from a server is the storage savings. When an application is loaded on a user's local computer, the application takes up drive space on that computer. If 20 users need an application suite loaded onto their computers, and the suite consumes 200MB of drive space, over 4GB of drive space would be consumed among the computers. In comparison, if all users access the same application from one MetaFrame server, the total space required to load the application would be 200MB. That's a storage savings of 3.8GB!

## Downtime

User *downtime* is another area that concerns companies. When a computer system is being repaired or troubleshot, the user's productivity plummets. In a terminal services environment, a spare system can be brought to the user's workplace as the original system is removed for repair. Since the applications the user needs are loaded onto the server and their workspace is on the server, the computer through which they access their session does not matter. If a user's computer happens to completely crash on them during a session, they can simply move to another computer and reconnect to their previous session, continuing their work.

To take it one step further, there are companies that ship special terminal devices for thin client terminal sessions. These devices connect to the terminal services computer when they are turned on and allow the user to connect to a session. They usually contain no drives and have very few moving parts, making them very reliable. If one device does fail, the technician simply plugs another in its place and allows the user to reconnect to the server. This is a big benefit over having to bring another computer to the user's desktop and possibly having to load on a new operating system and all of the applications that the user needs to perform the functions of their job.

## User Application Support

*Shadowing* is the ability to "see" the user's session from an administrator's session. The ability to take control of a user's session or to watch the session as the user accesses an application can be very beneficial to administrators. If a user is having difficulty running an application, the administrator can start a shadowed session and watch what the user is doing. The administrator can even take control of the session to demonstrate to the user the proper steps. This functionality is also extended to allow the administrator to take control of a server that is running terminal services. Whether the administrator is shadowing a user's session or a server running terminal services, they have the benefit of working with a user or performing administrative tasks as though they were sitting at the server without leaving their desk.

## Security

*Security* has been and always will be a major concern for organizations of all sizes. When an application is loaded on a user's computer, the user has access to the program files and could copy those files for use elsewhere or just inadvertently delete the files required for the application to execute. With terminal services, the applications are kept securely on a server. Users, by default, do not have access to the files required to execute the application, only to the shortcuts that are needed to launch the application. Furthermore, users have access only to those applications that the administrator has given them permissions to use. This keeps users from running applications that they are not supposed to use.

Data can also be secured more easily using terminal services. A user's profile is stored on a server. If they choose to save data in the My Documents folder, that folder is on the server. Restrictions can be put in place to keep the user's local drives hidden from them. Since data is stored on the servers, the files can be backed up using the line-of-business backup and restore utilities.

Most applications take advantage of a local file storage area known as the *temporary files directory*. This directory is used to hold file information downloaded from a server. If another user gains access to these temporary files, they could have access to sensitive information. *Page files* on the local computer can also pose a security risk for this same reason. If a page file on a local computer is not flushed, sensitive data could be retained on the hard drive of the local computer. With terminal services, applications running locally on the server use the temporary files, directories, and page file located on that server. The user's computer never hosts cached copies of the data. In a terminal services environment, an organization exerts greater security over their systems and data by controlling everything from a central location.

## MetaFrame Benefits

So far, we have been discussing benefits that apply at both the terminal services and MetaFrame level. MetaFrame has some additional benefits that extend terminal services functionality and allow it to become an enterprise-level service. Without MetaFrame, an organization is restricted to using Microsoft Windows operating systems as the clients when accessing Terminal Services. Support for other operating systems is gained from adding MetaFrame. Once it is added, Unix and Macintosh users will have access to the same line-of-business applications that Windows users employ. Once the applications are standardized for all of the clients, administrators will not have to support a large variety of applications on different platforms, thus lowering their support costs.

Citrix retained the rights to numerous add-on products that extend the functionality of Terminal Services. These add-ons included the Citrix ICA protocol, Load Manager, Installation Manager, Resource Manager, and several other features that we will take a look at in later chapters. In the meantime, though, let's take a brief look at these and other benefits in more detail.

### Independent Computing Architecture

The Citrix design goal for MetaFrame is Digital Independence. Simply stated, this means that applications should be available on all computing platforms. Administrators are not limited to the traditional "they don't have Windows so they can't run Office" mentality. Standardizing applications reduces the amount of administration an administrator needs to perform in a varied computing platform environment. Controlling those applications from a centralized location eases an administrator's workload.

There are four primary areas identified in Citrix's goal for digital independence: Any Client Device, Any Network Connection, *Any Network Protocol*, and Seamless Desktop Integration. Let's take a look at each of these.

### Any Client Device

While Microsoft has developed client software for virtually any Microsoft-based client, Citrix extends that ability to nearly every client type available. Table 1.1 lists the clients available when using MetaFrame.

**TABLE 1.1** Clients Available Using MetaFrame

| Platform | Clients |
|---|---|
| Windows 32-bit | Windows 9*x*, Windows NT 3.51, Windows NT 4.0, Windows 2000, Windows Me |
| Windows 16-bit | Windows 3.1, Windows for Workgroups 3.11, OS/2 2.1, OS/2 Warp Connect 3.0, OS/2 Warp Connect 4.0 |
| Windows CE | Client device running Windows CE 2.0 or later; see OEM specs for availability |
| EPOC/Symbian | EPOC release 5.0 |
| Java | Web browsers that support Sun's Java Virtual Machine or JDK 1.1 or later |
| Macintosh | 68040 or PowerPC microprocessor systems running System 7.1.2 or later with Apple's Thread Manager, System 7.5.3, MacOS 8 or later |
| Unix | Linux, SCO UnixWare 7, Hewlett-Packard HP-UX 10.*x* or greater, Sun Solaris 2.5.1 and above, Sun SunOS 4.1.4, Silicon Graphics IRIX 6.2 and above, Digital Unix 3.2 and above, IBM AIX 4.1.4 and above |
| DOS | DOS 4.0 running on a 386 or better platform |

With the inclusion of the Java client, any client with a web browser is able to access applications running on a Citrix MetaFrame server. Now you can run any operating system you choose and have access to applications that would normally run only on a Windows platform. MS-DOS 5.0 running Microsoft Office 2000 SR1, anyone?

### Any Network Connection

The ideal thin client solution allows a client to connect from anywhere across any connection type. This would include any connection from a T1 to a slow modem connection. The ICA protocol is optimized to utilize very little bandwidth when passing data from the server to the client. Users can dial in from their home computers across a slow modem connection and still view their full desktop and run applications as though they were running the applications locally on their computers.

### Any Network Protocol

The ICA protocol can be encapsulated within any routable protocol. An administrator can utilize an existing IPX/SPX, TCP/IP, NetBIOS, SLIP/PPP, or asynchronous network connection. When utilizing an asynchronous connection, there's no need for an administrator to configure a Remote Access Service (RAS) server for dial-up purposes.

### Seamless Desktop Integration

Ideally, you do not want your users to know that they are actually running their applications on a server. If you can make them think that the applications are executing on their local computer, users are less likely to send inquiries concerning the applications to their IT department. *Seamless desktop integration* is the terminology Citrix uses when defining the user's experience working within a session. The interaction between the user's session and their local desktop should appear seamless, as though everything is running locally. The following topics define the technologies that are encompassed in this design goal.

#### APPLICATION LAUNCHING AND EMBEDDING

Imagine firing up a browser and pointing it to a web page that contains an icon for Microsoft Word. Immediately, Microsoft Word launches in a separate window on your desktop. All of the functionality of Microsoft Word is available to you. *Application launching* allows the application to start in its own window on the user's desktop independently of the web page. Launching an application is the most versatile means of accessing a program through a web page. When launching an application, the user can access other web pages and even close the web browser window while running the application. The connection to the Citrix MetaFrame server is maintained until the application is ended.

Or perhaps you access your corporate web site and connect to a web page that has an Excel link listed. You click the link and an Excel spreadsheet appears within the main frame of the web page. *Application embedding* ties the application to the web page. Embedding an application into a web page allows you to limit the use of the application. Once the user leaves the web page, the application connection is lost. If the web page is closed, the application is closed also. MetaFrame XP allows an administrator to control how applications behave when accessed through a web page.

#### RESOURCE MAPPING AND REDIRECTION

*Resource mapping and redirection* is a term used to describe how MetaFrame interacts with the client's local resources. Drive mapping allows users to access their local hard drives with the same drive designations they had while running applications locally. Since most users are familiar with their C: drive as the local drive on their computer, it is easier for everyone involved to have that designation still apply to the local hard drive on the user's computer. Virtual drives in the client's session represent the client's local drives. When the client accesses the virtual C: drive while in a terminal session, they are accessing folders and files from their local hard drive. The server drives are mapped to other drive letters so that the client can still access them.

Printer mapping works similarly to drive mapping. A user's local printers are re-created in the user's sessions. Any documents sent to the printer are redirected to the user's local printer.

COM port redirection creates virtual ports on the server. When COM port redirection is used, the data is redirected to the user's local port. This allows the terminal session to use devices that are connected to the serial ports on the client's system.

Other resources that can be accessed by the server to give the user the impression that the applications are running locally are 16-bit stereo sound cards and the clipboard. Sound files pass from the server back to the client and are played through the stereo speakers. The clipboard can be utilized for copying information from applications that are running on the server and pasting that data to applications that are running locally on the client's computer, and vice versa.

#### SERVER FARMS

For administrators who have multiple servers, a *server farm* can be used to group the servers into a centralized administrative unit. The servers can then be used to deploy and manage applications. During setup, the MetaFrame server can be added to a server farm. All servers in a server farm then share a data store. This data store acts as a repository for information for the applications, administrators, and servers within the server farm. An administrator can create the data store using any ODBC-compliant database, including Microsoft SQL Server, Oracle, and Microsoft Access. There are many benefits to using server farms, including load balancing and installation services, that we will look at in later chapters.

### Scalability

When using Terminal Services alone, each client is directed to a server according to the settings within the Terminal Services client software. The only way to redirect a user is to change those parameters in the client software. Some administrators create multiple shortcuts on the user's desktop and direct them to connect to one server unless the session seems slow. In that case, they are directed to log out of that session and try the other server's shortcut on the desktop.

While the previous example will work, it is not a true load-balancing technique. Consider an organization that has five terminal servers and 100 users wanting to gain access to sessions. An administrator can configure the clients to connect to one of the servers so that only 20 users are accessing any one server at a time. This guarantees that the load on any of the servers will not become too great.

You may wonder, though, "What happens when users from one server are all logged on, but there are very few sessions started on any of the other servers?" One server will be loaded to its maximum while the others are barely taxed. This is not load balancing. MetaFrame has a load-balancing mechanism that directs a user to a server that is seen as the least busy, thus evening out the load on each server. If 40 users are logged on in this five-server environment, each server would have eight user sessions running. Each server is optimized and not overloaded, as resources are evenly distributed across the servers.

Throughout the remainder of the book, we will be discussing the technologies that make MetaFrame a necessary addition to Terminal Services.

## New Features

Although we will be addressing the new features of MetaFrame XP, those individuals familiar with MetaFrame 1.8 will need to know how to access their old familiar tools in this new product. Most of the items in the following list are new to MetaFrame XP; however, we have also noted which items are now augmented or changed from the MetaFrame 1.8 product.

**Application Save Position** *Application Save Position* saves user information about an application's last screen position and size.

**Centralized Data Storage** *Centralized Data Storage* stores in a database configuration information for servers in a server farm.

**Citrix Management Console** This new Java-based tool replaces some of the old familiar tools. Citrix Server Administration, Published Application Manager, Citrix Licensing, and Load Balancing Administration are now all combined into *Citrix Management Console* (*CMC*). Additional support for printers is also found within this tool.

**Citrix Network Manager** *Citrix Network Manager* works in conjunction with SNMP software such as HP OpenView to manage and monitor server farms.

**Citrix Resource Manager** One of the additional components of MetaFrame XPe, *Citrix Resource Manager* allows an administrator to monitor servers in a farm, configure alerts for processes on the servers, and collect data on the servers that can be used to provide reports and graphical data.

**Greater Color Depth** *Greater Color Depth* provides extended color support that allows applications to utilize high-color (65,535) and true-color (16.7 million) sessions.

**Greater Resolution** *Greater Resolution* allows a session to take advantage of resolutions up to the current maximum of 2700 × 2700.

**Independent Management Architecture** *Independent Management Architecture* is the framework that holds server farms together and allows you to easily manage an enterprise-level server farm across multiple segments and the hardware that secures them.

**Integrated Security** *Integrated Security* means that 40-, 56-, and 128-bit data security and 128-bit authentication encryption levels are built into the product.

**Licensing** *Licensing* provides single-point license installation and activation with support for license pooling.

**Logging of Shadowing** *Logging of Shadowing* provides logs of all the sessions that have been shadowed.

**Multi-Monitor Support** *Multi-Monitor Support* means that MetaFrame XP can span the display of the session across multiple monitors if the client is configured to allow it.

**Multiple Session Support** *Multiple Session Support* means that 16-bit ICA Clients can run multiple ICA sessions.

**NFuse** The *NFuse* tool allows administrators to publish applications within a web page so that users can start an application session with their web browser.

**Panning and Scaling** *Panning and Scaling* means that, when viewing an application on a handheld device, the user can opt to view the application full size and scroll it on the screen or reduce it to fit within the device's screen.

**Pass-Through Authentication** *Pass-Through Authentication* allows the user's current logon credentials to be passed to the MetaFrame server.

**Printer Management** *Printer Management* allows print driver configuration and installation replication through the server farm.

**Product and Connection Licenses** *Product and Connection Licenses* are now held in the data store database.

**Shadow Indicator** When a client is being shadowed, the indicator shows on their screen and they have the option to stop the shadow session from the *Shadow Indicator* dialog.

**Shadowing** *Shadowing* of ICA Client sessions can now be disabled during the MetaFrame XP setup.

**SNMP Agent** *SNMP Agent* allows MetaFrame XP servers to be monitored and managed through an SMTP console such as HP OpenView.

**SpeedScreen Latency Reduction** This provides configurable parameters for user response data. *SpeedScreen Latency Reduction* allows the computer to display information immediately on the screen when a user types information or selects an object with the mouse instead of having to wait on the server to respond with the screen updates.

**TCP-based ICA Browsing** *TCP-based ICA Browsing* uses TCP instead of UDP to discover a published application. It works through firewalls and other network devices.

**Web-based Client Install** Clients can use a web server to gain access to the files necessary to install the ICA Client software using *Web-based Client Install.*

# The Exam

Probably the more accurate question for this chapter's title would have been "Why Citrix MetaFrame XP certification?" Many questions seem to float around, especially now with the rush for administrators to keep their certification updated: "So why should anyone want to take another certification exam?" "Aren't there enough certifications already?" and "What is so special about the CCA exam?"

Good questions.

As with any technology, there needs to be a means of recording and certifying those individuals who excel at implementing and using that technology. Administrators who work for companies can prove their expertise by becoming certified. Consultants have a standard by which they can market their services. Companies looking for skilled individuals have a benchmark to use as they start their candidate-selection process.

The *Citrix Certified Administrator (CCA)* exam, at the time of this writing, does not count toward any other company's certification route. Unfortunately, it will not work as an elective to the *Microsoft Certified Systems Engineer (MCSE)* or the *Certified Novell Engineer (CNE)* certifications. It will, however, round out the scope of your certifications and enable you to stand out from the pack. For the administrators holding a premier certification from Microsoft or Novell, adding the CCA (or CCEA if you want to continue on!) to your arsenal can only help your chances for promotion or a new job. In addition, MetaFrame is becoming recognized as a viable alternative to upgrading legacy computers. As companies adopt this technology, they will look for those individuals who have already proven their worth. Earning your CCA will set you apart from the rest of the individuals vying for those positions.

Each of the areas covered in the exam is reflected in this book. We present material according to the objectives that Citrix has provided. In doing so, we have tried to present the information in a logical order. The early chapters in the study guide cover the objectives that are server based, and the later chapters segue into the client topics.

NOTE

For more information about the exam, look at the introduction to this book. You will find information about how to study, what the exam covers, and what to expect when you show up at the test center.

Before diving into Chapter 2, let's do a quick overview of each of Citrix's objectives for the MetaFrame XP 1.0 Certification exam:

**Objective 1: Introduction to MetaFrame XP** This chapter covers the topics associated with this objective. While this objective is not covered in great detail on the exam, every other objective spawns from this one. Each of the Objective 1 topics acts as the foundation for the rest of the objectives.

**Objective 2: MetaFrame Installation Process** It is generally believed that anyone can install an operating system and load applications now that wizards are available to walk you through the steps. Understanding the installation options and the ramifications of the installation procedures can make the difference between a stable, useful system and angry users!

**Objective 3: Using Citrix Technologies** It's time to break down MetaFrame into its base components. This objective covers the underlying technologies that make MetaFrame the impressive tool that it is. The topics include:

- The ICA Packet
- The benefits of SpeedScreen Technology
- The features of Independent Management Architecture
- Listener Ports, Idle Session, ICA Sessions, and Client Device Licensing

**Objective 4: MetaFrame XP Administration** Server administration starts here! Since MetaFrame allows us to perform server and application management at the server level, we need to look at the tools that make up our main administrative utilities.

**Objective 5: Additional Management Tools** Client administration is the second half of the administration puzzle. Included within MetaFrame are the tools to control and monitor user sessions.

**Objective 6: Load Management and Security** To ensure that a user's experience running MetaFrame is a good one, the servers hosting user sessions should not be overloaded. Servers can be set up in a server farm consisting of systems configured with the same applications and where the user session is directed to the least busy server.

Security has been, and probably will be, one of the main concerns of organizations doing business on and off of the Internet. Administrators need to know the impact security measures have on the systems they implement.

**Objective 7: Applications** Without applications, MetaFrame becomes just another means of accessing a remote desktop. While some applications are written to take advantage of a multiuser environment, many others are not. An administrator needs to know how to maintain the life cycle of an application as it exists on a MetaFrame server.

**Objective 8: Citrix ICA Client Software** As we move to the client side of MetaFrame, we look at the client software available and the installation of the software.

**Objective 9: Citrix Program Neighborhood** Program Neighborhood is the primary tool for controlling the user's environment at the client. This is one topic that everyone needs to know well!

**Objective 10: Web Connectivity** Nearly every computer has a web browser. MetaFrame has made it easy for an administrator to allow clients to access applications from their browser and either run the app within the browser interface or allow the app to be seen in its own window.

**Objective 11: Printing** Once the bane of every Citrix administrator's life, printing received an overhaul with MetaFrame XP.

**Objective 12: Monitoring and Troubleshooting MetaFrame XP Servers** No administrator's life is complete without the constant monitoring of systems within their environments. Citrix utilizes some of the Microsoft tools but also provides a set of their own.

NOTE

Exam objectives are subject to change at any time without prior notice and at Citrix's sole discretion. Please visit Citrix's Training and Certification website (`www.citrix.com/training/`) for the most current list of exam objectives.

# Summary

Although brief, this chapter introduced what MetaFrame is, the benefits of running Terminal Services and MetaFrame, and the test objectives that will be covered in the remainder of the book. MetaFrame is a very powerful tool that enables an administrator to control user sessions running on a server and design and manage a large enterprise client/server environment.

From here, we build on the topics and present the material in an orderly fashion. From the underlying technologies to Citrix Management Console to SpeedScreen to Load Manager and beyond, we will be taking a wild ride down the Citrix certification highway. So strap in and be prepared as we cover the topics for the CCA exam.

# Exam Essentials

**Understand the correlation between Microsoft's implementation of Terminal Services and Citrix Systems' MetaFrame XP.** Microsoft's Terminal Services runs remote sessions that allow clients to offload the processing of their applications. MetaFrame XP adds enterprise-level functionality to Terminal Services.

**Understand the new features of MetaFrame XP over MetaFrame 1.8.** All of the new features allow the administrator to more easily manage the MetaFrame environment and make the user's experience even more seamless than before.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Any Network Protocol

application embedding

application launching

Application Save Position

Application Savings

Centralized Data Storage

Certified Novell Engineer (CNE)

Citrix Certified Administrator (CCA)

Citrix Management Console (CMC)

Citrix MetaFrame XP

Citrix Network Manager

Citrix Resource Manager

Citrix WinFrame

client/server technology

direct costs

downtime

Greater Color Depth

Greater Resolution

Independent Computing Architecture

Independent Management Architecture

indirect costs

installation management

Installation Manager

Integrated Security

licensing

load balancing

Load Manager

Logging of Shadowing

Microsoft Certified Systems Engineer (MCSE)

Multi-Monitor Support

Multiple Session Support

multi-vendor support

MultiWin

Network Manager

NFuse

page files

Panning and Scaling

Pass-Through Authentication

Printer Management

Product and Connection Licenses

Resource Manager

resource mapping and redirection

seamless desktop integration

security

server farm

Shadow Indicator

shadowing

SNMP Agent

SpeedScreen Latency Reduction

TCP-based ICA Browsing

temporary files directory

terminal services

thin client technology

Web-based Client Install

Windows 2000 Server

Windows NT Server 4.0, Terminal Server Edition

Windows NT Server 3.51

XPa

XPe

XPs

# Review Questions

1. Which of the following is not provided with Microsoft's implementation of Terminal Services?

   **A.** Load balancing

   **B.** Remote administration of servers

   **C.** Centralized application support

   **D.** Centralized user support

2. When establishing the Total Cost of Ownership, which of the following can be calculated as a direct cost?

   **A.** The value of the time the administrator spends fixing software-configuration problems

   **B.** The cost of servers and client workstations

   **C.** The value of the time users spend waiting for their computer to be repaired

   **D.** The value of the time a technician spends applying service packs to computer systems

3. What is the name of the technology that Citrix developed that was licensed to Microsoft for inclusion in their Windows Server families?

   **A.** MultiFrame

   **B.** MultiSession

   **C.** MultiTerm

   **D.** MultiWin

4. What are the three versions of MetaFrame XP? (Choose all that apply.)

   **A.** XP

   **B.** XPa

   **C.** XPe

   **D.** XPs

**5.** Which of the following items are indirect costs? (Choose all that apply.)

**A.** The value of the time an administrator spends troubleshooting an application error

**B.** The cost of the client license to access Windows 2000 Server

**C.** The cost of a client's computer system

**D.** The value of the time spent installing applications on a client computer

**6.** Which is a benefit of implementing MetaFrame XP over Microsoft Terminal Services alone?

**A.** The ability to run a session from nearly any client operating system

**B.** The ability to run your user session on a server instead of your computer

**C.** The ability to assign applications to individual users

**D.** The ability to load a service pack one time and have all users updated

**7.** What does Application Save Position do for a user?

**A.** Saves the user's location within an application so that the next time the application is started, the user will be presented with the same data they were accessing when they closed the application.

**B.** Saves the screen location for an application so that it will open in the same position when the user starts it again.

**C.** Saves the application's configuration files on the client system so that the application will load faster when it is opened again.

**D.** Saves the application's configuration files in the user's profile so that the application will start faster.

8. Which of the client's resources can be used from within a session, otherwise known as Resource Mapping and Redirection? (Select all that apply.)

   **A.** Drives

   **B.** Sound cards

   **C.** COM ports

   **D.** Clipboard

9. When using a handheld device with a small screen, which feature of MetaFrame XP allows you to zoom in on an area of the desktop?

   **A.** Application Zoom

   **B.** Desktop Magnifier

   **C.** Panning and Scaling

   **D.** Zoom and Rotate

10. What is the logical grouping of MetaFrame XP servers that share configuration information called?

    **A.** Server farm

    **B.** Server corral

    **C.** Server group

    **D.** Server store

11. Within a MetaFrame XP environment, which of the following technologies allows you to view another user's session?

    **A.** Panning and Scaling

    **B.** Shadowing

    **C.** MultiWin

    **D.** ICA pass-through Client

**12.** Which of the following options are benefits of MetaFrame over Microsoft Terminal Services? (Choose the two best answers.)

**A.** Clients can run on any Windows operating system.

**B.** Clients can run on operating systems other than Windows.

**C.** The ICA protocol can be encapsulated within the TCP protocol.

**D.** The ICA protocol can be encapsulated within any transport protocol.

**13.** Which of the following are defined as part of Digital Independence? (Choose all that apply.)

**A.** Any Client Device

**B.** Any Network Connection

**C.** Any Network Protocol

**D.** Scalability

**14.** Which of the following technologies allows sessions to be redirected to the least-used server in the server farm, regardless of whether the server is running MetaFrame XP or MetaFrame 1.8?

**A.** Installation Manager

**B.** Load Manager

**C.** Network Manager

**D.** Resource Manager

**15.** Which of the following make up seamless desktop integration? (Choose all that apply.)

**A.** Application launching and embedding

**B.** Resource mapping and redirection

**C.** Published applications

**D.** Shadowing

**16.** Server-side processing of information sent from a client is known as ____________________? (Choose all that apply.)

**A.** Server-side processing

**B.** Client/server technology

**C.** Dumb terminal technology

**D.** Thin client technology

**17.** What are some of the benefits of running Citrix MetaFrame XP with Windows 2000 Terminal Services? (Choose all that apply.)

**A.** Lower Total Cost of Ownership (TCO)

**B.** Lower direct and indirect costs

**C.** Enhanced user application support

**D.** Enhanced security

**18.** What are some of the benefits of running Citrix MetaFrame XP that Windows 2000 Terminal Services alone cannot provide? (Choose all that apply.)

**A.** Support for Unix and Macintosh clients

**B.** Load management features

**C.** Resource and network monitoring features

**D.** Resource mapping and redirection

**19.** Which of the following features are new to MetaFrame XP? (Choose all that apply.)

**A.** SpeedScreen

**B.** Independent Management Architecture

**C.** Shadow logging

**D.** ICA protocol

**20.** Which technologies allow Citrix MetaFrame XP with NFuse to run applications from a web page? (Choose all that apply.)

**A.** Application encoding

**B.** Application embedding

**C.** Application execution

**D.** Application launching

# Answers to Review Questions

1. A. Terminal Services, as implemented by Microsoft, allows you to perform any of the options listed with the exception of load balancing. To provide the server farm the ability to direct clients to the least-busy system, you need to install MetaFrame XPa or XPe.

2. B. A direct cost is a cost whose value is easily calculated and is reflected on the company's balance sheet. The price paid for hardware and software is seen as a direct cost.

3. D. MultiWin is the technology that was created for the Microsoft Windows environment to allow a server to run multiple sessions at once.

4. B, C, D. The three versions of MetaFrame XP are XPs, the standard version that ships with no additional components; XPa, which ships with the load balancing add-on Load Manager; and XPe, which ships with all of the additional components, including Installation Manager, Load Manager, Resource Manager, and Network Manager.

5. A, D. An indirect cost is a value that is estimated for services rendered by individuals. The estimated dollar value of user downtime and technician's troubleshooting and repair time is seen as an indirect cost.

6. A. Terminal Services, as implemented by Microsoft, allows you to perform any of the options listed with the exception of running sessions from any client operating system. If clients are using a Macintosh, MetaFrame needs to be in place to allow the client to access the server and start a session.

7. B. When a published application is started, the screen location is recorded and used the next time the application is started.

8. A, B, C, D. All of these client resources can be used from within a user's session. Since these resources are to be used from within the session, the user can take advantage of local devices while processing the information on the server.

9. C. Panning and Scaling allows you to view a desktop on a handheld device, zoom into an area of the desktop, and pan from side to side and top to bottom.

10. A. The term *server farm* refers to one or more MetaFrame XP servers that are grouped together to share configuration information and published applications.

**11.** B. Shadowing allows you to view another user's session, and if the permissions allow, you can also take control of the session.

**12.** B, D. While the ICA Client can be run on any Windows platform and the ICA protocol can be encapsulated within the TCP protocol, this functionality is available using standard Terminal Services. The additional functionality of running on any operating system and utilizing any transport protocol is found only in MetaFrame.

**13.** A, B, C, D. All of these options are part of Citrix's vision for Digital Independence. Digital Independence separates the operating system and connection a user has available from the processing of the applications.

**14.** B. Load Manager is a service that is available with the XPa and XPe versions of MetaFrame XP. When Load Manager is installed in a mixed-mode server farm, all of the MetaFrame servers can participate in load balancing.

**15.** A, B, C. *Seamless desktop integration* is a term Citrix uses to describe the technologies that make the user think they are interacting with the applications as though they were running on the user's desktop instead of on a MetaFrame server. *Shadowing* is a tool used to view and interact with a user's session.

**16.** B, D. Having the server process information sent from a client system is called *client/server technology* and is sometimes referred to as *thin client* technology.

**17.** A, B, C, D. All of the options are benefits of running Citrix MetaFrame XP with Terminal Services.

**18.** A, B. While all of the options are benefits of running Citrix MetaFrame XP, Terminal Services cannot provide support for clients other than Windows clients and does not have any load management features.

**19.** B, C. The Independent Management Architecture and shadow logging features are new to MetaFrame XP. While MetaFrame XP takes advantage of SpeedScreen technology and the ICA protocol, they are not new to this release.

**20.** B, D. When NFuse is used with Citrix MetaFrame XP, applications can be executed from a link on a web page, thanks to application launching and embedding.

# Chapter 2

# Underlying Citrix MetaFrame XP Technologies

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **3. Using Citrix Technologies**

- 3a. Identify the components of the ICA Packet
- 3b. List the benefits of SpeedScreen Technology
- 3c. Discuss the features of Independent Management Architecture
- 3d. Recognizing Listener Ports, Idle Sessions, ICA Sessions and Client Device Licensing

There are many Citrix administrators. Some are good administrators and a few are great administrators. What differentiates a good administrator from a great one? A good administrator knows the utilities necessary to get the job done. A great administrator not only knows the utilities but also knows what happens when those utilities are used and understands the technologies that work behind the scenes.

### Real World Scenario

#### My Mechanic: Patching versus Troubleshooting

My van developed a strange vibration in the front end that I could not figure out. I decided to take the van to the dealership where I had purchased it. As is common in most dealerships, the service department was divided into separate specialties, not unlike what is done in the computer industry where groups are divided according to their specialties.

The van was delivered to the "tire guy." After running the front tires through a few tests, he discovered that one of the belts in the driver's side front tire was bad. He told me that I would need to replace the tire before the problem became much worse and caused further damage. So replace it I did, with a tire that they recommended.

Three weeks later, the vibration returned. Very slight at first, but then it started building to the point where it felt like the first tire had. I made another appointment for the van, and lo and behold, the belt on the tire they had replaced was going bad. The technician attributed it to a bad run of tires and they replaced it for free.

Well, you can probably guess where this is going. Another month went by and the same vibration returned. This time, I decided to take my van to a mechanic whom my father had trusted for many years. He looked over the van and called me with some information. He told me that the tire did indeed have a belt that was going bad, but the problem did not lie within the tire itself. The CV (constant velocity) joint was defective, and due to the vibrations it was putting out, the tire was affected. Through the course of a month, the belts in the tire would start to work loose, causing a vibration that I could feel through the steering.

We see this same thing in administrators. Some know how to work with the tools and make the changes that are necessary to patch the problem, while others know how to troubleshoot since they truly understand how things work.

In this chapter, you will be exposed to the technologies that make MetaFrame XP the great product that it is. We will focus all of our attention on the third objective domain of the MetaFrame XP 1.0 exam, “Using Citrix Technologies.” These technologies extend the functionality of terminal services and deliver enterprise-level centralized administrative capabilities. Some of these are the same tools that were present within MetaFrame 1.8, some have been given facelifts and now have additional functionality, while others are completely new to MetaFrame XP.

Citrix has integrated these technologies so that they work with legacy MetaFrame environments such as MetaFrame 1.8. To make everything run smoothly, MetaFrame server farms now have two modes, native and mixed. In *mixed mode*, MetaFrame 1.8 servers can exist in the same server farm as MetaFrame XP servers. Only when the server farm no longer hosts MetaFrame 1.8 servers should the server farm be switched to *native mode*.

In this next section, we will identify the technologies that perform differently when in native mode than in mixed mode. So let’s start by taking a look at the ICA protocol and dissecting the packet.

# Identifying the Components of the ICA Packet

When Citrix was designing WinFrame, they knew that they needed a protocol efficient enough to travel over any transport protocol. In order to design a protocol that complex, they developed a set of standards, or criteria.

Since Windows NT was the platform that Citrix was developing the ICA protocol for and TCP/IP was the protocol most widely used on that operating system, they decided that the first requirement would be that the protocol would have to build its own framing header. In the case of streaming protocols such as TCP, the packet was required to build its own frame set. *Framed protocols* such as IPX already have this functionality, so the framing header is not utilized.

Reliability was the second requirement since IPX/SPX was the second-most-popular transport protocol. Connectionless protocols such as IPX are then able to guarantee error-free transport of the encapsulated information. TCP, on the other hand, is a reliable connection-based protocol, so the reliable header is not used.

The other criteria that Citrix required in a protocol include the following:

**Ensuring the server's ability to execute all application logic** When an application launches within a session, all of the execution is performed on that server. The client computer does not process any of the information; it acts as a thin client only.

**Keeping network traffic to a minimum** This is achieved by transferring only screen updates, keystrokes, and mouse clicks between the client and the server. The client's only function is to interact with the user. Therefore, only the screen updates performed by the server and data input by the user are transferred across the network.

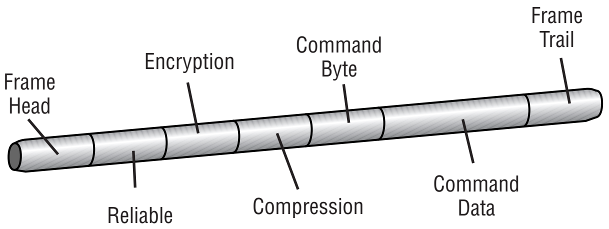
**Ensuring the ability to utilize any transport protocol** These include TCP/IP, IPX, SPX, NetBIOS, NetBEUI, PPP, Async, ISDN, Frame Relay, ATM, and any other existing or developing protocols. ICA Packets can be encapsulated into any transport protocol.

**Enabling the application to perform at LAN-like speed** This should be possible even when it's utilized through a low-bandwidth connection. The protocol efficiency should allow the client to interact with its session as though the user was accessing the applications locally.

**Permitting the latest 16-bit and 32-bit applications to run on legacy clients that would not normally have the resources to execute them** Because the server processes the entire application logic, the client system does not need the additional resources to host the Windows NT/2000 operating system or the latest applications.

## Pieces of the Packet

The ICA protocol, based on the criteria we just reviewed, is made up of multiple headers that surround a command byte and any command data. The following graphic illustrates the components of the ICA Packet:



As shown, the packet contains the following headers:

**Frame Head** The *Frame Head* header is used in stream-oriented communications such as TCP or Async to frame the data for reconstruction at the receiving computer.

**Reliable** The *Reliable* header is used in connectionless protocols such as IPX to provide reliable, error-free delivery.

**Encryption** The *Encryption* header is used as the preamble for managing any packets that contain encrypted data.

**Compression** The *Compression* header is used as the preamble for managing any packets that contain compressed data.

**Command Byte** The *Command Byte* header is the only required ICA command byte. This is the beginning of the base ICA protocol packet.

**Command Data** The *Command Data* header contains optional data bytes associated with the specific command. The length of the data is dependent on the command.

**Frame Trail** The *Frame Trail* header completes the packet for stream-oriented communications, such as Async and TCP.

The ICA Packet is built at the *Presentation layer* of the *Open Systems Interconnection (OSI) model*. This means that the protocol can be encapsulated within any of the transport protocols that exist in today's network environments. As the ICA Packet is built, it is passed through a series of drivers before it is encapsulated into the transport protocol. Depending upon the transport protocol and the additional technologies utilized, such as encryption, the command and command data have headers appended to them by these drivers. Just as with any protocol, the server adds these headers onto the packet. After the packet is encapsulated into the transport protocol, it is delivered to the client, which examines the headers and acts upon them to correctly access the command and command data.

The ICA Packet is the cornerstone for all of the technologies that Citrix has introduced over the years since WinFrame was developed. In the next few sections, we will take a closer look at some of these foundation technologies.

## The Benefits of SpeedScreen

While a server is processing the data for a client, frequent screen updates can occur. Mouse movements and keyboard entries are reflected on the screen. The results of commands are displayed on the screen, and the windows and applications that are opened from double-clicking an icon are also shown. During these screen updates, if the server needed to refresh every pixel on the screen for every update, far too much network traffic would occur. Even though the ICA Packet can be compressed to reduce traffic, screen updates still occur very rapidly. Citrix took this factor into consideration and developed a technology for the MetaFrame 1.8 product known as *SpeedScreen*, which allows the server to update only the portions of the screen that have changed.

When screen repaint information is prepared for transmission to the client, each screen item is compared to previously transmitted data. If the data has not changed, the server will not retransmit the information and the client will not have to reprocess the information. Any data that has changed is reflected on the user's display. With these enhancements alone, users have four times the performance gains over non-SpeedScreen sessions.

Screen repaints are not the only performance-enhancing feature with SpeedScreen. MetaFrame XP introduced new functionality, *local text echo* and *mouse click feedback*. These new technologies extend and enhance an already robust idea and make MetaFrame an even more viable solution when used in a slow-link situation. Both are configurable at the server level and are known collectively as *SpeedScreen Latency Reduction*.

If SpeedScreen Latency Reduction is turned on, local text echo goes into action. As soon as a user logs on to a MetaFrame session, the server pushes a series of screen images, which represent the screen fonts, to the client system. As the user enters information, the client system examines the data that is captured by the keyboard and determines what should be displayed on the screen. When the server processes the information, the actual screen updates are sent to the client. For the most part, the client will not see any difference when the screen repaint occurs. Usually, the only differences occur when the font changes and the client has not been updated with the new screen information.

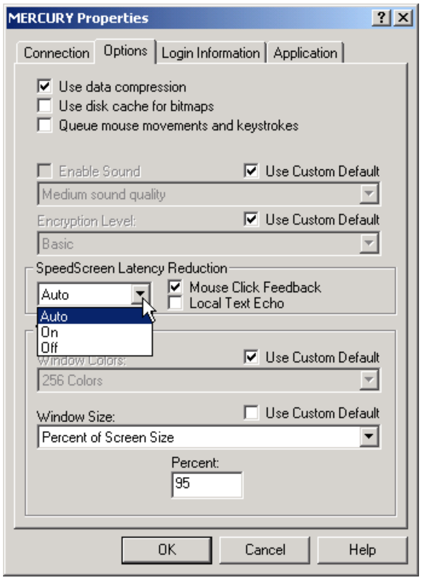
Mouse click feedback allows a user to see that the system is responding to a mouse-click action. This is especially useful on slow network links where the client system may not receive the screen update immediately. It may appear to the user that the mouse click was not received by the system. This becomes problematic when users are familiar with applications that run native on their computers. Since it appears as though the application did not respond to the mouse click, the user will again click the application. When it appears as though it is still not responding, the user will click again and again. This multiple clicking only causes further problems due to the additional data that is sent out for the server to process.

To alleviate this, mouse click feedback changes the pointer to an hourglass to indicate that the user has performed an action. After the server processes the client's action, the screen is updated to reflect that action, and the pointer returns to its normal shape. The major bonus to this feature comes from the server not having to process any additional mouse clicks. Hence, the users see what they think they should see, and the server processes only the data it should have to process.

These two SpeedScreen tools are configurable. From the client's Program Neighborhood, the options are applied for an entire application set or on the individual programs. You can set these options by opening Program Neighborhood and navigating to File ➢ Application Set Properties and selecting the Default Options tab. When applied at the application-set level, all applications within that set inherit the settings. If the properties for a published application are different than the application-set properties, the application overrides the set options. Program properties always override set properties. See the SpeedScreen Latency Reduction options in Figure 2.1.

We will provide more in-depth information on SpeedScreen and SpeedScreen Latency Reduction a bit later in Chapter 6, "Other Administrative Tools." For now, we will concentrate on more of the underlying technologies.

**FIGURE 2.1** SpeedScreen Latency Reduction options



MERCURY Properties

☑ Use data compression
☐ Use disk cache for bitmaps
☐ Queue mouse movements and keystrokes

☐ Enable Sound ☑ Use Custom Default
Medium sound quality

Encryption Level: ☑ Use Custom Default
Basic

SpeedScreen Latency Reduction
Auto ☑ Mouse Click Feedback
☐ Local Text Echo

Window Colors: ☑ Use Custom Default
256 Colors

Window Size: ☐ Use Custom Default
Percent of Screen Size

Percent:
95

# Client Resource Redirection and ICA Functionality

The server is responsible for performing the processing on behalf of the client, so all of the local resources for the server are made accessible to the user. There are instances when users need access to resources local to their workstations. MetaFrame provides file system redirection to some of the user's local resources by providing *drive mapping*, *printer mapping*, and *COM port redirection*.

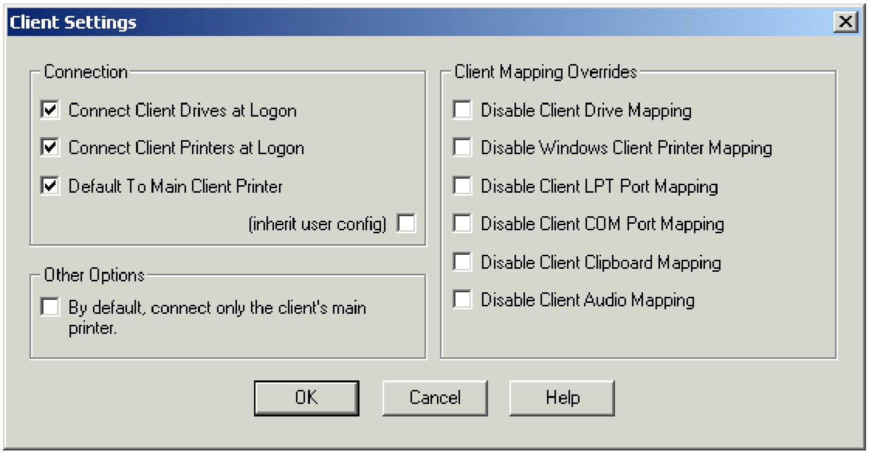
Drive mapping gives an administrator the ability to control what the user sees when they access system drives during a session. Each drive the user has on their local computer is available to them in their Citrix session. If the drives on the server have been remapped (which we'll talk about in Chapter 4, "Installing MetaFrame XP"), the user will access their local system drives using the same drive letter that they have on their local computer. Thus, the user's C: drive will appear as C: in the Citrix session. If the server's drive letters have not been remapped, the client's local system drives are mapped starting with the letter V: and working backward through the alphabet. The only deviation from this would be if the client had a drive letter already in use at the time of the mapping. In this scenario, the client's C: drive would appear as V:, and their D: drive would appear as U: in the Citrix session. If U: was already mapped before the connection to Citrix, then that letter would be skipped and the client's D: drive would then connect to the next available letter, T:. This mapping is handy when you want to transfer files or access files on your local computer while connected to a Citrix server.

Printer mapping applies the same theories to a printer. Just as you can connect to client drives, you can also connect and print to your local printer. Your print device is remapped to the Citrix server, so it appears in the client's printer list. You can set the connections to all of the printers defined on the computer or just to the Windows default printer. Also, in Chapter 13, "Printing," we will discuss how MetaFrame XP has alleviated a lot of the printing problems that this model created with MetaFrame 1.*x*. This is done with print driver deployment and management.

Finally, COM port redirection allows a COM port on a client computer to be redirected to a COM port on the Citrix server. A good use for this would be a mobile user downloading and uploading information in their PDA from their hotel room to the Citrix server back in the office.

Mapping of these items is accomplished by using the standard Windows device-redirection facilities. Client mappings appear as another network that represents the client devices. When you connect to a device, you will see (aside from the Microsoft network) a network with the name "client." The devices that can be connected appear as share points in the client network to which a drive letter or printer can be attached. You reach these options by opening Citrix Connection Configuration, right-clicking the connection you wish to configure, and choosing Edit. When the Edit Connection screen appears, click the Client Settings button to open the Client Settings screen shown in Figure 2.2.

**FIGURE 2.2** Client mapping options in Citrix Connection Configuration



Client Settings

Connection
☑ Connect Client Drives at Logon
☑ Connect Client Printers at Logon
☑ Default To Main Client Printer
(inherit user config) □

Other Options
□ By default, connect only the client's main printer.

Client Mapping Overrides
□ Disable Client Drive Mapping
□ Disable Windows Client Printer Mapping
□ Disable Client LPT Port Mapping
□ Disable Client COM Port Mapping
□ Disable Client Clipboard Mapping
□ Disable Client Audio Mapping

NOTE

For more information on how to configure the client settings, see Chapter 11, "Program Neighborhood." For more information on how to configure the global settings for all clients at the connection level, refer to Chapter 6.

ICA utilizes client clipboard mapping, which allows cut-and-paste functionality between the ICA session and Windows clients. This permits a client to copy or cut and paste between a client application and an application that is running in an ICA session on the Citrix server.

Client audio mapping is also supported in ICA Clients. Audio support allows application sounds and WAV files to be played on the client devices. You can assign the following settings in the Citrix Connection Configuration utility.

**Low** The low setting causes any waveform data passed to the client to be compressed to a maximum of 16Kbps before transmission. The CPU requirements and benefits are about the same as those for the medium setting, but the lower data rate allows for a low-bandwidth connection.

**Medium** The medium setting causes any waveform data passed to the client to be compressed to a maximum of 64Kbps before transmission. This setting is recommended for most LAN-based connections, and it is the default setting.

**High** The high setting allows the waveform data to be played on the client device in its native data rate. The high data rate requires about 1.3Mbps of bandwidth to play without disruption. This connection is recommended only when bandwidth is plentiful and sound quality is very important.

# Features of Independent Management Architecture

Independent Management Architecture (IMA) is not just another fancy name that Citrix pulled out of their collective minds when trying to come up with a selling point for their latest version of MetaFrame. IMA is a completely new architectural model that replaces many of the key components of MetaFrame 1.8, and it is a protocol for server-to-server communications within the server farm. The subsystems that make up the IMA include the following:

- ICA Browser
- Server Management
- Application Management
- Runtime
- Persistent Storage
- Distribution
- Remote Procedure Call
- User Management
- Printer Management
- Citrix License
- Program Neighborhood
- Load Management

While some of these topics are outside the scope of this book, we will discuss the items relevant to the exam.

In Citrix's own words, IMA is "a unified, enterprise-wide platform for installation management, maintenance, support, and security for your organization's server-based computing and application hosting services." This reworking of some of the key components of MetaFrame has created a more robust enterprise-level product. Some of the functionality IMA has brought to MetaFrame includes:

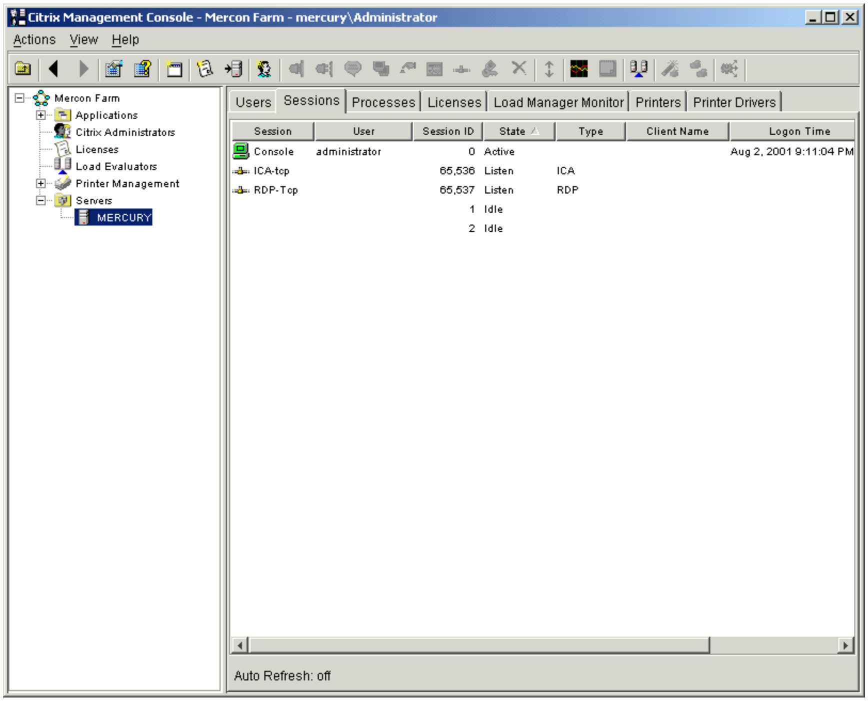
- Centralized administration of MetaFrame XP IMA
- Centralized configuration storage for all Citrix servers through a data store
- Centralized license management and pooling
- Discovery of published applications from ICA Clients without User Datagram Protocol (UDP) broadcasts
- Logging of shadowed sessions
- Support for Simple Network Management Protocol (SNMP)

Let's take a look at each of these features in detail.

## Centralized Administration

The new Citrix Management Console combines the functionality of several administrative tools: Citrix Licensing, Citrix Server Administration, Load Balancing, and Published Applications Manager. Since the console is Java-based, administrators are able to install it on Windows 2000, NT 4.0, and NT Server 4.0, TSE. With the tools located in a unified environment, the administrator is able to control the administration from one centralized tool instead of having multiple tools open at once. Figure 2.3 shows the Citrix Management Console with the nodes that are available to manage.

**FIGURE 2.3** Citrix Management Console



| Session | User | Session ID | State | Type | Client Name | Logon Time |
|---|---|---|---|---|---|---|
| Console | administrator | 0 | Active | | | Aug 2, 2001 9:11:04 PM |
| ICA-tcp | | 65,536 | Listen | ICA | | |
| RDP-Tcp | | 65,537 | Listen | RDP | | |
| | | 1 | Idle | | | |
| | | 2 | Idle | | | |

You control all applications that are published in your MetaFrame XP server farm through the Citrix Management Console. This is also the utility that you use to define the administrators who are assigned to your server farm, as well as control license counts for client access to applications. We cover each of these topics in greater detail in Chapter 5, "Administration and the Citrix Management Console."

## Centralized Configuration Storage

IMA acts as a central repository for configuration information for the server farm. All of the servers added to the farm report this information to the data store, which is a database that holds static and rarely changed information about the server farm. The data store can use either a *Microsoft Access*, *Microsoft SQL Server,* or *Oracle* database. In turn, this database is utilized in the farm in much the same manner as the Browser Service was used in MetaFrame 1.8. The data store holds the following information:

**Published Application** The Published Application section contains all of the configurable properties of the published application. These include the name of the application, user permissions, ICA connection properties, window size, color depth, encryption levels, and audio settings.

**Pooled License** The *Pooled License* section contains the license numbers and the total number of licenses available for pooling, which are reserved for individual servers.

**Server Configuration** The Server Configuration section holds information about the configuration of all servers in the server farm.

**User Configuration** The User Configuration section contains information about the configuration of all users in the server farm.

**Printers** The Printers section contains configuration and driver information for the printers available to the users.

Each MetaFrame XP server accesses the data store to send or retrieve configuration information. The servers are allowed to access the data store directly, or they can use another MetaFrame XP server as a proxy to access the data. These two access methods are known as direct access and indirect access. When configuring a server for direct access, known as putting it in direct mode, the server needs the *Open Database Connectivity (ODBC) drivers* installed for the database. If the administrator would rather not have the ODBC drivers installed on all of the servers, indirect mode will allow the server to indirectly access the data store through another server. One word of caution, however: the failure of the server configured with direct access will prevent the other servers from accessing the data store.

One of the key differences of MetaFrame XP over MetaFrame 1.8 is the way the servers in the farm handle information. In version 1.8, all of the servers in the farm held configuration information in their Registry. When the server came online, it would read the Registry and apply the configuration data to the server's Program Neighborhood. As changes were made, each server would notify the other servers in the farm of the changes. In addition, the master browser would keep a cached copy of the configuration information within an in-memory database. Although this allowed all of the servers to process information about all of the other servers in the farm and allowed clients to find published applications within the farm, there were issues with the amount of network traffic that was generated. All changes were sent to all servers as a complete change list, not an incremental one. The updates were also sent as UDP broadcasts, which limited the functionality of the update process.

With MetaFrame XP, servers no longer send all of the configuration information and configuration changes to every server. Instead, the configuration information is delivered to the data store. As servers are added to the server farm or started after a shutdown, they read the information contained in the data store and add it to their local host cache.

Each server within the server farm has a *local host cache*, which is actually a Microsoft Access database that holds a subset of the information contained in the data store. As information changes in the server farm, the server is notified of the changes, and it then downloads any changed information into the local host cache. This cached configuration is utilized for two purposes: to allow the server to still function when the data store is offline and to allow clients to resolve applications locally.

All MetaFrame XP servers replicate the information from the data store when they are first started. This information includes which servers are in the farm and the current published applications they host. The IMA service will continue to send updates to the server as changes are made to the server farm. When a client attempts to resolve access to an application, the server's local host cache can direct the client to the proper server since it contains information concerning the application configuration. This enhances the response time for the client when a published application is requested.

If the data store goes offline for any reason, MetaFrame XP servers can still perform the application resolution for up to 48 hours. After 48 hours, the licensing information expires and the server will not perform these functions until the data store is back online. The IMA service will continue to try to reestablish connection with the data store during this time. As soon as the data store comes back online, the server will refresh its licensing information and the local host cache. At that point, the client will function as normal.

NOTE

For more information on configuring the data store database, see Chapter 4.

## Centralized License Management and Pooling

When the first MetaFrame XP server is added to the server farm, the MetaFrame XP server performs license pooling. All licenses available in the server farm are by default combined into a license group and available for all clients. This alleviates the problem of assigning a static number of licenses to each individual server. With licenses combined in one large database, any user can connect to the farm and gain access to resources on any server on the farm. Any user accessing resources will consume only one license, even if the resources they are accessing are physically located on different servers.

NOTE For more information on client device licensing, see the section "Basics of Client Device Licensing" later in this chapter.

## Discovering Published Applications

Whenever a client searched a MetaFrame 1.8 server farm for published applications, the client would send out a broadcast message that would be answered by a MetaFrame server that was configured as the master browser. This broadcast was sent out as a UDP broadcast. If the subnet that contained the client computer did not have a browser gateway installed, the client would not receive a full list of published applications. Published applications from other subnets would not be seen, only those published applications on the local subnet.

MetaFrame XP alleviates this problem by storing all of the server farm configuration information in the data store and then passing copies of it to all of the servers in the farm. When a client opens Program Neighborhood, the local MetaFrame server delivers a list of all of the published applications to the client.

The original version of the ICA browser is now replaced with IMA. Of course, Citrix includes support for the legacy browser, but by default the XP servers take over the master browser function in a mixed-mode server farm. Browser elections are still performed within the server farm, and MetaFrame XP is given the highest *election criteria*—a version number of 20. Since the MetaFrame XP server will win an election, MetaFrame 1.*x* servers should have their browser election setting configured so that they never become browsers in the farm. This will reduce the amount of network traffic generated when a MetaFrame 1.*x* server is rebooted.

IMA divides the farm into *zones* to ease administration and to reduce network traffic. Each zone defines a physical area in which servers are grouped. The zone's *data collector* gathers any changes made within the *server farm* and distributes the changes to other zones in the farm. Each zone has one data collector that is elected along the same way a master browser was elected in previous versions of MetaFrame.

The election criteria for choosing a data collector are these:

1. Highest master number version: The number 1 is used for all MetaFrame XP servers.
2. Lowest master ranking: A server with the number 1 is the most preferred; a server with the number 4 is not preferred.
3. Highest host ID: The host ID is assigned at installation. It is a random number in the range of 0 through 65,536.

Elections are triggered in the following situations:

- A member server loses contact with the data collector.
- The data collector goes offline.
- A server is brought online within the server farm.
- The `querydc -e` command is invoked.
- The zone configuration changes, such as a change in the zone name, the election preference of member servers, or the server membership.

If a new data collector is elected, the servers will contact the data collector to verify that it is available. If the data collector is available, the servers will transmit their configuration information. If the data collector does not change, the servers that were online before the election will not send their configuration data. Servers that lost connection will send a complete update to the data collector.

Each of the data collectors has a connection to every data collector for each of the other zones in the farm. After an election is forced, if the existing data collector loses the election, it will contact the other data collectors and notify them of the change. Data collectors from other zones will then establish a connection with the new data collector.

As session information changes, the data collectors update one another. Communications among them are initiated immediately when any of the following changes occur:

- ICA Client logon or logoff
- ICA session reconnect or disconnect
- Server and application load changes

- License acquisition and release
- Server brought online or goes offline
- Published application changes
- IP and MAC address changes

Since each zone collector has a connection open to all other data collectors in the farm, all data collectors are aware of the server load, licensing, and session information for every server in the farm. If no communications have been received from a member server in a zone within a certain time interval, the zone's data collector pings (an internal function known as an IMA ping) that server to verify that it is online. The default time interval is once per minute. A single zone supports up to 256 member servers.

IMA reduces network traffic by taking advantage of the data collector model to distribute information quickly and efficiently. When a change is made on a member server, the member server sends the updated information to the data collector for the zone it is in. The data collector then sends update notifications to the data collectors for which it has connections. Each data collector that receives the update sends the update to the member servers in its own zone.

For example, when a Citrix administrator opens the Citrix Management Console and publishes a new print driver, the following steps occur:

1. The server writes information to the data store.
2. The server sends the change to its zone's data collector.
3. The zone's data collector distributes the change to all member servers in its zone.
4. The zone's data collector sends the change to all other zone data collectors.
5. The other zone's data collectors receive the change and distribute it to all member servers within their respective zones.
6. All member servers receive the change and update their local host cache as requested.

Normally, data collectors are synchronized through constant updates. Occasionally, an update sent from one data collector to another data collector can fail. Instead of flooding the network with constant requests to the failed server, the data collector waits a specified interval (five minutes by default) before attempting communication again.

## Logging Shadowed Sessions

One of the most convenient features of MetaFrame is the ability to *shadow* a client. To shadow is to view the session of a client from within an administrator's session, more commonly know as a *shadowed session*. There are many benefits to shadowing. Companies have implemented shadowing for troubleshooting purposes, allowing remote control and providing users with application support. Many administrators take advantage of the ability to control a server from a remote computer. They can interact with the computer as though they were sitting locally and can control any resource on the computer with one tool.

### Real World Scenario

#### Administrators on the Go

Most administrators like to sit and control everything on their network from one central location. Their workstation becomes their command center. For some smaller companies, however, the administrator may not have that luxury. The administrator may be the only tech support person at that location. Responsible for everything, they are too busy to have the luxury of a command center.

Steve is one such administrator. He is the lone wolf who fields every helpdesk question, fixes every problem with client machines and printers, and administers all of the systems on his network. He is one very busy person.

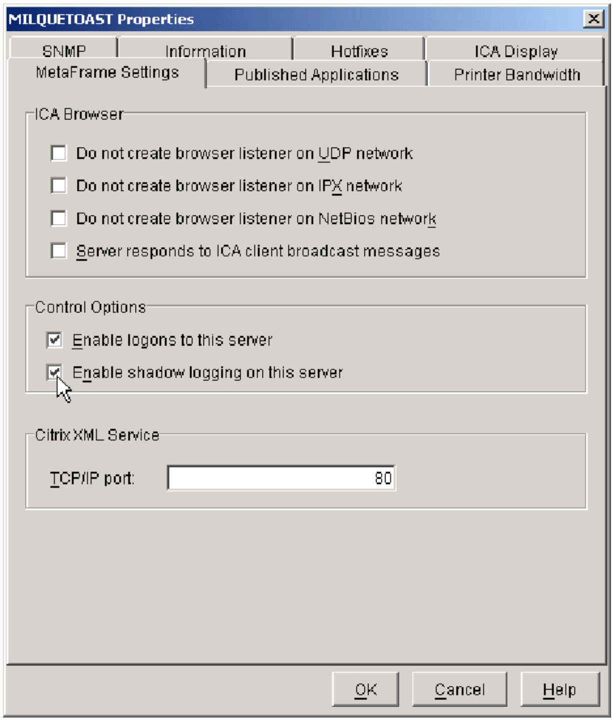
After installing Microsoft Windows 2000 Advanced Server on his network, Steve took advantage of Terminal Services so that if the occasion arose, he could load the client on a user's system and administer his servers and shadow other users having problems in their sessions. Though he did like the convenience, he did not like having to load the client software each time he used someone's computer that did not already have it installed. Loading the client also caused problems with those users who wanted to know what it did.

After purchasing MetaFrame XP and installing it to allow remote clients to use the Web features, he came up with an idea to make his own life a little easier. He purchased a Compaq iPaq and loaded the Windows CE client on it. With the addition of a wireless network adapter, he is now able to administer his servers from anywhere in the building. Having the client software running on the Windows CE operating system allows him to view the entire remote desktop on the screen, or he can use the Panning and Scaling feature to have a full-size desktop.

Now as he is walking through the building putting out fires, he can start a session on his handheld and manipulate any of his servers. If he needs to answer a call from a user who is having problems with an application, and that user is running a session, he can shadow that session and assist the user with their problem. Now he has the best of both worlds.

Shadowed sessions are not logged by default. To allow sessions to be logged to Event Viewer, the server must have the option enabled within the Citrix Management Console. You can reach this option by opening Citrix Management Console, right-clicking your server within the Servers node, selecting Properties, and choosing the MetaFrame Settings tab. Then click the Enable Shadow Logging On This Server check box, as shown in Figure 2.4. With this feature enabled, the application log records information concerning the session that is shadowed as well as the session that performed the shadowing. The event appears as an Event ID 1001. While shadowing can be a vital tool, logging can curtail any abuse.

**FIGURE 2.4** Enabling shadowed session logging



MILQUETOAST Properties

ICA Browser

☐ Do not create browser listener on UDP network

☐ Do not create browser listener on IPX network

☐ Do not create browser listener on NetBios network

☐ Server responds to ICA client broadcast messages

Control Options

☑ Enable logons to this server

☑ Enable shadow logging on this server

Citrix XML Service

TCP/IP port: 80

NOTE For more information on shadowing, refer to Chapter 6.

## Simple Network Management Protocol Support

*Simple Network Management Protocol (SNMP)* is a network tool that is used by many companies to monitor their networked devices. It has been in use for many years and is a well-proven protocol. Citrix provides support for SNMP monitoring of MetaFrame XP servers. Each of the servers in the server farm can provide administrative event notification to a third-party management console such as Hewlett Packard's HP OpenView product. The SNMP service loaded on a MetaFrame XP server also allows a basic level of administration of the server. If MetaFrame XPe is installed, Citrix Network Manager is available for use as an SNMP agent for the server farm. With this product, the entire server farm can be monitored and managed using SNMP.

# Working with Listener Ports

When MetaFrame is installed, a special service is created known as the *listener port*. By default, each protocol installed has one listener port created for it. This service monitors the packets received by the server's interfaces for client connection attempts.

To view and administer listener ports, walk through the steps in Exercise 2.1.

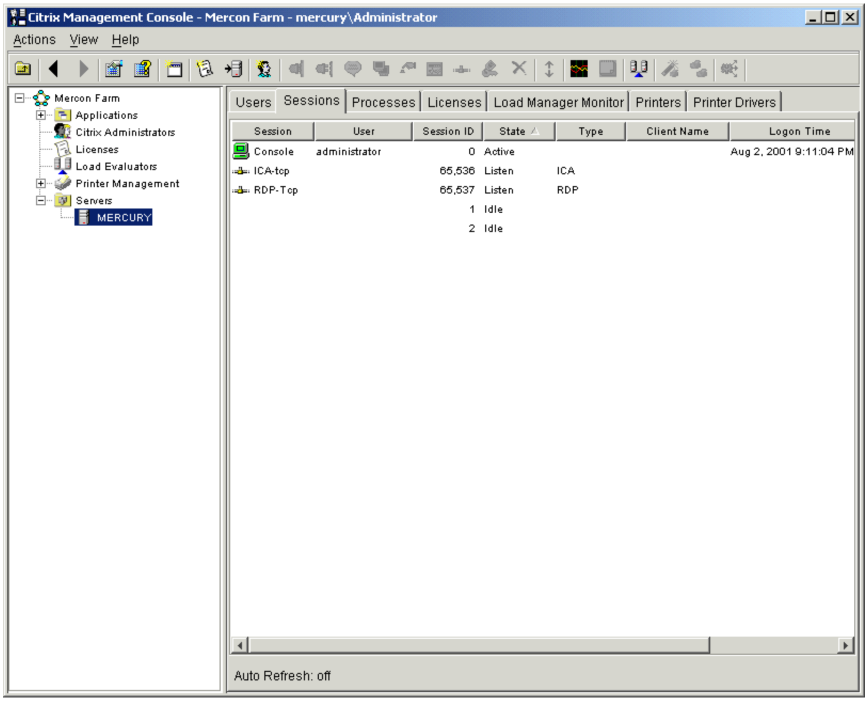
**EXERCISE 2.1**

### Viewing Listener Ports

In this exercise, we will open the Citrix Management Console to view the listener ports.

1. Click the Citrix Management Console icon from the Citrix ICA Administrator toolbar or access it from the Start menu: Start ➢ Programs ➢ Citrix ➢ Citrix Management Console.
2. Expand the Servers node and select a server object.
3. Click the Sessions tab, as shown here.

## EXERCISE 2.1 *(continued)*



| Session | User | Session ID | State | Type | Client Name | Logon Time |
|---|---|---|---|---|---|---|
| Console | administrator | 0 | Active | | | Aug 2, 2001 9:11:04 PM |
| ICA-tcp | | 65,536 | Listen | ICA | | |
| RDP-Tcp | | 65,537 | Listen | RDP | | |
| | | 1 | Idle | | | |
| | | 2 | Idle | | | |

4. Under the State column, locate the listener port for each of the protocols.

If users are reporting difficulties accessing the Citrix server, an administrator may need to reset a listener port. You can do this from within Citrix Management Console also. To accomplish this, follow the steps in Exercise 2.2.

## EXERCISE 2.2

### Resetting Listener Ports

1. Click the Citrix Management Console icon from the Citrix ICA Administrator toolbar or access it from the Start menu: Start ➢ Programs ➢ Citrix ➢ Citrix Management Console.

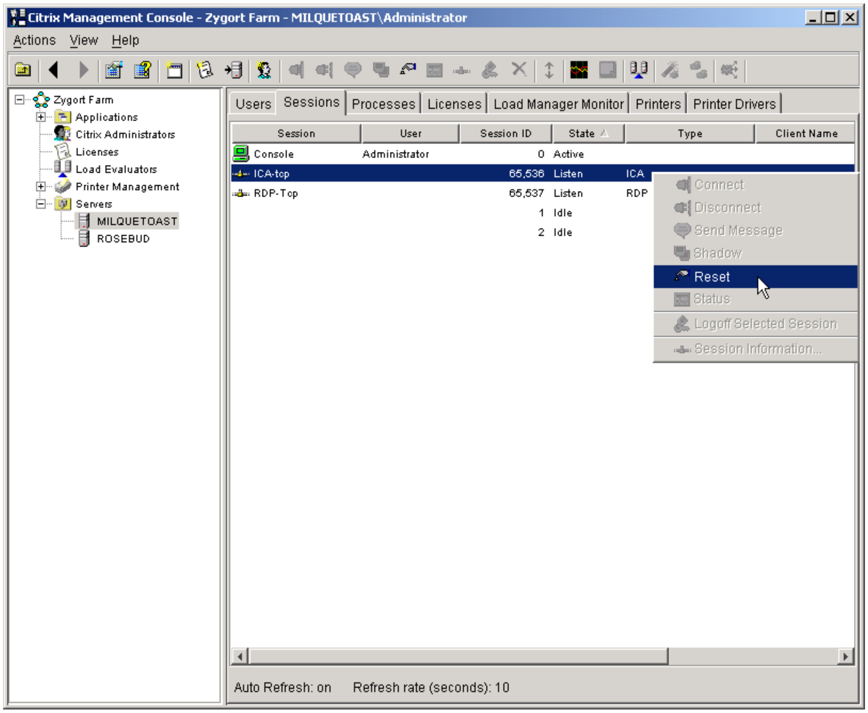
2. Expand the Servers node and select a server object.

**EXERCISE 2.2 *(continued)***

3. Click the Sessions tab.

4. Right-click the listener port for the protocol that you need to reset.

5. Select Reset from the context menu, as shown below.



| Session | User | Session ID | State | Type | Client Name |
|---|---|---|---|---|---|
| Console | Administrator | 0 | Active | | |
| ICA-tcp | | 65,536 | Listen | ICA | |
| RDP-Tcp | | 65,537 | Listen | RDP | |
| | | 1 | Idle | | |
| | | 2 | Idle | | |

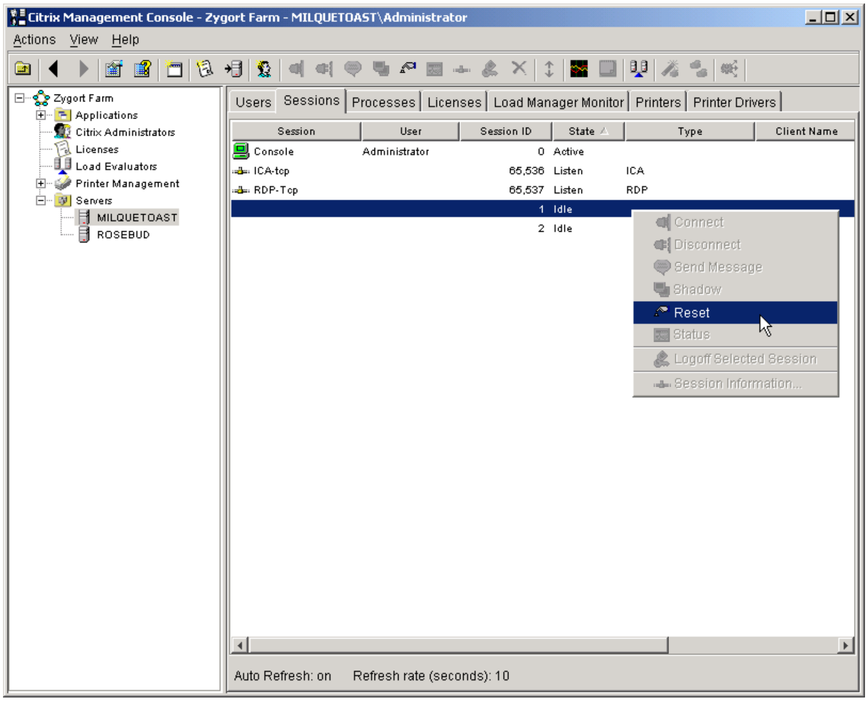
Auto Refresh: on    Refresh rate (seconds): 10

When a client attempts a connection to the server, the listener port responds by initiating a conversation with the client and prepares the server for the user's session. This includes passing the required information to an idle session.

# Working with Idle Sessions

An idle session is created for each protocol loaded on the server. These sessions are aptly named *idle sessions* since they are sessions that are created on the server but have not yet been assigned to a client. Since they consume only 1.7MB of memory each, the resource consumption is minimal. The main advantage to these sessions is that they are already created and waiting for a client connection. Because the connections are not created from scratch as the client initiates a session, the session can be activated much faster. Although it is rare, idle sessions may need resetting. The procedure is the same as for resetting a listener port, as shown in Figure 2.5. Now let’s look at what happens as a client attempts to create a session.

**FIGURE 2.5** Resetting idle sessions from within the Citrix Management Console



| Session | User | Session ID | State | Type | Client Name |
|---|---|---|---|---|---|
| Console | Administrator | 0 | Active | | |
| ICA-tcp | | 65,536 | Listen | ICA | |
| RDP-Tcp | | 65,537 | Listen | RDP | |
| | | 1 | Idle | | |
| | | 2 | Idle | | |

Auto Refresh: on    Refresh rate (seconds): 10

# Maintaining and Configuring ICA Sessions

As the listener port directs a client request to the idle session, the session state changes from *Idle* to *ConnQ* as the connection is in the process of connecting. Once connected, the session state changes to *Conn*. The session remains in this state while the user logs on. The session state will change one more time, this time to *Active*, when the user has successfully logged on to the server.

As long as the user is accessing applications within the session, the state of the connection will remain Active. Once the user logs off from the session, that session is discarded and the resources reserved for it are released back to the operating system.

One other state that you may see when looking at the session information in Citrix Management Console is *Disc*, which stands for Disconnected. Users can disconnect from their sessions, which keeps the session alive on the server, but the window in which they were viewing their session is closed on the client. As soon as the user logs back on to the server, the idle session that is presented with the session request redirects the user to their existing disconnected session. The user sees the same session they were running previously, with all applications that were processing still active.

Of course, allowing users the option of disconnecting their sessions can cause other problems. New users have a tendency to become confused when presented with the option to either log off or disconnect. Administrators should have rules in place for dealing with disconnected sessions. In Chapter 4, we will look at ways to configure what happens to a disconnected session. For now, let's look at the final section, and probably the section over which most administrators cry with despair.

# Basics of Client Device Licensing

*Client Device Licensing* is analogous to per-seat licensing in Windows 2000. Licenses are allocated to the client, which allows the client to access any resource from within the server farm, regardless of which server the resource resides on. Since a user consumes only one license when connected to published applications or desktops, the number of licenses is conserved. Case in point, if Jami starts a session that runs Microsoft Excel, the server that is hosting the session allocates one license from the pool to Jami's account. After starting that session, she opens another session that runs WinZip. Even if the session controlling WinZip is on another server than the session running Microsoft Excel, Jami's account consumes only one license.

There is one exception to this rule. If the client connecting to the server farm is using client software from MetaFrame 1.0, the connections made to the servers in the farm must all be with the same protocol. If a user connects to Server A and Server B with TCP/IP, only one license will be consumed. As soon as the client connects to Server C using IPX/SPX, another license will be consumed, effectively wasting a license.

# Summary

As you have perused the pages of this chapter, you have been exposed to the technologies that, for the most part, work behind the scenes. Citrix's Independent Computing Architecture and Independent Management Architecture work together to give the end user a sense of working at their local workstation, while at the same time making administration of the entire enterprise easier for the administrator. These technologies and everything they have to offer, from client device licensing to shadowed sessions, are the building blocks for the chapters to come. As in any profession, the better you know how things work, the better your administrative acumen will be.

Studying this chapter will also give you insight into the exam. The exam touches on every topic in this chapter, whether in the context of underlying technologies or in the context of one of the administrative tools. From here we move on to the meat of the book.

# Exam Essentials

**Know how to control what users see when accessing system drives.** Drive mapping gives an administrator this ability. MetaFrame provides file system redirection to some of the users' local resources by providing drive mapping, printer mapping, and COM port redirection.

**Understand client mappings.** Client mappings allow devices and software running on a user's system to be used while they are in an ICA session.

**Know the parts of the ICA Packet.** The ICA Packet contains the command byte that tells the client or server what is contained in the packet. Other headers are included for additional functionality depending on the transport protocol used.

**Understand the benefit of SpeedScreen.** SpeedScreen is the technology that allows the server to determine what needs to be sent to the client so that the screen is updated efficiently and the data transmission is optimized.

**Understand the benefits of SpeedScreen Latency Reduction.** Local text echo, the ability to let the client device make changes to the screen output before the server responds, and mouse click feedback, having the mouse pointer change to an hourglass after the mouse button is clicked, help the user see that an action has been performed.

**Know the features of IMA.** The features of IMA are as follows:

- Centralized administration of MetaFrame XP and legacy Citrix servers
- Centralized configuration storage for all Citrix servers through a data store
- Centralized license management and pooling
- Discovery of published applications from ICA Clients without UDP broadcasts
- Logging of shadowed sessions
- Support for SNMP

**Understand the benefits of Client Device Licensing.** Client Device Licensing allows a client to connect to as many servers in the server farm as necessary to access their applications and still use only one connection license.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Active

Client Device Licensing

COM port redirection

Command Byte

Command Data

Compression

Conn

ConnQ

data collector

Disc

drive mapping

election criteria

Encryption

Frame Head

Frame Trail

framed protocols

Idle

idle sessions

listener port

local host cache

local text echo

Management Console

Microsoft Access

Microsoft SQL Server

mixed mode

mouse click feedback

native mode

Open Database Connectivity (ODBC) drivers

Oracle

Open Systems Interconnection (OSI) model

Presentation layer

Pooled License

printer mapping

Reliable

server farm

shadow

shadowed session

Simple Network Management Protocol (SNMP)

SpeedScreen

SpeedScreen Latency Reduction

zones

# Review Questions

1. At what layer of the OSI model does the ICA Packet work?

   A. Physical

   B. Network

   C. Transport

   D. Application

   E. Presentation

2. When the ICA Packet is used within a TCP/IP network, what headers are added to the packet before it is encapsulated within the TCP packet? (Choose all that apply.)

   A. Frame Head

   B. Frame Trail

   C. Reliable

   D. Reliable Trail

3. Which of the following client resources cannot be accessed from a session by means of redirection?

   A. Clipboard

   B. Drive partition

   C. Network card

   D. Serial port

   E. CD-ROM drive

4. Which transport protocol is used to encapsulate ICA Packets? (Choose all that apply.)

   A. TCP

   B. IPX

   C. NetBEUI

   D. Frame Relay

   E. ATM

5. What technology allows a server to resolve requests for published applications?

   A. Local text echo

   B. Local host referral

   C. Local host resolution

   D. Local host cache

6. What are the two new technologies used in SpeedScreen to enhance the user's experience while accessing the session over a slow link? (Choose all that apply.)

   A. Mouse redirection

   B. Mouse click feedback

   C. Local text echo

   D. Local text referral

7. A client connecting to the server farm with a MetaFrame 1.0 client accesses four servers. With Server 1, the connection is made with TCP/IP. Server 2 is connected to using IPX/SPX. Server 3's connection is through TCP/IP, and Server 4 is using NetBEUI. How many licenses does the one client use?

   A. 1

   B. 2

   C. 3

   D. 4

8. Which of the following components can be part of an ICA Packet? (Choose all that apply.)

   A. Frame Head

   B. Compression

   C. Encryption

   D. Command Data

9. The ICA Packet is built at the ________ layer of the OSI model.

   A. Presentation

   B. Session

   C. Application

   D. Transport

10. A MetaFrame XP server that can interoperate with MetaFrame 1.8 servers is running in _______ mode.

    A. Native

    B. Interoperability

    C. Mixed

    D. Rollback

11. What is the only required byte in the ICA Packet?

    A. Command Data

    B. Command

    C. Reliable

    D. Frame Head

12. What utility would you use on the client side to make changes to the SpeedScreen settings?

    A. SpeedScreen Latency Reduction Configuration

    B. Program Neighborhood

    C. Citrix Connection Configuration

    D. Custom ICA Connections

13. You have many users on your network who use audio with their presentation software. You would like to give them the ability to use the presentation software over an ICA connection. Some users are at a remote location that is connected to the main location through a dial-up network link. What would be the best setting in the Citrix Connection Configuration utility for these users?

A. Low

B. Medium

C. High

14. The high audio setting in the Citrix Connection Configuration utility requires about _______ of bandwidth to play without disruption.

A. 64Kbps

B. 512Kbps

C. 1.024Mbps

D. 1.3Mbps

15. What new feature of MetaFrame XP replaces the old broadcast-based way of communication with MetaFrame 1.*x*?

A. XML

B. TCP/IP+HTTP

C. IMA

D. ICA

16. Each MetaFrame XP server in the farm has a subset of the information that is contained in the data store. This is known as what?

A. Local data store

B. Data store cache

C. Local data cache

D. Local host cache

17. Which of the following will trigger a data collector election? (Choose all that apply.)

A. A member server loses contact with the data collector.

B. A server is brought online within the server farm.

C. A member server is brought down within the server farm.

D. The data collector goes offline.

**18.** How many member servers can a zone support?

**A.** 64

**B.** 128

**C.** 256

**D.** 1024

**19.** What path will an update travel in an IMA-based MetaFrame farm?

**A.** When a change is made on a member server, the member server sends the updated information to the data collector for the zone it is in. The data collector then sends update notifications to the data collectors for which it has connections. Each data collector that receives the update sends the update to the member servers in its own zone.

**B.** When a change is made on a member server, the member server sends the updated information to the data collector for the zone it is in. The data collector then sends information back to the member server stating the location of the other data collectors that it knows about. The member server then updates each data collector directly.

**C.** When a change is made on a member server, the member server sends a request to the data collector for the zone it is in, asking for the location of the other zone collectors. The data collector then sends information back to the member server stating the location of the other data collectors that it knows about. The member server then updates each data collector directly.

**D.** When a change is made on a member server, the member server sends the updated information to the data collector for the zone it is in. The data collector then sends a request to the data collectors for which it has connections, asking for the location of the member servers of those zones. The data collector then sends the update directly to those member servers.

**20.** Which of the following is *not* a feature of IMA?

**A.** Centralized logging of ICA Client downloads

**B.** Centralized license management and pooling

**C.** Discovery of published applications from ICA Clients without UDP broadcasts

**D.** Centralized configuration storage for all Citrix servers through a data store

# Answers to Review Questions

1. E. The ICA protocol is created at the Presentation layer on the sending system and is translated by the receiving computer at the same layer.

2. A, B. When ICA is used on a TCP/IP network, the Frame Head and Frame Trail headers are added to the packet. This is because TCP is not a frame-based protocol. Since TCP is a streaming protocol, the framing is added to check the reassembly of the data within the packet.

3. C. The client's network card cannot be accessed for use from within a session on the server. The rest of the options are available for use through redirection. The clipboard can be used to share information between applications running on the local workstation and those that are running within a server session. Drive partitions and CD-ROMs may be remapped for use by the session. Serial port data can be captured and redirected for use within the session also.

4. A, B, C, D, E. All of the transport protocols used in popular networks can encapsulate the ICA Packet and transfer it to its destination.

5. D. The local host cache allows a server to resolve a client's query for access to a published application, even if the data store is unavailable.

6. B, C. Local text echo displays information on the user's display screen before the server returns the screen updates, and mouse click feedback turns the pointer into an hourglass when a user clicks an item on the screen.

7. C. Since two of the connections are made through TCP/IP, only one license is used for those two servers. However, since the user is connecting using a legacy client, the other two connections consume one license each because they are connecting through other protocols.

8. A, B, C, D. All of the above are possible components of an ICA Packet. Depending on the type of communication you are using, you can see any of these parts.

9. A. The ICA Packet is built at the Presentation layer of the OSI model. This means that the protocol can be encapsulated within any of the transport protocols that are in existence in today's network environments. As the ICA Packet is built, it passes through a series of drivers before it is encapsulated into the transport protocol.

10. C. MetaFrame server farms now have two modes: native and mixed. In mixed mode, MetaFrame 1.8 servers can exist in the same server farm as MetaFrame XP servers.

11. B. The Command header is the only required ICA command byte. This is the beginning of the base ICA protocol packet.

12. B. From the client's Program Neighborhood, you can configure the two SpeedScreen tools (local text echo and mouse click feedback). You can apply the options to the entire application set or to individual programs.

13. A. The low setting causes any waveform data passed to the client to be compressed to a maximum of 16Kbps before transmission. The CPU requirements and benefits are about the same as that of the medium setting, but the lower data rate allows for a low-bandwidth connection.

14. D. The high setting allows the waveform data to be played on the client device in its native data rate. The high data rate requires about 1.3Mbps of bandwidth to play without disruption.

15. C. Independent Management Architecture (IMA) is a completely new architectural model that replaces many of the key components of MetaFrame 1.8. It is also a protocol for server-to-server communications within the server farm.

16. D. Each server within the server farm has a local host cache. The local host cache is actually a Microsoft Access database that holds a subset of the information contained in the data store.

17. A, B, D. Events that will trigger a data collector election are a member server losing contact with the data collector, the data collector going offline, a server being brought online within the server farm, invoking the `querydc -e` command, or the zone configuration changing. Bringing down a member server that is not a data collector will have no effect on election criteria.

18. C. A single zone can support up to 256 member servers.

19. A. IMA reduces network traffic by taking advantage of the data collector model to distribute information quickly and efficiently. When a change is made on a member server, the member server sends the updated information to the data collector for the zone it is in. The data collector then sends update notifications to the data collectors for which it has connections. Each data collector that receives the update sends the update to the member servers in its own zone.

20. A. Of all of the options stated, the only function that is not a feature of IMA is the logging of ICA Client downloads to client devices.

Chapter 3

# Planning the Installation of MetaFrame XP

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **2. MetaFrame Installation process**

- 2a. Identify the Software and Hardware requirements for MetaFrame XP
- 2b. Perform Server Planning and Sizing Issues

Before you deploy any product, you should put it through an extensive planning process. As many administrators have found, simply installing an application onto a server and turning it loose for users is not a viable option. Every product has its nuances, and MetaFrame XP is no exception. Throughout this chapter, we will look at the criteria needed to install MetaFrame XP and the options available to the administrator. Simultaneously, we will create a checklist for our installation. It will include all of the design issues we are reviewing in this chapter as well as the additional items we will need to complete the installation. When you are comfortable with the larger view of the installation, we will dive in for a closer look in the next chapter and examine the installation steps.

### The Checklist

Throughout this chapter, we will take a look at the items that you should enter on an installation *checklist*. This checklist will include everything from license numbers to the entries we will make in the Setup Wizard. You should define three areas on the checklist: Preinstallation, Installation, and Post-installation. Then keep the checklist with you as you perform the installation. After completing this chapter, you should have all of the information necessary to perform an effortless install of MetaFrame XP.

## Minimum Requirements

As with any software written, there are *minimum requirements* that must be met on the host computer. As computer systems get faster and the resources become more powerful, software architects continue to take advantage of that power. MetaFrame XP is no exception. Hardware that was state of the art four years ago may not support the advanced features built into this product. Most of the requirements are due to the base operating system and not MetaFrame itself.

## Hardware Requirements

MetaFrame can be installed on any of the following operating systems: Windows NT Server 4.0, Terminal Server Edition, Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server. Each operating system has minimum requirements set forth by Microsoft. Table 3.1 describes the minimums.

**TABLE 3.1** Microsoft Minimum Operating System Requirements

| Platform | Processor | Memory | Free Drive Space |
|---|---|---|---|
| Windows NT Server 4.0, Terminal Server Edition | Pentium or better | 32MB | 128MB |
| Windows 2000 Server and Advanced Server | Pentium 133 or better | 256MB | 2GB drive w/1GB free |
| Windows 2000 Datacenter Server | 8-way Pentium Xeon | 256MB | 2GB drive w/1GB free |

In addition to the operating system requirements, MetaFrame XP has its own requirements that must be met before the operating system is loaded onto the server. Remember though, just like the Microsoft minimum requirements, these are just that, minimums. If you wish to do much more with your server, you will need more resources than those listed here.

Following are the minimum requirements for MetaFrame XP:

- 75MB of free disk space for the MetaFrame system files and Citrix documentation.
- 200MB of hard drive space for the client connection files.
- 10MB for the SNMP agent that is required if you are running a third-party network management tool like HP OpenView or Tivoli NetView.
- 20MB for hard drive space for the NFuse services.

- 64MB of RAM for IMA and other services.
- 1.7MB of RAM for each idle session on the server. The default setting for idle sessions is two.

**Checklist**

**Preinstallation:** Although this probably goes without saying, you should have all of your hardware ready for the installation. Still, in the planning stage, you should enter this line item on your checklist just to make sure you don't forget anything!

## Software Requirements

Because MetaFrame XP is actually an add-on product to Microsoft's Terminal Services, you must meet some software-specific requirements before you start the installation. The following list details the preinstallation requirements identified by Citrix Systems:

- Prior to installing MetaFrame XP, you will need to have either Windows NT Server 4.0, Terminal Server Edition or one of the Windows 2000 Server family members with Terminal Services installed. In addition, if you use Windows 2000, you should have Terminal Services Licensing installed on a domain controller in your environment. Of course, Terminal Services should be configured to run in Application Server mode. Otherwise, the server will allow only two connections for administrative use, and only members of the Domain Admins group will be allowed to log on to these sessions.
- Because TCP/IP is installed by default during the Windows 2000 Server setup, you will not have to install it, but if you want to use MetaFrame XP across any other protocols, you will need to install those protocols before installing MetaFrame XP. You can install additional protocol support later if necessary, but having all the protocols you need to use installed as you set up MetaFrame allows all of the listener ports to be created at once and all of the necessary clients to connect.
- Simple Network Management Protocol (SNMP) is now supported with MetaFrame. You can monitor each of your servers by using an SNMP management console such as HP OpenView or Tivoli NetView. Prior to installing MetaFrame XP and the MetaFrame XP agent, you need to install the SNMP service on your Windows-based server.

- To use NFuse on the same server that acts as the web server for the clients connecting with web technologies, you will need to install IIS 4.0 or later along with the *Microsoft Java Virtual Machine (JVM)*. Because IIS 5.0 is installed by default during a Windows 2000 Server installation, you need to install only the JVM on these machines.
- If you need to use the NetWare client for user access to Novell NetWare-based computers, you should install version 4.7 (with updates) or 4.8 or later prior to the MetaFrame installation.
- If you're using Oracle or Microsoft SQL Server as the database for the data store, you must have the database server built and the database created prior to installing the first MetaFrame XP server.
- All of the MetaFrame XP servers that directly access the data store database will need the appropriate ODBC driver installed.

Once you are sure that you have met all of the requirements, you are ready to start planning the rest of the installation. However, before getting too deep into those topics, we need to take a brief look at the main management tool used in MetaFrame XP, the Citrix Management Console.

## Installing the Citrix Management Console

The management tool that performs a majority of the administrative functions on any MetaFrame XP server and controls the servers in a server farm is the *Citrix Management Console (CMC)*. The Citrix Management Console is installed by default on every MetaFrame XP server in the server farm. Most administrators will agree that they do not want to go to the server whenever they want to perform a task. They want to have the ability to perform tasks from their local system, and they do not want a server with MetaFrame installed on it as their local system. To alleviate these problems, any workstation that meets the following requirements may have the Citrix Management Console installed on it:

- The workstation must have Windows NT 4.0 or Windows 2000 as the operating system.
- The *Sun Java Runtime Environment (JRE)* version 1.3 must be installed on the workstation.
- The workstation must have 25MB of hard disk space to accommodate JRE and the Citrix Management Console.

- The workstation must have a minimum of 64MB of RAM (in addition to system requirements) to run the Citrix Management Console.
- The workstation must have a Pentium-class processor or better.

**Checklist**

**Post-installation:** One of the line items on your checklist should be which computers in your organization will host the Citrix Management Console. Take time to consider where the administration is performed and which users will perform it.

The Citrix Management Console is a Java-based application that requires that the Sun Java Runtime Environment version 1.3 be installed. During installation, if this version of JRE is not installed, setup will install the correct version. Any previous versions of JRE are not affected by this installation.

After you install the Citrix Management Console on a workstation, the same functionality and features that are available on a server running the console are available to the administrator at their local workstation. For most situations, administration of the server farm is transparent to the administrator. Again, with the Citrix tools, the administrator is allowed to enjoy the best of both worlds: centralized control of resources with a decentralized management concept.

More information on the Citrix Management Console, including the steps detailing the installation of the console on an administrator's workstation, can be found in Chapter 5, "Administration and the Citrix Management Console." There you will discover the true power of this management tool. For now, let's continue focusing on planning and deployment issues.

# Planning the Deployment

For this section, we are going to assume that you have already tested and purchased your hardware. Our first concern will be planning the MetaFrame XP environment. Expanding into the application and load-testing process is beyond the scope of this book and the level of expertise required for the exam. When you find yourself ready to tackle the application and load-testing process, you can refer to the Citrix website at `http://www.citrix.com` and review the many white papers and articles that Citrix has published on the subject. For now, let's jump into the planning issues surrounding our installation.

## The Necessities

When installing any software, you should have certain items handy. Starting with the obvious, you need the software itself. Though this may seem almost too obvious, you may not have the software media available to you, as it may have been placed on a server in your network. Be sure you know where to access the software before you get started. The initial steps of the installation depend upon how you access the setup files. If you are installing from the compact disc, most computer systems will execute the `autorun` command on the CD. In MetaFrame XP's case, the CD will execute the `autorun` sequence and will display the splash screen that allows you to start the installation. If you are running the installation from the network, you will need to know the server and directory where the installation files reside. You will also need to have the correct permissions for the shared directory so that you are able to access the files.

### Checklist

**Preinstallation:** If you are installing from a CD, make note to gather the setup CD as well as any supporting CDs. MetaFrame XP ships with the main installation CD and a CD that holds the client images.

If you are installing from a network share point, make note of the location of the files. Determine whether you have the appropriate level of access to the installation files so that you are able to perform the installation from that server.

You should purchase all of the appropriate licenses prior to the install. While you can enter the licenses after the install is complete, entering them during the install guarantees that everything has been completed during the installation process. Citrix has separate licenses for different options, such as connections and product licensing. The following list describes the licenses available:

**Product license** The *product license* enables MetaFrame XP server. Until this license type is added, the MetaFrame server will not accept connections.

**Connection license** A *connection license* allows clients to connect to a MetaFrame server and start a session. These licenses are pooled in a server farm so that any server can use an available license.

**Connection migration license** A *connection migration license* converts a MetaFrame 1.8 user license to a MetaFrame XP connection license.

**Connection upgrade license pack** A *connection upgrade license pack* allows the upgrade of connection licenses from one version of MetaFrame XP to another: MetaFrame XPs to MetaFrame XPa to MetaFrame XPe.

Each of the license types has an associated product code that you must enter before the license will allow connections on the server. MetaFrame XP will choose a product code for entry if you add a known license type. If you have another product code, you can override the suggested option. And of course, if you enter an invalid code, you will receive an error, and the license will not be activated until you enter a proper code.

**Checklist**

**Preinstallation:** Collect all of the license numbers and associated product codes for all of the license types you need to enter.

If you plan to use Microsoft SQL Server or Oracle as the database software that will host your data store database, you will need to install the software on a separate server prior to the installation of MetaFrame XP. If you're using Microsoft SQL Server 7, you must apply the SQL Service Pack 2 or greater. If you're using either Microsoft SQL Server 7 with SQL SP2 or Microsoft SQL 2000 Server, you can create the database on only one server. If you're using Oracle, you must use version 7.3.4, 8.0.6, or 8i. Due to performance issues, the database server should never be installed on the MetaFrame XP server. The resource consumption of these products does not allow you to take advantage of all of the memory, processor, and other subsystems of the server for ICA sessions.

Each MetaFrame XP server that connects directly with the database must have the appropriate ODBC client loaded. A MetaFrame XP server can either connect directly with the database or access the database indirectly by connecting to another MetaFrame XP server. Therefore, you must determine which MetaFrame XP servers will need the ODBC client configured on them. For those servers that will directly connect to the database, you will need either the 8.01.55.00 or later version of the Oracle ODBC driver or the 3.70.08.20 or later SQL ODBC driver (you should also be able to use 7.3.43 with Oracle 7 or 8.0.6 with Oracle 8).

Either of these databases will allow the database to be replicated to another server. When you're planning to replicate the database, you should install MetaFrame XP before you configure the replication. This configuration can be especially useful when you have servers on subnets that are separated by WAN links. Those servers will be able to access the replica of the database locally and will not utilize the WAN link when accessing the configuration information. Any farm maintenance performed should take place on the master database. This will ensure that there are no problems resulting from synchronization of the databases.

Of course, if you decide to use the default database, Microsoft Access, your planning is reduced considerably. If you choose to use this database, it is automatically installed on the first MetaFrame XP server you install, and the client is automatically installed on every Windows 2000 Server as the operating system is installed.

**Checklist**

**Preinstallation:** Install and configure the database server prior to the installation of MetaFrame XP if you are planning to use SQL Server or Oracle. Also, make sure that the appropriate client licenses have been purchased so that each of your MetaFrame servers can access the database legally!

No matter which database type you decide to use, you should always back up the database after the install is complete. This will safeguard you in case the database becomes corrupted. You should also back up the database any time changes are made to the server farm configuration. It's always better to be safe than sorry. Now let's take a look at some other software considerations.

## Software Considerations

We need to consider a couple of topics prior to the install. Software that users run in their sessions has an impact on the server. Some applications perform better than others in a multiuser environment. It's usually best to examine the software issues before purchasing the hardware and size the servers accordingly.

Windows NT 4.0 and Windows 2000 are *32-bit operating systems* that take advantage of the ability to separate applications into their own memory areas. This safeguards the operating system when an application fails. Since the operating system does not occupy the same memory area, the application does not affect the processing of the operating system. Also, other applications are not usually affected by another application failing.

The prime candidates written to take advantage of this functionality in a MetaFrame environment are the 32-bit applications. There are still many programs in business environments that are legacy applications written to the *16-bit operating system* specifications. These applications are not able to function in the native 32-bit operating system environment. A special program known as *WOW (Win16 On Win32)* monitors the execution of the 16-bit applications, translates system function calls from the 16-bit command to a native 32-bit command, and then redirects the results to the application. Due to the additional processing required and the inherent inefficiency of the 16-bit applications, these applications increase RAM requirements for a user session by 25 percent over a 32-bit application. Processor utilization can increase by nearly 20 percent for each 16-bit application. If there is a business need for executing a 16-bit application in a MetaFrame environment, you should consider these issues.

**Checklist**

**Post-installation:** You should note all of the applications that are to be installed on the server. This allows you to have a record of some of the post-installation tasks to be performed.

## Hardware Sizing Considerations

Prior to actually installing MetaFrame XP, an administrator needs to consider certain factors. Because MetaFrame is a multiuser environment, the resources on the server need to be able to meet the demands of running additional desktop and application sessions. To determine the resource requirements of user sessions and application usage, we will perform a function known as baselining.

## Baselining

*Baselining* is the process of testing resources on a server to determine the limits of the server. The following is a list of the factors that affect hardware requirements beyond those of a simple installation:

**The number of users or clients connecting to the MetaFrame XP server farm** Power users are those users who use two or three applications simultaneously, cut and paste between local and remote applications, and consume more resources than typical users who run only one application at a time. A power user usually equals two typical users in terms of processor utilization and RAM requirements.

**The number of processors on the MetaFrame XP server** A MetaFrame XP server scales linearly (utilizes multiple resources equally) when going from single to dual processors, subject to performance constraints from other system resources.

MetaFrame XP does not scale linearly from dual to quad processors.

**Types of applications** The applications on the server can affect the hardware requirements. You can run System Monitor, which is included with Windows 2000 Server, to help determine the resources required to run an application.

**User location** How the user connects to the server, either by LAN, WAN, async, or through the Internet, can affect hardware requirements.

Taking these factors into consideration, the administrator should not estimate the percentage of each resource a user will consume. Educated guesses could come back to haunt an administrator who did not foresee conflicts between applications—or worse yet, did not think an application would consume the level of resources that it actually does. The only true test of an application's behavior is to test it. The administrator should actually test the applications and examine the stress on the server while users are running sessions. This trial run and stress testing of servers is known as creating a baseline.

To determine your requirements, establish a baseline with at least five users. When developing the baseline, you should take into consideration several object counters provided in *Performance Monitor* (Windows NT 4.0) or *System Monitor* (Windows 2000). These counters give you an accurate reading as to the resources used during server sessions. You should not run Performance or System Monitor on the server itself, however. Doing so will only skew the data by adding the additional processing of the monitor itself. See Table 3.2 for a list of counters that should be monitored.

**TABLE 3.2** Performance/System Monitor Counters for Creating a Baseline

| Object | Counter | Purpose |
|---|---|---|
| Processor | %Processor Time | Determines the percent of time the processor is processing user requests. |
| Memory | Pages per Second | Tracks the number of hard page faults that occur when the system requests data that is not in memory. |
| Network | %Network Utilization | Indicates the amount of data transferred across the network from the server. |
| Physical drive | Disk Transfers per Second | Indicates the amount of data transferred to and from the hard drive. |

When you use Windows NT 4.0, you can add the administrative tools, including Performance Monitor, to any Windows NT 4.0 Workstation or Windows 9*x* workstation. When the administrative tools are installed on these platforms, you can select which server you want to monitor and add the appropriate counters.

**EXERCISE 3.1**

### Adding the Administrative Tools to Windows NT 4.0 Workstation

The following steps add the administrative tools to a Windows NT 4.0 Workstation so that an administrator can monitor a MetaFrame server across the network:

1. Locate the Windows NT Server 4.0 CD and load it into the Windows NT 4.0 Workstation.
2. Open a command prompt and change directories to the CD drive: `\Clients\Srvtools\Winnt`.
3. Enter **setup** at the command prompt.
4. Close the command-prompt window.

Windows 2000's System Monitor can be added to any Windows 2000 system but cannot be added to any other operating system platform. System Monitor is included as a snap-in available for use with the Microsoft Management Console (MMC). You load the administrative snap-ins by accessing a Windows Installer Package on the Windows 2000 Server CD, *`adminpak.msi`*. This file resides in the `I386` directory. After installing the administrative tools, you can access System Monitor by going to Start ➤ Administrative Tools ➤ Performance. When the Performance MMC loads, select System Monitor from the Containers pane. By right-clicking the System Monitor screen, you can choose to add counters to the interface and begin monitoring.

**EXERCISE 3.2**

### Adding the Administrative Tools to Windows 2000 Professional

The following steps add the Administrative tools to Windows 2000 Professional so that an administrator can monitor a MetaFrame server across the network:

1. Locate the Windows 2000 Server or Advanced Server CD and load it into the Windows 2000 Professional computer.
2. Open Windows Explorer.
3. Navigate to the `I386` directory.
4. Locate and double-click `adminpak.msi`.
5. At the Administration Tools Setup splash screen, click Next.
6. After the files have been copied to the hard drive, click Finish.

Most administrators will want to create a log over the period of time the users are testing the server. To perform this function, choose *Performance Logs and Alerts* from the Containers pane of the Performance snap-in within Windows 2000, or open Performance Monitor within Windows NT. Performance logs are especially useful when the administrator wants to create reports of the activity generated during the baseline tests.

Once you've configured the performance log, the baseline test is ready to proceed. You can perform various tests to capture data. Some administrators prefer to test one user as they access programs on the MetaFrame servers, while others prefer to have a number of users perform their daily tasks. The typical guideline is to use five test subjects. As these five users access the programs that they normally utilize during their work session, the log tracks the resource usage on the server.

NOTE Application usage scales linearly on MetaFrame. Therefore, as you test the system and discover the resource usage for the applications monitored, you will have data to use to calculate the total number of users who will be able to use the system.

## Other Hardware Considerations

When preparing to baseline the system or working with vendors and obtaining quotes, you should consider certain hardware issues. These considerations include the hardware that will be included in the server configuration. After all, not all hardware is created equal. The following topics explain the preferred hardware for a MetaFrame installation:

**Bus architecture** PCI and EISA bus types should be used. They offer higher data transfer rates than ISA bus architecture.

**Memory** RAM requirements for MetaFrame XP are 16MB plus 4MB for each typical user and 8MB for each power user. In most cases, a RAM upgrade will be more beneficial than a processor upgrade.

**Hard disks** Hard disk performance is very important when planning a MetaFrame XP installation. Integrated Device Electronics (IDE) and Enhanced Small Device Interface (ESDI) adapters cannot compete with the Small Computer System Interface (SCSI) adapters on the market now. The best-performing SCSI adapters are Fast Narrow SCSI (SCSI 2), Fast Wide SCSI, Wide Ultra SCSI, and Wide Ultra 2 SCSI.

SCSI disks configured in a Redundant Array of Independent Disks (RAID) provide the best disk performance. RAID controllers automatically span data across multiple drives, increasing disk performance and improving data reliability.

**Network interface** Even though the ICA protocol is quite thin, the MetaFrame XP server handles all requests from all clients. For this reason, a high-performance network interface card (NIC) is preferred. If a multiport async adapter is being used for serial connections, be sure to use an intelligent (microprocessor-based) adapter to reduce interrupt overhead and increase throughput.

## Client and Server Communication

There are several issues to take into consideration when you start examining the communication between client and server in a MetaFrame environment. Since there are different client types, and since we can throw MetaFrame 1.8 into the mix, you need to understand the communication that occurs. The following are issues when planning a deployment of MetaFrame XP, ICA Clients, and NFuse services:

**ICA browsing** *ICA browsing* should be configured within a mixed-mode server farm so that ICA Clients can communicate with the ICA Master Browser when locating MetaFrame XP servers and published applications.

**Firewalls** Network *firewalls* should allow communication among ICA Clients, MetaFrame XP servers, and NFuse.

**Interoperability** Your server farm should operate with MetaFrame 1.8. This *interoperability* allows you to have a smooth upgrade path when moving from MetaFrame 1.8 to MetaFrame XP.

When planning the client installation, you must take care when deciding upon the client communication parameters. What you choose during the installation can affect deployment issues related to ICA browsing. The communication protocol used by the client to locate servers dictates which protocol is loaded on the server. Certain components such as NFuse require the user to connect via TCP/IP. Different functions require that protocol ports be available.

Citrix recommends using TCP/IP+HTTP as the network protocol for the ICA Client. Using this protocol allows the client to communicate with the XML service for browsing. Of course, you should enter the name of the server in the address list of the Program Neighborhood settings so that the client can access the server, but if the field is empty, the client will try another method to resolve the server name. The client will automatically attempt a DNS query for the server name “ICA.” If the DNS server has a host record mapping ICA to a MetaFrame XP server, the field is automatically populated with the server’s address. If the DNS query fails, the client will attempt a WINS query for the same information.

### Checklist

**Preinstallation:** Add the required entries within DNS or WINS with the hostname ICA mapping to one or more of your MetaFrame XP servers.

**Post-installation:** Configure the client with the protocol that will be used to communicate with the server.

When TCP/IP+HTTP is selected and addresses are defined in the address list field, the ICA Client communicates with the Citrix XML service for ICA browsing. The XML service receives HTTP requests on port 80 of the MetaFrame server and communicates with the client through port 80. TCP/IP+HTTP has several advantages. Since XML data is encapsulated in HTTP packets, these packets use port 80, which most firewalls already have open. Since all of the packets use TCP for the transport mechanism, not UDP broadcasts, the data is routable between subnets. Not only does this reduce the amount of data that clutters your network, but clients are able to locate servers on other subnets without having to rely on the ICA browsing architecture.

In addition to network connections, MetaFrame XP supports async serial connections. Async connections allow a user to connect directly with a MetaFrame XP server without the need to install RAS or worry about the overhead RAS places on your server. For ICA async connections, Citrix recommends using high-speed serial port hardware or intelligent multiport adapters on the server. If you decide to use a multiport adapter, install it before you install MetaFrame XP. You can install modems that will be connected to the adapter before or during the MetaFrame XP install. Telephony API (TAPI)-capable modems are detected during the setup process, and setup will use Windows' installation and configuration utilities to manage the modem. If there are no modems installed on the server, MetaFrame XP setup will give you the opportunity to install them.

### Checklist

**Preinstallation:** If you're using an intelligent multiport modem adapter to allow users to directly dial in to the server, install the hardware prior to the MetaFrame XP install.

## ICA Browsing

When you're using an ICA Client, the communication initiated by the client is in the form of either ICA browsing or an ICA session. During an ICA session, the client communicates directly with the server that is executing the session on behalf of the client. ICA browsing is the act of discovering a MetaFrame server or published application. Browsing occurs in the following instances:

- When a user launches a published application, the ICA Client requests an application on the MetaFrame XP server. If the Citrix Load Manager is installed, the client receives the address of the server with the lightest load.
- When a user selects the Application Set list in the Find New Application Set Wizard in Program Neighborhood.
- When creating a new connection with the Add New ICA Connection Wizard, the user displays the Server or Published Applications list.

If you choose to operate the farm in mixed mode so that you will have the ability to use your MetaFrame 1.8 servers and migrate them to the new MetaFrame XP farm, the IMA service takes over the ICA Browser function. Your MetaFrame XP server will become the master ICA Browser and accept browsing requests from ICA Clients. This also facilitates the sharing of licenses and load balancing between MetaFrame 1.8 and MetaFrame XP servers.

### Checklist

**Installation:** During installation of the first MetaFrame XP server, you are asked to supply the server farm name. If you will need to interoperate with the MetaFrame 1.8 server farm, you will have to supply an identical name to the existing farm. You should already have this information on your checklist. If not, add it now.

## Firewall Configuration

NFuse makes it very easy for an administrator to allow clients to start a session on a MetaFrame XP server by simply accessing a web page. As clients connect to the website and are redirected to a MetaFrame server that processes their session, they are accessing the network. As we all know, allowing everyone access to the network resources is not a good thing. There are plenty of scurrilous individuals in this world who would like nothing better than to gain access to a network and play havoc with the internal resources. We need to block their access. At the same time, we still need to allow those users who do require access to the network to perform the functions the network was set up for in the first place. Protecting servers and the data they hold is of utmost importance.

We use firewalls to protect our servers and their resources. To allow ICA Clients from outside the physical network to connect to MetaFrame XP servers behind a firewall, you must allow packets to pass on specific communication ports used by ICA Clients and other Citrix components. One of the most important ports to open is 1494. When a client's session is active, all communication between the client and the server is passed on this port. Most firewall configurations do not have this port open for inbound or outbound traffic, so you may need to configure the port on your firewall or request that the router administrator allow data to pass on that port.

There are some other ports that you must take into consideration when planning your deployment. Many of your clients may connect through the Web, either with a direct ICA connection or with NFuse. If a server outside of your firewall needs to access the data store, you may need to punch a hole in the firewall to allow that server to communicate directly with the data store or indirectly by communicating with another MetaFrame XP server. Here is a list of the default TCP port settings that MetaFrame XP uses to communicate:

**80** Used by ICA Clients using TCP/IP+HTTP to communicate with MetaFrame XP servers. This port must be open for inbound traffic. Use the command `ctxxmlss /rnn` to change the port the client uses, where *nn* is the port number you would like to use.

**139, 1433, 443** Used by MetaFrame XP to communicate with Oracle or SQL. If Oracle or SQL is used as the data store, these ports must be open for inter-server communication.

**443** Used by *Secure Sockets Layer (SSL)* Relay. SSL Relay is used to secure communications between an NFuse-enabled web server and the MetaFrame XP server farm. You can change this via the SSL Relay Configuration Utility.

**1494** Used by clients using TCP to connect and communicate with the MetaFrame XP server farm. This port must be open for inbound traffic. Use the command `icaport: xxxx` to change the port number, where *xxxx* is the number of the new port.

**2512** Used for server-to-server communication in a MetaFrame XP server farm. You can make data store port number modifications in the Registry of the server that accesses the data store: `HKeyLocalMachine\Software\Citrix\IMA\Runtime\ImaPort`. Servers using an indirect connection to the data store through the server with the direct connection record the port number in their Registry at `HKeyLocalMachine\Software\Citrix\IMA\PsServerPort`.

**2513** Used by the Citrix Management Console to access MetaFrame XP servers in a server farm. This port is not configurable.

In a mixed-mode environment, the following UDP port needs to be opened:

**1604** Used by ICA Clients to communicate with the ICA Browser service. Used only if MetaFrame XP is set to mixed mode or the broadcast options are enabled in the MetaFrame Settings tab of the server in the server farm. Not used if the ICA Client is connecting with the TCP/IP+HTTP protocol.

**Checklist**

**Preinstallation:** Configure the firewall to allow the appropriate protocols to pass prior to the installation of MetaFrame.

**Post-installation:** After the server is configured, test connectivity from outside the firewall to ensure that proper communication is available.

## Interoperability

Most new installations of MetaFrame XP will be tied into existing installations of MetaFrame 1.8. During the migration from MetaFrame 1.8 to MetaFrame XP, administrators need the two systems to work together, whether for license sharing or published-application load balancing. Setting the MetaFrame XP server farm in mixed mode allows the two versions to coexist. Mixed mode provides the backward compatibility necessary for the server farms to work together. As you install the first server in the farm, you can choose to operate the farm in mixed mode, or you can change the server farm to mixed mode at a later time by using the Citrix Management Console.

NOTE

For more information about using Citrix Management Console and changing the server farm to mixed mode or native mode, see Chapter 5, "Administration and the Citrix Management Console."

Because mixed mode is designed for migrations, it is not recommended as a permanent solution. After all servers are migrated to MetaFrame XP, the farm should be set to operate in native mode using the Citrix Management Console. If switched from mixed mode to native mode, the farms become completely separate entities. You will no longer have license pooling or load balancing available between them. Also, the MetaFrame XP server farm will no longer perform the ICA browsing functions for the MetaFrame 1.8 server farm. These are some other issues involved with mixed- and native-mode server farms:

- The names given to MetaFrame 1.8 and MetaFrame XP server farms must be identical, including alphabetic case.
- Connection license counts are pooled between the MetaFrame XP and MetaFrame 1.8 servers in the IP subnet and are available to both MetaFrame XP and MetaFrame 1.8 servers.
    - MetaFrame 1.8 connection migration license counts cannot be pooled across MetaFrame 1.8 subnets in mixed mode because all MetaFrame 1.8 license gateways are disabled in mixed mode. MetaFrame 1.8 connection migration licenses stay on their local subnets.
    - MetaFrame 1.8 migration licenses are not displayed in the CMC and cannot be activated using the CMC.
- Applications are published and managed on MetaFrame XP servers using the Citrix Management Console. Applications are published and managed on MetaFrame 1.8 by using Published Applications Manager.
- If you're publishing an application in mixed mode, the application must be published in the MetaFrame 1.8 server farm before it is published in the MetaFrame XP server farm.
- MetaFrame XP uses IMA to communicate with servers. When MetaFrame XP is running in mixed mode with MetaFrame 1.8 servers, the master ICA browser architecture is used for communication between servers. This makes license sharing and load balancing possible between servers in the farm.
- A MetaFrame XP server will become the master ICA browser in the farm in mixed mode. It can take up to 20 minutes for this to take place. During this time, published applications may not be available.
- MetaFrame 1.8 servers that have not had SP2 installed must have the Program Neighborhood service stopped and restarted after the MetaFrame XP server farm has been switched to mixed mode.

- All ICA Clients can access both MetaFrame 1.8 and MetaFrame XP servers.
- Only the ICA features that are supported on both the ICA Client and the version of MetaFrame server being accessed are available.

**Checklist**

**Installation:** Decide on the server farm name early in the process so that during this phase you will have it recorded and will not be scrambling to figure out what you want to name it.

## Zones

Server farms can grow to the point where they have numerous servers. They can also span network links, including slow wide area network links. To reduce the amount of traffic generated by these servers and to control the amount of data that passes across your WAN links, MetaFrame XP allows you to create *zones* within your server farms. Analogous to a site within Windows 2000, a zone defines a subnet or collection of subnets that contains MetaFrame XP servers that communicate directly with one another when distributing configuration data and ICA browsing information.

If you have one large, well-connected network, you may be able to configure all of your servers in one zone, thus easing your administrative duties. However, if the traffic on your network is increasing to unacceptable limits, you may need to divide the server farm into zones. When determining how to divide the server farm and where to place the servers, you should take certain criteria into consideration. You should determine the logon and logoff frequency for users, and you should group the MetaFrame XP servers that process their sessions within the same zone. This is critical when trying to provide them with a positive experience. In addition, you should consider the servers that work together in a load-balanced environment and the traffic that is generated by the load-management tools when placing servers. When you place servers in the same zone, configuration information and load-management tools receive immediate updates. If you place them in separate zones, you are at the mercy of the data collectors to send the data between zones.

After deciding in which zones to place the servers, you will need to configure a MetaFrame XP server to be the zone's *data collector*. A data collector communicates with all of the servers in the farm and gathers the configuration information from them. This information includes the published applications and load settings if load balancing is configured. By configuring one server as the dedicated data collector, you can control which server communicates with data collectors from other farms and passes configuration information to and from them.

**Checklist**

**Preinstallation:** Decide where the servers will be located and whether you should configure a zone to segregate the configuration information that is passed between the servers.

## Other Setup Options and Issues

We have now touched on the major issues and the new options available when installing MetaFrame XP. Now we are going to look over the other options available when installing MetaFrame XP. Some of these will look familiar to those of you who have installed previous versions of MetaFrame, but we need to look at them now and make decisions according to our current environment.

### Citrix XML Service

As you step through the Setup Wizard, you are asked to provide information concerning the XML service. The XML service was introduced with MetaFrame 1.8 Feature Release 1 and is installed by default with MetaFrame XP. It is essential for efficient client-to-server and server-to-server communications. You will need to supply the port number that the XML service is going to use and indicate whether that port number is shared with the web server.

You are presented with two options when choosing the XML service port. The first option, the default, is to share the port with Internet Information Services (IIS). If you leave this as the default configuration, an ISAPI extension is added into the IIS server so that both the web server and the XML service can use port 80 as the default communication port. This is not the recommended design, however.

**Checklist**

**Installation:** If you change the port number that the XML service uses, make note of the port number here and in the Post-installation section so that all client configuration uses the same port.

The second option separates IIS ands NFuse. Citrix recommends that the web server and NFuse be installed on a separate server from the MetaFrame XP server for performance reasons. Any additional services running on a server diminish the efficiency of a MetaFrame server. By separating the services, you allow the MetaFrame server to handle more user sessions. This configuration is not without its drawbacks, however. You must use a separate port for XML support in this case. You must also change the port configuration for each of the clients if you want them to use the XML service to locate servers and published applications. After the port has been changed, all of the MetaFrame XP servers will need to use the same port for XML support. If the servers do not agree on the port, they will be unable to see each other to pass configuration information.

NOTE

For more information on using the XML service with the client systems, and for the communication protocol options, see Chapter 10, "ICA Client Software."

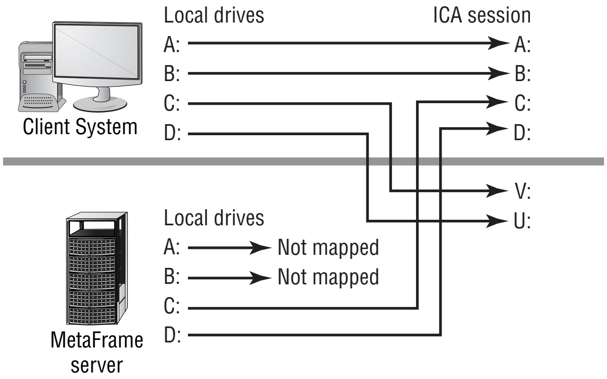
## Drive Mapping

When users start a session, their local drives are available to them through a client-mapping process known as *drive mapping*, which allows them to access the drives to store and retrieve data. With this capability, the applications the client is running in their session can use the data on the server and the client's system. The design decision becomes which drives should have the friendly mapping of C: and D:—the client's own local drives or the server's drives. Most users who have worked in a networked environment have become accustomed to seeing their local drives as C: and D: and the server drives mapped on their computer as higher drive letters. You can retain this look and feel by remapping the server's drives during setup.

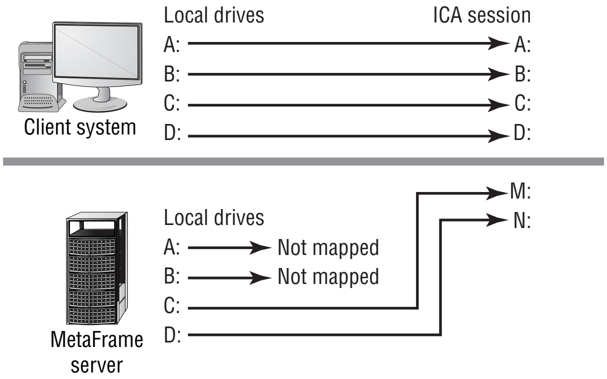
The default setting, however, is to have the server drives mapped as the C: and D: drives. In this configuration, when the user saves data to the C: drive, they are actually saving their information on the hard drive of the server. By default, the user's drives are mapped starting with the C: drive mapped as the V: drive letter, the D: drive mapped with the U: drive letter, and so on up the alphabet. If any of the letters happens to be already mapped to a network drive, then that letter is skipped by MetaFrame, with the session using the next-available drive letter.

During setup, you are prompted as to whether you would like to change the server's drive letters. If the server's drive letters are remapped, C: becomes M:, D: becomes N:, and the letters increase from there, depending on the number of drives you have on the server. Of course, you can select the drive letter you want to start the remapping at; M: was probably chosen to represent MetaFrame. After the drive mapping is complete and the client connects to the Citrix server, the local C: and D: drives will appear as C: and D: within the ICA session.

In the following graphic, the server's drives have not been remapped, causing the client's drives to be mapped starting with V:



If the drives on the server have been remapped during setup, the drive lettering for the client's drives in the session will appear as normal to the user, as shown here:



One word of caution when you plan to remap the drives on the server: If any applications are already loaded on the server, they may become unusable after the drive letters are changed. To use those applications again, you may need to reinstall the applications.

**Checklist**

**Installation:** Are you going to remap the drive letters on the server? If so, make note of it here, along with the drive letter where you want to start the re-lettering, so that you will know what to do when the question arises during setup.

## Shadowing

Session shadowing is an administrator's best friend. Whether used for remote administration or to assist a user in troubleshooting a problem, shadowing has become one of the most widely used and accepted technologies within MetaFrame. With shadowing, you are able to view what is occurring within a client session, and you can take control of the session as though it was your own desktop.

During installation, you can limit or disable shadowing. If legal privacy requirements prohibit shadowing of users' sessions, you can disable shadowing of ICA sessions on all servers in the server farm. You may also want to disable shadowing on servers that host sensitive applications, such as personnel or payroll applications. MetaFrame XP setup provides many options on the Shadowing Setup page for you to limit or disable shadowing.

NOTE

Shadowing restrictions are permanent. If during setup you disable shadowing, or disable certain features, the restrictions cannot be changed at a later time.

There are two main options available during setup to control session shadowing on a MetaFrame XP server. The first option, Allow Shadowing Of ICA Sessions On This Server, enables shadowing support on the server. Three subordinate settings further control how shadowing is configured on the server:

**Prohibit Remote Control Of ICA Sessions** The default settings allow the administrator to input keystrokes and mouse control during shadowing. If this restriction is chosen, administrators can only view the session, not interact with it.

**Prohibit Shadow Connections Without Notification** By default, MetaFrame XP notifies the user when another user attempts to shadow them. Use this setting if you want to deny another user the ability to shadow without notification.

**Prohibit Shadow Connections Without Logging** Shadow attempts, including both successes and failures, can be logged in the Windows event log. You can view these events by using Event Viewer and examining the application log.

The other main option you can choose during setup is Do Not Allow Shadowing Of ICA Sessions On This Server. This option permanently disables shadowing by anyone on all ICA sessions on the server. All of these restrictions, if selected during setup, are permanent and can be changed only by reinstalling MetaFrame XP on the server. Use caution when making changes to the default setting. (If you leave the default, Enable Shadowing, and do not select any of the subordinate settings during installation, you can add them in later without having to reinstall MetaFrame. The only time this has a permanent affect is when you select the subordinates during installation.)

**Checklist**

**Installation:** Indicate the level of shadowing you need within your organization. The decision to use, or restrict the use of, shadowing is irreversible.

This section presented the planning issues that arise when installing MetaFrame XP. From hardware to software requirements and planning ideas, we have looked at what is necessary for the installation and the options that are available to the administrator performing the installation. In the next section, we take a look at some of the options and planning criteria necessary when migrating from MetaFrame 1.8 to MetaFrame XP.

# Migrating from MetaFrame 1.8

Many companies have an earlier version of WinFrame or MetaFrame already installed and functioning. With the additional tools, greater functionality, and more efficient communication of MetaFrame XP, those installations are probably interested in moving to MetaFrame XP. Citrix has tried to make the transition effortless and painless, but there are some issues you should take into consideration.

You should perform certain preinstallation tasks before attempting any type of migration. As with any type of configuration change, you should back up all information on the server on which you are going to work. This ensures that the server can be brought back to life if something goes wrong. Remember the three rules of disaster recovery that you have probably heard many times over: Back up, back up, back up.

You should also familiarize yourself with the license agreement. While it is not the most exciting, interesting, or clearly written document, you are bound by the license agreement once you start the installation. And while we are talking about licenses, you should make note of all of the licenses so that you will know what you need to upgrade as the servers are migrated to MetaFrame XP.

Any of the Citrix family of products, from WinFrame to MetaFrame 1.*x*, is upgradeable to MetaFrame XP. During the migration, all of the servers are able to communicate with one another as long as the MetaFrame XP server farm is kept in mixed mode. Once the server farm is changed to native mode, the two farms become separate entities. In mixed mode, the IMA service in the MetaFrame XP server farm acts as the master ICA browser for the MetaFrame 1.*x* and WinFrame servers. This allows the two farms to work together and allows clients to see the server and published applications in each farm.

Two different upgrade methodologies are possible. The first option is to perform an in-place upgrade from the legacy software to MetaFrame XP. In this instance, the server software is upgraded on the existing hardware and then the license upgrades are applied. This is the easiest upgrade path as the server is already configured for user access and the applications are already installed.

The second option is to perform a fresh install of MetaFrame XP. After installing the software, you should add the license from the previous server to the new server and add the migration licenses to the new server. You should then remove the MetaFrame or WinFrame software from the original server. You will need to reinstall all applications on the new server to make it fully operational for the users.

You should add the migration license packs to the server after the migration is complete to convert the user licenses to connection licenses. Citrix offers special license packs that allow you to upgrade your system easily. The Migration Starter System includes the installation software on CD along with a MetaFrame XP server product license and connection licenses in varying amounts. Migration connection license packs contain the additional licenses you need to upgrade the WinFrame or MetaFrame 1.*x* user licenses to MetaFrame XP connection licenses. They are provided in several user-count sizes. Check with a Citrix representative to determine the number of licenses you need.

Once all of the appropriate license packs and software are in place, you are ready to perform the migration. You should have a plan detailing which servers will be migrated and when. When you are ready to start, you should migrate the first server and create a new server farm. For interoperability with the existing systems, the new server farm should have the same name as the existing server farm.

During the migration of the first server, you will be prompted to provide the licenses. If this is a new server migration, you will need to enter the licenses from the server that is being replaced by this new server. Then you will need to enter the migration license packs to convert all legacy user licenses to connection licenses.

All other servers in the farm can now be migrated according to your migration timeline. The only differences between migrating the first server and the remaining servers are that all other servers will need to be pointed to the data store and you are not required to enter any new license information. The licenses will already exist in the data store. Once all of the servers have been migrated to MetaFrame XP, you can switch the server farm to native mode.

NOTE

For information on how to change the server farm to native mode, see Chapter 5.

Now that we have looked at the installation planning criteria and discussed migration techniques, it is time to perform the installation. Chapter 4, "Installing MetaFrame XP," will guide you through all of the options necessary to perform the installation.

# Summary

We have introduced you to the topics that form the building blocks of our installation. It is mandatory that you know the hardware and software requirements for MetaFrame XP. If you do not know the requirements, your installation may fail—or at the very least, be delayed due to not having the proper equipment and software in place.

Planning also plays a large part in our rollout of MetaFrame XP. You must consider each step and every line item prior to the installation if you want the installation to succeed. It's no longer easy to rebuild computer systems that failed because of a lack of planning. Computers have become the backbone of our companies. Most companies need them running at all times. In this chapter, we have presented the items that you need to take into consideration when installing or upgrading your systems.

In the following chapter, we will be applying the information we gathered here. So let's get ready—we are finally going to install MetaFrame XP on our computer.

# Exam Essentials

**Understand the minimum requirements for the base operating system.** Since MetaFrame XP requires Windows 2000 Server or Windows NT Server 4.0, Terminal Server Edition, the minimum requirements for each of those operating systems become the minimum requirements for MetaFrame XP also.

**Understand the additional requirements for MetaFrame XP.** The installation of MetaFrame XP forces additional requirements on a server. You should know what those requirements are not only for the system files, but also for any additional files, such as the client connection files.

**Understand why baselining is so important.** Without baselining, an administrator will not know the true impact an application or a user running multiple applications will have on a system.

**Understand the impact applications have on MetaFrame XP.** Since 16-bit applications do not process as efficiently as their 32-bit counterparts, if it is necessary to run 16-bit applications, you should test them for their resource usage.

**Understand the hardware considerations when baselining resources.** The bus architecture, memory requirements, hard drive types, and network interface all play an important role in the efficiency of the system.

**Understand the ports required by client-to-server and server-to-server communication when determining what to allow through your firewall.** MetaFrame XP requires that several ports be open on your firewall. Depending upon what communication you need, you should know what protocols are required.

**Understand the need for zones.** Zones allow you to control the communication between servers by segregating the MetaFrame XP servers into their own server communication groups.

**Understand how the XML service works.** The XML service is responsible for notifying clients and servers of the location of servers and the published applications within the farm.

**Understand drive mapping.** Clients can access their own drives from within their MetaFrame session, and the drives can be mapped with the same letters as their local system. Know how to configure drive mapping during setup.

**Understand the implications of making changes to session shadowing during setup.** Once the settings for shadowing are configured during setup, they cannot be changed without reinstalling MetaFrame XP.

**Know how to migrate from a MetaFrame 1.8 server farm to a MetaFrame XP server farm.** Know how to perform the upgrade to MetaFrame XP and which license to apply once the upgrade is complete.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

16-bit operating system

32-bit operating system

`adminpak.msi`

baselining

checklist

Citrix Management Console (CMC)

connection license

connection migration license

connection upgrade license pack

data collector

drive mapping

firewalls

ICA browsing

interoperability

Microsoft Java Virtual Machine (JVM)

minimum requirements

Performance Logs and Alerts

Performance Monitor

product license

Secure Sockets Layer (SSL)

Sun Java Runtime Environment (JRE)

System Monitor

WOW (Win16 On Win32)

zone

# Exercise

To prepare your system for the installation of MetaFrame XP, let's install Windows 2000 Server at this point and include Terminal Services.

## EXERCISE 3.3

### Installing Windows 2000 Server and Terminal Services

1. Load the Windows 2000 Server CD into the computer system and boot from the CD-ROM drive.
2. At the Setup Notification screen, press Enter.
3. At the Welcome To Setup splash screen, press Enter.
4. At the Windows 2000 License Agreement screen, read the complete agreement and press F8.
5. If you are installing on an existing partition, choose the partition you wish to use and press Enter. Proceed to step 9.
6. If you are installing onto a drive that does not have any partitions created, press the C key.
7. Enter the amount of space you need for your installation in the Create Partition Of Size In (MB) text box. For this exercise, 2500MB should suffice. After making your entry, press Enter.
8. Select the partition you wish to use and press Enter.
9. Select the Format The Partition Using The NTFS File System option and press Enter.

**EXERCISE 3.3** ***(continued)***

After the drive is formatted, the system will reboot. Make sure there are no floppies in the drive.

10. When the installation program restarts, click the Next button on the Welcome To Windows 2000 Server Setup Wizard splash screen.
11. Click Next on the Regional Settings screen.
12. Enter your name in the Name text box and **Zygort** in the Organization text box of the Personalize Your Software screen. Click Next to continue.
13. On the Your Product Key screen, enter the product code for your version of Windows 2000 Server. Click Next to continue.
14. On the Licensing Modes screen, click the Per Server option and enter **10** in the Number Of Concurrent Connections text box. Click Next to continue.
15. When the Computer Name And Administrator Password screen appears, enter the name of your server (something you will remember for later labs) and enter **citrix** (all lowercase) as the Password and Confirm Password entries. Click Next to continue.
16. The Windows 2000 Components screen appears at this point. Scroll through the options, select Terminal Services, and click the Details button.
17. Verify that only the Enable Terminal Services option is selected, and click OK.
18. Click the Next button on the Windows 2000 Components screen.
19. Verify your Date and Time settings. Click Next to continue.
20. On the Terminal Services Setup screen, select Application Server Mode, and click Next.
21. Choose the option Permissions Compatible With Windows 2000 Users, and click Next.

**EXERCISE 3.3** ***(continued)***

22. Choose the Typical Settings option on the Network Settings page unless you have special networking requirements. Click Next.

23. When the Workgroup Or Computer Domain screen appears, verify that the No, This Computer Is Not On A Network, Or On A Network Without A Domain option is chosen. Enter **ZYGORT** as the Workgroup name. Click Next.

24. At this point, the network options are applied. The next screen to appear is the Performing Final Tasks screen. The system will install and configure the options that were chosen during the installation wizard.

25. When the Completing The Windows 2000 Setup Wizard screen appears, click Next.

The server is now ready for the exercises in the next chapter, which will install MetaFrame XP.

# Review Questions

1. Browsing occurs when which of the following are executed? (Choose all that apply.)

   A. A user launches a published application.

   B. A user selects the Application Set list in the Find New Application Set Wizard in Program Neighborhood.

   C. A user installs a new version of the ICA Client software.

   D. A user connects to a server or a published application.

2. On which of the following platforms can you install MetaFrame XP 1.0? (Choose all that apply.)

   A. Windows NT Server 4.0

   B. Windows 2000 Server

   C. Windows 2000 Advanced Server

   D. Windows 2000 Datacenter Server

3. When upgrading to MetaFrame XPa from MetaFrame XPs, which of the following license types is required to allow users to continue connecting to the server via ICA connections?

   A. Connection license

   B. Connection migration license

   C. Connection upgrade license

   D. Product license

4. When installing MetaFrame XP on Windows NT Server 4.0, Terminal Server Edition, what is the minimum hard drive free space requirement for the operating system?

   A. 128MB

   B. 512MB

   C. 1GB

   D. 2GB

**5.** When installing MetaFrame XP on Windows 2000 Server, what is the minimum hard drive free space requirement for the operating system?

**A.** 128MB

**B.** 512MB

**C.** 1GB

**D.** 2GB

**6.** After MetaFrame XP is installed, what is the main administrative tool used to control the MetaFrame XP farm?

**A.** Citrix Administration Manager

**B.** Citrix Management Console

**C.** Citrix Services Manager

**D.** Terminal Server Services Manager

**7.** Citrix MetaFrame XP can run on all of the following platforms except which one?

**A.** Windows NT Server 4.0, Terminal Server Edition

**B.** Windows 2000 Server

**C.** Windows 2000 Advanced Server

**D.** Windows 2000 Professional

**8.** Each idle session on a MetaFrame XP server uses how much RAM?

**A.** 3.4MB

**B.** 5.4MB

**C.** 1.7MB

**D.** 2.1MB

9. Ron wants to install Citrix MetaFrame XP on one of his servers and install the ICA Client files so his users can automatically download the latest ICA Client. He picks a server that is running Windows 2000 Server, has a Pentium II 450MHz processor, 256MB of RAM, and a 4GB hard drive with 225MB free. What will he have to upgrade in order to install MetaFrame XP?

   A. The operating system

   B. The processor

   C. The amount of RAM

   D. The hard drive

10. Which of the following must be done on a workstation (non-MetaFrame XP server) in order to run the Citrix Management Console?

   A. The Java permissions in the Microsoft Virtual Machine on the web browser must be set to medium safety.

   B. The ICA Client version 6.01.693 must be installed on the workstation.

   C. The Sun Java Runtime Environment (JRE) version 1.3 must be installed on the workstation.

   D. The client's computer account must be added to the Citrix Administrators list in the Citrix Management Console.

11. Susan wants to manage her MetaFrame XP servers from her desktop computer. On which operating system will she be able to load the Citrix Management Console? (Choose all that apply.)

   A. Windows 95

   B. Windows 98 SE

   C. Windows NT 4.0 Workstation

   D. Windows 2000 Professional

**12.** During the installation of MetaFrame XP, you reach the licensing page only to discover that you do not have the appropriate license paperwork available to activate the software. After finishing the installation, you decide to add the license that will allow MetaFrame to accept connections. Which of the following license types is required before any ICA connections are allowed?

**A.** Connection license

**B.** Connection migration license

**C.** Connection upgrade license

**D.** Product license

**13.** After upgrading a server from MetaFrame 1.8 to MetaFrame XP, what type of license needs to be installed on the server for it to convert the MetaFrame 1.8 user licenses to MetaFrame XP connection licenses?

**A.** Connection license

**B.** Connection migration license

**C.** Connection upgrade license

**D.** Product license

**14.** After months of using MetaFrame XPs, Don has decided that he wants to take advantage of the additional tools contained in MetaFrame XPe. What type of license should he include after upgrading his systems?

**A.** Connection license

**B.** Connection migration license

**C.** Connection upgrade license

**D.** Product license

**15.** What tool would Bill use if he wants to baseline his MetaFrame server that is using Windows 2000 Server as the operating system?

**A.** Citrix Management Console

**B.** Microsoft Management Console

**C.** Network Monitor

**D.** Performance Logs and Alerts

**16.** What default port must be open on a firewall to allow a user to communicate with a MetaFrame server session in a native mode server farm?

**A.** 80

**B.** 1494

**C.** 1604

**D.** 2512

**17.** Which tool is used to configure published applications hosted on a MetaFrame 1.8 server when the MetaFrame 1.8 server farm and the MetaFrame XP server farm interoperate?

**A.** Citrix Connection Manager

**B.** Citrix Management Console

**C.** Citrix Services Manager

**D.** Published Application Manager

**18.** During installation of her MetaFrame XP server, Denise chose the option Prohibit Shadow Connections Without Notification. The manager in charge of temporary employees wants to be able to monitor the employees. Which of the administrative tools would you use to change the shadow settings?

**A.** Citrix Connection Manager

**B.** Citrix Management Console

**C.** Published Application Manager

**D.** Setup

**19.** Sam has a single Metaframe XP farm operating in native mode. When he installs the ICA Client on workstations, he selects the TCP/IP+HTTP protocol for connection. When he clicks the drop-down list to see which servers are available, he gets an error message. What else does Sam need to do to be able to see the servers?

**A.** Add the address of the data collector in the Address List section of the Custom ICA Connection window.

**B.** Make sure his WINS settings are configured properly.

**C.** Make sure the farm is operating in mixed mode.

**D.** Make sure his DNS settings are configured properly.

**20.** The Citrix XML protocol uses which port for communication by default?

**A.** 1604

**B.** 80

**C.** 21

**D.** 1494

# Answers to Review Questions

1. A, B. When a user launches a published application, the ICA browser checks to see which servers are running the application. The ICA Client requests an application on the MetaFrame XP server. If Citrix Load Manager is installed, the client receives the address of the server with the highest load.
   When a user selects the Application Set list from the Find New Application Set Wizard, the ICA browser returns the list of servers and published applications in the farm.

2. B, C, D. The entire Windows 2000 Server family has the ability to run Terminal Server, so MetaFrame XP will load on each one of them. To use MetaFrame XP on a Windows NT Server 4.0, you need the Terminal Server Edition.

3. C. To upgrade the licenses from one version of MetaFrame XP to another, you need to apply a connection upgrade pack for all of the connections within the farm.

4. A. Windows NT Server 4.0, Terminal Server Edition requires 128MB of free hard drive space. Additional free space is required to load Citrix MetaFrame XP.

5. C. Windows 2000 Server requires 1GB of free hard drive space on a 2GB drive or larger. Additional free space is required to load Citrix MetaFrame XP.

6. B. Citrix Management Console is installed by default when MetaFrame XP is installed on the system. It is the main administrative tool for MetaFrame XP. If MetaFrame XP interoperates with MetaFrame 1.8, other tools are available.

7. D. MetaFrame XP can run only on server-based platforms. MetaFrame XP will run on Windows NT Server 4.0, Terminal Server Edition as well as Windows 2000 Server, Advanced Server, and Datacenter Server. All of the Windows 2000 Server platforms must have Terminal Services installed.

8. C. Each idle session on a MetaFrame XP server uses 1.7MB of RAM. Each server has two idle sessions by default.

9. D. While the hard drive is large enough to install the MetaFrame XP installation files, it is not large enough to install the client files. The MetaFrame XP installation will take up about 75MB of hard disk space. The ICA Client files will use about 200MB of hard disk space.

10. C. The Sun Java Runtime Environment version 1.3 is required to run the Citrix Management Console on a workstation.

11. C, D. The Citrix Management Console can be installed only on Windows NT and Windows 2000 platforms. The only other requirement is for the operating system to have the Java Runtime Environment version 1.3 installed prior to installing Citrix Management Console.

12. D. Without a product license installed, MetaFrame XP will not allow any connections. Once the product license is installed, temporary connections may be made for up to 35 days until a connection license is installed.

13. B. Upgrading Citrix MetaFrame 1.8 to MetaFrame XP does not automatically upgrade the user's connection licenses. Citrix provides connection migration packs that contain the installation code that converts the user licenses to connection licenses.

14. C. To upgrade the licenses from one version of MetaFrame XP to another, the licenses need to be upgraded by applying a connection upgrade pack for all of the connections within the farm.

15. D. Baselining is the act of determining the resource usage on a server. When running Windows 2000 Server, he must use the Performance Logs and Alerts snap-in to create a performance log of activity while the system is running.

16. A. Port 80 is the default port that clients use to access server and published application information. Port 1494 is used to initiate a session on a MetaFrame session. Port 1604 is used with legacy clients to communicate with an ICA browser. Port 2512 is used for server-to-server communication.

17. D. Applications published on MetaFrame 1.8 servers are still published using Published Application Manager. Publishing an application in MetaFrame XP is performed in the Citrix Management Console.

18. D. The only way to change any of the shadow settings that were configured during setup is to reinstall MetaFrame XP.

19. A. When using TCP/IP+HTTP to connect to a server farm, Sam must enter the address of an ICA server in the Address List section of the Custom ICA Connections window.

20. B. The Citrix XML protocol uses port 80 by default. This can be changed using the Citrix Management Console. If IIS is installed on a different server than the Metaframe XP server, you should change this port to another number.

Chapter

4

# Installing MetaFrame XP

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **2. MetaFrame Installation process**

- 2c. Installing MetaFrame and various setup options

We're finally to the point where we are going to install MetaFrame XP on a server. In the first part of this chapter, we will discuss the preparation phase, installation steps, and migration issues, and then the remainder of the chapter will be a step-by-step lab for performing the install. After finishing this chapter, you should have a good understanding of the steps required to install MetaFrame XP. First up, let's look at the prep phase.

## Preparing for Installation

The first order of business is to collect all of the necessary information (licenses, protocols, drive mapping, configuration options) and software. After reading the previous chapter, you should have a good understanding of the requirements for MetaFrame XP. You should have a plan in place for the items required to install MetaFrame XP. If you have not developed a plan, this is the time to sit down and develop one. Some administrators design their own checklist of everything they need to perform the installation. Checklists include not only the items necessary for the install, such as the MetaFrame XP CD and the licenses, but also the configuration options, including the protocols to install, the parameters to use for those protocols, and how the drives are mapped.

As you work your way down the checklist, you will assemble all of the items needed for the install. Of course, the MetaFrame XP CD is required, unless you have previously placed the installation files on a network share.

NOTE

For more information concerning the configuration options and planning the installation, read Chapter 3, "Planning the Installation of MetaFrame XP."

The data store configuration is required before you can install a database other than Microsoft Access. Two other products are available for use as the data store, and they are probably the most widely used databases at this time: Microsoft SQL Server and Oracle. While you can use either of these products as the data store, the configuration of these is beyond the scope of this book. Citrix has extensive documentation dealing with the configuration of these two products if you wish to use them as the database for the data store.

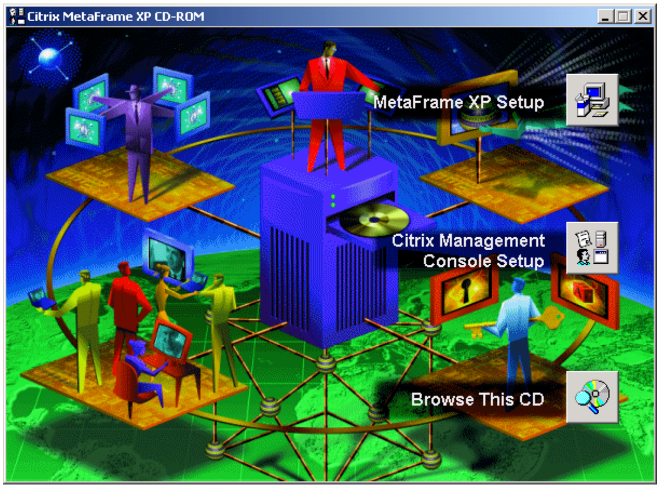
As mentioned in the previous chapter, you should have already installed all of the hardware necessary for communication if you're using asynchronous connections. This guarantees that you will be able to configure the async connections during the install. You can always install the communications equipment at a later time. Now let's take a look at the steps necessary to install MetaFrame XP.

# Performing a New Installation

As you prepare to install the software, if your server is configured for autorun, the MetaFrame splash screen will appear. The autorun feature of the CD-ROM will execute a program called *autoroot.exe*. This program checks the operating system and determines which version of MetaFrame XP Setup to start. Luckily, you are not required to carry the MetaFrame XP CD with you every time you need to install the software on a server. As with most software, you can load the installation files onto a distribution server. From the installation point, you can execute the autoroot.exe program, and it will perform in the same manner as the CD installation. You may find that a network-based install is actually more efficient than the CD-based install.

When the splash screen appears, as shown in Figure 4.1, select the MetaFrame XP Setup button to start the installation process. The Setup Wizard presents several screens, each with one or more options to configure. This is where your checklist and configuration sheets come in very handy. Let's look at the installation steps.

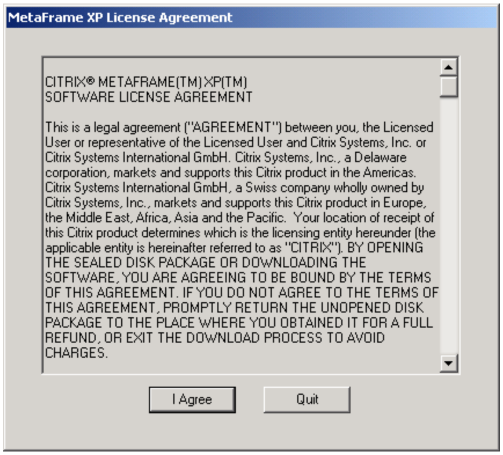
**FIGURE 4.1** Citrix MetaFrame XP installation splash screen



## MetaFrame XP License Agreement

First up is the ubiquitous *MetaFrame XP License Agreement*, shown in Figure 4.2. If this is the first installation of MetaFrame XP you have performed, take the time to read the agreement before proceeding. Included in this agreement are the rules and regulations that you are bound by when you click the I Agree button. If you are unsure of any of the requirements, do not agree to the terms. Of course, at this point in the process, we are going to move forward.

**FIGURE 4.2** MetaFrame XP License Agreement

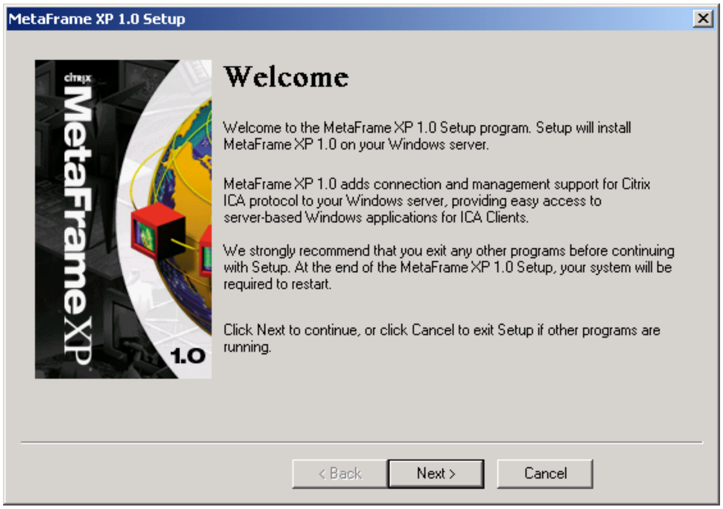


CITRIX® METAFRAME(TM) XP(TM)
SOFTWARE LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between you, the Licensed User or representative of the Licensed User and Citrix Systems, Inc. or Citrix Systems International GmbH. Citrix Systems, Inc., a Delaware corporation, markets and supports this Citrix product in the Americas. Citrix Systems International GmbH, a Swiss company wholly owned by Citrix Systems, Inc., markets and supports this Citrix product in Europe, the Middle East, Africa, Asia and the Pacific. Your location of receipt of this Citrix product determines which is the licensing entity hereunder (the applicable entity is hereinafter referred to as "CITRIX"). BY OPENING THE SEALED DISK PACKAGE OR DOWNLOADING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNOPENED DISK PACKAGE TO THE PLACE WHERE YOU OBTAINED IT FOR A FULL REFUND, OR EXIT THE DOWNLOAD PROCESS TO AVOID CHARGES.

After you click the I Agree button, a friendlier Welcome screen appears. As shown in Figure 4.3, this screen contains the typical warnings about stopping all other applications that may be running. Considering the files that are needed by the Setup program and the new files that are added to the system, you should not be running other applications that could affect the installation. When the installation is complete, Setup will initiate a restart of the system. If no other programs are running, click Next to continue.

**FIGURE 4.3** Welcome screen



Welcome

Welcome to the MetaFrame XP 1.0 Setup program. Setup will install MetaFrame XP 1.0 on your Windows server.

MetaFrame XP 1.0 adds connection and management support for Citrix ICA protocol to your Windows server, providing easy access to server-based Windows applications for ICA Clients.

We strongly recommend that you exit any other programs before continuing with Setup. At the end of the MetaFrame XP 1.0 Setup, your system will be required to restart.

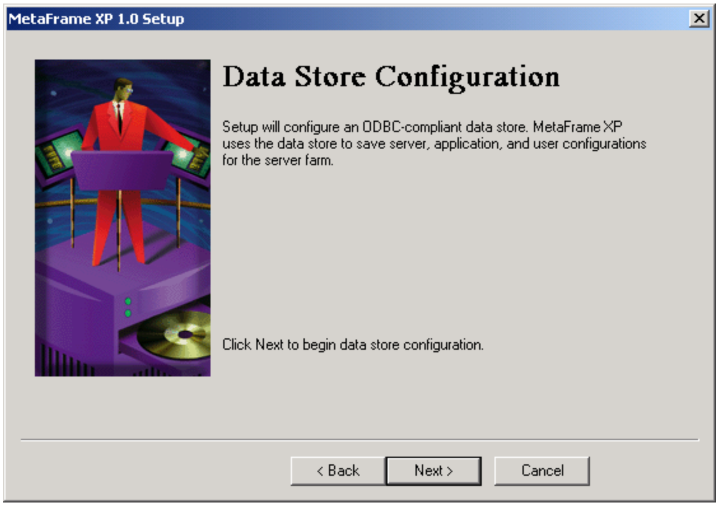
Click Next to continue, or click Cancel to exit Setup if other programs are running.

## Data Store Configuration

The Data Store Configuration information screen appears next, as shown in Figure 4.4, allowing you to configure the database used for the data store. Again, if you are using another product besides Microsoft Access for the database, that database should already be configured. Click Next to start the data store configuration.

On the Server Farm Selection screen, shown in Figure 4.5, you are presented with two options: Create A New Server Farm and Join An Existing Server Farm. Since you are adding your first MetaFrame XP server, choose the first option. Even if you have a MetaFrame 1.8 server farm already in place, you still choose Create A New Server Farm since a MetaFrame XP server cannot exist in a MetaFrame 1.8 farm. The two farms can interoperate, but the two server types cannot coexist in the same farm. Of course, if a MetaFrame XP server farm already exists, and you want to add the server to the existing farm, you should choose the latter of the two options. Then click Next to continue.

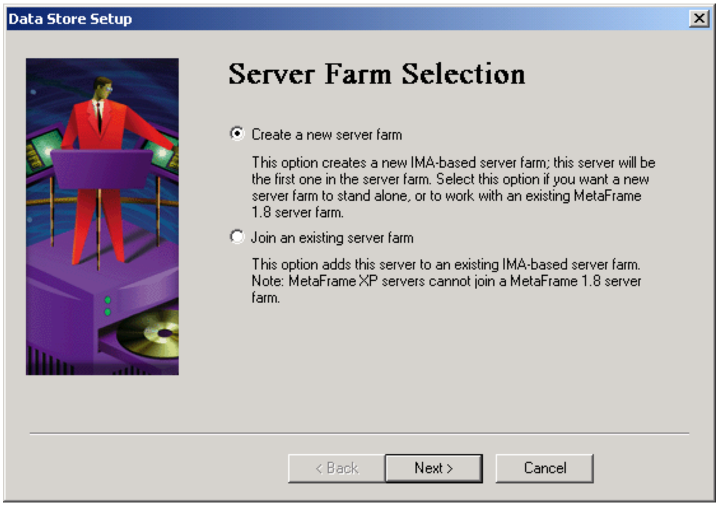
**FIGURE 4.4** Data Store Configuration screen



Setup will configure an ODBC-compliant data store. MetaFrame XP uses the data store to save server, application, and user configurations for the server farm.

Click Next to begin data store configuration.

**FIGURE 4.5** Server Farm Selection screen



● Create a new server farm

This option creates a new IMA-based server farm; this server will be the first one in the server farm. Select this option if you want a new server farm to stand alone, or to work with an existing MetaFrame 1.8 server farm.

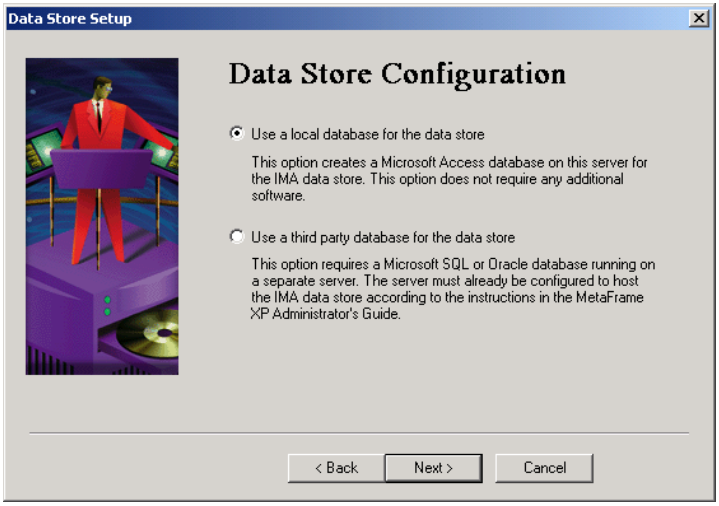
○ Join an existing server farm

This option adds this server to an existing IMA-based server farm. Note: MetaFrame XP servers cannot join a MetaFrame 1.8 server farm.

Figure 4.6 displays the options that became available when you chose Create A New Server Farm from the previous screen. The option you select here depends on what database software you are using. If you are planning to use Access as your database, you should select Use A Local Database For The Data Store. This option prompts Setup to automatically install and configure the data store using Access as the database engine. This is the easiest method of data store configuration, although the database then runs on the first MetaFrame server.

The other option presented to you when you chose to create a new farm is Use A Third Party Database For The Data Store. Select this option if you are planning to use either Microsoft SQL Server or Oracle. If you use either of these databases, it cannot coexist on the same server where MetaFrame XP is loaded. It must be installed and have a database configured prior to the installation of MetaFrame XP. If you don't complete this process prior to performing the MetaFrame install, Setup will not allow you to continue.

**FIGURE 4.6** Data Store Configuration screen



● Use a local database for the data store

This option creates a Microsoft Access database on this server for the IMA data store. This option does not require any additional software.

○ Use a third party database for the data store

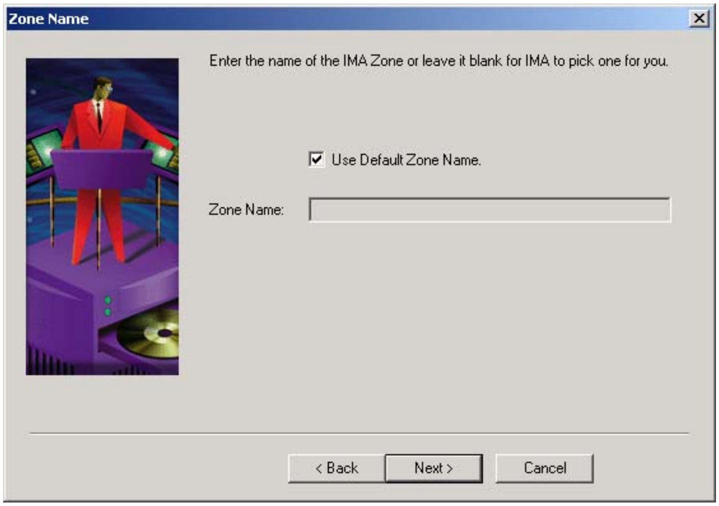
This option requires a Microsoft SQL or Oracle database running on a separate server. The server must already be configured to host the IMA data store according to the instructions in the MetaFrame XP Administrator's Guide.

If instead you chose to join an existing farm, you will be presented with the options Direct Data Store Connection and Connect To Data Store Set Up Locally On Another Server. If you select the former option, you must choose one of two modes to access the data store. The first choice is to access the database through ODBC-compliant drivers. These drivers will have to be loaded onto the server and configured to access the database that is loaded onto another server. The other option is to use indirect access, which uses port 2152 to connect to another MetaFrame XP server that acts as a proxy for the server you are configuring. Using this method, your server does not need to have the ODBC drivers loaded and configured. The drawback to this configuration is that if the server configured with the ODBC drivers fails, none of the other servers utilizing it will have access to the data store. A single point of failure is never acceptable.

If you select the latter option, Connect To Data Store Set Up Locally On Another Server, you will need to point your MetaFrame XP server to another server that has the data store database installed on it. This is actually the server running the database software, and you will need to supply the name of the data store server and the port used to access the database. Once you select these options, Setup moves on to configuring the zone information.

As seen in Figure 4.7, Setup prompts you for the zone name. If you decide to choose the default zone name, the subnet address of the server will be used to identify the zone. If this is not what you had planned on, you can enter your own descriptive zone name by deselecting the check box next to Use Default Zone Name and entering the desired name into the Zone Name field. After making the zone name selection, click Next to move on to the Server Farm Name screen.

**FIGURE 4.7** Zone Name screen



Zone Name

Enter the name of the IMA Zone or leave it blank for IMA to pick one for you.

☑ Use Default Zone Name.

Zone Name:

At this point, the installation of the data store varies between the automated setup of Microsoft Access and that of Microsoft SQL or Oracle. The Access installation is completely automated, while the other databases require you to supply configuration options. If Oracle is available, the only configuration options are those shown below:

**Service** The name of the database used for the data store.

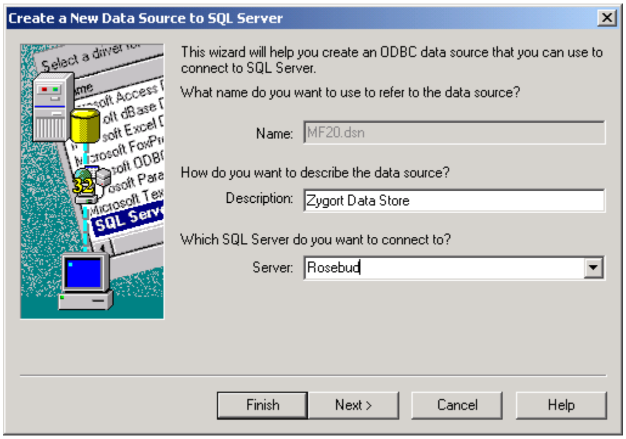
**User Name** The username with the appropriate permissions to the database.

**Password** The password used by the username presented in the previous step.

On the other hand, if you choose to utilize Microsoft SQL Server, you will see the screen shown in Figure 4.8, which prompts you for the ODBC configuration information. In the Name field, you should enter the name that is used for the data store. The default name of MF20.dsn is filled in automatically. You can also enter a description of the data store database, which is used for informational purposes only. The last entry on this screen allows you to choose the server that is used to host the data store database. Your options for the entry in the Server field include the following:

- You can select a server from the list.
- You can type a server name into the list.
- You can select (Local) from the list to select a database on the local server. This option is not viable for MetaFrame XP and should be disregarded.

**FIGURE 4.8** ODBC data source configuration



Create a New Data Source to SQL Server

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name: MF20.dsn

How do you want to describe the data source?

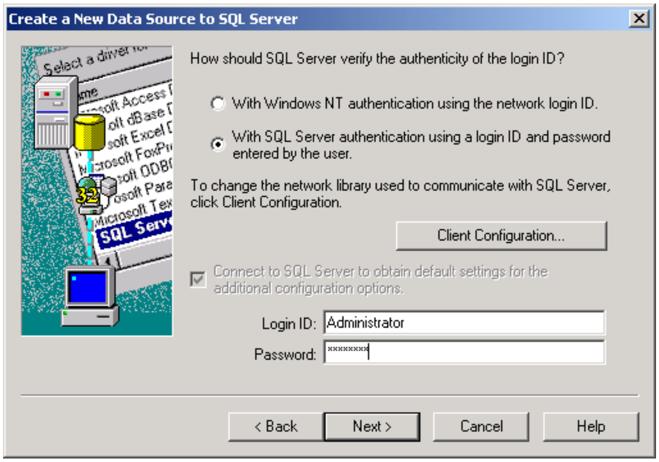
Description: Zygort Data Store

Which SQL Server do you want to connect to?

Server: Rosebud

After configuring the database options, you are presented with the authentication options for the database, as shown in Figure 4.9. The first option, With Windows NT Authentication Using The Network Login ID, allows the system to use the system's current login ID for authentication to the SQL Server. When you use this authentication method, the user account used to authenticate the service must have the Act As Part Of The Operating System right associated with it. The other option, With SQL Server Authentication Using A Login ID And Password Entered By The User, dictates that the administrator must supply a user account and password with the appropriate permissions to the database on the SQL Server.

**FIGURE 4.9** Authentication methods


Create a New Data Source to SQL Server

How should SQL Server verify the authenticity of the login ID?

○ With Windows NT authentication using the network login ID.

● With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

☑ Connect to SQL Server to obtain default settings for the additional configuration options.

Login ID: Administrator

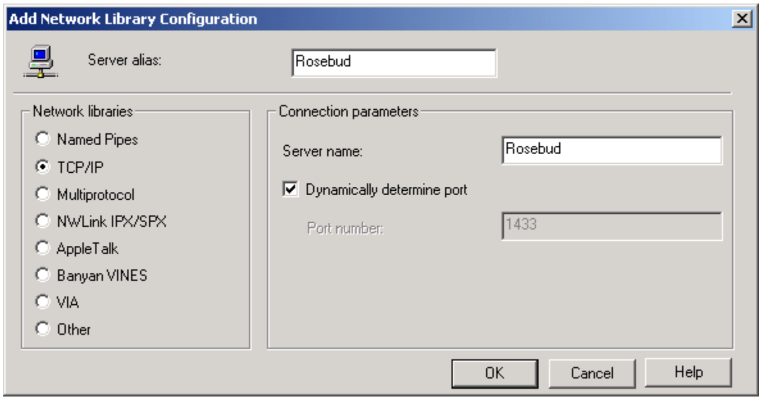
Password: ********

By clicking the Client Configuration button on this screen, you cause Setup to display the network library connection options, as shown in Figure 4.10. Within this screen, the administrator can configure the connection options to the SQL Server. In the Server Alias field, you must enter the SQL Server's server name. In the Network Libraries section, you can choose any of the standard connection types. At this point, MetaFrame supports only TCP/IP and Named Pipes. Depending on which option you choose, you will be presented with configuration options in the right-hand panel.

NOTE

If your MetaFrame XP environment includes a wide area network connection, do not select Named Pipes. Named Pipes utilizes NetBIOS and will not work in a routed environment.

**FIGURE 4.10** Add Network Library Configuration screen



Add Network Library Configuration

Server alias: Rosebud

Network libraries

- ○ Named Pipes
- ● TCP/IP
- ○ Multiprotocol
- ○ NWLink IPX/SPX
- ○ AppleTalk
- ○ Banyan VINES
- ○ VIA
- ○ Other

Connection parameters

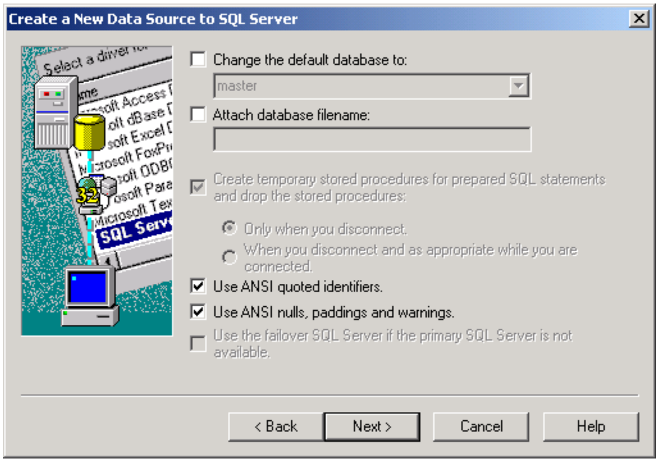
Server name: Rosebud

☑ Dynamically determine port

Port number: 1433

The next step in the data store configuration is specifying the correct parameters for the data source. The first option, as seen in Figure 4.11, is the default database name. The way in which the SQL administrator has configured the SQL database dictates what you supply in this field. SQL lets you configure a default database that can be accessed by a login ID. If this is the case with the data store's database, you may leave this field blank. If not, you will need to enter the name of the default database that the data store will use.

**FIGURE 4.11** Data source configuration



Create a New Data Source to SQL Server

☐ Change the default database to: master

☐ Attach database filename:

☑ Create temporary stored procedures for prepared SQL statements and drop the stored procedures:

- ● Only when you disconnect.
- ○ When you disconnect and as appropriate while you are connected.

☑ Use ANSI quoted identifiers.

☑ Use ANSI nulls, paddings and warnings.

☐ Use the failover SQL Server if the primary SQL Server is not available.

The second field allows you to specify the database filename that you want to attach as the primary file. MetaFrame XP uses the entry specified in the Change The Default Database To field for the database name.

If you are using a version of SQL Server prior to SQL 7.0, you can specify how the temporary stored procedures are dropped or ended. The two options available are Only When You Disconnect, which allows you to drop the procedure only when the SQLDisconnect function is called, and When You Disconnect And As Appropriate While You Are Connected, which drops the procedures when the SQLDisconnect, SQLFreeHandle, SQLPrepare, and SQLExecDirect functions are called. If you select the former option, the server will retain the stored procedures for a longer period of time, allowing them to be reused without having to reload them, while the latter option will stop the procedures from consuming additional resources but may cause additional processing as they are continually reloaded when needed.

The Use ANSI Quoted Identifiers option allows the SQL Server to enforce the quotation rules. With this option selected, the SQL Server allows only double quotes to surround identifiers, while allowing only single quotes to enclose character strings.

Selecting the next check box in Figure 4.11 makes the SQL Server enforce ANSI rules regarding NULL characters and the trimming of trailing blanks and zeros. With this option selected, standard SQL calls must use the standard ANSI rules, while Transact-SQL calls are not affected.

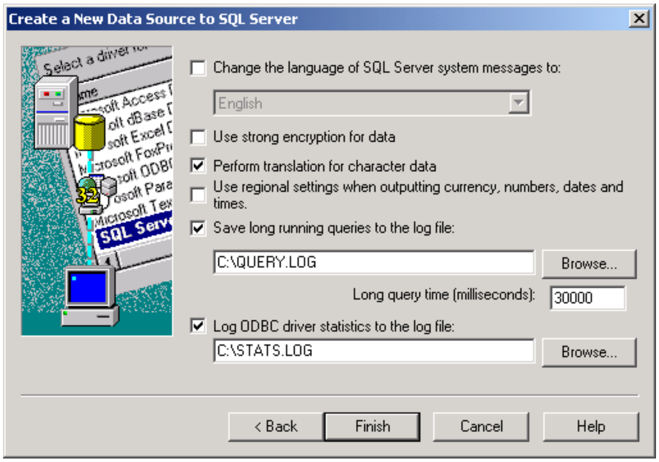
The final check box allows for failover in case the primary SQL Server becomes unavailable. If the primary SQL Server does fail, the current transaction is reversed and retried. If the server still remains unavailable and the SQL Server is configured for failover, the secondary server will be contacted.

Click the Next button to move to the second page of data source configuration, as shown in Figure 4.12. The language option at the top of the screen allows you to specify in which language the system messages are displayed. This is especially handy in case you have a different language on the server and you wish to have the system messages displayed in your language.

The Perform Translation For Character Data check box enforces ANSI to Unicode conversion between the client and the server. This reduces the amount of misinterpreted data resulting from extended ANSI characters sent between the client and server.

The Use Regional Settings When Outputting Currency, Numbers, Dates And Times option forces the SQL Server to use the regional settings of the client's system when making a connection to the data store.

**FIGURE 4.12** Data source parameters



Create a New Data Source to SQL Server

□ Change the language of SQL Server system messages to:

English

□ Use strong encryption for data

☑ Perform translation for character data

□ Use regional settings when outputting currency, numbers, dates and times.

☑ Save long running queries to the log file:

C:\QUERY.LOG

Long query time (milliseconds): 30000

☑ Log ODBC driver statistics to the log file:

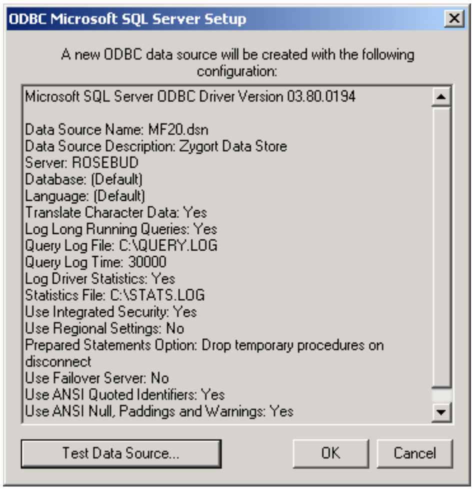
C:\STATS.LOG

If you want to monitor which queries are taking an inordinate amount of time to process, you will want to select the option Save Long Running Queries To The Log File. All queries that exceed the amount of time listed in the Long Query Time field are noted in the log file specified in that section.

Finally, if you want to log the SQL Server statistics, you can enter the name of the log file in the Log ODBC Driver Statistics To The Log File text box.

Once you have entered all of the data store database options, you can check the connectivity to the database. Click Finish, and a summary screen of the configuration appears, as shown in Figure 4.13. You can test the connection by clicking the Test Data Source button. If everything works correctly and you are able to make a connection, you will be presented with a TESTS COMPLETED SUCCESSFULLY message, as shown in Figure 4.14. Click OK to continue.

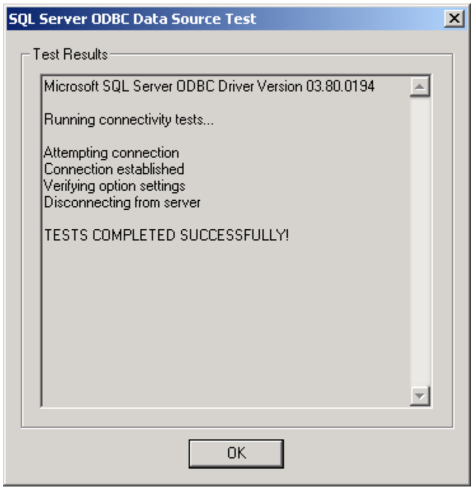
**FIGURE 4.13** Data source configuration confirmation



A new ODBC data source will be created with the following configuration:

```
Microsoft SQL Server ODBC Driver Version 03.80.0194

Data Source Name: MF20.dsn
Data Source Description: Zygort Data Store
Server: ROSEBUD
Database: (Default)
Language: (Default)
Translate Character Data: Yes
Log Long Running Queries: Yes
Query Log File: C:\QUERY.LOG
Query Log Time: 30000
Log Driver Statistics: Yes
Statistics File: C:\STATS.LOG
Use Integrated Security: Yes
Use Regional Settings: No
Prepared Statements Option: Drop temporary procedures on
disconnect
Use Failover Server: No
Use ANSI Quoted Identifiers: Yes
Use ANSI Null, Paddings and Warnings: Yes
```

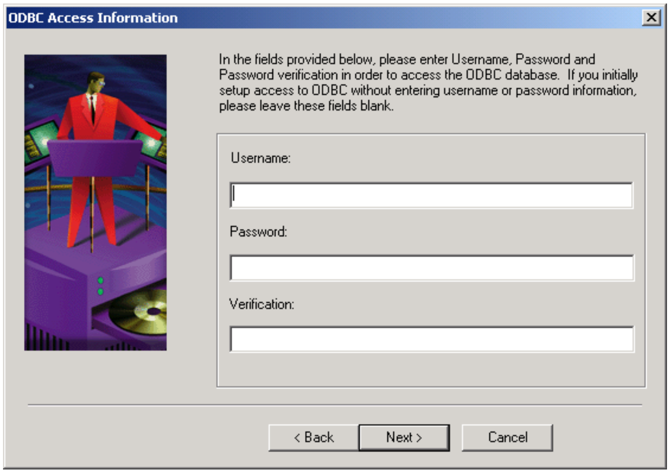
**FIGURE 4.14** Test Results



```
Microsoft SQL Server ODBC Driver Version 03.80.0194

Running connectivity tests...

Attempting connection
Connection established
Verifying option settings
Disconnecting from server

TESTS COMPLETED SUCCESSFULLY!
```

The final step before progressing is to enter the name and password of the account that will be used to access the SQL Server database, as shown in Figure 4.15. Enter the username and password, along with a verification of the password (just in case you don't enter it right the first time), and you are ready to finalize the data store configuration. Click Next to continue.

**FIGURE 4.15** ODBC Access Information screen



ODBC Access Information

In the fields provided below, please enter Username, Password and Password verification in order to access the ODBC database. If you initially setup access to ODBC without entering username or password information, please leave these fields blank.

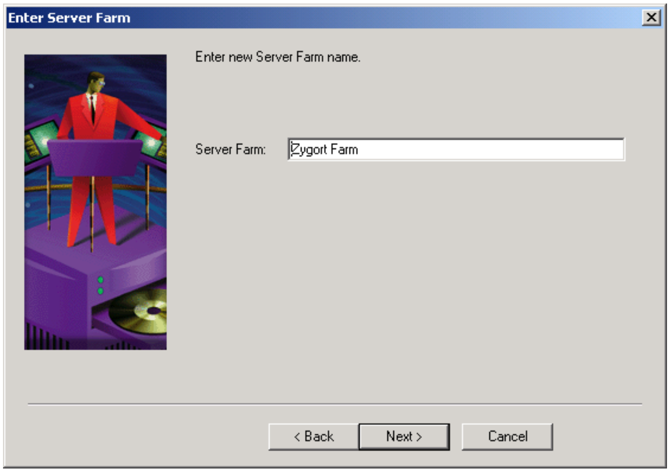
Username:

Password:

Verification:

The various database configurations converge back at this point. Now that you have supplied all the required information, installed the appropriate drivers, and made the connections, you need to specify the name of your server farm, as shown in Figure 4.16. Consult the checklist from Chapter 3, "Planning the Installation of MetaFrame XP," for the appropriate farm name. Remember, for interoperability with a MetaFrame 1.8 server farm, the farms must have identical names. Once you have entered the name and clicked Next, the confirmation screen appears, as shown in Figure 4.17. Click Next once again.

**FIGURE 4.16** Enter Server Farm screen

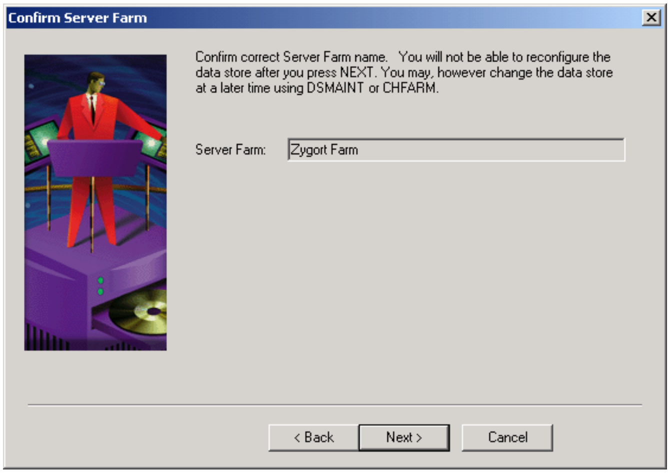


Enter Server Farm

Enter new Server Farm name.

Server Farm: Zygort Farm

**FIGURE 4.17** Confirm Server Farm screen



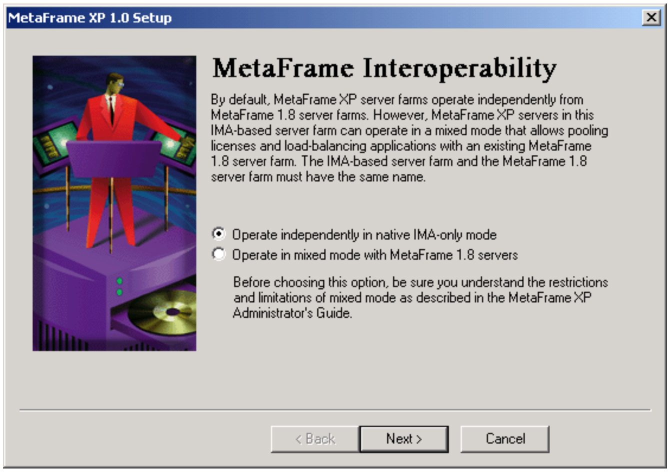
Confirm Server Farm

Confirm correct Server Farm name. You will not be able to reconfigure the data store after you press NEXT. You may, however change the data store at a later time using DSMAINT or CHFARM.

Server Farm: Zygort Farm

As you approach the end of the data store installation, you are allowed to choose the interoperability mode for working with MetaFrame 1.8 and MetaFrame XP server farms, as shown in Figure 4.18. If any MetaFrame 1.8 servers exist in a MetaFrame 1.8 server farm, the MetaFrame XP server farm should be configured to run in mixed mode. As soon as the last MetaFrame 1.8 server is upgraded, the farm can be changed to native mode to take advantage of the additional IMA functionality. After making your selection, click Next to continue.

**FIGURE 4.18** MetaFrame Interoperability screen



MetaFrame XP 1.0 Setup

MetaFrame Interoperability

By default, MetaFrame XP server farms operate independently from MetaFrame 1.8 server farms. However, MetaFrame XP servers in this IMA-based server farm can operate in a mixed mode that allows pooling licenses and load-balancing applications with an existing MetaFrame 1.8 server farm. The IMA-based server farm and the MetaFrame 1.8 server farm must have the same name.

● Operate independently in native IMA-only mode

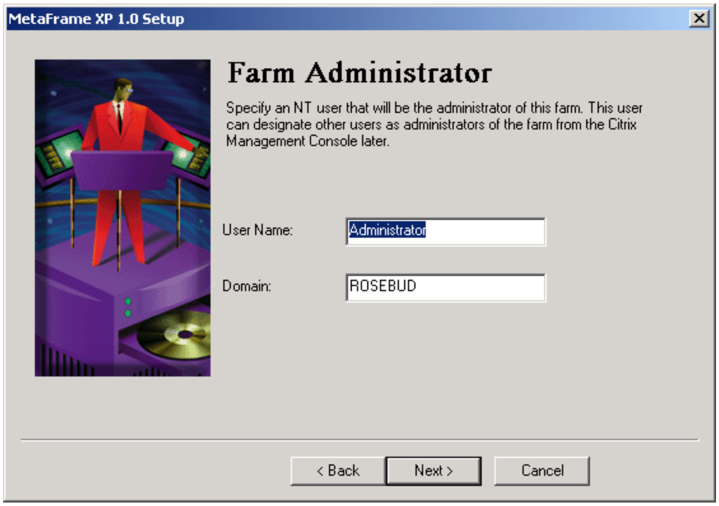
○ Operate in mixed mode with MetaFrame 1.8 servers

Before choosing this option, be sure you understand the restrictions and limitations of mixed mode as described in the MetaFrame XP Administrator's Guide.

The last option you need to configure for the data store is the administrator account for the farm, as shown in Figure 4.19. This account is added to the Administrators list and will have permissions to use the Citrix Management Console to modify and control the servers in the server farm. You can add other administrators later. After you enter the information, Setup will prompt you to verify that the information is correct, as shown in Figure 4.20. At this point, the data store configuration is complete, and you can move on to configuring the network connections.

NOTE See Chapter 5, "Administration and the Citrix Management Console," for instructions on how to add administrators to the Citrix Administrators list.

**FIGURE 4.19** Farm Administrator screen


MetaFrame XP 1.0 Setup

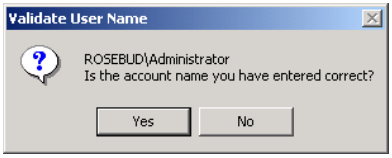
Farm Administrator

Specify an NT user that will be the administrator of this farm. This user can designate other users as administrators of the farm from the Citrix Management Console later.

User Name: Administrator

Domain: ROSEBUD

**FIGURE 4.20** Validate User Name dialog

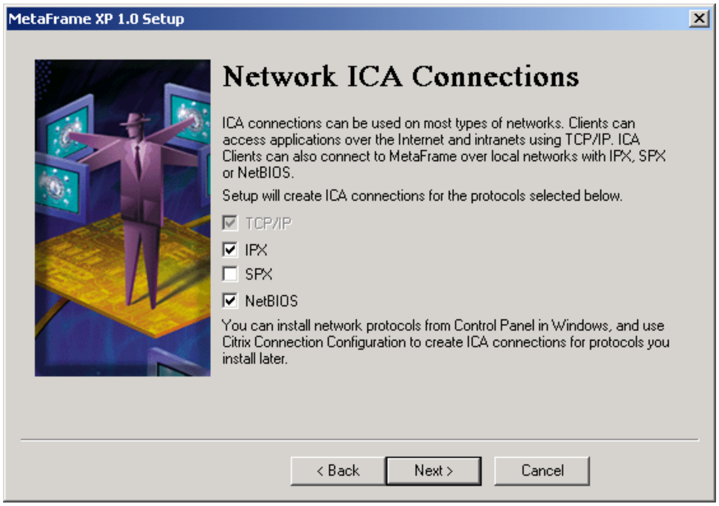

Validate User Name

ROSEBUD\Administrator
Is the account name you have entered correct?

## Network Connections

When the Network ICA Connections screen opens, the protocols installed on the server appear. MetaFrame XP can utilize TCP/IP, IPX, SPX, and NetBIOS, as shown in Figure 4.21. If a protocol is not installed, it is grayed out. All of the network protocols that MetaFrame utilizes can be selected or deselected from this screen except for TCP/IP. If you plan to use only TCP/IP as the network protocol for your sessions, deselect the check boxes next to the other protocol names.

**FIGURE 4.21** Network ICA Connections screen



Network ICA Connections

ICA connections can be used on most types of networks. Clients can access applications over the Internet and intranets using TCP/IP. ICA Clients can also connect to MetaFrame over local networks with IPX, SPX or NetBIOS.

Setup will create ICA connections for the protocols selected below.

☑ TCP/IP
☑ IPX
□ SPX
☑ NetBIOS

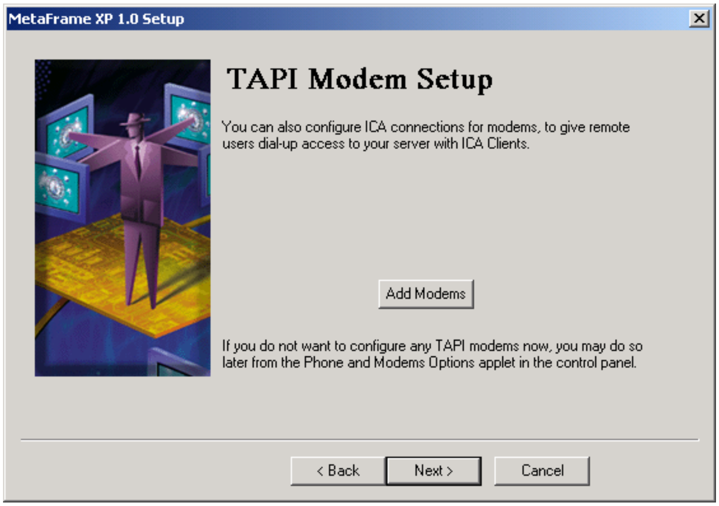
You can install network protocols from Control Panel in Windows, and use Citrix Connection Configuration to create ICA connections for protocols you install later.

When you select a protocol, MetaFrame creates a listener port for that protocol during installation. Likewise, if a protocol is not selected or not installed, Setup will not create the listener port for that protocol. You can add protocols after Setup is complete if you need to run sessions on the additional protocol. Since TCP/IP cannot be deselected, you will always have a listener port created for TCP/IP. Click Next to continue.

## TAPI Modem Setup

If your users need to connect directly into the MetaFrame server, you can create an async connection at this point. As shown in Figure 4.22, you can click the Add Modems button and then use the Phone And Modem Options screen, shown in Figure 4.23, to select the modems to be used as async dial-in connections. Any modem that you select cannot be used by any other service on the server, including RAS.

**FIGURE 4.22** TAPI Modem Setup screen



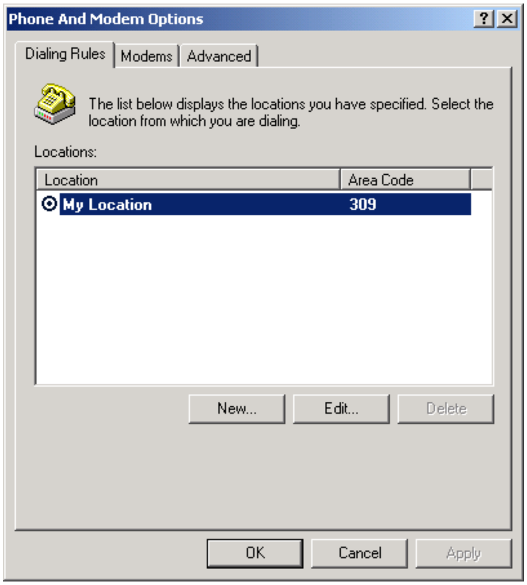
MetaFrame XP 1.0 Setup

TAPI Modem Setup

You can also configure ICA connections for modems, to give remote users dial-up access to your server with ICA Clients.

If you do not want to configure any TAPI modems now, you may do so later from the Phone and Modems Options applet in the control panel.

**FIGURE 4.23** Phone And Modem Options screen



Phone And Modem Options

The list below displays the locations you have specified. Select the location from which you are dialing.

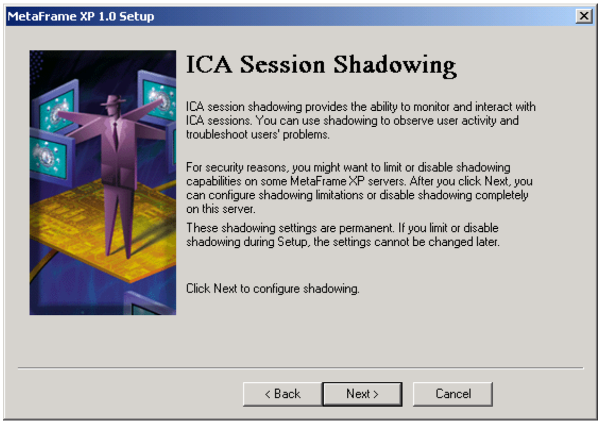
Locations:

| Location | Area Code |
|---|---|
| ● My Location | 309 |

## ICA Session Shadowing

After you configure the modems, the shadowing options are the next installation decision, as shown in Figure 4.24. Again, you should have already planned the allowed level of shadowing for your organization; this process is generally known as *ICA session shadowing*. Consult the checklist you created in Chapter 3, select the appropriate options, and click Next. Remember, shadowing restrictions selected during Setup, as shown in Figure 4.25, are not reversible. Once MetaFrame is installed, the only way to make changes to these shadowing settings is to reinstall MetaFrame on the server. Click Next to continue.

**FIGURE 4.24** ICA Session Shadowing screen



ICA Session Shadowing

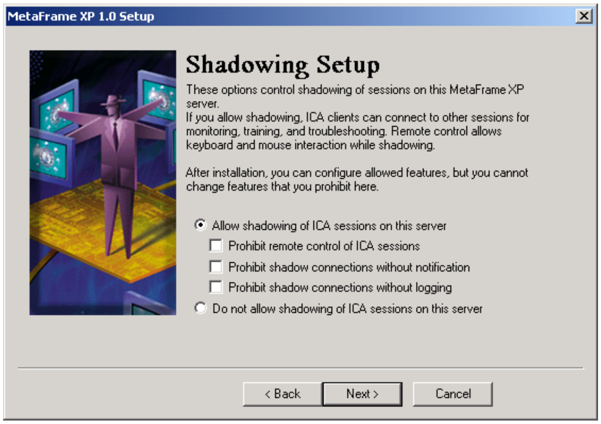
ICA session shadowing provides the ability to monitor and interact with ICA sessions. You can use shadowing to observe user activity and troubleshoot users' problems.

For security reasons, you might want to limit or disable shadowing capabilities on some MetaFrame XP servers. After you click Next, you can configure shadowing limitations or disable shadowing completely on this server.

These shadowing settings are permanent. If you limit or disable shadowing during Setup, the settings cannot be changed later.

Click Next to configure shadowing.

**FIGURE 4.25** Shadowing Setup screen



Shadowing Setup

These options control shadowing of sessions on this MetaFrame XP server.
If you allow shadowing, ICA clients can connect to other sessions for monitoring, training, and troubleshooting. Remote control allows keyboard and mouse interaction while shadowing.

After installation, you can configure allowed features, but you cannot change features that you prohibit here.

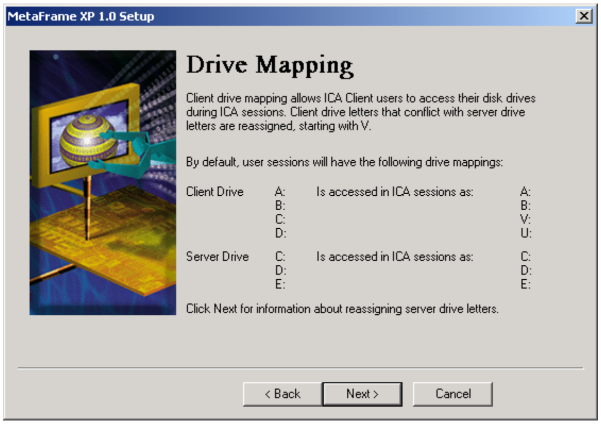
● Allow shadowing of ICA sessions on this server
- □ Prohibit remote control of ICA sessions
- □ Prohibit shadow connections without notification
- □ Prohibit shadow connections without logging

○ Do not allow shadowing of ICA sessions on this server

## Drive Mapping

After choosing the shadowing settings, you are presented with the drive mapping options. The initial screen, shown in Figure 4.26, displays the default configuration for the drive lettering. After you click the Next button, you are allowed to make changes to the drive letter assignments, as shown in Figure 4.27. Note that when you remap the drive letters, if any applications were installed prior to the MetaFrame setup, a warning dialog box like the one shown in Figure 4.28 will appear. Click OK to proceed with server drive mapping. As discussed in Chapter 3, the applications installed prior to the installation of MetaFrame may need to be reinstalled if they are used in user sessions.

**FIGURE 4.26** Drive Mapping screen



MetaFrame XP 1.0 Setup

Drive Mapping

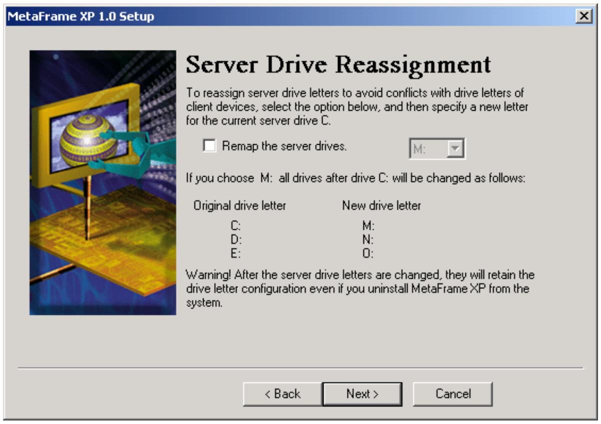
Client drive mapping allows ICA Client users to access their disk drives during ICA sessions. Client drive letters that conflict with server drive letters are reassigned, starting with V.

By default, user sessions will have the following drive mappings:

| | | | |
|---|---|---|---|
| Client Drive | A:<br>B:<br>C:<br>D: | Is accessed in ICA sessions as: | A:<br>B:<br>V:<br>U: |
| Server Drive | C:<br>D:<br>E: | Is accessed in ICA sessions as: | C:<br>D:<br>E: |

Click Next for information about reassigning server drive letters.

**FIGURE 4.27** Server Drive Reassignment screen



MetaFrame XP 1.0 Setup

Server Drive Reassignment

To reassign server drive letters to avoid conflicts with drive letters of client devices, select the option below, and then specify a new letter for the current server drive C.

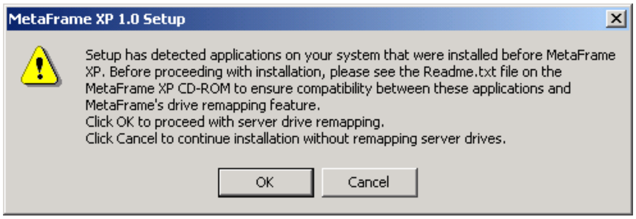
☐ Remap the server drives. M:

If you choose M: all drives after drive C: will be changed as follows:

| Original drive letter | New drive letter |
|---|---|
| C: | M: |
| D: | N: |
| E: | O: |

Warning! After the server drive letters are changed, they will retain the drive letter configuration even if you uninstall MetaFrame XP from the system.

**FIGURE 4.28** Warning about previously installed applications



MetaFrame XP 1.0 Setup

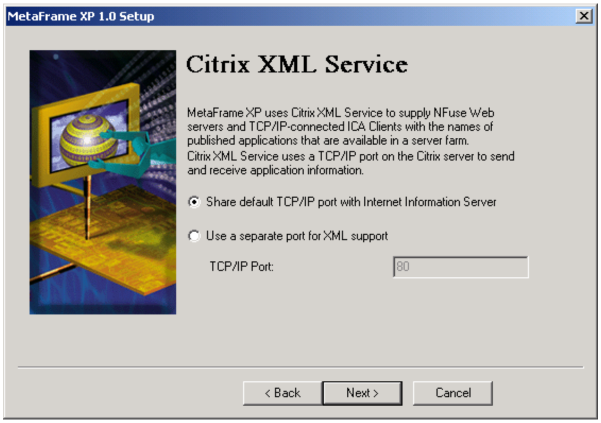
Setup has detected applications on your system that were installed before MetaFrame XP. Before proceeding with installation, please see the Readme.txt file on the MetaFrame XP CD-ROM to ensure compatibility between these applications and MetaFrame's drive remapping feature.
Click OK to proceed with server drive remapping.
Click Cancel to continue installation without remapping server drives.

This warning appears only when you choose to remap the server's drive letters.

## Citrix XML Service

You are now presented with the *Citrix XML Service* dialog box, with the options shown in Figure 4.29. When choosing the installation options for the XML service, again consider your checklist. This service allows web-based clients to see the names of the published applications in the farm. The default settings, shown in the NFuse Setup dialog box in Figure 4.30, generally work for most companies. If you have a reason not to use the default settings, then you must reconfigure the clients and the NFuse web server to use the new port number.

**FIGURE 4.29** Citrix XML Service screen



MetaFrame XP 1.0 Setup

Citrix XML Service

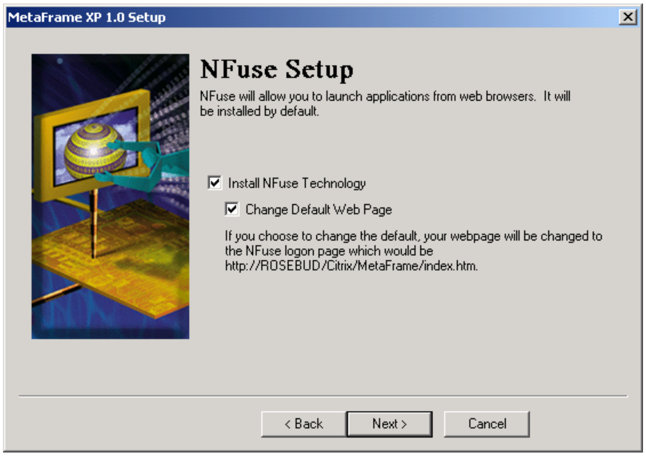
MetaFrame XP uses Citrix XML Service to supply NFuse Web servers and TCP/IP-connected ICA Clients with the names of published applications that are available in a server farm.
Citrix XML Service uses a TCP/IP port on the Citrix server to send and receive application information.

● Share default TCP/IP port with Internet Information Server

○ Use a separate port for XML support

TCP/IP Port: 80

**FIGURE 4.30** NFuse Setup screen



MetaFrame XP 1.0 Setup

NFuse Setup

NFuse will allow you to launch applications from web browsers. It will be installed by default.

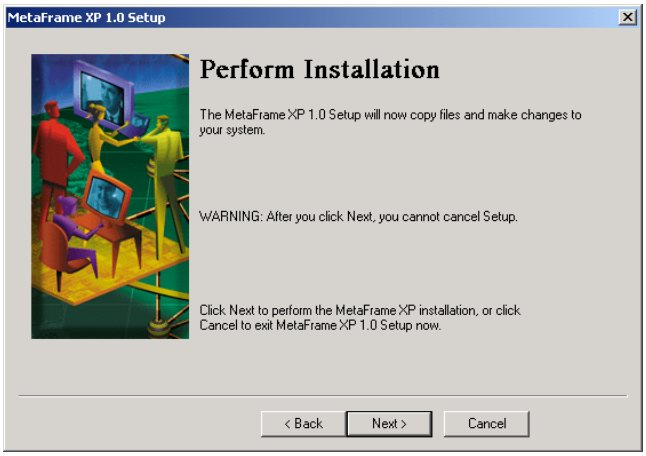
☑ Install NFuse Technology

☑ Change Default Web Page

If you choose to change the default, your webpage will be changed to the NFuse logon page which would be http://ROSEBUD/Citrix/MetaFrame/index.htm.

After you click the Next button, the Perform Installation screen appears. Setup now warns you that you will not be able to stop the installation if you click Next again, as shown in Figure 4.31. If you are ready to start the installation, click the button. Setup will start copying all of the required files to the server and install NFuse, Citrix Management Console, the ICA pass-through Client, and the encryption service. A progress indicator starts and shows the current installation progress. When this portion of the install completes, you are presented with the Citrix ICA Client Distribution Wizard.

**FIGURE 4.31** Perform Installation warning message



MetaFrame XP 1.0 Setup

Perform Installation

The MetaFrame XP 1.0 Setup will now copy files and make changes to your system.

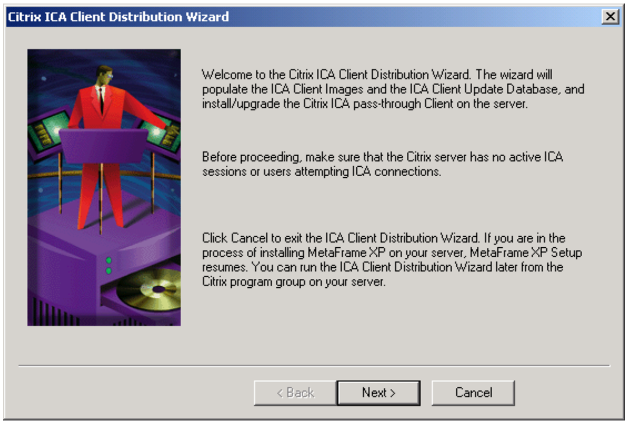
WARNING: After you click Next, you cannot cancel Setup.

Click Next to perform the MetaFrame XP installation, or click Cancel to exit MetaFrame XP 1.0 Setup now.

## Citrix ICA Client Distribution Wizard

As shown in Figure 4.32, the *Citrix ICA Client Distribution Wizard* welcome screen appears and informs you of the next step in the process. This step requires 200MB of free space on the server if you are adding all of the client installation software to the server. Once you have chosen the path to the ICA Client files and clicked Next, as shown in Figure 4.33, the wizard will notify you that it is attempting to locate the files at the location you specified. If you are installing from CD-ROM, you will see the screen shown in Figure 4.34. At this point, the installation of the Client files will proceed. You can to cancel the installation of these files, but the ICA pass-through Client will still install.

**FIGURE 4.32** Citrix ICA Client Distribution Wizard welcome screen



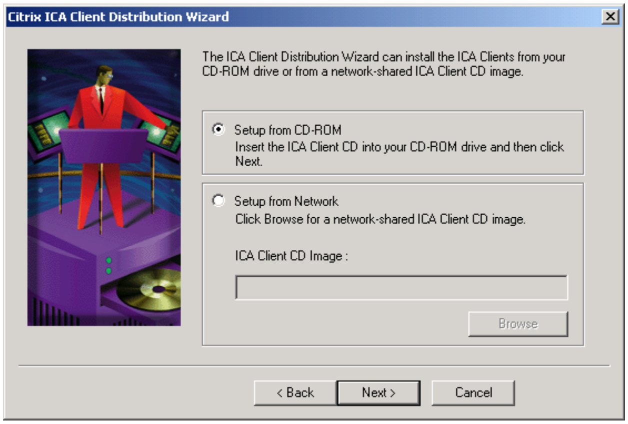
Citrix ICA Client Distribution Wizard

Welcome to the Citrix ICA Client Distribution Wizard. The wizard will populate the ICA Client Images and the ICA Client Update Database, and install/upgrade the Citrix ICA pass-through Client on the server.

Before proceeding, make sure that the Citrix server has no active ICA sessions or users attempting ICA connections.

Click Cancel to exit the ICA Client Distribution Wizard. If you are in the process of installing MetaFrame XP on your server, MetaFrame XP Setup resumes. You can run the ICA Client Distribution Wizard later from the Citrix program group on your server.

**FIGURE 4.33** ICA Client Distribution setup screen



Citrix ICA Client Distribution Wizard

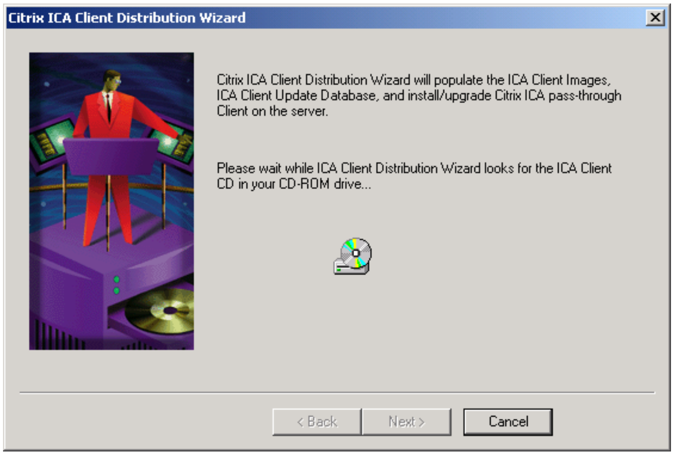
The ICA Client Distribution Wizard can install the ICA Clients from your CD-ROM drive or from a network-shared ICA Client CD image.

● Setup from CD-ROM
Insert the ICA Client CD into your CD-ROM drive and then click Next.

○ Setup from Network
Click Browse for a network-shared ICA Client CD image.

ICA Client CD Image :

**FIGURE 4.34** Locating the ICA Client files



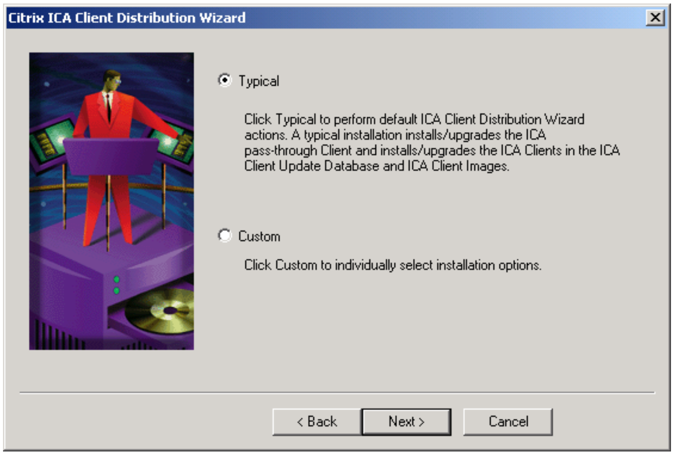
Citrix ICA Client Distribution Wizard

Citrix ICA Client Distribution Wizard will populate the ICA Client Images, ICA Client Update Database, and install/upgrade Citrix ICA pass-through Client on the server.

Please wait while ICA Client Distribution Wizard looks for the ICA Client CD in your CD-ROM drive...

Once it locates the files, Setup prompts you to choose whether you want all of the ICA Client types installed or want to select the clients to install. The two options available at this point for *ICA Client Installation* are shown in Figure 4.35: Typical and Custom. The Typical option installs all of the ICA Client files, while the Custom option allows you to select the Client types you want to use in your environment. Choosing the Custom option brings up more choices for *ICA Client Distribution*, the first of which is seen in Figure 4.36.

**FIGURE 4.35** ICA Client installation choices



Citrix ICA Client Distribution Wizard

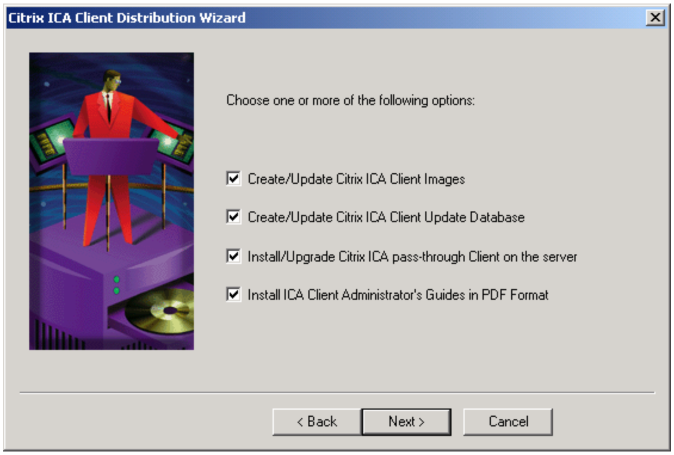
● Typical

Click Typical to perform default ICA Client Distribution Wizard actions. A typical installation installs/upgrades the ICA pass-through Client and installs/upgrades the ICA Clients in the ICA Client Update Database and ICA Client Images.

○ Custom

Click Custom to individually select installation options.

**FIGURE 4.36** ICA Client distribution options



Choose one or more of the following options:

☑ Create/Update Citrix ICA Client Images

☑ Create/Update Citrix ICA Client Update Database

☑ Install/Upgrade Citrix ICA pass-through Client on the server

☑ Install ICA Client Administrator's Guides in PDF Format

If you select the first option, Create/Update Citrix ICA Client Images, another screen will appear, shown in Figure 4.37, allowing you to choose the Client images you want to install on your MetaFrame server. These images are copied to the `%systemroot%\System32\Clients\ICA` directory. Once they are installed, you can install the client on systems within your environment and create the ICA Client installation disks. The Client images available for installation are as follows:

- DOS
- Internet
  - Windows CE
  - Windows 3.*x*/9*x*, NT
  - Java
  - Macintosh
  - Unix
- Java
- Macintosh
- Unix
  - SunOS
  - Solaris 86

- Solaris
- SGI
- SCO
- Linux x86
- Linux ARM
- IBM
- HP
- DEC

Windows (3.*x*/9*x*/NT)

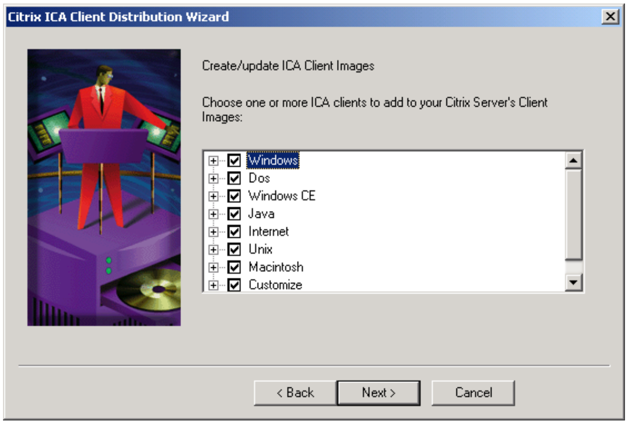
Windows CE

- x86
- SH3
- SH4
- PPC
- MIPS
- ARM

Customize

- ICA File Creator
- Customized Citrix ICA Client

**FIGURE 4.37** Create/Update ICA Client Images options



Citrix ICA Client Distribution Wizard

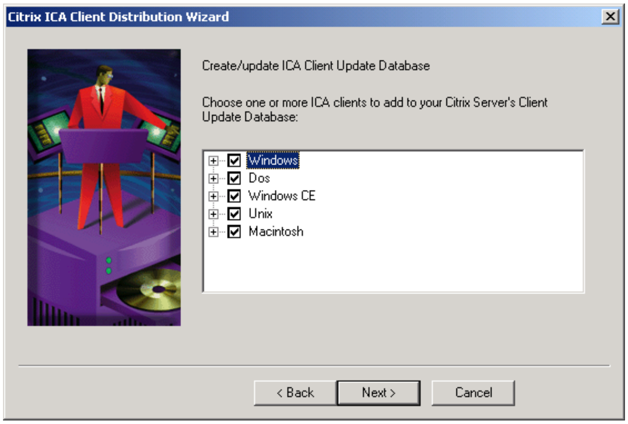
Create/update ICA Client Images

Choose one or more ICA clients to add to your Citrix Server's Client Images:

- ☑ Windows
- ☑ Dos
- ☑ Windows CE
- ☑ Java
- ☑ Internet
- ☑ Unix
- ☑ Macintosh
- ☑ Customize

Select the second option from the ICA Client installation options, and Setup will present you with the Create/Update ICA Client Update Database options screen, as seen in Figure 4.38. This database holds the updated Client images for use with the ICA Client Update Configuration utility. Any of the clients you choose from this screen are added to the database and are subsequently used to update the ICA Client software.

**FIGURE 4.38** Create/Update ICA Client Update Database options



Create/update ICA Client Update Database

Choose one or more ICA clients to add to your Citrix Server's Client Update Database:

- ☑ Windows
- ☑ Dos
- ☑ Windows CE
- ☑ Unix
- ☑ Macintosh

The third check box on the ICA Client distribution options screen allows you to upgrade or install the Citrix ICA pass-through Client on the server. This client is installed to allow those clients that cannot utilize Program Neighborhood to access a session that runs Program Neighborhood. With this functionality, all clients—not just the Java, NFuse, or Win32 clients—can take advantage of published applications.

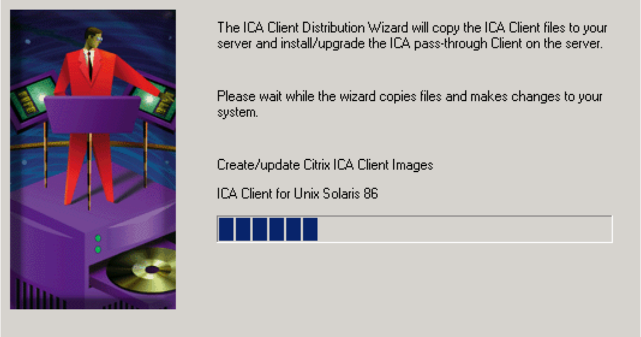
NOTE

For more information on the Citrix ICA pass-through Client, see Chapter 11, "Program Neighborhood."

Select the last check box, Install ICA Client Administrator's Guides In PDF Format, and Setup will install the documentation on the server for all of the clients you have chosen. Since the files are in PDF format, you must install Adobe Acrobat on any system that needs to access them. To conserve space, you can install these files on only one server.

After you click Next, the ICA Client Distribution Wizard progress screen appears, as shown in Figure 4.39, indicating how much has been installed on the server and how much remains. Once this process is complete, the database is updated, the pass-through Client is installed, and all of the documents are loaded onto the server.

**FIGURE 4.39** ICA Client installation progress



The ICA Client Distribution Wizard will copy the ICA Client files to your server and install/upgrade the ICA pass-through Client on the server.

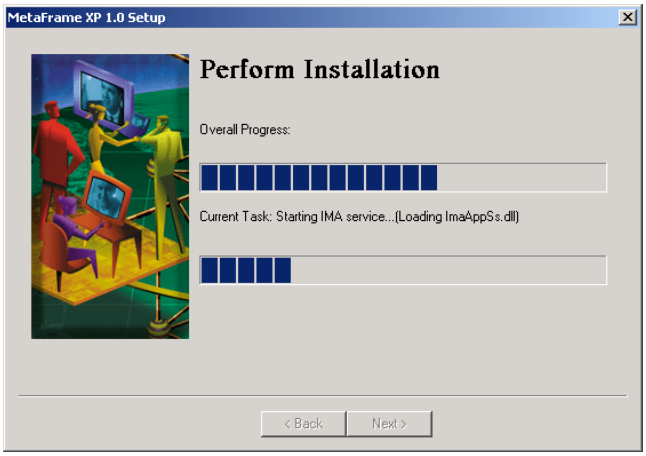
Please wait while the wizard copies files and makes changes to your system.

Create/update Citrix ICA Client Images

ICA Client for Unix Solaris 86

As the IMA service is started and the licensing database is activated, a progress indicator appears, as shown in Figure 4.40. After everything in this phase completes, you will see the licensing screen.

**FIGURE 4.40** Installation progress



MetaFrame XP 1.0 Setup

Perform Installation

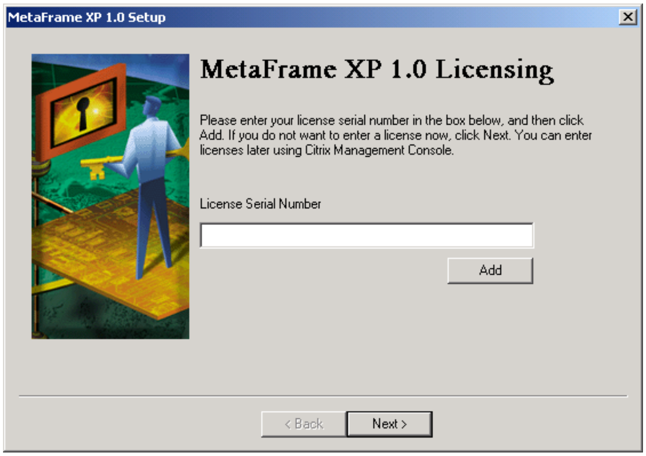
Overall Progress:

Current Task: Starting IMA service...(Loading ImaAppSs.dll)

## MetaFrame Licensing

Be prepared to have your license serial number available at this point. Even though MetaFrame's Setup will complete if you do not have a license serial number, you will not be able to create sessions until the product is licensed. Enter the number in the License Serial Number field, as shown in Figure 4.41. You can enter other connection licenses at this time, or you can enter them after Setup is complete. Click Next to continue.

**FIGURE 4.41** MetaFrame XP 1.0 Licensing screen



MetaFrame XP 1.0 Licensing

Please enter your license serial number in the box below, and then click Add. If you do not want to enter a license now, click Next. You can enter licenses later using Citrix Management Console.

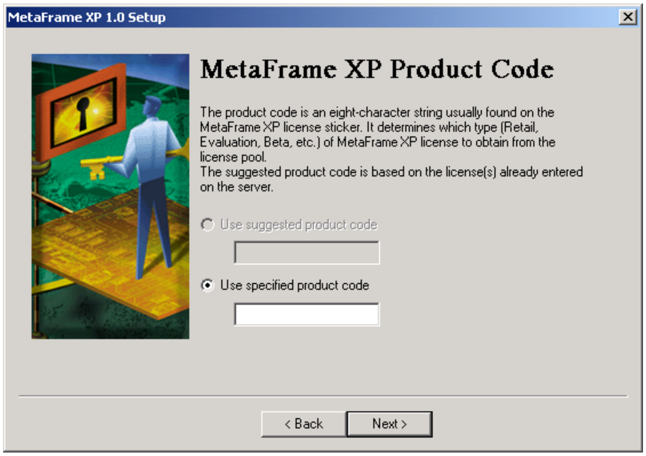
License Serial Number

After you enter the license numbers, you must provide the product code, as shown in Figure 4.42. You can use the suggested product code (Setup will use a code that is associated with the product you are implementing), or you can enter a code that has been provided to you. This information should also be included on your checklist. Click Next to continue.

After you enter all the information for the licensing, the system will commit the licensing to the data store. Setup will present you with the final screen, shown in Figure 4.43, informing you that it will now restart the system. At this point, the entire installation process is complete. Click the Restart button and the system will reboot.

Your installation is complete. Once the system reboots, the server is ready to accept connections. From this point, we will start looking at the tools available to us that allow administration of the server.

**FIGURE 4.42** MetaFrame XP Product Code screen



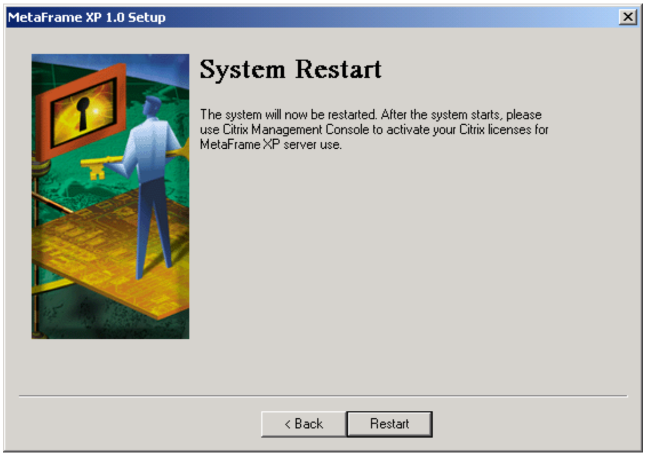
MetaFrame XP Product Code

The product code is an eight-character string usually found on the MetaFrame XP license sticker. It determines which type (Retail, Evaluation, Beta, etc.) of MetaFrame XP license to obtain from the license pool.
The suggested product code is based on the license(s) already entered on the server.

○ Use suggested product code

● Use specified product code

**FIGURE 4.43** System Restart screen



System Restart

The system will now be restarted. After the system starts, please use Citrix Management Console to activate your Citrix licenses for MetaFrame XP server use.

# Summary

Chapter 4 has brought us to the point where we have finally installed MetaFrame XP on our servers. We can simplify this process by following the checklist we created in Chapter 3. Even though the Setup Wizard makes the installation easier, we still have many options to decide upon. None of these should be taken lightly, as the performance of the server and the server farm depends on a successful installation. Choosing the data store database ahead of time and having it configured is essential; otherwise, the administrator will have to configure the database during the installation process, taking up more time. Also important to decide ahead of time are which clients to add to the server's database, whether or not to include documentation, and which licenses to add.

In the chapters that follow, we will look at the Citrix Management Console and other administrative tools used to configure and control our MetaFrame XP server.

# Exam Essentials

**Understand the steps required to install MetaFrame XP.** There are many steps required when performing a MetaFrame XP setup. The wizard presents the required information, but the administrator must know the appropriate settings to apply.

**Understand the implications of changing the default shadowing options.** If any of the shadowing options are changed, they are changed permanently. The only way to restore the shadowing options is to reinstall the server.

**Understand the data store database installation steps.** The data store database can be Microsoft Access, Microsoft SQL Server, or Oracle, but the setup is different for each. You should understand all of the setup options available and know how to configure MetaFrame XP to access each database type.

**Understand the Oracle database connectivity options.** Know the options necessary to connect to the Oracle ODBC-compliant database.

**Understand the SQL database connectivity options.** Know the options necessary to connect to the Microsoft SQL ODBC-compliant database.

**Understand the ICA Client database installation options.** When installing the ICA Client images, you should understand the implications of installing the images to the update database and how each of the clients can be added to the database during setup.

**Understand the options required to allow client connectivity to the server.** Understand how drive mapping is configured during setup and how to configure NFuse and the XML service.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

`autoroot.exe`

Citrix ICA Client Distribution Wizard

Citrix XML Service

ICA Client Distribution

ICA Client Installation

ICA session shadowing

MetaFrame XP License Agreement

# Exercises

The installation of Windows 2000 Server and Terminal Services must be completed before attempting this exercise.

In this exercise, you will install Citrix MetaFrame XP on the first server in the farm. We will assume that you will be using Microsoft Access as the data store.

**EXERCISE 4.1**

### Installing MetaFrame XP

1. Place the Citrix MetaFrame XP product CD-ROM in the server.
2. If autorun is enabled on your system, you will see a Citrix MetaFrame XP splash screen. If not, navigate to the root of the CD-ROM and launch `autoroot.exe`.

**EXERCISE 4.1 *(continued)***

Note: If you are installing from a shared directory on a distribution server, enter the UNC path (\\*server**share*) to the MetaFrame XP installation files and run `autoroot.exe`.

3. From the Citrix MetaFrame XP splash screen, select MetaFrame XP Setup.
4. If you receive an NFuse warning, click Yes. If IIS is not installed on the same server where you are installing MetaFrame XP, you will see this message.
5. On the MetaFrame XP License Agreement page, select I Agree.
6. On the Welcome screen, click Next.
7. On the Data Store configuration page, click Next.
8. Click the Create A New Server Farm radio button, and click Next.
9. Click the Use A Local Database For The Data Store radio button, and click Next.
10. Make sure there is a check in the box labeled Use Default Zone Name, and click Next.
11. If the Zone Name window pops up, type the name of the server farm here, and click Next.
12. In the Citrix Farm Administrator page, type **administrator**, and click Next.
13. In the Validate Information window, click Yes.
14. On the ICA Connections page, uncheck any protocols you do not want to use for ICA connections, and click Next. Remember that only protocols installed on the server before installation of MetaFrame will be available for selection. TCP/IP is the only protocol that cannot be unchecked.
15. On the TAPI Modem Setup page, click Next.
16. On the Shadowing page, click Next.
17. Leave the Allow Shadowing Of ICA Sessions On This Server radio button selected, and click Next.

**EXERCISE 4.1 *(continued)***

Warning: Do not select any of the options on this screen except for the Allow Shadowing Of ICA Sessions On This Server. If you choose any other options, the shadowing labs in later chapters will not function. The only way to reinstate the options is to reinstall MetaFrame XP on the server.

**18.** On the Drive Mapping page, click Next.

**19.** On the Server Drive Assignment page, make sure the box labeled Remap The Server Drives is not selected, and click Next.

**20.** On the XML Service screen, you can choose to share port 80 with IIS if IIS 4.0 or above is installed on the same server where you are installing MetaFrame XP. If IIS 4.0 or above is not installed on the server you are installing to, that choice is grayed out and you must select another port to use. If IIS is running on a different server, you should change this port. We'll use port 80. Click Next to continue.

Note: NFuse is installed at this point, and it might take a few moments to complete.

**21.** On the Perform Install screen, click Next.

**22.** When the Client Distribution Wizard window appears, click Next.

**23.** Place the ICA Clients CD in the CD-ROM tray, select Setup From CD-ROM, and click Next.

Note: If the client files are on the network, specify the path to the files, making sure there are no spaces in the path.

**24.** Choose Typical as the installation type for the clients, and click Next.

**25.** On the License Serial Number page, enter a valid license number, and click Add. When you have finished entering the serial numbers, click Next.

**26.** On the MetaFrame XP Product Code page, select the radio button for Use Suggested Product Code, and click Next.

**27.** On the System Restart window, select Restart.

In this exercise, you will install Citrix MetaFrame XP on a second server in the farm and point the data store to an existing data store. We will assume that you are using Microsoft Access as the data store.

**EXERCISE 4.2**

### Installing Citrix MetaFrame XP and Adding a Second Server to an Existing Farm

1. Place the Citrix MetaFrame XP product CD-ROM in the server.
2. If autorun is enabled on your system, you will see a Citrix MetaFrame XP splash screen. If not, navigate to the root of the CD-ROM and launch `autoroot.exe`.

   Note: If you are installing from a shared directory on a distribution server, enter the UNC path (\\*server*\*share*) to the MetaFrame XP installation files and run `autoroot.exe`.
3. From the Citrix MetaFrame XP splash screen, select MetaFrame XP Setup.
4. If you receive an NFuse warning, select Yes. If IIS is not installed on the same server where you are installing MetaFrame XP, you will see this message.
5. On the MetaFrame XP License agreement page, select I Agree.
6. On the Welcome screen, click Next.
7. On the Data Store configuration page, select Next.
8. Click the Join An Existing Server Farm radio button, and click Next.
9. Click the Connect To A Data Store Set Up Locally On Another Server radio button, and click Next.
10. On the Indirect Access screen, type in the name of the first server and leave the port as 2512. Then click Next.
11. On the Citrix Administrator Login page, keep the default entries, type in the administrator password, and click Next.
12. Click the check box labeled Use Default Zone Name, and click Next.

**EXERCISE 4.2** ***(continued)***

13. If the Zone Name window pops up, enter the name of the server farm, and click Next.

14. In the Citrix Farm Administrator page, type **administrator**, and click Next.

15. In the Validate Information window, click Yes.

16. On the ICA Connections page, uncheck any protocols you do not want to use for ICA connections, and click Next. Remember that only protocols installed on the server before the installation of MetaFrame will be available for selection. TCP/IP is the only protocol that cannot be unchecked.

17. On the TAPI Modem Setup page, click Next.

18. On the Shadowing page, click Next.

19. Click the radio button labeled Allow Shadowing Of ICA Sessions On This Server, and click Next.

    Warning: Do not select any of the options on this screen except for Allow Shadowing Of ICA Sessions On This Server. If you choose any other options, the shadowing labs in later chapters will not function. The only way to reinstate the options is to reinstall MetaFrame XP on the server.

20. On the Drive Mapping page, click Next.

21. On the Server Drive Assignment page, make sure the check box labeled Remap The Server Drives is not selected, and click Next.

22. On the XLM Service screen, if IIS 4.0 or above is installed on the same server where you are installing MetaFrame XP, you can share port 80 with IIS. If IIS 4.0 or above is not installed on the server you are installing to, that choice is grayed out and you must select another port to use. If IIS is running on a different server, you must change this port. We'll use port 8181. Enter **8181** in the text box, and click Next.

    Note: NFuse is installed at this point, and it might take a few moments to complete.

**EXERCISE 4.2** ***(continued)***

23. On the Perform Install screen, click Next.

24. When the Client Distribution Wizard window appears, click Next.

25. Place the ICA Clients CD in the CD-ROM tray, select Setup From CD-ROM, and click Next.

    Note: If the client files are on the network, specify the path to the files, making sure there are no spaces in the path.

26. Choose Typical as the installation type for the clients, and click Next.

27. On the License Serial Number page, enter a valid license number, and click Add. When you have finished entering serial numbers, click Next.

28. On the MetaFrame XP Product Code page, select the radio button for Use Suggested Product Code, and click Next.

29. On the System Restart window, select Restart.

# Review Questions

1. If you are installing MetaFrame XP from a network share point, what program is used to initiate the install?

   **A.** `autoboot.exe`

   **B.** `autoexec.exe`

   **C.** `autoroot.exe`

   **D.** `autorun.exe`

2. Which of the following database types is not allowed for use as the data store?

   **A.** Microsoft SQL Server

   **B.** Microsoft Access

   **C.** Oracle

   **D.** dBASE 4

3. When changing the network library configuration within the client configuration while setting up the ODBC database, what two protocols are allowed?

   **A.** AppleTalk

   **B.** Named Pipes

   **C.** NWLink

   **D.** TCP/IP

4. If you have servers on each side of a WAN, what protocol would you choose for use in the network library configuration?

   **A.** AppleTalk

   **B.** Named Pipes

   **C.** NWLink

   **D.** TCP/IP

5. When configuring the server farm name, what requirement must you meet if you need interoperability with a MetaFrame 1.8 server farm?

   A. Both farms names must be in all capital letters.

   B. Both farm names must be in all lowercase letters.

   C. Both farm names can only contain letters—no numbers or special characters.

   D. Both farm names must be identical.

6. When you select the Citrix Administrator account, what special rights are assigned to the account?

   A. The account will have the ability to run the CMC and configure the server farm and all servers in the farm.

   B. The account will be made a member of the Domain Admins group for the domain of which the MetaFrame XP server is a member.

   C. The account will be made a member of the server's local Administrators group.

   D. The account will be made a member of the server's Power Users group.

7. Which mode must the server farm be in when MetaFrame 1.8 servers are used in conjunction with MetaFrame XP?

   A. Integrated

   B. Mixed

   C. Native

   D. Synchronized

8. Which protocol cannot be deselected in the ICA Network Connections screen?

   A. IPX

   B. NetBIOS

   C. SPX

   D. TCP/IP

9. During setup you are allowed to choose the protocols that will be used by the server. What is created during the installation after you choose the protocols?

   **A.** Connection port

   **B.** Data port

   **C.** Listener port

   **D.** Protocol port

10. When attempting to add modems, the administrator installing MetaFrame XP has which options available?

    **A.** Only those modems that are not used for RAS are displayed as available for use as async connections.

    **B.** All modems are displayed, and the administrator may choose to share the modem between RAS and async connections.

    **C.** All modems are displayed, and the administrator may choose to disconnect the modem from use with RAS and enable it for use as an async connection.

    **D.** No modems are displayed, the administrator must configure a modem connection from this screen, and the modem must be added later.

11. Which of the following statements is true if shadowing restrictions are set during install of MetaFrame XP?

    **A.** These settings will affect this server as soon as setup is complete, but a Citrix administrator may change them in Citrix Management Console at a later time.

    **B.** These settings will affect this server as soon as setup is complete, but a Citrix administrator may change them in Published Applications Manager at a later time.

    **C.** These settings will affect this server as soon as setup is complete, but a Citrix administrator may change them in Citrix Connection Configuration at a later time.

    **D.** These settings will affect this server as soon as setup is complete, and they cannot be modified without reinstalling the MetaFrame XP software.

**12.** What are the default drive mappings? (Choose all that apply.)

**A.** The client drives are mapped with the first drive mapped as C:, and the drive letters increase for each drive on the client system.

**B.** The client drives are mapped with the first drive mapped as V:, and the drive letters decrease for each drive on the client system.

**C.** The server drives are mapped with the first drive mapped as C:, and the drive letters increase for each drive on the client system.

**D.** The server drives are mapped with the first drive mapped as M:, and the drive letters increase for each drive on the client system.

**13.** During the install, if IIS is installed on the same server where MetaFrame XP is installed, what is the default setting for the XML port?

**A.** 21

**B.** 80

**C.** 443

**D.** 8080

**14.** How much free space is necessary on the server drive where the Client images will be installed?

**A.** 100MB

**B.** 150MB

**C.** 200MB

**D.** 250MB

**15.** If you do not have a product license to enter during setup, what occurs?

**A.** Setup continues, but the MetaFrame services will fail after the first reboot. Reinstallation of MetaFrame XP is required at this point.

**B.** Setup continues, but the server will refuse any ICA connections until a valid product license is entered.

**C.** Setup will not continue until you provide a valid product code.

**D.** Setup will provide a temporary license and you can use the server for 35 days before having to supply a valid product license.

**16.** You are installing MetaFrame XP on the first server in your MetaFrame XP server farm that will be used in a load-balanced environment with other servers in a MetaFrame 1.8 server farm. You want to use Microsoft Access as the database server for the data store. Which options should you choose during the setup? (Choose all that apply.)

**A.** Create A New Farm.

**B.** Join An Existing Farm.

**C.** Use A Local Database For The Data Store.

**D.** Use A Third Party Database For The Data Store.

**17.** You are installing MetaFrame XP on the first server in your MetaFrame XP server farm that will be used in a load-balanced environment with other servers in a MetaFrame 1.8 server farm. You want to use Microsoft SQL 2000 Server as the database server for the data store. Which options should you choose during the setup? (Choose all that apply.)

**A.** Create A New Farm.

**B.** Join An Existing Farm.

**C.** Use A Local Database For The Data Store.

**D.** Use A Third Party Database For The Data Store.

**18.** You have a small office and have purchased MetaFrame XP for a Windows 2000 Server running Terminal Services. You do not have any other MetaFrame servers. You want to use the easiest method to install the data store. What option do you choose?

**A.** Use A Local Database For The Data Store.

**B.** Use A Third Party Database For The Data Store.

**C.** Direct Data Store Connection.

**D.** Connect To Data Store Set Up Locally On Another Computer.

19. If you choose to use the default zone name during setup, what will the zone name be?

    A. The same as the name of the server

    B. The same as the domain or workgroup of which the server is a member

    C. The same as the IP address of the server

    D. The same as the subnet ID on which the server resides

20. If applications were previously installed on a Microsoft Windows 2000 Server running Terminal Services, and during the installation of MetaFrame XP you chose to remap the server drives, what will you need to do to those previously installed applications?

    A. Nothing. The applications will not be affected.

    B. You will need to update the application drive access information within the Registry before the application will function.

    C. You will need to reinstall the applications in order for the applications to function correctly after setup.

    D. You will need to run the application's compatibility script to correct the drive mapping.

# Answers to Review Questions

1. C. When running the installation from a network share, or if the CD-ROM drive does not support autorun, you will need to run the `autoroot.exe` file. This file examines the server and determines what operating system is loaded on the server. It will then execute the appropriate Setup program for either Windows NT Server 4.0, Terminal Server Edition or Windows 2000 Server.

2. D. Microsoft Access, Microsoft SQL Server, and Oracle are all ODBC-compliant databases that are supported for use as the data store for the server farm.

3. B, D. When connecting to a data store database hosted on a SQL Server, you have the option of using Named Pipes or TCP/IP. The other options available are AppleTalk, MultiProtocol, Banyan VINES, NWLink, IPX/SPX, and DECNet.

4. D. Of the two protocol choices available, Named Pipes and TCP/IP, only TCP/IP will function in a WAN environment. Named Pipes relies upon NetBIOS, which will not work, by default, in a WAN situation.

5. D. If you create a MetaFrame XP server farm that will interoperate with a MetaFrame 1.8 server farm, the farm names must be identical to one another. If the names match, the IMA service will then act as the master browser for the MetaFrame 1.8 server farm.

6. A. The account you enter as the Administrator account during the installation of MetaFrame XP is added to the Citrix Administrators group and will have the ability to run the CMC and control the MetaFrame resources in the server farm. Other administrators may be added later, but this is the default administrator with full Read-Write control.

7. B. Mixed mode allows the server farm to interoperate with MetaFrame 1.8 servers by using the IMA service as the browser service for those systems. Native mode is used when no MetaFrame 1.8 servers are used.

8. D. TCP/IP is the default protocol for MetaFrame XP and cannot be deselected during setup of the server. In addition, there will always be at least one listener port created, the one for TCP/IP.

**9.** C. Every protocol that is chosen for use during the installation of MetaFrame XP has an associated listener port created for it. TCP/IP always has a listener port created for it since it is the default protocol and cannot be deselected.

**10.** A. If a modem is already configured for use by the RAS server, it will not be displayed within the TAPI Modem Setup screen. The administrator will be able to configure only the modems that are not associated with RAS.

**11.** D. Any changes you make to ICA Session Shadowing that restrict the shadowing setting are applied as MetaFrame XP is installed and are not reversible without reinstalling MetaFrame XP.

**12.** B, C. By default, the client's drives are mapped as V:, U:, and they decrease for every drive on the client system. The server drives are mapped as C:, D:, and they increase for every drive on the server. The administrator may modify this configuration during setup.

**13.** B. The default option, if IIS is installed on the server where MetaFrame XP is being installed, is to share the same port as the World Wide Web service. If this option is accepted, an ISAPI extension is added to the IIS server, allowing both services to use port 80.

**14.** C. The Client images, if all of them are installed on the server and added to the client distribution database, will consume 200MB of hard drive space.

**15.** B. Setup will warn you that the license was invalid. Setup will continue and the MetaFrame XP server will start normally. However, it will not allow any connections until the product license is provided. This will not affect RDP connections provided through Terminal Services, but no MetaFrame functionality will be available.

**16.** A, C. Even though a MetaFrame 1.8 server farm exists, the MetaFrame XP server farm is a separate entity that works in conjunction with the MetaFrame 1.8 server farm. After choosing to create a new farm, you choose the Use A Local Database For The Data Store option to have Access automatically loaded and configured on your first server.

17. A, D. Even though a MetaFrame 1.8 server farm exists, the MetaFrame XP server farm is a separate entity that works in conjunction with the MetaFrame 1.8 server farm. After choosing to create a new farm, you choose the Use A Third Party Database For The Data Store option to have the Setup program prompt you for the information required to connect to the database.

18. A. When you select the Use A Local Database For The Data Store option, Microsoft Access is installed and configured automatically during setup.

19. D. The zone name will default to the subnet ID of the segment on which the server resides. You can specify your own zone name during setup, but the default is to use the subnet ID for the zone name.

20. C. If applications are already installed on the server when setup remaps the server's drives, the applications will need to be reinstalled in order to function.

Chapter

5

# Administration and the Citrix Management Console

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **4. MetaFrame XP Administration**

- 4a. Administering using the Citrix Management Console
- 4b. Identify Published Application, Server and Citrix Administrator Properties
- 4c. Understanding Citrix Management Console

We like the remote control so much that we've created one for nearly every electronic item we've built: television, satellite dish, VCR, DVD, stereo receiver, CD player, and tape deck. We even have remote controls to unlock our vehicles and start them up. As a matter of fact, we have remote controls for the stereos in our vehicles that are within arm's reach!

As administrators, we like to have our own variety of remotes. Loading management tools onto our desktop systems so that we can remotely control our computer systems has not only become a handy tool, in this age of wide area computing where our servers could be hundreds or even thousands of miles away, it has become a necessity. For example, if an administrator headquartered in Tulsa needed to travel to Chicago every time a configuration change was necessary, the company would incur heavy costs.

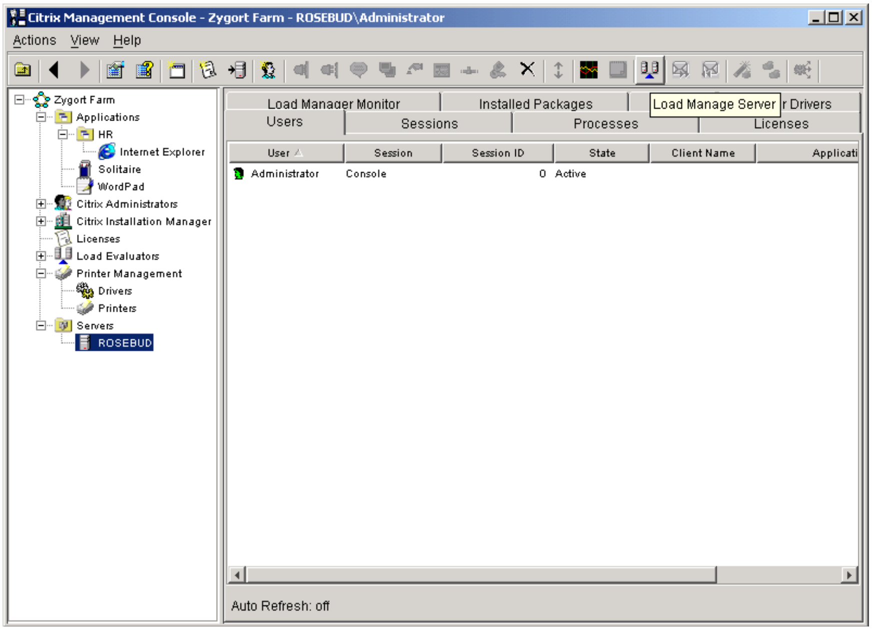
The Citrix Management Console (CMC) allows us to control our server resources in the server farm from one centralized tool. But not only does this tool give us the ability to remotely manage our systems, it has an added benefit. Just like those fancy universal remotes, it combines several tools into one management tool. Of course, we can appreciate having all of our favorite tools in one. How many times have you sat with four or five remotes in your lap trying to control the television, DVD player, stereo, and satellite dish or cable all at the same time? In this chapter, we will look at the functionality of the Citrix Management Console and discuss its importance in the MetaFrame XP server farm.

# Introduction to Citrix Management Console

When developing the Citrix Management Console, Citrix Systems listened to administrators when they said that they wanted all of the management tools in one. Within this one tool, we have the ability to manage and monitor nearly every aspect of our MetaFrame XP servers and server farm. Since we now have a centralized data store, the Citrix Management Console actually taps into the information held in the data store and presents the information in a unified console. From the administrator's viewpoint, nearly everything required to manage their farm is at their fingertips.

Citrix Management Console displays information based on the features installed on your MetaFrame XP server. If you have installed MetaFrame XPa, for example, Load Manager is displayed, as shown in Figure 5.1. If you have installed MetaFrame XPe and loaded Installation Manager, Resource Manager, or Network Manager, those items will be displayed.

**FIGURE 5.1** Citrix Management Console with Load Manager installed



| User | Session | Session ID | State | Client Name | Applicati |
|---|---|---|---|---|---|
| Administrator | Console | 0 | Active | | |

Auto Refresh: off

Citrix Management Console is loaded by default on every MetaFrame XP server, but it is not limited to the MetaFrame XP server alone. As with any good management tool, it is installable on client machines as long as they meet the requirements of the tool. In this case, the requirements are as follows:

- Windows NT 4.0 or Windows 2000 platform
- Sun Java Runtime Engine 1.3 (JRE 1.3) or later

When installing Citrix Management Console on an administrator's workstation, you will need to load the MetaFrame XP server CD into the workstation or run the `autoroot.exe` program from a network share point. When the splash screen appears, select the option to install Citrix Management Console. If Setup detects that the workstation does not have JRE 1.3 or later loaded, it will give you the option to load it. On those computers that already have another version of JRE installed, the installation process will load JRE 1.3 in a separate directory and allow the original version to function as before.

Once installed on a server or client workstation, Citrix Management Console is able to perform many administrative functions. A few of the actions that you can perform on a server farm from Citrix Management Console are shown here:

- Configure server and farm settings from any connected workstation.
- View information about *current sessions*, *users*, and *processes*.
- Set up and manage printers for ICA Clients.
- *Publish applications* and monitor application usage.
- Enter, activate, and assign MetaFrame XP licenses.
- Monitor, reset, disconnect, and reconnect ICA Client sessions.
- Send messages to ICA Client users and shadow their sessions.

The Citrix Management Console consists of two panes. The pane on the left contains the nodes used to administer the servers and the server farm, and the pane on the right contains the actual configuration objects. By default, the following nodes are available:

**Farm node** The *Farm node* contains the name of the farm and is the area where global settings are made.

**Applications node** The *Applications node* lists published applications and the settings used to control them.

**Citrix Administrators node** The *Citrix Administrators node* contains the accounts that have administrative control in the farm and shows the level of control they are allowed.

**Licenses node** The *Licenses node* lists all licenses installed in the farm.

**Load Evaluators node** The *Load Evaluators node* contains the load-balancing criteria for the servers in the server farm.

**Printer Management node** The *Printer Management node* contains all of the printers and print drivers installed in the server farm.

**Servers node** The *Servers node* contains all of the servers in the farm and allows the configuration of each one.

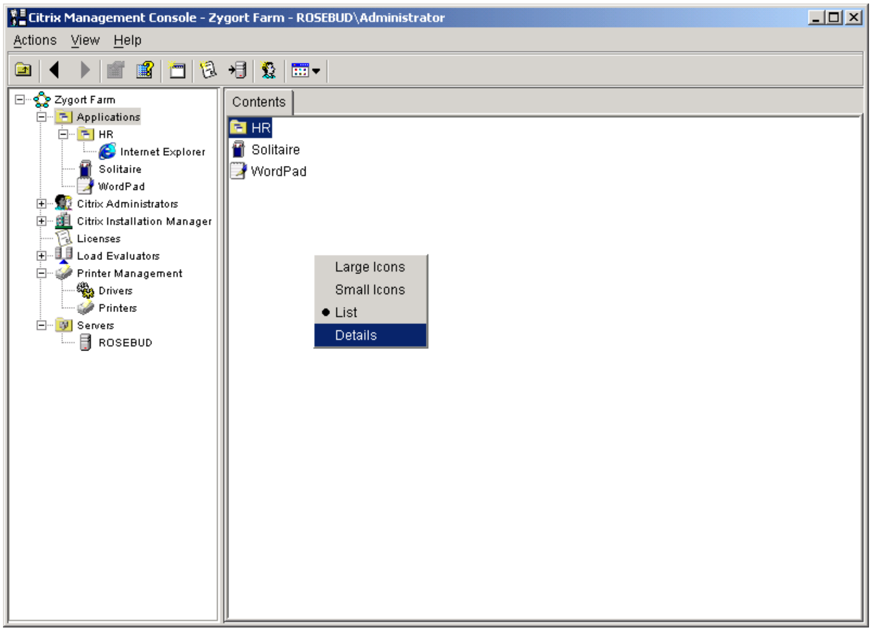
# The Tabs

From within each of these nodes, you can view and modify information concerning objects within the server farm. The node or object you select in the left-hand pane dictates the options available in the right-hand pane. The information is organized by the use of tabs. Let's look at each tab closely.

## Contents Tab

The *Contents tab* appears in every node with the exception of the Licenses node. Use this tab to display lower-level nodes and objects. You can view any object by double-clicking it. To see additional information for the objects in the Contents tab, right-click anywhere in the Contents tab and select Details from the context menu, as shown in Figure 5.2. Doing so displays other columns containing data about the objects. Unfortunately, this is only a short-term view. Once you select another object or node, the view resets itself to List. All other views, including Large Icons, Small Icons, and List, remain as the view of choice, but as soon as you select Details and then move to another object or node, List becomes the view type.

**FIGURE 5.2** Selecting the Details view



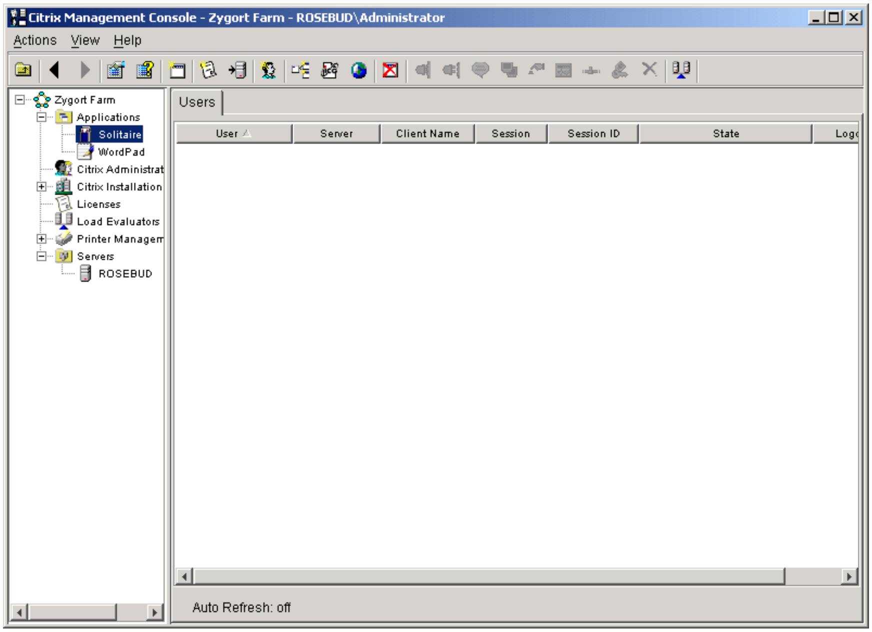
When you select Details view, the following columns may be available in the Contents tab. Not all of the nodes contain all of these columns.

| Column | Function |
|---|---|
| Name | Available wherever the Contents tabs are located, it identifies the name of the nodes or objects within the currently selected node. |
| Type | In the Applications and Farm nodes, it identifies the object. In the Servers node, it identifies the operating system of the MetaFrame XP server. |
| Folder | Found in the Applications node, it identifies the location of a published application. |
| Status | Found in the Applications node, it indicates whether or not the published application is enabled for use. |
| User Connection Type | Found in the Applications node, it identifies whether a published application requires an account to access it or whether it can be accessed anonymously. |
| Required Encryption | Found in the Applications node, it indicates the level of encryption required by a client to access a published application. |
| Privilege | Found in the Citrix Administrators node, it identifies whether a Citrix administrator has Read-Write or Read-Only privileges when using Citrix Management Console. |
| TCP/IP Address | Found in the Servers node, it identifies the server's TCP/IP address. |
| Connected | Found in the Servers node, it reveals the number of connections made to the server. |

## Users Tab

When you select an application from within the Applications node, the *Users tab* is available so that you can view the status of the users connected to a server utilizing an application. From here, you can determine how long a user has been connected, which sessions have been disconnected, and which connection types are used to access a published application. Select the application object to see the User, Server, Client Name, Session, Session ID, State, and Logon Time columns, as shown in Figure 5.3. You can also find this tab in the Servers node and for any of the server objects. When you view the columns from the Servers node or by selecting a server object, you will find the Applications column along with all the columns previously mentioned with application objects.

**FIGURE 5.3** The Users tab



Auto Refresh: off

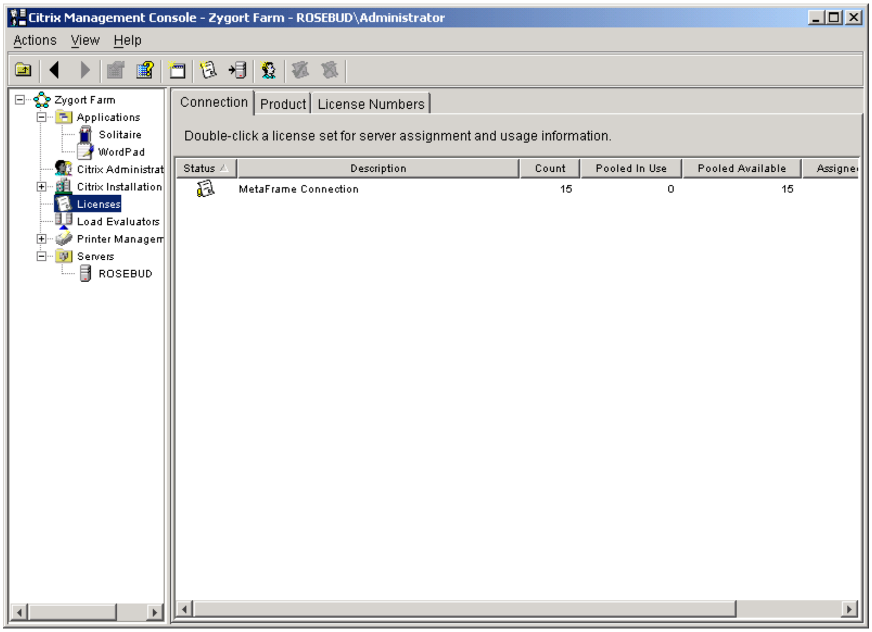
The Users tab contains the following columns:

| Column | Function |
|---|---|
| User | Identifies the account used to start the session and access the published application. |
| Server | Names the server on which the published application is running. Found in the Applications and Servers nodes. |
| Application | Lists the published applications currently running in an ICA session in the Servers node or for a server object. |
| Client Name | Shows the name of the device connected to the session and published application. |
| Session | Identifies the connection used. This is a combination of the connection type and the ICA session ID. |
| Session ID | Provides a unique identifier associated with a session. |
| State | Indicates whether the session accessing the published application is in Active or Disconnected state. |
| Logon Time | Displays the time the published application was started. |

## Connection Tab

The *Connection tab* is found only in the Licenses node. All of the MetaFrame XP connection licenses that have been installed for the server farm are located here, as shown in Figure 5.4. Note that when you add a connection license pack to the farm, each individual license number does not appear. Instead, the license pack type is listed along with the total number of licenses for that pack.

**FIGURE 5.4** The Connection tab



Double-click a license set for server assignment and usage information.

| Status | Description | Count | Pooled In Use | Pooled Available | Assigne |
|---|---|---|---|---|---|
| | MetaFrame Connection | 15 | 0 | 15 | |

The columns available are shown here:

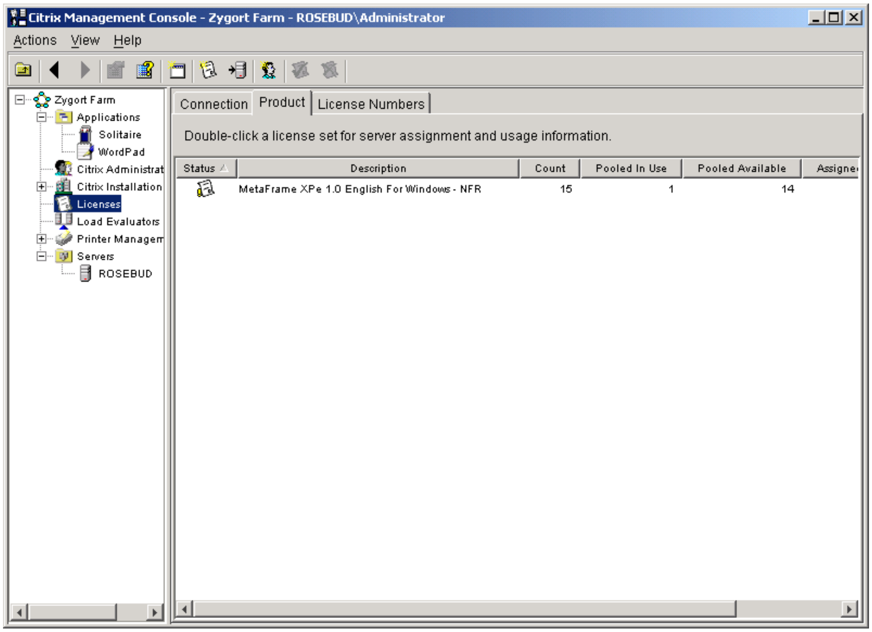
| Column | Function |
|---|---|
| Status | Denotes whether the license pack status is Activated, Evaluation, Unactivated, or Expired. |
| Description | Shows the name of the connection license pack. |
| Count | Indicates the total number of individual licenses that are available in this pack. |
| Pooled In Use | Indicates the number of licenses that are in use from ICA connections. |
| Pooled Available | Indicates the number of licenses that are not in use. |

| Column | Function |
|---|---|
| Assigned | Indicates the number of licenses from the set that are dedicated to individual servers and not available to the pool. |
| Assigned In Use | Indicates the number of licenses from the Assigned licenses that are currently in use. |

## Product Tab

The *Product tab* is found only in the Licenses node. All product licenses are listed here. If you purchase and install MetaFrame XPe, for example, you will have an XPe license listed here, as shown in Figure 5.5. The same holds true for XPa and XPs.

**FIGURE 5.5** The Product tab



Citrix Management Console - Zygort Farm - ROSEBUD\Administrator

Double-click a license set for server assignment and usage information.

| Status | Description | Count | Pooled In Use | Pooled Available | Assigne |
|---|---|---|---|---|---|
| | MetaFrame XPe 1.0 English For Windows - NFR | 15 | 1 | 14 | |

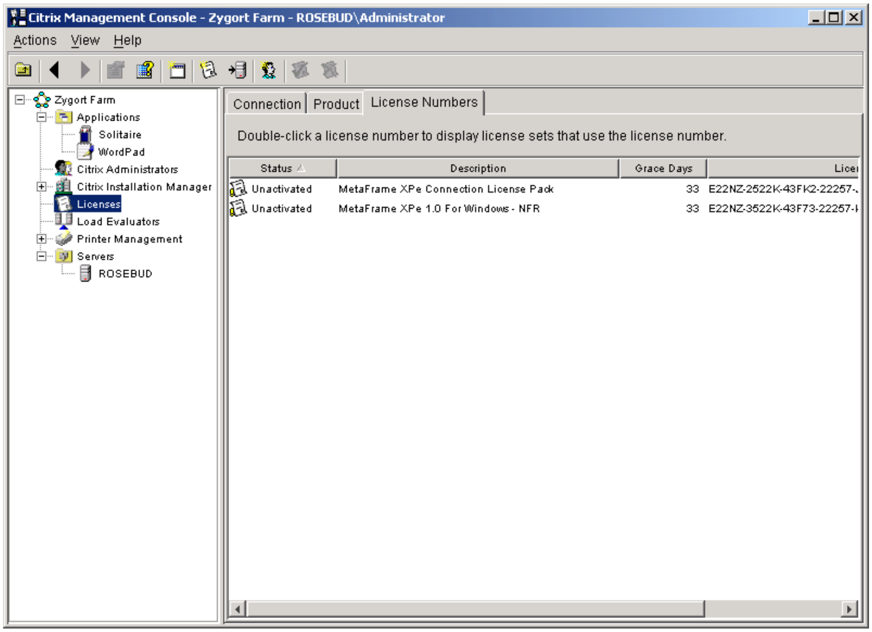
The columns available are listed here:

| Column | Function |
|---|---|
| Status | Denotes whether the license pack status is Activated, Evaluation, Unactivated, or Expired. |
| Description | Shows the name of the product license pack. |
| Count | Indicates the total number of server licenses that are available in this pack. |
| Pooled In Use | Indicates the number of licenses that are in use by servers in the farm. |
| Pooled Available | Indicates the number of licenses that are not in use. |
| Assigned | Indicates the number of licenses from the set that are dedicated to individual servers and not available to the pool. |
| Assigned In Use | Indicates the number of licenses from the Assigned licenses that are currently in use. |

## License Numbers Tab

Displayed when the Licenses node is selected, the License Numbers tab shows the licenses that have been entered into the server farm, whether or not they are activated for permanent use, and the grace period available for use if they are not activated, as shown in Figure 5.6.

**FIGURE 5.6** The License Numbers tab



Double-click a license number to display license sets that use the license number.

| Status | Description | Grace Days | Licei |
|---|---|---|---|
| Unactivated | MetaFrame XPe Connection License Pack | 33 | E22NZ-2522K-43FK2-22257-. |
| Unactivated | MetaFrame XPe 1.0 For Windows - NFR | 33 | E22NZ-3522K-43F73-22257-I |

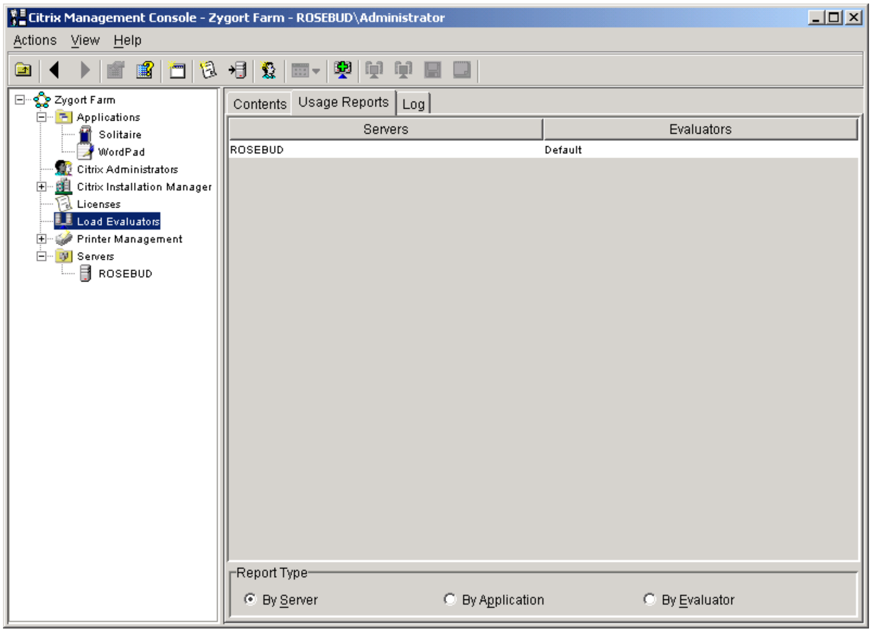
The following columns are available:

| Column | Function |
|---|---|
| Status | Displays whether the license is Activated, Unactivated, Evaluation, or Expired. |
| Description | Identifies the license type. |
| Grace Days | Indicates the number of days remaining before an unactivated license expires. |
| License Number | Shows the serial number of the license pack installed on the server. |

## Usage Reports Tab

Figure 5.7 shows the *Usage Reports tab*, which appears when you select the Load Evaluators node. The columns shown on this tab resolve the relationship between applications, servers, and the load evaluators assigned to each.

**FIGURE 5.7** The Usage Reports tab



| Servers | Evaluators |
|---|---|
| ROSEBUD | Default |

Report Type

● By Server ○ By Application ○ By Evaluator

The following columns are available:

| Column | Function |
|---|---|
| Applications | Indicates published applications that have load evaluators attached to them. |
| Evaluators | Shows the evaluators that are attached to the servers and the published applications within the farm. |
| Servers | Shows MetaFrame XP servers that have load evaluators attached to them. |

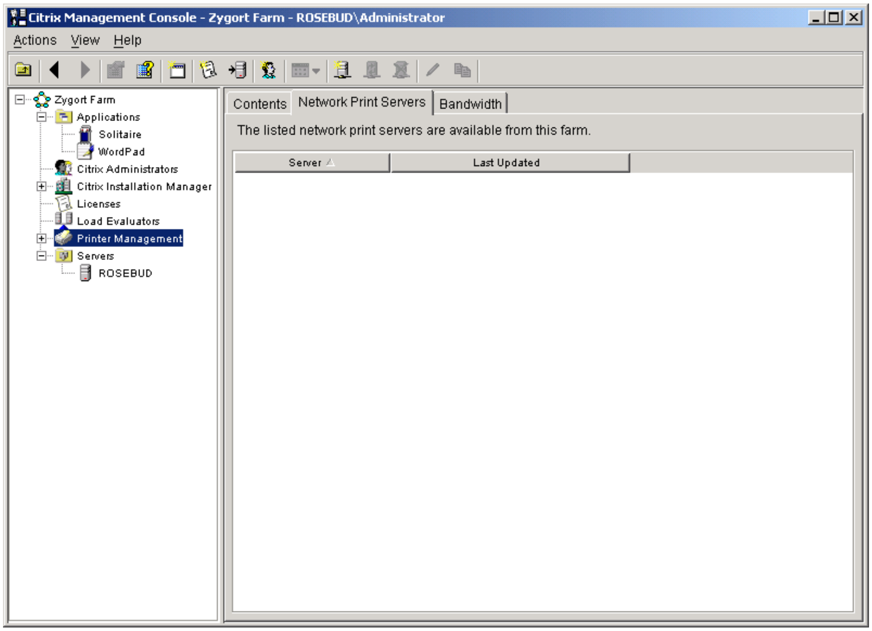
## Log Tab

The *Log tab* displays any load evaluator log entries. There are no additional columns on this screen, just the log file entries written from exceptions to the load evaluator information.

## Network Print Servers Tab

The Network Print Servers tab lists the print servers that are located outside the server farm, as shown in Figure 5.8. You must manually update all information on these servers.

**FIGURE 5.8** The Network Print Servers tab



The listed network print servers are available from this farm.

| Server | Last Updated |
|---|---|

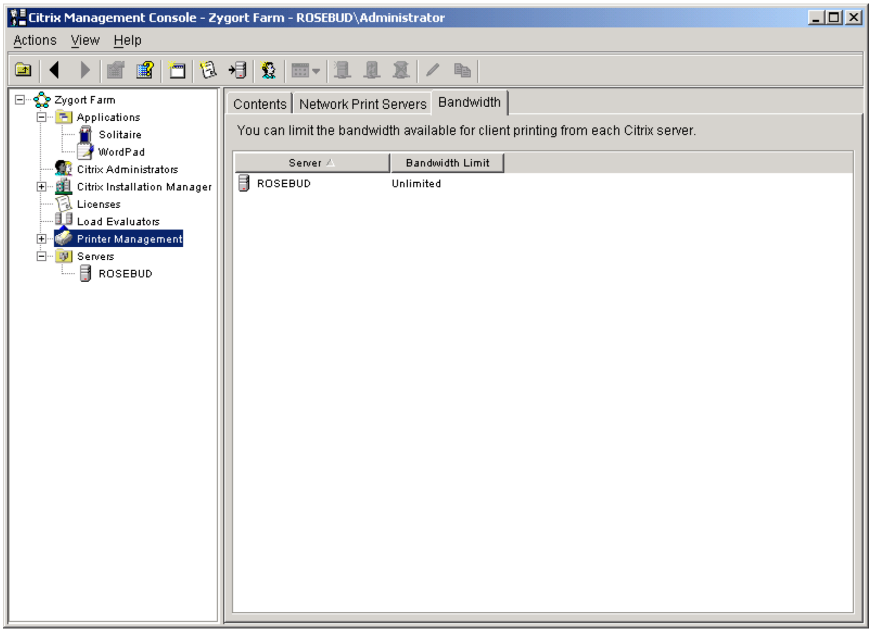
The following columns are available:

| Columns | Function |
|---|---|
| Server | Shows the name of the foreign print server. |
| Last Updated | Indicates the last time the print server information was manually updated. |

## Bandwidth Tab

Select the Printer Management node to view the Bandwidth tab, as shown in Figure 5.9. The same information can be found when you select the Servers node.

**FIGURE 5.9** The Bandwidth tab



You can limit the bandwidth available for client printing from each Citrix server.

| Server | Bandwidth Limit |
|---|---|
| ROSEBUD | Unlimited |

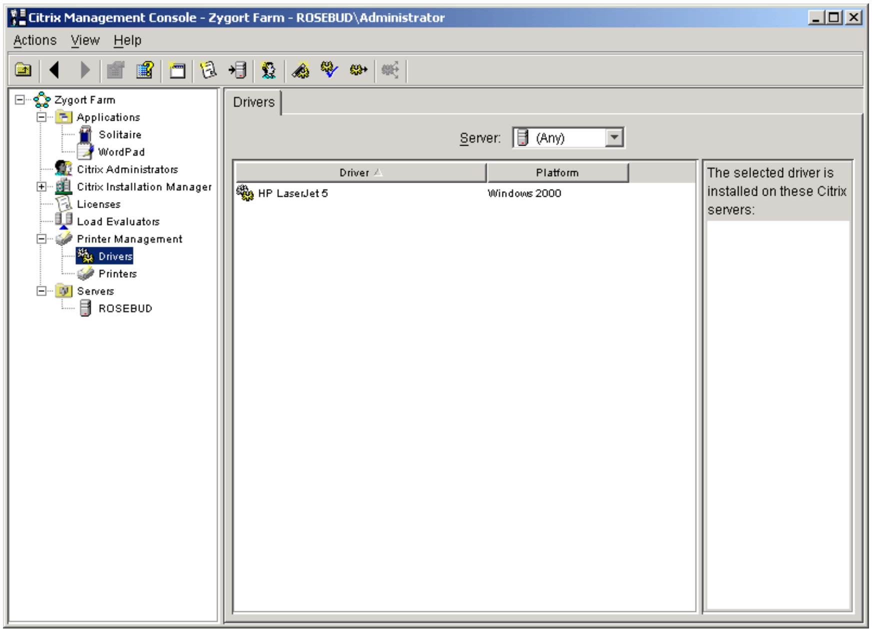
The following columns are available:

| Columns | Function |
|---|---|
| Server | Names the server used as a print server. |
| Bandwidth Limit | Indicates the bandwidth restriction placed on print jobs sent to the print server. |

## Drivers Tab

When you select the Drivers object from the Printer Management node, you will see the Drivers tab, as shown in Figure 5.10. This tab displays the print drivers installed in the server farm, the servers the driver is installed on, and the platform using the print driver.

**FIGURE 5.10** The Drivers tab



Server: (Any)

| Driver | Platform |
|---|---|
| HP LaserJet 5 | Windows 2000 |

The selected driver is installed on these Citrix servers:

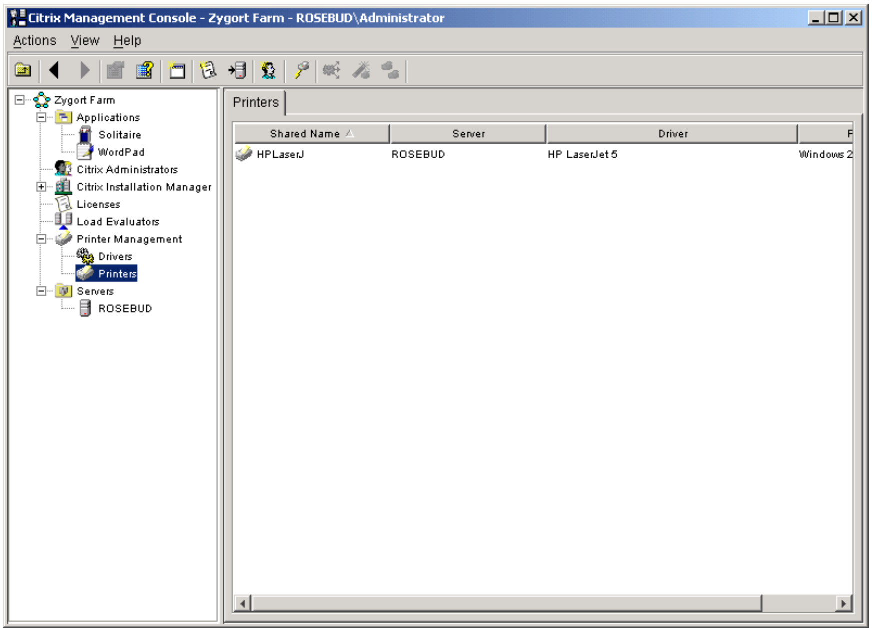
The following columns are available:

| Columns | Function |
|---|---|
| Driver | Indicates the driver used in the server farm. |
| Platform | Indicates the operating system the print driver is written for. |

## Printers Tab

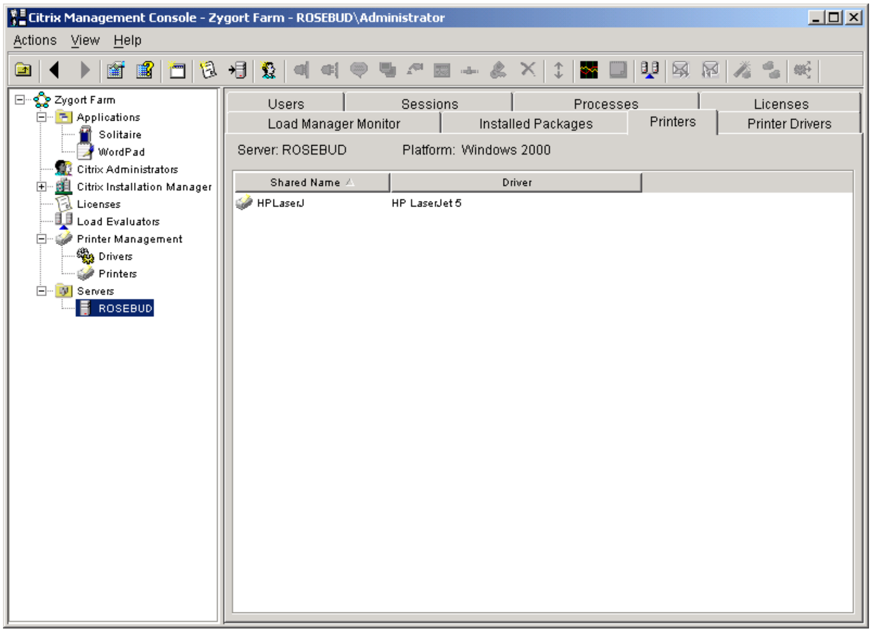
From the Printers object within the Printer Management node, the Printers tab displays the printers available in the server farm, as shown in Figure 5.11. From a server selected in the Servers node, the Printers tab lists all printers loaded on that server, as shown in Figure 5.12.

**FIGURE 5.11** The Printers tab in the Printer Management node



| Shared Name | Server | Driver | F |
|---|---|---|---|
| HPLaserJ | ROSEBUD | HP LaserJet 5 | Windows 2 |

**FIGURE 5.12** The Printers tab for a server object



Server: ROSEBUD Platform: Windows 2000

| Shared Name | Driver |
|---|---|
| HPLaserJ | HP LaserJet 5 |

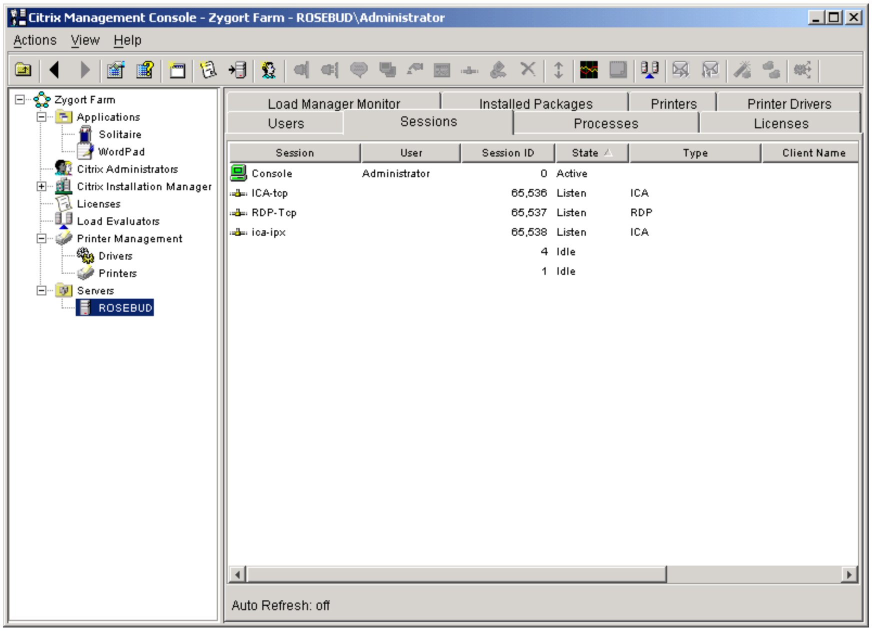
The following columns are available:

| Columns | Function |
|---|---|
| Shared Name | Shows the name used to access the printer from the network. |
| Server | Indicates the server that hosts the printer. |
| Driver | Indicates the print driver used to format print jobs. |
| Platform | Shows which operating system the print driver is written for. |

## Sessions Tab

When you select a server in the Servers node, the Sessions tab is available, as shown in Figure 5.13. On this tab, an administrator can view the session state and see who is connected to the server.

**FIGURE 5.13** The Sessions tab



| Session | User | Session ID | State | Type | Client Name |
|---|---|---|---|---|---|
| Console | Administrator | 0 | Active | | |
| ICA-tcp | | 65,536 | Listen | ICA | |
| RDP-Tcp | | 65,537 | Listen | RDP | |
| ica-ipx | | 65,538 | Listen | ICA | |
| | | 4 | Idle | | |
| | | 1 | Idle | | |

Auto Refresh: off

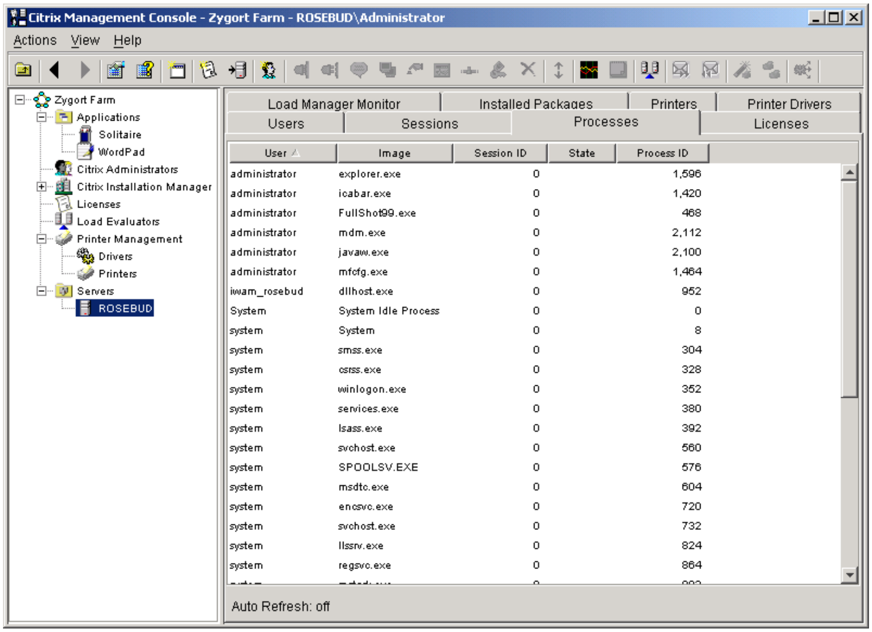
The following columns are available:

| Column | Function |
|---|---|
| Session | Shows the session name, which is a combination of the connection and an identifying number for each session. |
| User | Indicates the account used to initiate the session. |
| Session ID | Provides an identifying number for the session. |
| State | Shows the current state of the session: Active, Disconnected, Conn, ConnQ, Idle, or Listen. |
| Type | Indicates the protocol used to initiate the session: ICA or RDP (Remote Desktop Protocol). |
| Client Name | Provides the name of the device used to connect to the session. |
| Logon Time | Gives the timestamp used to identify the session start. |
| Application | Shows the name of a published application, if one was selected to start the session. |

## Processes Tab

When you select a server from the Servers node and choose the *Processes tab*, you will see the current processes running on that server. The user who is currently running the process in their session is listed here also, as shown in Figure 5.14.

**FIGURE 5.14** The Processes tab



| User | Image | Session ID | State | Process ID |
|---|---|---|---|---|
| administrator | explorer.exe | 0 | | 1,596 |
| administrator | icabar.exe | 0 | | 1,420 |
| administrator | FullShot99.exe | 0 | | 468 |
| administrator | mdm.exe | 0 | | 2,112 |
| administrator | javaw.exe | 0 | | 2,100 |
| administrator | mfcfg.exe | 0 | | 1,464 |
| iwam_rosebud | dllhost.exe | 0 | | 952 |
| System | System Idle Process | 0 | | 0 |
| system | System | 0 | | 8 |
| system | smss.exe | 0 | | 304 |
| system | csrss.exe | 0 | | 328 |
| system | winlogon.exe | 0 | | 352 |
| system | services.exe | 0 | | 380 |
| system | lsass.exe | 0 | | 392 |
| system | svchost.exe | 0 | | 560 |
| system | SPOOLSV.EXE | 0 | | 576 |
| system | msdtc.exe | 0 | | 604 |
| system | encsvc.exe | 0 | | 720 |
| system | svchost.exe | 0 | | 732 |
| system | llssrv.exe | 0 | | 824 |
| system | regsvc.exe | 0 | | 864 |

Auto Refresh: off

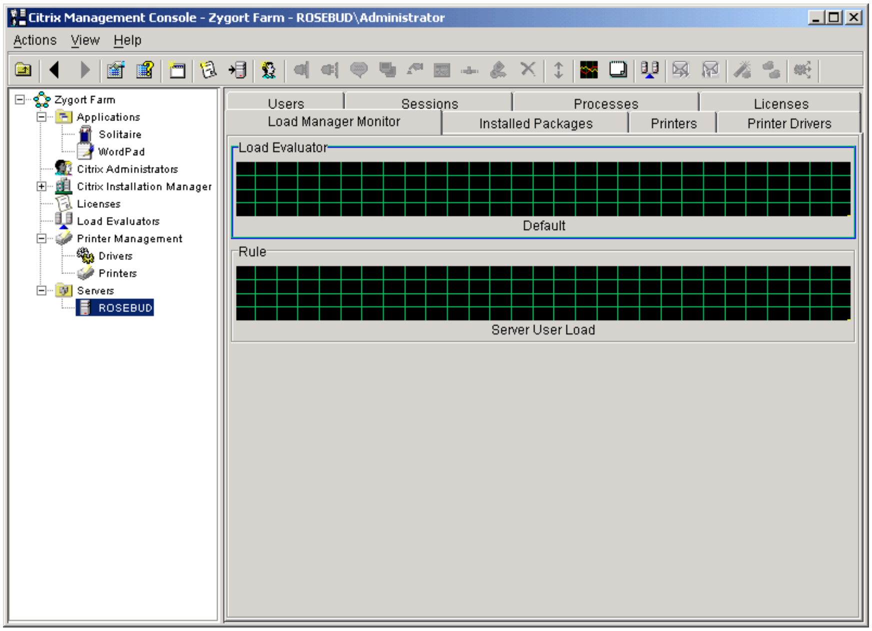
The following columns are available:

| Column | Function |
|---|---|
| User | Lists the user who initiated the session from which the process is running. |
| Image | Indicates the process filename. |
| Session ID | Shows the session in which the process is running. |
| State | Indicates the current state of the process. |
| Process ID | Provides an identification number for the operating system to identify the process. |

### Load Manager Monitor Tab

The *Load Manager Monitor* tab is available when you select a server in the Servers node. This tab displays the load evaluator and the associated rules, as shown in Figure 5.15.

**FIGURE 5.15** Load Manager Monitor tab



## The Icons

The icons shown at the top of the Citrix Management Console make it easier to perform tasks. They act as shortcuts to areas within the Citrix Management Console and other administrative tools, and you can use them to control your work environment. Table 5.1 shows each of the icons and its function.

**TABLE 5.1** Citrix Management Console Icons

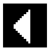
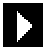
| Icon | Function |
|---|---|
| | Moves up one level in the node tree. |
|  | Moves back to the previously selected location in the tree. |
|  | Moves forward to the previously selected location in the tree. |
| | Shows the properties of the selected node or object. |
| | Displays help for Citrix Management Console. |
| | Opens the Application Publishing Wizard. |
| | Opens the Add License screen. |
| | Opens the New Assignment Wizard, allowing a license to be allocated to a server. |
| | Opens the Create Citrix Administrator screen. |
| | Deletes the selected Citrix Administrator. |
| | Opens the View menu, allowing you to change the information display in the right-hand pane. |
| | Creates a copy of the currently selected published application. |
| | Opens the Create ICA File Wizard. |
| | Opens the Create HTML File Wizard. |
| | Deletes the selected published application. |
| | Connects a Citrix Administrator to a disconnected or active session. The administrator must be currently in an ICA session to connect to a disconnected or active session and can be connected only to connections that were disconnected from the console. |
| | Disconnects an ICA session. |

**TABLE 5.1** Citrix Management Console Icons *(continued)*

| Icon | Function |
|---|---|
| 💬 | Opens the Send Message screen. |
| 🖥 | Opens the Start Shadowing screen. |
|  | Resets the ICA session and terminates all processes running within that session. |
|  | Opens the Session Status screen, which displays user and I/O information. |
|  | Displays session information, including processes and the client cache. |
|  | Logs a user off their current session. |
| ✕ | Ends a process running in a session. |
| ↕ | Opens the Change Assignment screen, allowing an administrator to adjust the license count allocated to a server. |
|  | Opens the Load Manager Monitor. |
|  | Opens the Load Manager screen, allowing you to edit, create, or delete the load evaluators. |
| ✓ | Opens the Activate License screen. |
| ✗ | Deletes the selected license. |
|  | Opens the New Evaluator screen, allowing you to create a load evaluator. |
| 🟩 | Enables the logging of load information. |
| 🟥 | Stops the logging of load information. |
| 💾 | Saves the load information log. |
| □ | Deletes the load information from the load evaluator display in Load Manager Monitor and clears the log. |

**TABLE 5.1** Citrix Management Console Icons *(continued)*

| Icon | Function |
|---|---|
| | Opens the Duplicate Evaluator screen, allowing an administrator to create a copy of the selected evaluator. |
| | Opens the Modify Evaluator screen, allowing an administrator to make changes to the selected evaluator. |
| | Deletes the selected load evaluator. |
| | Opens the Import Network Print Server screen, which allows an administrator to add a print server that is not part of the server farm. |
| | Updates information from imported print servers, which is not performed automatically; the information must be manually updated. |
| | Deletes the selected print server. |
| | Opens the Edit Bandwidth screen, which allows you to control print job bandwidth usage. |
| | Opens the Copy Bandwidth screen, which allows you to copy the settings from the currently selected server to another server. |
| | Opens the Auto-replication screen, which controls the print driver replication to other servers. |
| | Opens the Driver Compatibility screen, which controls which print drivers clients can use. |
| | Opens the Driver Mapping screen, which maps the client printer to a driver listed on the server. |
| | Forces replication of printer drivers to selected servers within the server farm. |
| | Opens the Client Printers screen, which controls the printer mappings for DOS and Windows CE clients. |

**TABLE 5.1** Citrix Management Console Icons *(continued)*

| Icon | Function |
|---|---|
| | Opens the Auto-creation Settings screen, which controls the printers that are automatically created for clients at session startup. |
| | Opens the Copy Auto-creation Settings screen, which copies the accounts that have permissions to use the selected printer to another printer. |

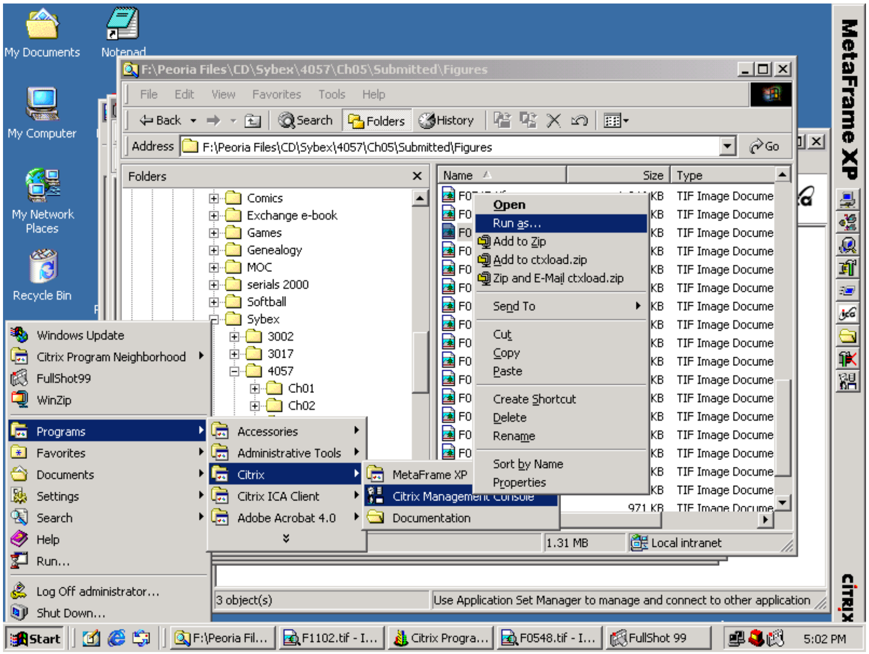
In the upcoming sections, we will be looking at these icon functions in greater detail. First, however, let's take a look at the Citrix Administrators node. All users who can initiate changes to servers and the server farm must be listed in this node, so you need to know how to add accounts for administrative use.

# Configuring Administrators

Simply installing the Citrix Management Console does not give you the right to use it. As you installed MetaFrame XP in the previous chapter, you were asked to supply an Administrator account for the server farm. Immediately after installation, this is the only account that is authorized to use the Citrix Management Console. You are not required to log on to the network with this account, however, just to use the Citrix Management Console. You may log on to the system using a regular user account, and when you access the Citrix Management Console, you are prompted to authenticate to the server farm.

While this may seem like a hassle at first (after all, we are starting to get used to that One Account, Single Logon theory), using an administrative account for everyday network activity may actually pose a security risk. The preferred method of network access is to use an account that does not have any administrative privileges for normal activities such as e-mail and report writing. When necessary, you can run the Citrix Management Console with an account configured as a *Citrix Administrator*, and if you are using Windows 2000, you can run applications with administrative privileges by using the Run As command. Almost any application can be started this way if you hold down the Shift key while right-clicking the application's shortcut. The Run As option will appear in the context menu, as shown in Figure 5.16.

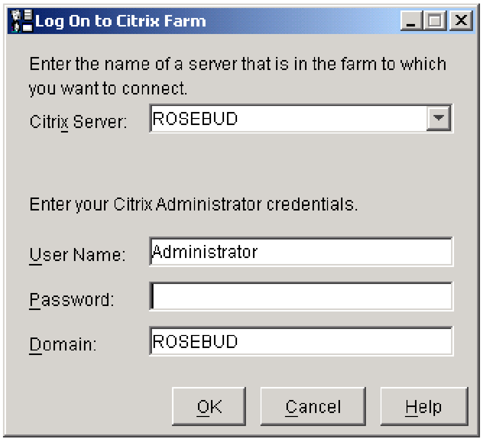
**FIGURE 5.16** The Run As option is available when you right-click a shortcut



To configure additional Citrix Administrators, you will need to start the Citrix Management Console using the account you specified as the Citrix Administrator during installation. To use the Citrix Management Console, go to Start ➢ Programs ➢ Citrix ➢ Citrix Management Console, or click the Citrix Management Console icon on the ICA toolbar. This brings up the authorization screen shown in Figure 5.17.

On the authorization screen, you have the choice of connecting to servers that check the server farm authorization list. This field is not completed by default. Only those servers that you have successfully connected to are displayed in subsequent connections. This is actually a nice security feature because anyone who loads Citrix Management Console on their system will not be able to receive an automatic update listing all of the servers in the server farm.

**FIGURE 5.17** The Citrix Management Console authorization screen



Log On to Citrix Farm

Enter the name of a server that is in the farm to which you want to connect.

Citrix Server: ROSEBUD

Enter your Citrix Administrator credentials.

User Name: Administrator

Password:

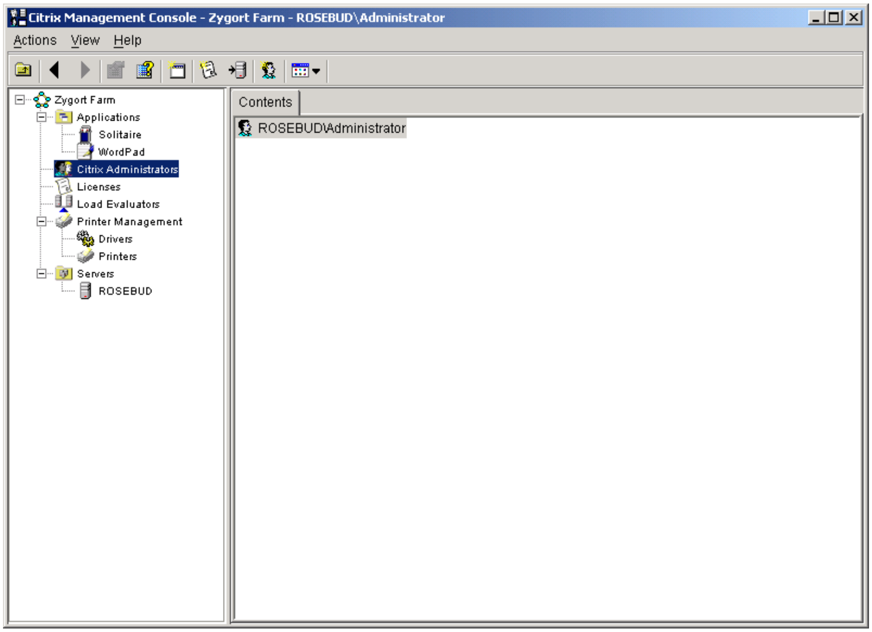
Domain: ROSEBUD

After entering the logon credentials, you will be presented with the configuration nodes for the server farm. Notice the Citrix Administrators component in the left-hand pane, as shown in Figure 5.18. When you select this node, the Citrix Administrators are displayed in the Contents tab in the right-hand pane. The only administrator that will appear at this point is the account we identified during setup. To add other accounts as Citrix Administrators, follow these steps:

1. Right-click the Citrix Administrators node.
2. Choose Add Citrix Administrator from the context menu.
3. In the dialog box that appears, choose where you want the accounts to come from, and select the users and groups you want to become Citrix Administrators.

That's all there is to it. Once added, those accounts have permission to start and use the Citrix Management Console. Use discretion while adding accounts as these accounts have absolute control over your server farm and the servers in it. Of course, you can choose to limit the abilities of some of the administrators by making them Read-Only.

**FIGURE 5.18** The Citrix Administrators node

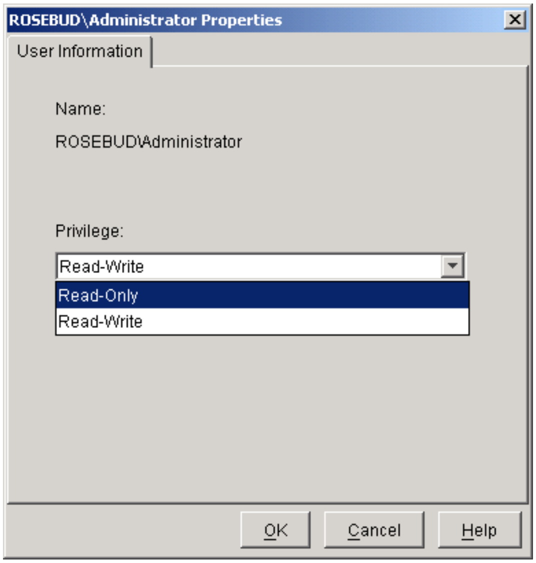


ROSEBUD\Administrator

Read-Only administrators are not allowed to perform certain functions from within the server farm. They are unable to modify or add any accounts to the Citrix Administrators group. They are even restricted from making changes to their own accounts. Of course, this is a good thing so that they cannot change their account from being Read-Only! To give a Citrix Administrator the Read-Only privilege, right-click the account from within the Citrix Administrators node and select Properties. You can then select the privilege level from the Properties sheet, as shown in Figure 5.19.

Read-Only administrators are also unable to run certain commands that affect ICA sessions, which prevents them from tampering with other sessions. Connect, Disconnect, Shadow, and Reset are all restricted commands. Imagine for a minute that an administrator, trying to ascertain information about the company or other employees, decided to shadow someone in the Human Resources department. While most of us think that the administrators we hire would have higher morals than that, restricting administrators' privileges does allow us to give them some authority without handing over the keys to the farm. Once we deem that they will make good administrators and we can trust them, we can change their accounts to Read-Write.

**FIGURE 5.19** Changing the administrator to Read-Only



ROSEBUD\Administrator Properties

Name:
ROSEBUD\Administrator

Privilege: Read-Write

## Real World Scenario

### Whom Do You Trust?

While we think that we can trust the administrators of our network, there are always those instances that make us sit back and think about the amount of power we hand over to individuals.

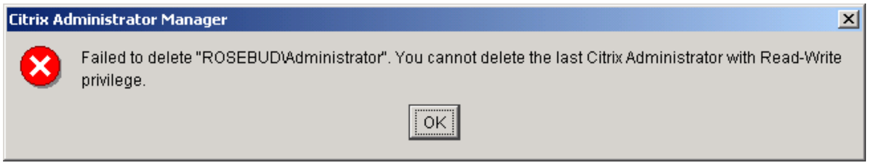
A large banking institution had MetaFrame installed so that the office staff could take advantage of the features we have been discussing. The information technology staff loved the centralized control they had over the users and applications, and management loved the money they saved when they found out they could replace computer systems with thin client terminals. They loved it until they found out what Jack was doing, that is.

Jack was an administrator from one of the branch locations. He had a small office and was located on site for the sole purpose of putting out fires when problems cropped up. Jack's account was added as a Citrix Administrator so that he would be allowed to shadow users and help them with their problems. But the ability to shadow was the problem.

As it turned out, Jack had changed the shadowing settings so that the users were not notified that they were being shadowed. He would then shadow the sessions of Human Resources personnel as they performed their daily duties. He became privy to sensitive information that he should not have been able to access. Of course, once he was discovered, he was quickly dismissed, and the bank locked down the administrative control of the servers a little tighter. But it took a hard slap in the face for the bank staff to realize what they had done wrong.

After adding accounts to the Citrix Administrator node and giving at least one account Read-Write control, you can remove any other account, even the initial account you assigned when you installed MetaFrame. The only restriction upon this node is that there has to be one account remaining that can modify accounts. You are allowed to delete any account from the list of administrators, until you are down to one last account with Read-Write privileges. Figure 5.20 displays the warning message you will receive if you try to remove the last account with Read-Write privileges.

**FIGURE 5.20** Last Citrix Administrator warning message



Citrix Administrator Manager

Failed to delete "ROSEBUD\Administrator". You cannot delete the last Citrix Administrator with Read-Write privilege.

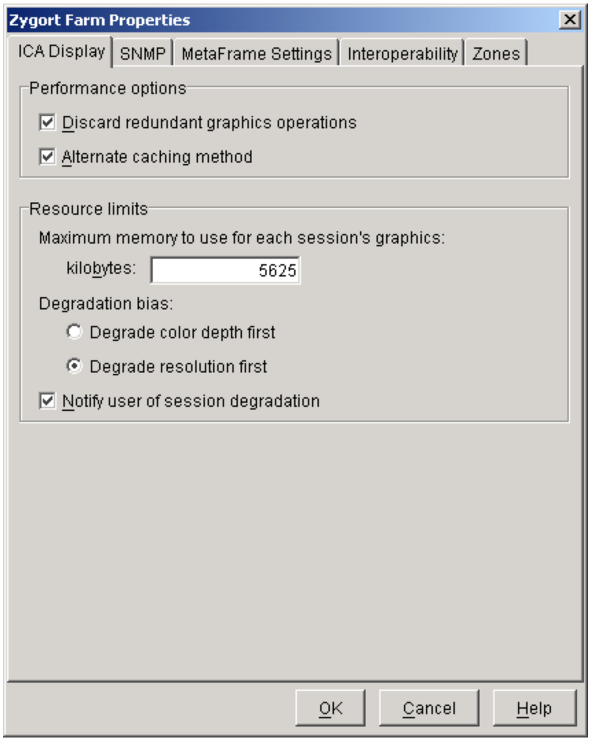
Now that you have added administrators and they can control the server farm and all of the servers in it, let's look at the other nodes in the Citrix Management Console. These nodes configure the way everything works, from the published applications to the printers to the communication channels.

## Global Farm Configuration

Once you have authenticated to a server in the server farm, you are presented with the nodes to configure your environment. The left pane of the Citrix Management Console shows the server farm name at the top of the list. This is where you make all of the global setting changes to the farm. Once you configure an option here, it is inherited throughout the farm. Individual settings configured at another area can override these settings, however.

If you right-click the Farm node and select Properties, the Properties sheet appears, as shown in Figure 5.21. The Properties sheet contains several tabs, each one controlling a different aspect of your server farm. We will look at each of these in turn.

**FIGURE 5.21** The server farm Properties sheet



Zygort Farm Properties

Performance options

☑ Discard redundant graphics operations

☑ Alternate caching method

Resource limits

Maximum memory to use for each session's graphics:

kilobytes: 5625

Degradation bias:

○ Degrade color depth first

● Degrade resolution first

☑ Notify user of session degradation

## ICA Display Tab

The options on the ICA Display tab control the server's communication and display performance. As shown in Figure 5.21, the upper portion of this screen contains the Performance options. If you select the Discard Redundant Graphics Operations option, the server will not send any graphics information that another graphic will obscure. Therefore, the hidden data does not have to travel to the client, consuming less bandwidth. The second option, Alternate Caching Method, forces the server to use the caching algorithm that was used with MetaFrame 1.8 servers. If the farm is in mixed mode, this is the preferable way to cache graphics. However, if you switch the farm to native mode, you must deselect this option to enable the server to use the new caching algorithms.

The Resource Limits section of this screen controls the amount of memory that graphics processing consumes and the color degradation. You can set the maximum amount of memory each client can consume in the Maximum Memory To Use For Each Session's Graphics text box. Enter the number of kilobytes you wish to allow a user to consume when processing graphics. You can then designate how you want to control the processing once this limit has been reached. You can reduce the number of colors available to the session by selecting the Degrade Color Depth First radio button, or you can reduce the color resolution by selecting the Degrade Resolution First radio button. The final option in this section is the Notify User Of Session Degradation check box. If you don't want to field phone calls from users complaining that their session does not look right, you may want to check this option.

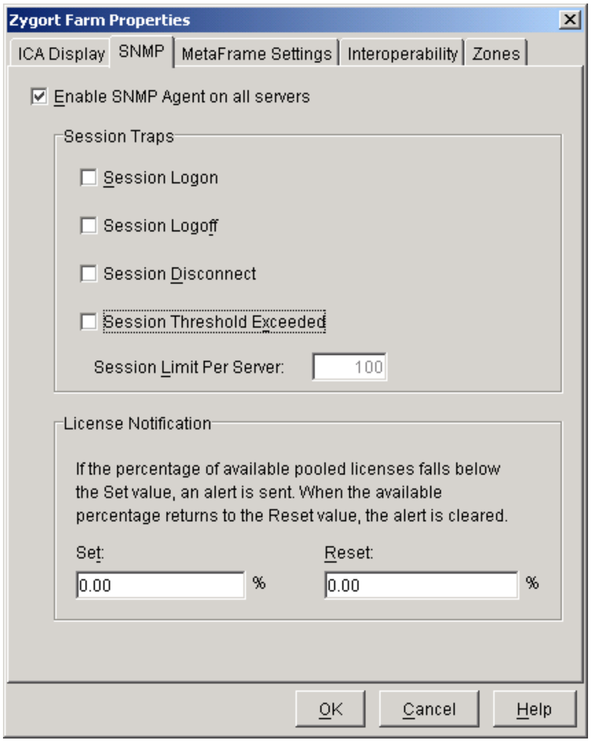
NOTE

If you select the option to reduce the resolution, your users may not be allowed to run a published application as a seamless window. The screen resolution required by the client system may be set higher than the server will allow once the degradation options are put into effect. If this is the case, the published application will start in a remote desktop instead of a seamless window. Try reducing the color depth first. If the system still doesn't perform well due to the graphics subsystem, then reduce the resolution but inform users as to why the applications look different.

## SNMP Tab

The settings contained on the SNMP tab control how servers in your farm send notifications to the SNMP manager. Figure 5.22 displays the options available on this tab. Once you configure any of the options on the SNMP tab, the settings are, by default, enforced on all servers in the server farm. Each server can override the settings configured at this point. For more information how to set individual server settings, see "Working with Servers," later in this chapter.

**FIGURE 5.22** The SNMP tab



Zygort Farm Properties

☑ Enable SNMP Agent on all servers

Session Traps

☐ Session Logon

☐ Session Logoff

☐ Session Disconnect

☐ Session Threshold Exceeded

Session Limit Per Server: 100

License Notification

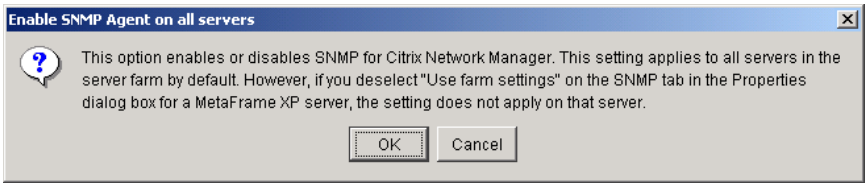
If the percentage of available pooled licenses falls below the Set value, an alert is sent. When the available percentage returns to the Reset value, the alert is cleared.

Set: 0.00 %

Reset: 0.00 %

Selecting Enable SNMP Agent On All Servers activates the options on this tab. When you choose to enable SNMP, you are presented with a warning screen, shown in Figure 5.23, informing you that you will need to make changes to individual servers if you do not want them to participate in SNMP monitoring.

**FIGURE 5.23** SNMP activation warning screen



Enable SNMP Agent on all servers

This option enables or disables SNMP for Citrix Network Manager. This setting applies to all servers in the server farm by default. However, if you deselect "Use farm settings" on the SNMP tab in the Properties dialog box for a MetaFrame XP server, the setting does not apply on that server.

Individual options are available under the Session Traps section. Selecting any of these options causes the servers to start sending traps to the management server. These options include the following:

**Session Logon** Sends a trap when a user logs on to a session.

**Session Logoff** Sends a trap when a user logs off from a session.

**Session Disconnect** Sends a trap when a user disconnects from a session.

**Session Threshold Exceeded** Sends a trap when the session limit entered in the Session Limit Per Server text box is exceeded.

The License Notification section enables the servers to send traps whenever the number of available licenses within the license pool reaches the criteria listed. If the percentage of available licenses falls beneath the value entered in the Set text box, the server will send out a trap. The system remains in the alert state until the percentage of available licenses reaches the amount set in the Reset text box.

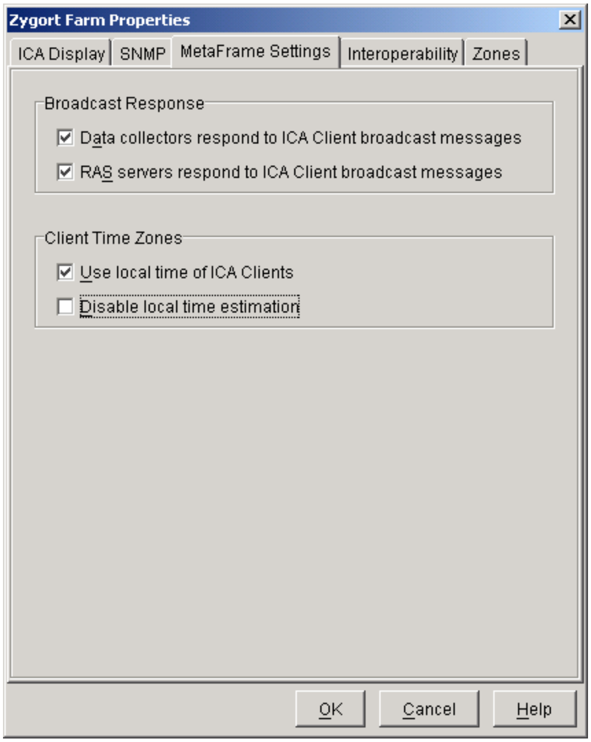
## MetaFrame Settings Tab

The global MetaFrame Settings determine how the data collectors and RAS servers respond to legacy ICA Clients when they use UDP broadcasts. When a client is configured to use TCP/IP instead of TCP/IP+HTTP, and the server location is set to Auto-locate, the client sends out a UDP broadcast. To allow a legacy client to discover servers and published applications, set the first option, Data Collectors Respond To ICA Client Broadcast Messages, to On by selecting the check box, as shown in Figure 5.24.

Since clients that connect to a RAS server communicate only with the RAS server itself, they need a method of discovering published applications and servers. If you check the second check box, RAS Servers Respond To ICA Client Broadcast Messages, the RAS server can accept the UDP broadcast and resolve the information for the client.

Files that users create while in their sessions have timestamps applied to them just as they would if the user created the files locally on their computer. Legacy clients do not report their actual time; it is estimated from the server's time and the time zone information for the client. MetaFrame XP allows newer clients to send their time information to the server. If the administrator selects the Use Local Time Of ICA Clients option, the timestamp for a file will be generated from the user's actual time. If you would rather not use the client's time, then deselect the check box so that the server's time will be used.

**FIGURE 5.24** MetaFrame Settings tab



Zygort Farm Properties

Broadcast Response

☑ Data collectors respond to ICA Client broadcast messages

☑ RAS servers respond to ICA Client broadcast messages

Client Time Zones

☑ Use local time of ICA Clients

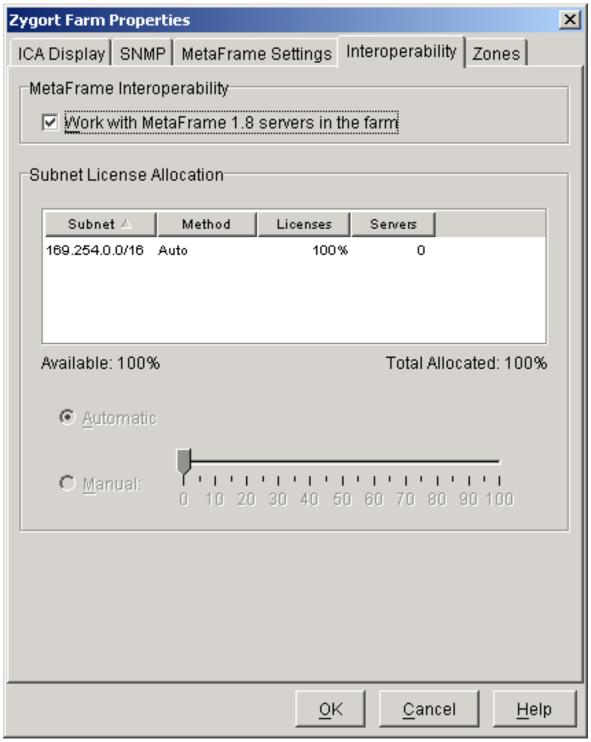
□ Disable local time estimation

The last check box in this section, Disable Local Time Estimation, authorizes the administrator to not allow time estimation. If the client cannot report its time, the server's time will be used as the timestamp when creating new files.

## Interoperability Tab

You can change the server farm from mixed mode to native mode on this tab. By selecting one check box, you can change whether your MetaFrame XP servers will communicate and function with MetaFrame 1.8 servers. Figure 5.25 shows the *Interoperability* tab, and Figure 5.26 displays the warning message received when the Work With MetaFrame 1.8 Servers In The Farm check box is deselected. Once you deselect this option, the server farm operates in native mode and ignores any MetaFrame 1.8 servers that are installed.

**FIGURE 5.25** The Interoperability tab



MetaFrame Interoperability

☑ Work with MetaFrame 1.8 servers in the farm

Subnet License Allocation

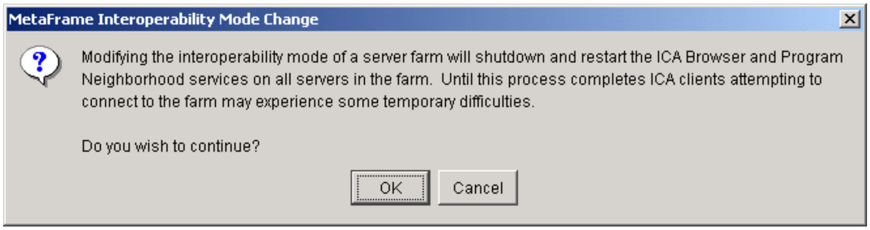
| Subnet | Method | Licenses | Servers |
|---|---|---|---|
| 169.254.0.0/16 | Auto | 100% | 0 |

Available: 100% Total Allocated: 100%

● Automatic

○ Manual:

**FIGURE 5.26** The Interoperability warning



Modifying the interoperability mode of a server farm will shutdown and restart the ICA Browser and Program Neighborhood services on all servers in the farm. Until this process completes ICA clients attempting to connect to the farm may experience some temporary difficulties.

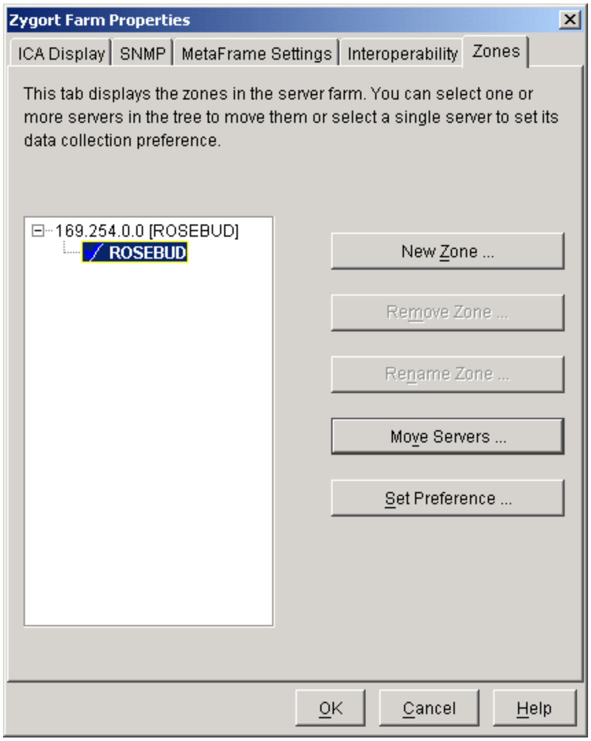
Do you wish to continue?

If the server farm is in mixed mode, the Subnet License Allocation section is available on the Interoperability tab. From here, you can allocate to individual subnets the number of licenses pooled for MetaFrame XP servers. If you select the Automatic radio button, the licenses are evenly distributed among the subnets without regard to the number of servers in the subnet. If you want to control the number of licenses allocated to each subnet, select the Manual radio button. Then select each subnet and move the slider to configure the percentage of licenses allocated to each.

## Zones Tab

As discussed in Chapter 3, "Planning the Installation of MetaFrame XP," *zones* are subnets or collections of subnets that send configuration data directly among the servers within that subnet and communicate with other zones through the data collectors in their zone. The Zones tab, shown in Figure 5.27, displays the zones in the server farm and the servers that are zone members. This tab allows you to create new zones, rename existing zones, move servers between zones, and configure the servers' data collector election criteria.

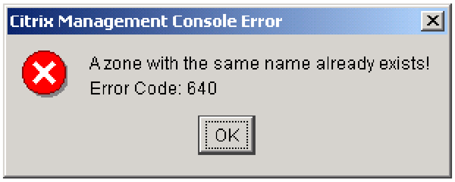
**FIGURE 5.27** The Zones tab



This tab displays the zones in the server farm. You can select one or more servers in the tree to move them or select a single server to set its data collection preference.

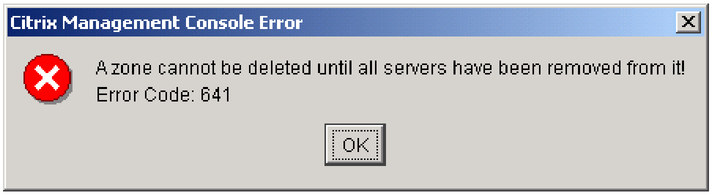
There are certain rules that apply at this screen: You cannot create a new zone with the same name as an existing zone (see the error message in Figure 5.28); you cannot rename a zone to an existing zone name; and you cannot remove a zone that contains a server (see the error message in Figure 5.29).

**FIGURE 5.28** Attempting to rename a zone to an existing name



A zone with the same name already exists!
Error Code: 640

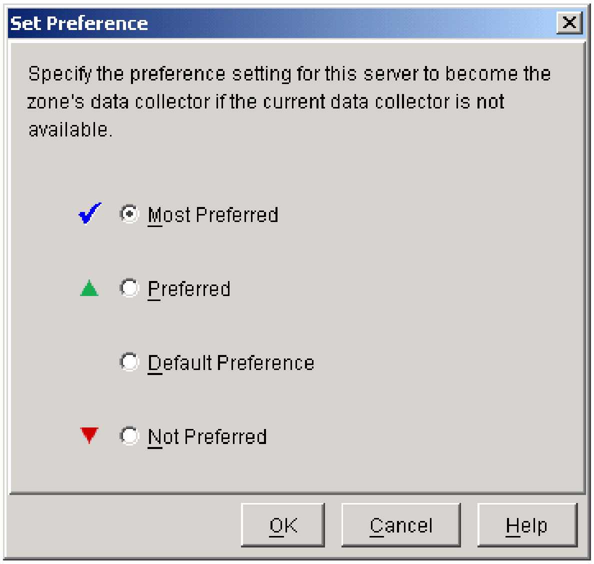
**FIGURE 5.29** Zone deletion warning



A zone cannot be deleted until all servers have been removed from it!
Error Code: 641

If you want to change the election criteria for a server, select that server and click the Set Preference button. The preferences shown in Figure 5.30 specify the server's criteria when an election occurs after the data collector cannot be detected. The Most Preferred setting identifies the server as the best candidate to become the data collector. Only one server in the zone should be configured with this setting, as a server having this setting will be made the data collector. Initially, the first server installed to the server farm has this preference. If no servers are currently online with the Most Preferred setting, a server configured with Preferred becomes the next-most-likely candidate. All servers are given the Default Preference when they are added to the farm. Servers with this option will be elected data collectors only when servers with the two higher settings are not online. Servers set with the final option, Not Preferred, will not become data collectors unless no other server configured with another option is available. After configuring your zone, you should set one server with the Most Preferred option so that you can control which server becomes your data collector.

**FIGURE 5.30** Zone data collector preferences



Set Preference

Specify the preference setting for this server to become the zone's data collector if the current data collector is not available.

✓ ● Most Preferred

▲ ○ Preferred

○ Default Preference

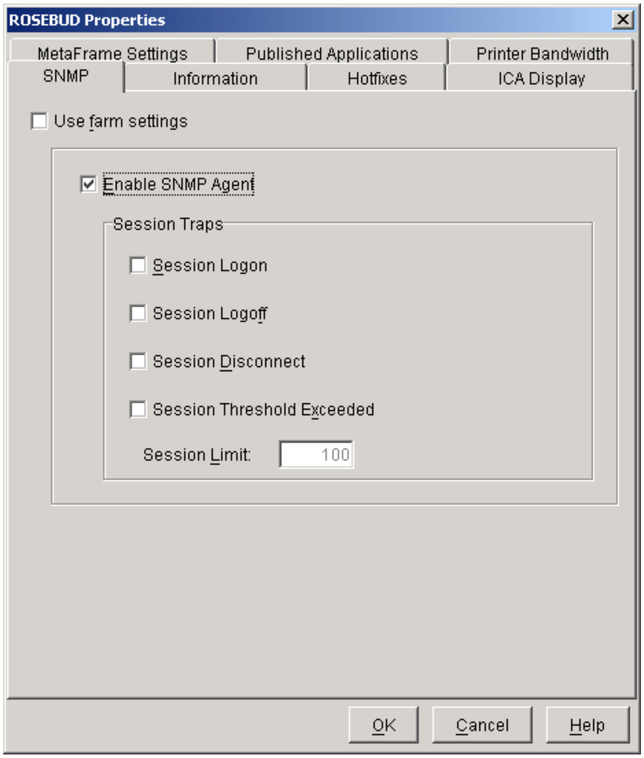
▼ ○ Not Preferred

In this section, we have looked over the options available to control all of the servers in the server farm by selecting options from within the farm properties. In the next section, we will look at configuring the options at the server level.

## Working with Servers

Servers within a server farm inherit the farm settings we just discussed as long as you do not change the default settings on the server's properties. The default settings allow you to configure the server farm so that any server added to the farm is automatically configured to your standards. More often than not, you will want to configure the individual servers to have specific settings. You can accomplish this by opening the server's properties. From the Servers node, right-click the server that you wish to configure and select Properties. The Properties sheet contains several tabs, as shown in Figure 5.31, a few of which should look familiar from the previous topic. Let's take a look at each one.

**FIGURE 5.31** Server Properties sheet



☐ Use farm settings

☑ Enable SNMP Agent

Session Traps

☐ Session Logon

☐ Session Logoff

☐ Session Disconnect

☐ Session Threshold Exceeded

Session Limit: 100

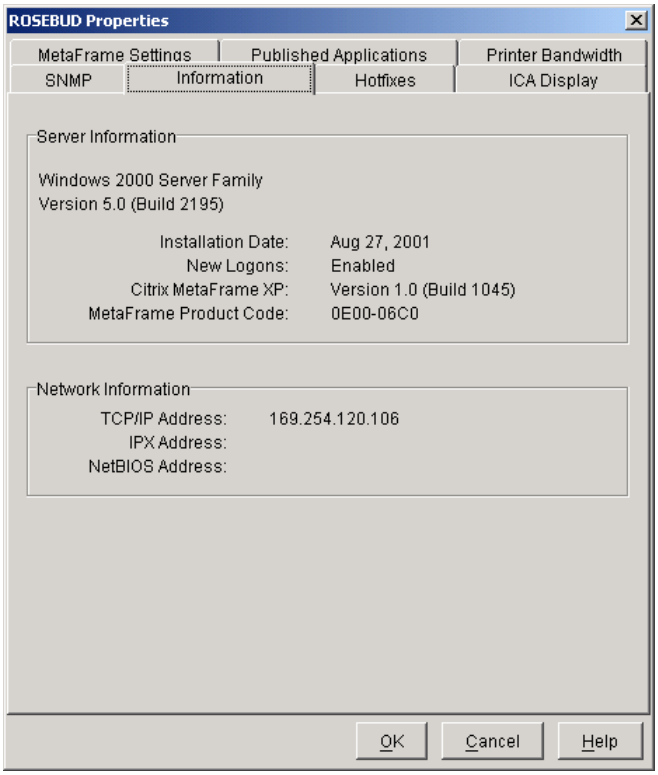
## SNMP Tab

As with the Farm node, you can enable your server to send traps to an SNMP manager from the Servers node. The default setting here, though, is Use Farm Settings. This allows the server to operate based on the settings you configured at the Farm node. If you wish to have this server perform differently, deselect the Use Farm Settings check box and configure the options based on what you want to trap.

## Information Tab

This tab contains exactly what it says—information about the server. The information contained on this tab includes the operating system on which MetaFrame is installed, the installation date, whether access is allowed to the server, the MetaFrame XP build number, the product code for the server, and the network addresses, as shown in Figure 5.32.

**FIGURE 5.32** The Information tab



Server Information

Windows 2000 Server Family
Version 5.0 (Build 2195)

Installation Date: Aug 27, 2001
New Logons: Enabled
Citrix MetaFrame XP: Version 1.0 (Build 1045)
MetaFrame Product Code: 0E00-06C0

Network Information

TCP/IP Address: 169.254.120.106
IPX Address:
NetBIOS Address:

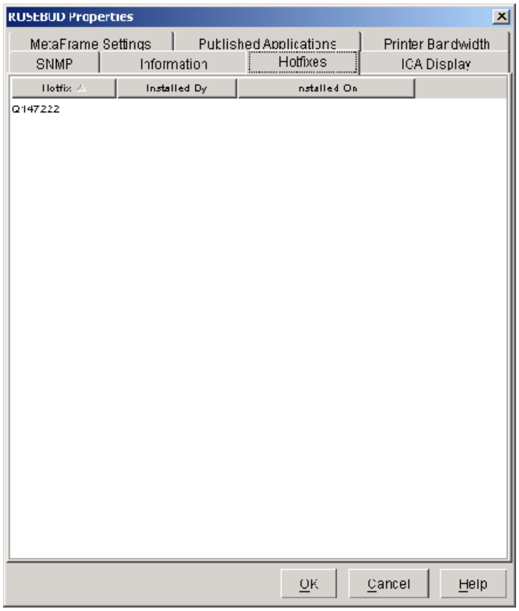
## Hotfixes Tab

Hotfixes are repairs that usually fix only one error or very few errors found within the software. You can obtain these hotfixes from the Citrix website. If any hotfixes have been installed on your MetaFrame XP server, they will be listed here. If you are trying to determine whether you need to load a hotfix, or determine which hotfixes have been loaded when you need to load another one, you will find the hotfix number listed here. You may even need to determine who loaded the hotfix, and that information is here, too. See Figure 5.33 for details.

## ICA Display Tab

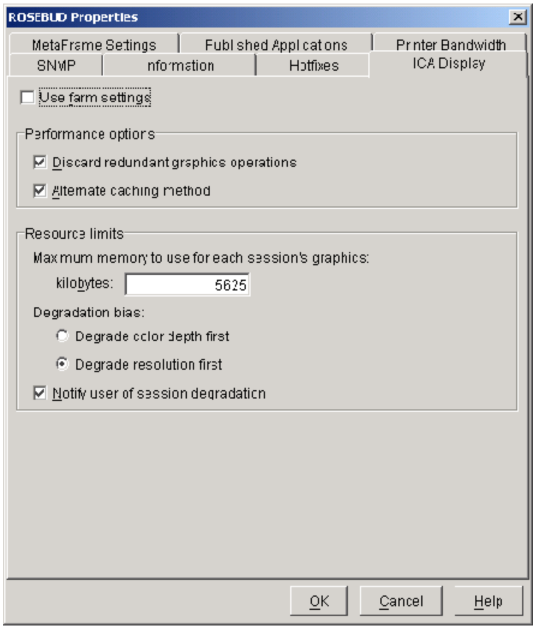
This is another tab that should look familiar from the previous topic. If you want to use the server farm defaults, keep the Use Farm Settings check box selected; otherwise, deselect that option on the ICA Display tab, shown in Figure 5.34, to override any of the farm settings.

**FIGURE 5.33** The Hotfixes tab



| Hotfix | Installed By | Installed On |
|---|---|---|
| Q147222 | | |

**FIGURE 5.34** The ICA Display tab



□ Use farm settings

Performance options

☑ Discard redundant graphics operations

☑ Alternate caching method

Resource limits

Maximum memory to use for each session's graphics:

kilobytes: 5625

Degradation bias:

○ Degrade color depth first

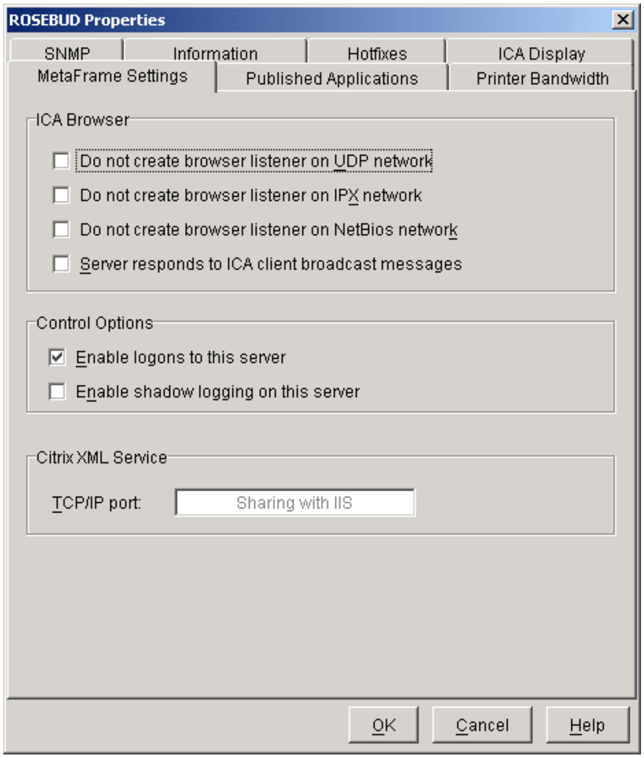
● Degrade resolution first

☑ Notify user of session degradation

## MetaFrame Settings Tab

As shown in Figure 5.35, the upper section of the MetaFrame Settings tab contains several check boxes that allow you to control which protocols the server will listen to for browser requests. You can select any of the listed protocols to disable the browser listener for that protocol. The selection Server Responds To ICA Client Broadcast Messages is available only in a native-mode server farm.

**FIGURE 5.35** The MetaFrame Settings tab



ICA Browser

□ Do not create browser listener on UDP network

□ Do not create browser listener on IPX network

□ Do not create browser listener on NetBios network

□ Server responds to ICA client broadcast messages

Control Options

☑ Enable logons to this server

□ Enable shadow logging on this server

Citrix XML Service

TCP/IP port: Sharing with IIS

In the middle section, you will find a check box labeled Enable Logons To This Server. If you need to disable logons, for example, if you want to install an application to the server or perform maintenance on the server, you need only deselect the check box. Just make sure that you come back and reselect the check box once you have finished, though!

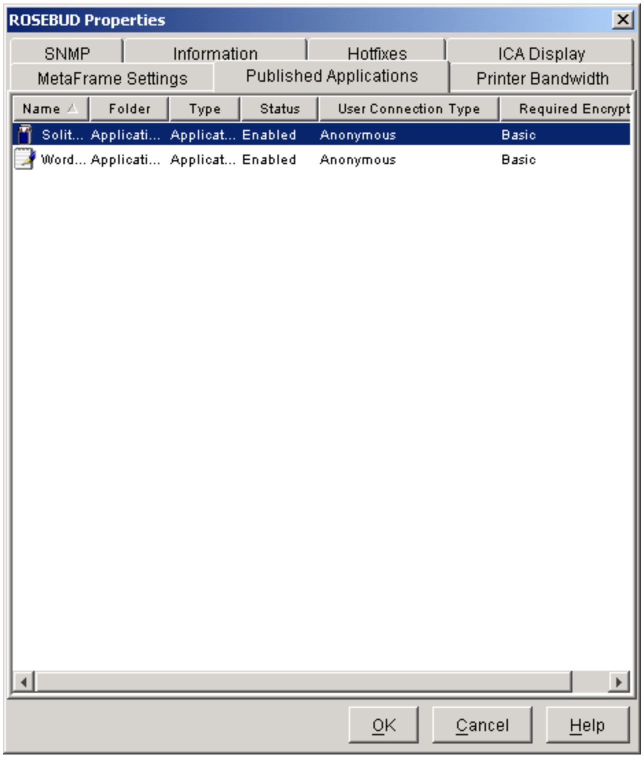
The Enable Shadow Logging On This Server check box allows information to be sent to the event log every time shadowing is initiated on a session on this server. As with any type of logging, the events take up space on the server's hard drive and use additional resources when activated. Make sure you actually need to monitor the shadowing on your server before you select this option.

The final section allows you to view the XML port that the server is using. If you keep the default option, Sharing With IIS, the port number is 80. If you need to change this number for any reason, from the command line type **`ctxxmlss /rnnn`** where ***nnn*** is the port number you are using for the XML service. After you stop and restart the XML service, the new port number will appear in this box.

## Published Applications Tab

This tab shows the applications that are published on the server. Next to the name of the application is information about the folder in which the application is installed, whether or not the application is enabled for use by clients, the connection type (Explicit or Anonymous), and the required encryption level, as shown in Figure 5.36.

**FIGURE 5.36** Published Applications tab

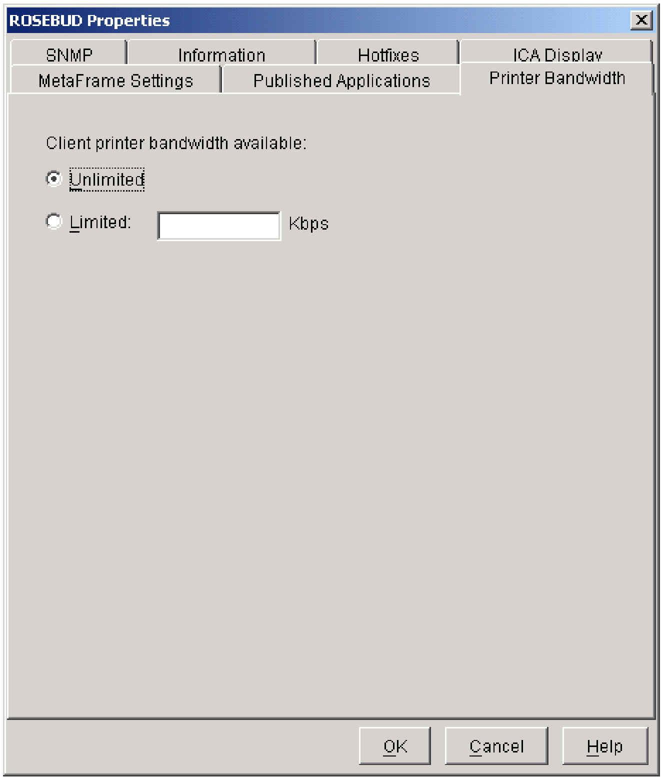


| Name | Folder | Type | Status | User Connection Type | Required Encrypt |
|---|---|---|---|---|---|
| Solit... | Applicati... | Applicat... | Enabled | Anonymous | Basic |
| Word... | Applicati... | Applicat... | Enabled | Anonymous | Basic |

## Printer Bandwidth Tab

If there is a reason to limit the amount of bandwidth that print jobs sent to a client printer can consume, you can enter that amount in Kbps in the Printer Bandwidth tab, shown in Figure 5.37. By reducing the amount of bandwidth a printer can use, you guarantee that the print jobs don't consume too much of the network's bandwidth and that the client sessions can interoperate better.

**FIGURE 5.37** The Printer Bandwidth tab



Client printer bandwidth available:

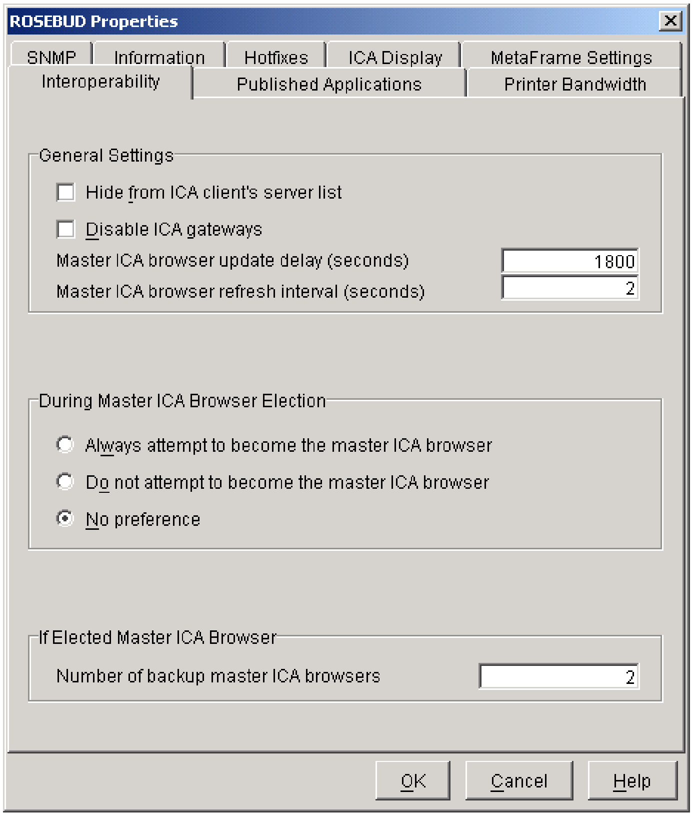
● Unlimited

○ Limited: Kbps

## Interoperability Tab

The final tab, Interoperability, shown in Figure 5.38, is available only when the server farm is in mixed mode. This tab allows you to configure how the server works with the ICA browser. By default, the ICA browser function is taken over by a MetaFrame XP server once the server farm is put in mixed mode.

**FIGURE 5.38** The Interoperability tab



General Settings

☐ Hide from ICA client's server list

☐ Disable ICA gateways

Master ICA browser update delay (seconds): 1800

Master ICA browser refresh interval (seconds): 2

During Master ICA Browser Election

○ Always attempt to become the master ICA browser

○ Do not attempt to become the master ICA browser

● No preference

If Elected Master ICA Browser

Number of backup master ICA browsers: 2

If you want to prevent clients from seeing the server, and allow them to see only the published applications on the server, you can select the Hide From ICA Client's Server List option. This will allow you to use the server to host published applications but not allow clients to use it to start a desktop session by using the name of the server. This will not stop a user from starting a session by using the IP address of the computer, however. The second option in this tab allows you to disable the ICA gateway function on the server.

To control the *ICA browser* updates and refreshes, you can make entries in the Master ICA Browser Update Delay (Seconds) and Master ICA Browser Refresh Interval (Seconds) fields. The update option specifies how long you want to wait after a client connects to or disconnects from the server until the ICA browser on this server updates the master ICA browser of the connection or disconnection. The refresh interval is the length of time the ICA browser waits before updating the master ICA browser about its current status.

The middle section of this tab controls the election criteria for the ICA browsing service. Do not confuse this with the data collector election. The ICA browser is used only in a mixed-mode server farm—and then only so that legacy clients are able to find servers and published applications. The higher the setting, the more likely a server will become the master ICA browser should the original fail. The Always Attempt To Become The Master ICA Browser setting causes the server to always force an election when it is rebooted. The Do Not Attempt To Become The Master ICA Browser setting keeps the server from participating in elections. No Preference is the default setting, and only when no other servers are configured to Always Attempt will the server try to become the master ICA browser.

At the bottom of the tab is the Number Of Backup Master ICA Browsers text box. When a server is elected as a master ICA browser, it needs to determine the license allocation for the server farm. The backup ICA browsers collect this information from the prior master ICA browser and send it to the new master ICA browser on a periodic basis. By entering a number here, you can control the number of backup ICA browsers that collect and send the license information.

So, we have looked over the settings that affect all servers in the farm by configuring the farm properties, and then we examined the individual server settings by opening up the server properties. Using these two in conjunction with one another, we can control our entire server farm and then make changes on a server-by-server basis. Now let's take a look at how to publish applications and grant users access to those applications.

## Working with Published Applications

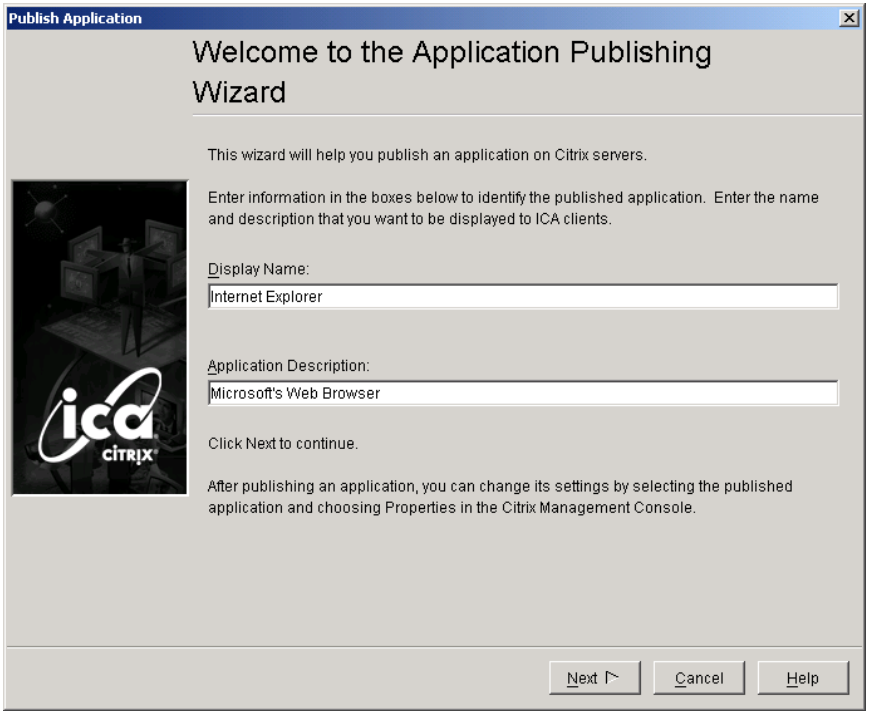
This section will not go into detail on how to install applications, that topic has been reserved for Chapter 9, "Application Support." What this section does offer is information on how to publish an application for user access. A user can start published applications without a desktop session running for the application. Applications can be published on each server that has the application installed, and the published applications can take advantage of load balancing in a MetaFrame XPa or XPe environment.

To publish an application, you will need to open the Citrix Management Console and do one of the following:

- Click the Published Application icon.
- Right-click the Application node and select Publish Application from the context menu.
- Use the Ctrl+P key combination.

Once the Publish Application screen appears, as shown in Figure 5.39, you can enter the name you want displayed to users in the Display Name field. This name should identify the application to the users of the program. You can also enter identifying information in the Application Description field. You can then view this information by changing the view in Citrix Management Console or Program Neighborhood. Once you have entered this information, click Next.

**FIGURE 5.39** Application Publishing Wizard: Selecting a display name



Welcome to the Application Publishing Wizard

This wizard will help you publish an application on Citrix servers.

Enter information in the boxes below to identify the published application. Enter the name and description that you want to be displayed to ICA clients.

Display Name: Internet Explorer

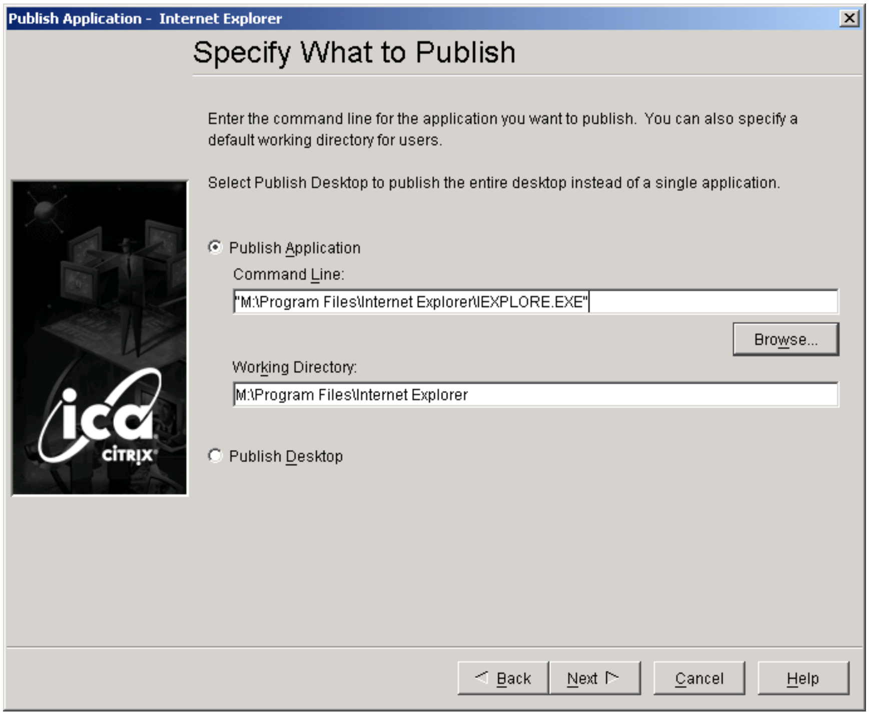
Application Description: Microsoft's Web Browser

Click Next to continue.

After publishing an application, you can change its settings by selecting the published application and choosing Properties in the Citrix Management Console.

On the Specify What To Publish page, shown in Figure 5.40, you are prompted to enter the command line for what you wish to publish. If you choose to publish the desktop, you will have no other information to enter and can go on to the next step. If you wish to publish an application, you can enter the path and the working directory for the application, or you can click Browse to find the executable file. Once you've entered all of the information, click Next to move to the Program Neighborhood settings.

**FIGURE 5.40** Application Publishing Wizard: Specify What To Publish screen



Publish Application - Internet Explorer

Specify What to Publish

Enter the command line for the application you want to publish. You can also specify a default working directory for users.

Select Publish Desktop to publish the entire desktop instead of a single application.

● Publish Application

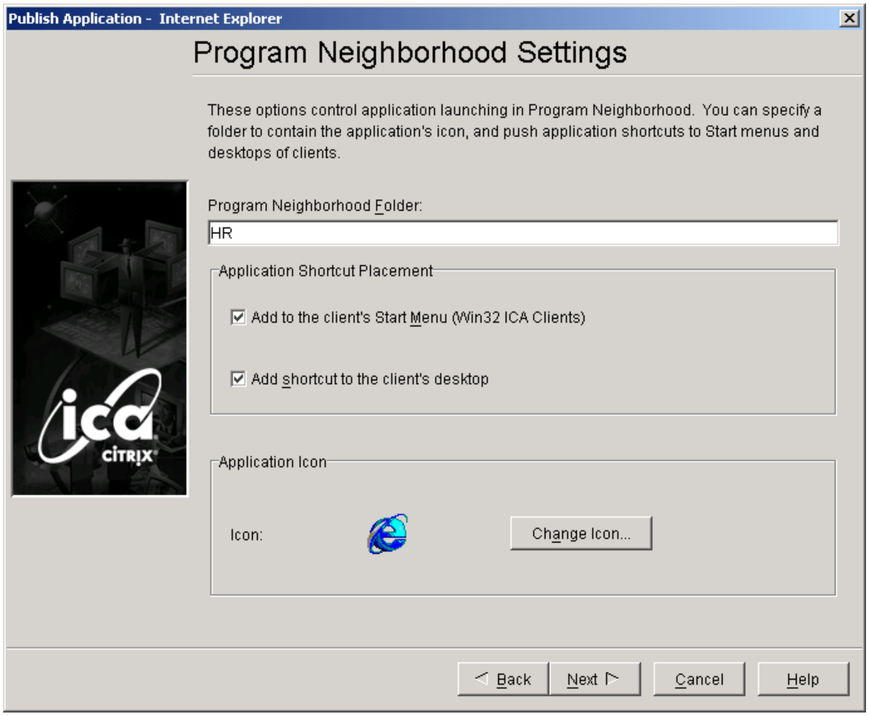
Command Line: "M:\Program Files\Internet Explorer\IEXPLORE.EXE"

Working Directory: M:\Program Files\Internet Explorer

○ Publish Desktop

The Program Neighborhood Settings screen provides the options that affect how Program Neighborhood reacts to a published application assigned to users, as shown in Figure 5.41. If you want to publish the same application but assign different permission sets to the application, you can specify folders into which the application is published. This screen also allows you to specify whether the application's icon will be pushed down to the desktop and Start bar of the users who have permission to use the application. Finally, if you wish to change the icon that is displayed, you may do so by clicking the Change Icon button and selecting a new icon for the published application. Click Next to continue.

**FIGURE 5.41** Application Publishing Wizard: Program Neighborhood Settings screen



Publish Application - Internet Explorer

Program Neighborhood Settings

These options control application launching in Program Neighborhood. You can specify a folder to contain the application's icon, and push application shortcuts to Start menus and desktops of clients.

Program Neighborhood Folder: HR

Application Shortcut Placement

☑ Add to the client's Start Menu (Win32 ICA Clients)

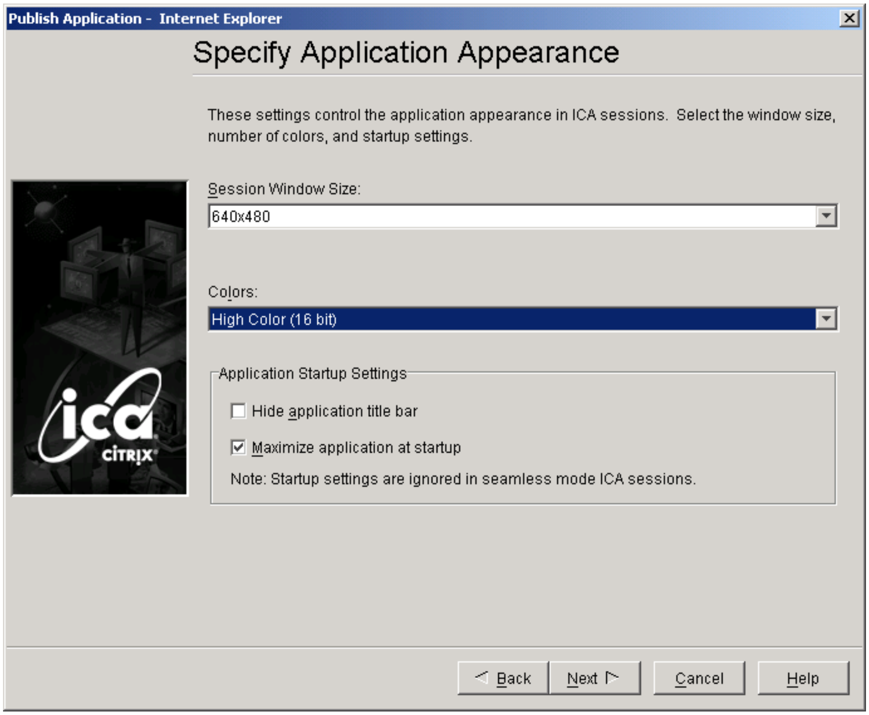
☑ Add shortcut to the client's desktop

Application Icon

Icon:

The options available to control the appearance of the application are shown in Figure 5.42. Session Window Size controls the maximum size the application will resort to, while Colors dictates the total number of colors used while the session is running. The more colors used, the more memory consumed. The last two options control the startup settings for the application. Hide Application Title Bar hides the application's title bar when the application is started within a desktop session. This keeps the user from seeing two title bars, one on top of the other, during the session. Maximize Application At Startup brings the application to the forefront of the desktop session as soon as it is started so that the user sees the application they wanted to run.

**FIGURE 5.42** Application Publishing Wizard: Specify Application Appearance screen



Specify Application Appearance

These settings control the application appearance in ICA sessions. Select the window size, number of colors, and startup settings.

Session Window Size: 640x480

Colors: High Color (16 bit)

Application Startup Settings

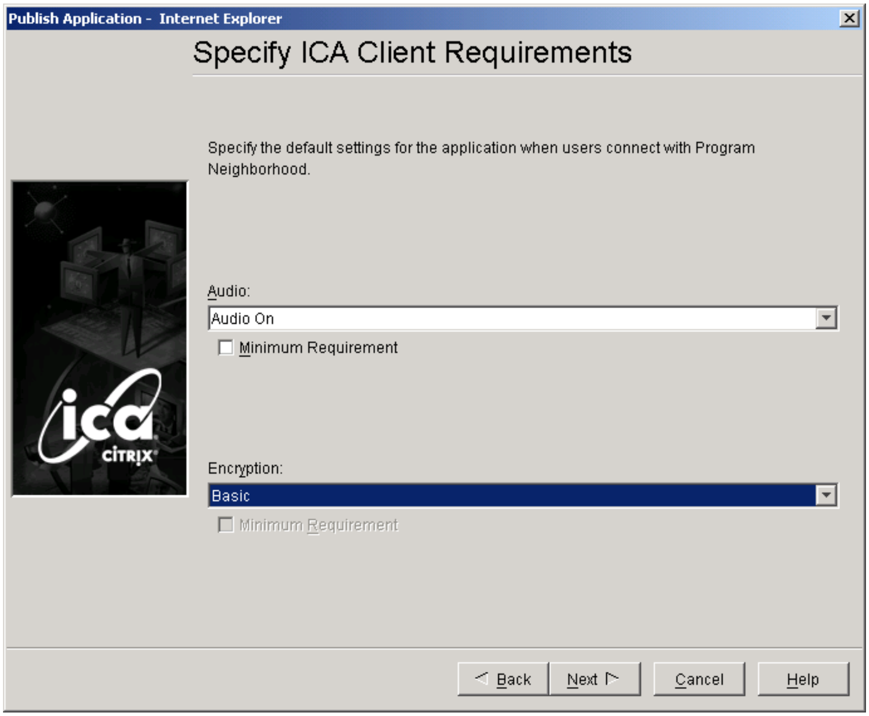
□ Hide application title bar

☑ Maximize application at startup

Note: Startup settings are ignored in seamless mode ICA sessions.

After clicking the Next button, you are presented with the Specify ICA Client Requirements screen, as shown in Figure 5.43. These are the minimum requirements needed by the application when a user starts a session. You can require that the user meet these requirements by selecting the check boxes beneath each of the options. Audio requirements are either Audio On or Audio Off, while the Encryption setting has several options to choose from. For more information on encryption levels, see Chapter 8, “Security.” Click Next to continue.

**FIGURE 5.43** Application Publishing Wizard: Specify ICA Client Requirements screen



Publish Application - Internet Explorer

Specify ICA Client Requirements

Specify the default settings for the application when users connect with Program Neighborhood.

Audio: Audio On

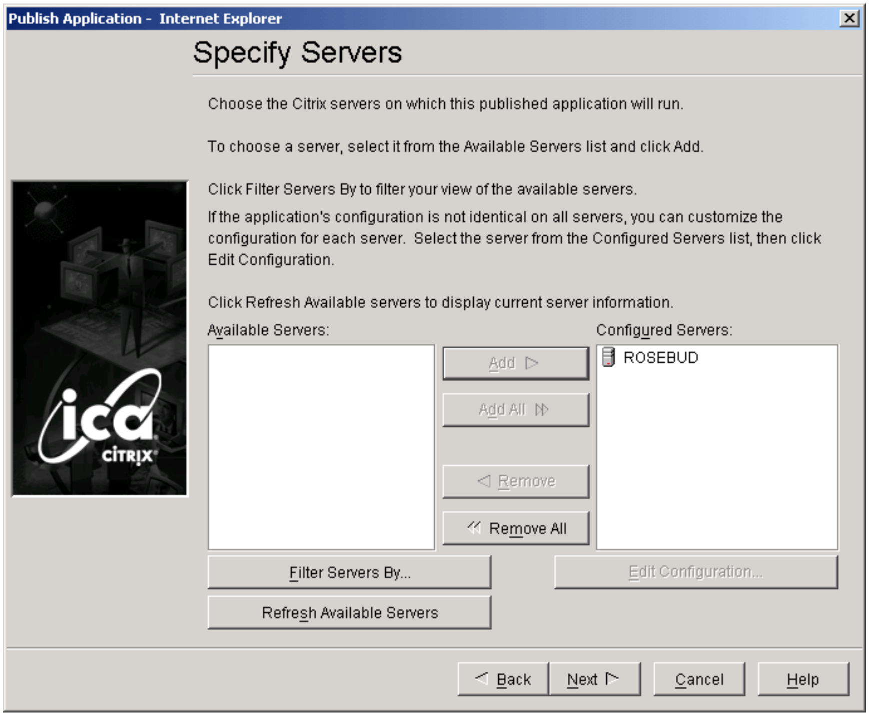
□ Minimum Requirement

Encryption: Basic

□ Minimum Requirement

Figure 5.44 displays the Specify Servers screen, which allows you to configure the servers that will publish the application. Select the servers you want to use from the Available Servers column, and click the Add button. If you want every server in your server farm to host the published application, Citrix made it easy for you—just click the Add All button. This button comes in very handy if you want all but a few of your servers to host the published application; you can add all of them and then remove those you don't want from the Configured Servers list by selecting them and clicking Remove.

**FIGURE 5.44** Application Publishing Wizard: Specify Servers screen



Publish Application - Internet Explorer

Specify Servers

Choose the Citrix servers on which this published application will run.

To choose a server, select it from the Available Servers list and click Add.

Click Filter Servers By to filter your view of the available servers.

If the application's configuration is not identical on all servers, you can customize the configuration for each server. Select the server from the Configured Servers list, then click Edit Configuration.

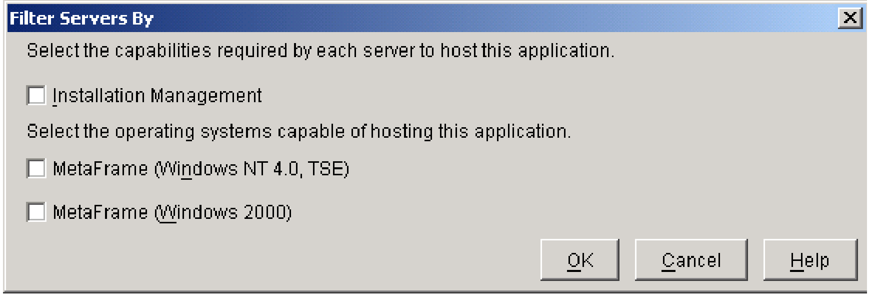
Click Refresh Available servers to display current server information.

Available Servers:

Configured Servers:
ROSEBUD

The server list can be modified to show only those servers that are running Windows NT Server 4.0, TSE or Windows 2000 Server, or only those that have Installation Management installed, by clicking the Filter Servers By button and selecting the servers you want displayed. Figure 5.45 shows the Filter Servers By screen.

**FIGURE 5.45** Application Publishing Wizard: Filter Servers By screen



Filter Servers By

Select the capabilities required by each server to host this application.

☐ Installation Management

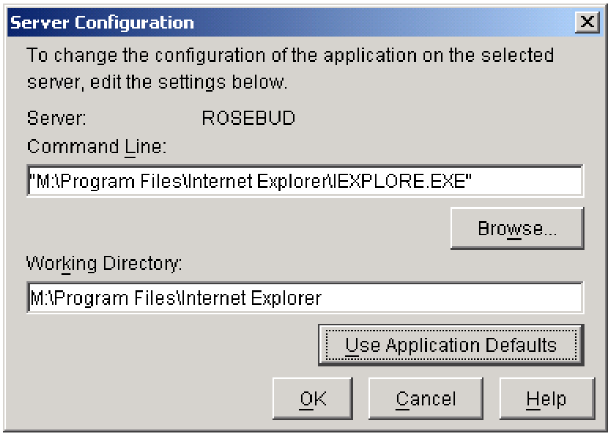
Select the operating systems capable of hosting this application.

☐ MetaFrame (Windows NT 4.0, TSE)

☐ MetaFrame (Windows 2000)

Once the servers are added to the Configured Servers list, they will be used when users attempt to start this published application. However, before you go on, you may need to configure the application executable and working directory path on some of your servers. If the applications are not installed into the same directory on all servers, select each server and click the Edit Configuration button. This brings up the dialog box seen in Figure 5.46, where you can modify the path to the application on that individual server.

**FIGURE 5.46** Application Publishing Wizard: Server Configuration screen



Server Configuration

To change the configuration of the application on the selected server, edit the settings below.

Server: ROSEBUD

Command Line:

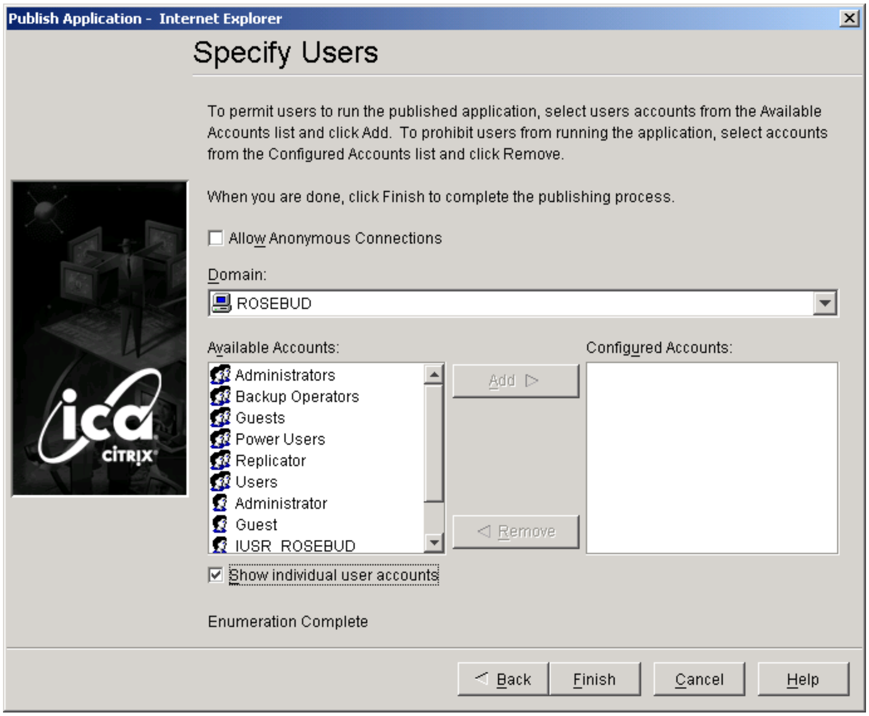
"M:\Program Files\Internet Explorer\IEXPLORE.EXE"

Working Directory:

M:\Program Files\Internet Explorer

After choosing the server to use, you specify who can use the application in the Specify Users screen, shown in Figure 5.47. By default, no user is listed as having the ability to run a published application; you must add them here or add them later by editing the properties of the published application. To choose groups, select the domain in the Domain pull-down list, select the group account, and click the Add button. User accounts do not show by default, so if you want to add a user to the permission list, you will need to select the Show Individual User Accounts check box. This is not the recommended method, hence the hidden accounts, because it is easier to add accounts into groups by using the standard Windows administration tools than it is to open Citrix Management Console every time another user requests access. You can grant anonymous access by simply checking the Allow Anonymous Connections check box near the top of the screen. Users starting applications with anonymous access do not need to authenticate when starting the published application.

**FIGURE 5.47** Application Publishing Wizard: Specify Users screen



Publish Application - Internet Explorer

Specify Users

To permit users to run the published application, select users accounts from the Available Accounts list and click Add. To prohibit users from running the application, select accounts from the Configured Accounts list and click Remove.

When you are done, click Finish to complete the publishing process.

□ Allow Anonymous Connections

Domain: ROSEBUD

Available Accounts:

- Administrators
- Backup Operators
- Guests
- Power Users
- Replicator
- Users
- Administrator
- Guest
- IUSR_ROSEBUD

Configured Accounts:

☑ Show individual user accounts

Enumeration Complete

After you have finished configuring the application by working through the wizard, click Finish to complete the publishing process. The application will appear in the Applications node of Citrix Management Console. It is here that you can control the application by editing the configuration and enabling or disabling the application. If you right-click the application, you will see the menu shown in Figure 5.48.

Choose Properties to edit any of the entries made while running the Application Publishing Wizard. The only items that were not shown in the wizard and the Properties screen are the Application Name field and the Disable Application check box on the Application Name tab shown in Figure 5.49. If you need to disable the published application, selecting the option on this tab will prohibit any server from allowing connections to the application.

**FIGURE 5.48** The published application context menu

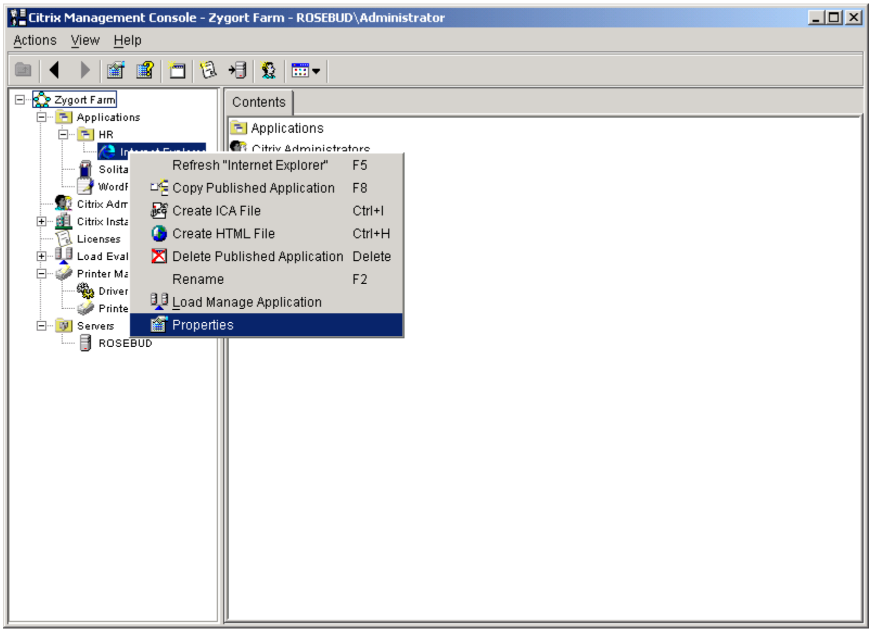
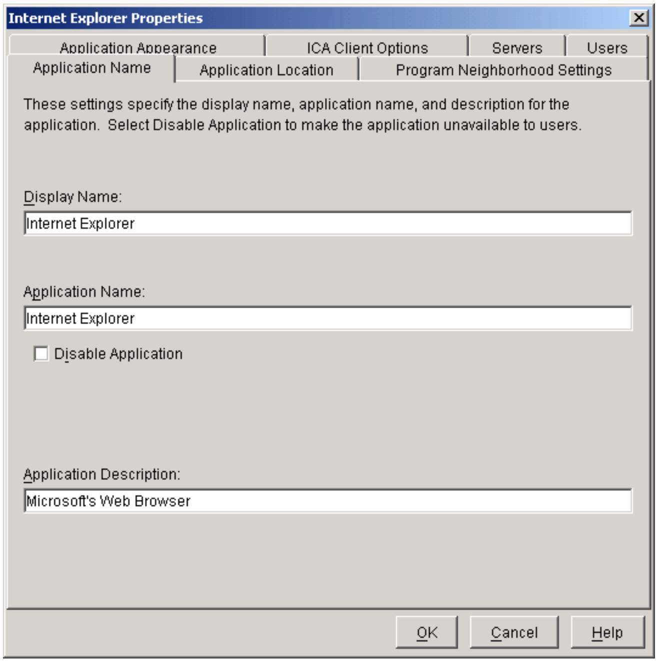


**FIGURE 5.49** The published application Properties sheet: Application Name tab



These settings specify the display name, application name, and description for the application. Select Disable Application to make the application unavailable to users.

Display Name: Internet Explorer

Application Name: Internet Explorer

☐ Disable Application

Application Description: Microsoft's Web Browser

Choose the other options on the context menu to perform the following actions on the application:

**Refresh *"Application Name"*** Display any changes made to the application.

**Copy Published Application** Make an identical copy of the application with the words *Copy of* added to the beginning of the name.

**Create ICA File and Create HTML File** Both of these options are used to create web pages and the files necessary to access the application from a web browser.

NOTE For more information on web access to a published application, see Chapter 12, "Web Connectivity and NFuse."

**Delete Published Application** Delete the selected application.

**Rename** Rename the application. You can also do this from within the properties of the published application on the Application Name tab.

**Load Manage Application** If MetaFrame XPa or XPe is installed, this option will open the Load Manage Application window and allow the administrator to control the load evaluators assigned to each server.

As we mentioned before, more information concerning the installation of applications is included in Chapter 9. This section is included to provide you with the necessary information to publish those applications. From here, we move on to the Licensing node.

# Licensing

At first, one of the most confusing topics when investigating MetaFrame is licensing. Let's face it; any type of licensing is confusing. However, software developers use licensing to keep the initial cost of the software at a minimum so that companies of any size can afford it, and then they charge on a per-connection basis. This way, smaller companies are not hit so hard when they purchase the software, and buying a few licenses is not nearly as expensive as it would be for a large company that needs hundreds or thousands of connections.

Licenses can be added either while setting up a server or after the servers are already installed and running. If you need to add connection licenses after all of the servers have been installed, you can enter those licenses from the Licenses node of Citrix Management Console. Conversely, if you included a large number of licenses in the license pool, you are not required to add licenses during the installation of a new server. The new server will be able to take advantage of licenses that are pooled in the server farm for the product level you have identified for that server.

Citrix licensing takes many forms. As discussed briefly in Chapter 3, "Planning the Installation of MetaFrame XP," the license types available for use are product license, connection license, connection migration license, and connection upgrade license pack. Each of these is available in packs of multiple licenses. If you need only five connection licenses, you would purchase a connection license five-pack. Let's take a look at each of these license types and what they offer.

## Product License

First up is the all-important product license. A product license identifies the MetaFrame XP product and the associated services that can be installed. The following table lists the services that are enabled, depending on the product license that is installed. Each product license enables MetaFrame XP.

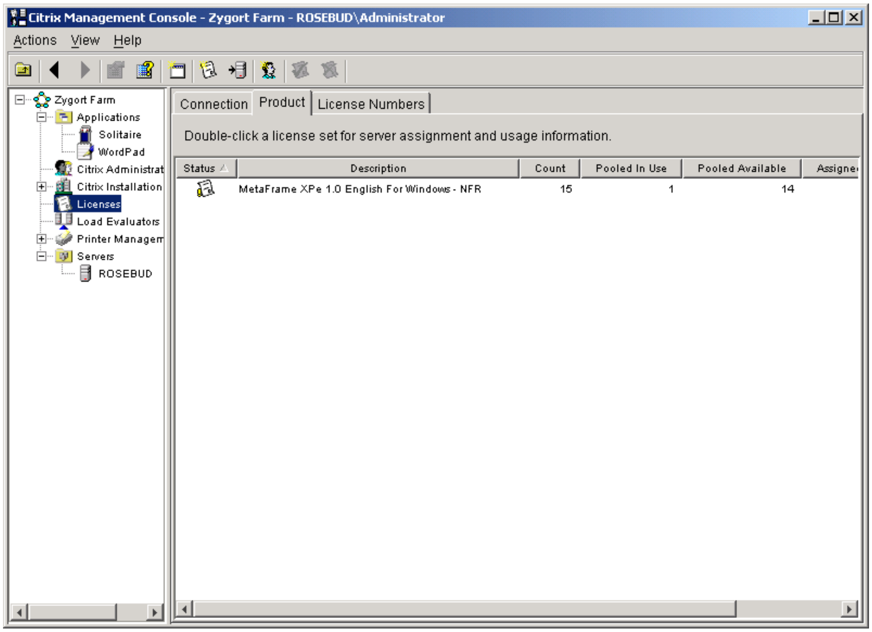
| Product License | Services Enabled |
|---|---|
| MetaFrame XPs | No additional services |
| MetaFrame XPa | Load Manager |
| MetaFrame XPe | Installation Manager, Load Manager, Network Manager, and Resource Manager |

NOTE

Without a product license, the server will not accept any connections, not even temporary connections.

To add a product license, open Citrix Management Console and select the Licenses node in the Server Farm tree. In the right-hand pane, you will see three tabs. The second tab is the product license tab, named Product in Figure 5.50. From this tab, you can identify all of the product licenses added to your server farm.

**FIGURE 5.50** Identifying product licenses



Double-click a license set for server assignment and usage information.

| Status | Description | Count | Pooled In Use | Pooled Available | Assigne |
|---|---|---|---|---|---|
| | MetaFrame XPe 1.0 English For Windows - NFR | 15 | 1 | 14 | |

Right-click anywhere within this tab, and you will see the Add License option on the context menu (see Figure 5.51). Select this option to bring up the Add License dialog box, as shown in Figure 5.52. Refer to your product's packaging to locate the serial number and *product code*. Enter the serial number in the Add License dialog box. This will place the licenses associated with the license pack into the license pool. All of the licenses will then be available for any server in the server farm.

**FIGURE 5.51** Choosing Add License from the menu

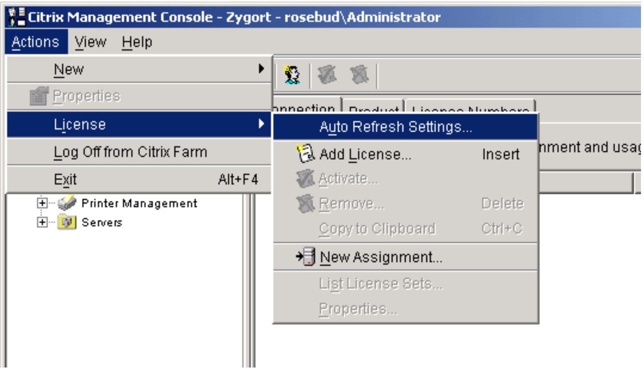
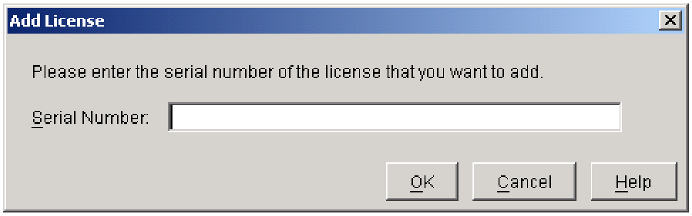


**FIGURE 5.52** The Add License dialog box



Add License

Please enter the serial number of the license that you want to add.

Serial Number:

TIP

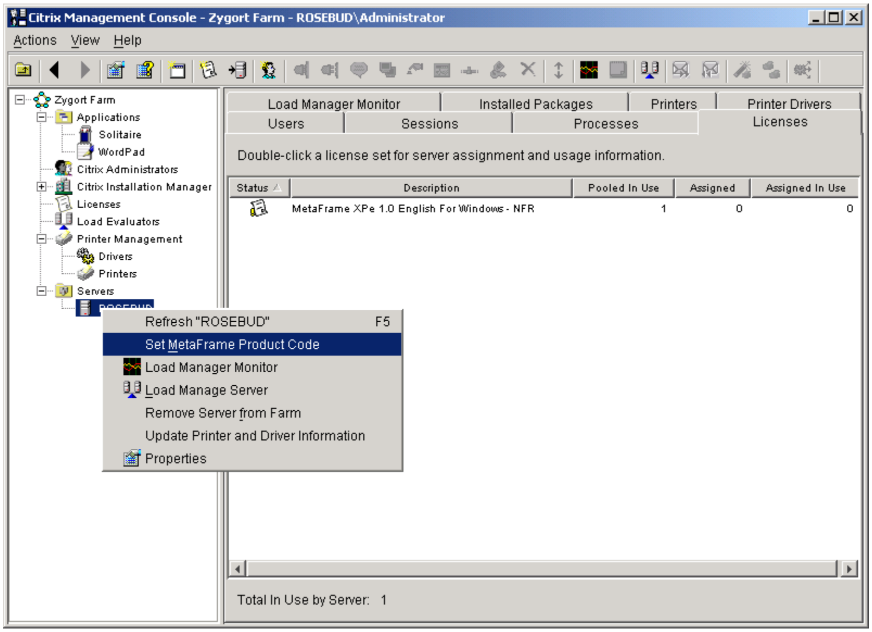
From any of the License node tabs, you can press the Insert key and the Add License screen will appear.

One advantage of Citrix's licensing model is that all product licenses are pooled for use by any server in the server farm. When a server is shut down, it releases its product license for use by another server using the same product level. Of course, this means that any server running MetaFrame XPs will not be allowed to use a license for MetaFrame XPe. And that is where the product code comes into play.

The product code is included on the same tag as the serial number on the product's packaging. This nine-character code identifies the product level that is installed, the services that are enabled, and whether the product is a retail, evaluation, or not-for-resale version. Usually, you would enter the product code during the installation of MetaFrame XP, but you can omit this step and enter the code after the installation is complete. To do so, open the Servers node and right-click the server where you want to add the code. Select Set MetaFrame Product Code from the context menu, as shown in Figure 5.53. When the Set MetaFrame Product Code screen appears, enter the code for the product you are using, as shown in Figure 5.54.

Once you have entered the license serial number into the server farm and the product code for the server, the server will request a product license from the license pool. As soon as the license has been granted to the server, the server is able to accept ICA connections. The product code also specifies which license type will be requested from the license pool. If there are no licenses available for that product level, the server will not be allowed to accept ICA connections. Any time you need to use other services, you will have to enter the appropriate server code to enable those services to function on the MetaFrame XP server.

**FIGURE 5.53** Changing the product code

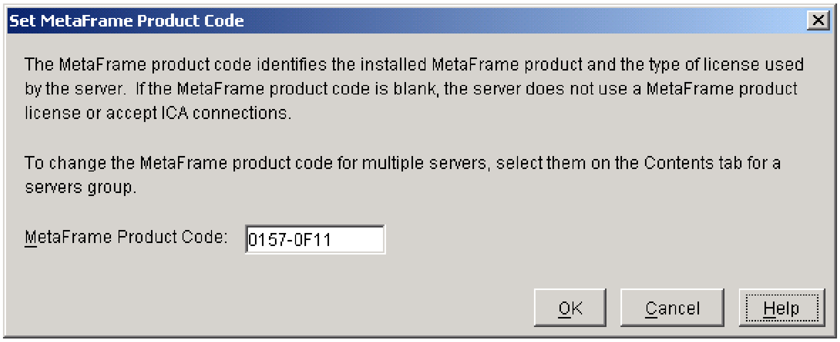


Double-click a license set for server assignment and usage information.

| Status | Description | Pooled In Use | Assigned | Assigned In Use |
|---|---|---|---|---|
| | MetaFrame XPe 1.0 English For Windows - NFR | 1 | 0 | 0 |

Total In Use by Server: 1

**FIGURE 5.54** Entering the new product code



The MetaFrame product code identifies the installed MetaFrame product and the type of license used by the server. If the MetaFrame product code is blank, the server does not use a MetaFrame product license or accept ICA connections.

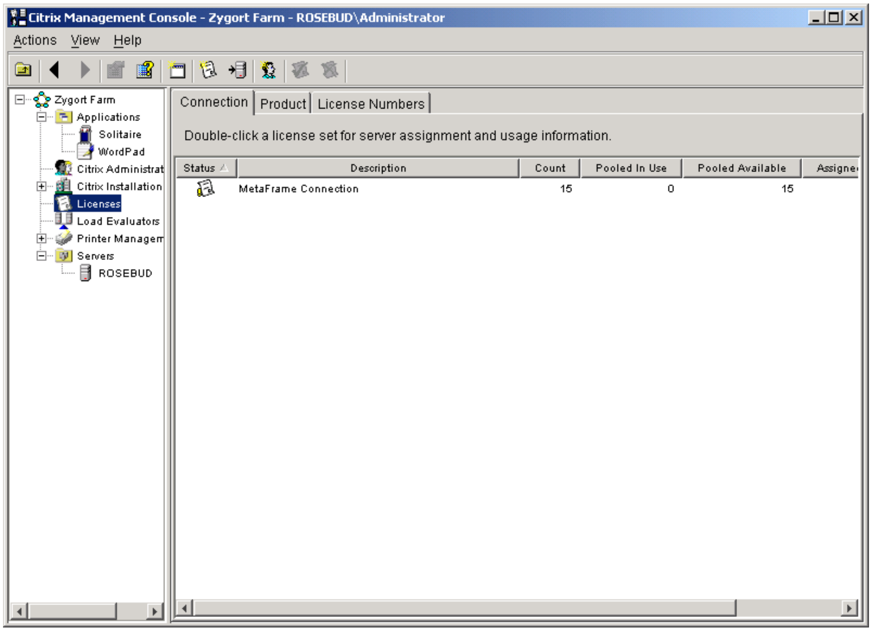
To change the MetaFrame product code for multiple servers, select them on the Contents tab for a servers group.

MetaFrame Product Code: 0157-0F11

## Connection Licenses

Connection licenses specify how many client connections are allowed within the server farm. After you add a connection license pack, the number of connections to the server farm allowed by that pack is added to the pool. If you view the Connection tab within the Licenses node, as shown in Figure 5.55, you will see the total number of licenses all of the license packs provide, in this case, 15. If you have added one connection license pack with 50 licenses and another with 35, the total number of licenses displayed on the Connection tab will be 85.

**FIGURE 5.55** The connection licenses



Double-click a license set for server assignment and usage information.

| Status | Description | Count | Pooled In Use | Pooled Available | Assigne |
|---|---|---|---|---|---|
| | MetaFrame Connection | 15 | 0 | 15 | |

Adding connection licenses follows the same method as installing the product licenses. All of these connection licenses are available for all connections regardless of the products that are installed in the server farm. You can access MetaFrame XPs, XPa, and XPe using the pooled connection licenses. The major benefit of this is that the connection license tracks only the connections made to the server farm from the client, not the number of servers that are connected. In this case, the client can access published applications that reside on separate servers and still require only one license.

## Connection Migration Licenses

To ease the sting of moving from MetaFrame 1.*x* or WinFrame 1.*x* to MetaFrame XP, Citrix provides connection migration licenses to change the existing user license in legacy MetaFrame or WinFrame to a connection license in MetaFrame XP. Since these product licenses are less expensive than the full connection license, a company can cost-justify the migration from their original environment to the MetaFrame XP environment.

When you migrate a server from a previous version of MetaFrame or WinFrame, you can upgrade the product license during the setup process. The server's product code must match the product code provided on the migration product packaging. Without this product code, the server will not be allowed to utilize one of the original licenses provided to the legacy version.

Any server that is directly upgraded to MetaFrame XP automatically sends the current licensing information to the data store. When the licensing screen appears, enter the serial number from the connection migration license pack, and when prompted, enter the product code for the server.

When you don't use the original hardware during the migration from a previous version of MetaFrame, extra steps are necessary. During setup, don't enter any licensing information. Once setup is complete, open Citrix Management Console and select the Licensing node. Open the Add License Wizard, and enter the user licenses from the previous version of MetaFrame. After adding all of the licenses, enter the connection migration license pack information. Finally, open the Servers node and select the new server. Add the product code to the server to allow that server to take advantage of the original license counts. Make sure the original server is taken offline to comply with the license.

## Connection Upgrade Pack

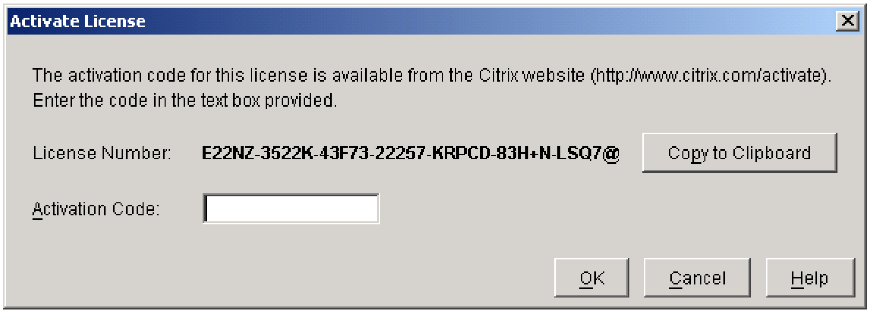
In order to upgrade a server from MetaFrame XPs to XPa or XPe, you will need to purchase an upgrade license pack. These special packs include the additional software necessary to add the additional services and a product code to allow the server to request a product license for that level of server. The nice part of all this is that these packs cost less. Since you already have MetaFrame XP, you need to purchase only the additional services.

## Activating Licenses

When you add a license to the license pool, that license is available for use only during the grace period unless you activate it, making it a permanent license. The benefit of this scenario is that you can experiment with MetaFrame before making anything permanent. Once the license is activated, it can be used until it is deactivated.

The process of activating licenses is rather painless. Open the Licenses node in Citrix Management Console, choose the License Numbers tab, and right-click the license you wish to activate. From the context menu, select Activate. This brings up the Activate License screen with the license number displayed, as shown in Figure 5.56. Citrix's forward thinking provided for a Copy To Clipboard button, which you can click to copy the entire license number to the Clipboard so you do not have to write it down and possibly mistype it later.

**FIGURE 5.56** The Activate License dialog box



Activate License

The activation code for this license is available from the Citrix website (http://www.citrix.com/activate). Enter the code in the text box provided.

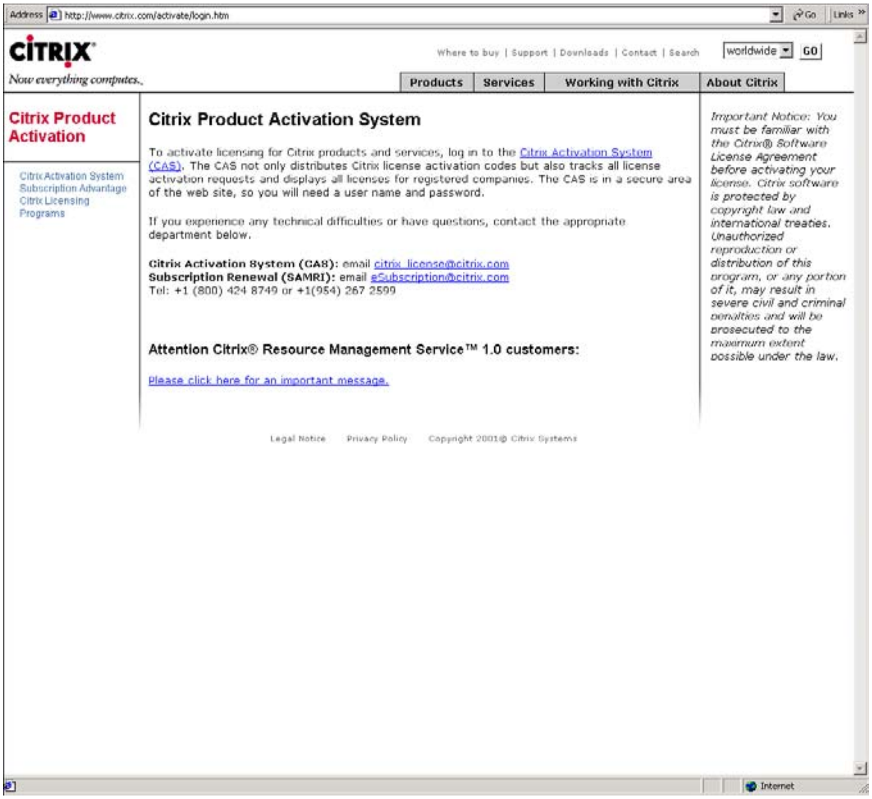
License Number: E22NZ-3522K-43F73-22257-KRPCD-83H+N-LSQ7@

Activation Code:

The following steps assume that you have a connection to the Internet. If not, you can paste the number to a Notepad document and transport it to a computer that does have Internet access. Point your web browser to `www.citrix.com/activate`, as shown in Figure 5.57. As you are navigating through the website, you can paste in the license number when prompted to do so. The web page will return an activation code. Copy this number to the Activate License screen shown previously, and click OK. The status of the license should now show as Activated in the License Numbers tab.

Each of the activation codes generated by the web page is unique to the serial number and the randomly generated machine code that is appended to the serial number when the license is entered in the Licenses node. Therefore, the chances of having an identical full license code twice when entering the information are very slim. This guarantees that the licenses that Citrix sells are protected from misuse.

**FIGURE 5.57** The Citrix Product Activation System screen



Citrix Product Activation System

To activate licensing for Citrix products and services, log in to the Citrix Activation System (CAS). The CAS not only distributes Citrix license activation codes but also tracks all license activation requests and displays all licenses for registered companies. The CAS is in a secure area of the web site, so you will need a user name and password.

If you experience any technical difficulties or have questions, contact the appropriate department below.

**Citrix Activation System (CAS):** email citrix_license@citrix.com
**Subscription Renewal (SAMRI):** email eSubscription@citrix.com
Tel: +1 (800) 424 8749 or +1(954) 267 2599

**Attention Citrix® Resource Management Service™ 1.0 customers:**

Please click here for an important message.

*Important Notice: You must be familiar with the Citrix® Software License Agreement before activating your license. Citrix software is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties and will be prosecuted to the maximum extent possible under the law.*

Legal Notice Privacy Policy Copyright 2001© Citrix Systems

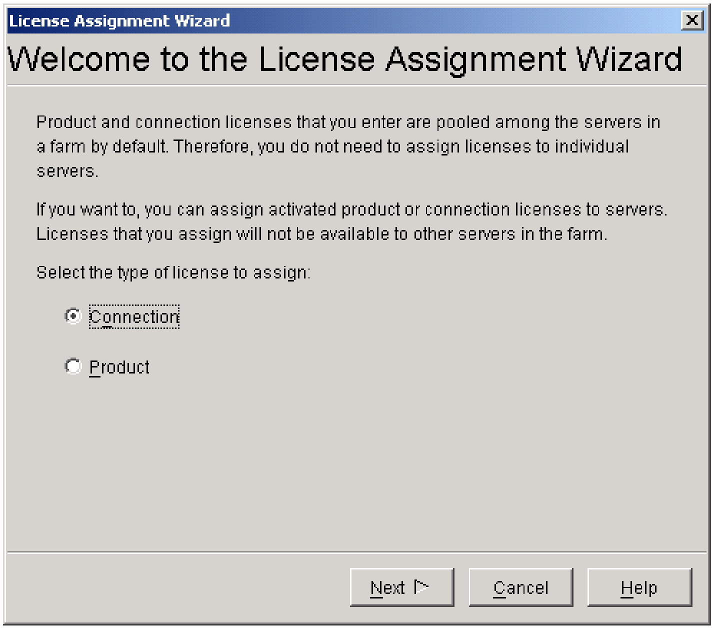
## Assigning Licenses

In previous versions of MetaFrame, pooled licenses were available for use for any connection made within a server farm. When the allotted licenses ran out, no other connections could be made, including a connection attempt by an administrator. Many administrators would designate, or assign, one license per server for administrative use so that the administrator would always have a license available to connect with. However, this would reduce the number of licenses available to the pool by one for each server where a license was assigned. MetaFrame XP does not have this restriction. Each server has a license allocated to it for an administrative connection.

License assigning is still available with MetaFrame XP so that you can identify licenses that are available only for an individual server. You can use this functionality if you have servers for which you want to guarantee that a certain number of connections are available at all times or if you have a specific product license that needs to be associated with the server.

When assigning licenses, open the Licenses node in Citrix Management Console, right-click anywhere in the right pane, and select New Assignment from the context menu. This brings up the License Assignment Wizard, as shown in Figure 5.58. Specify which license type you want to assign and click Next. From the list of licenses available, choose the license you want to assign. Then click Next again, and select the server the license will be assigned to. As users connect to the server, the reserved licenses are used before the server requests the use of a pooled license.

**FIGURE 5.58** Assigning licenses to a server



License Assignment Wizard

Welcome to the License Assignment Wizard

Product and connection licenses that you enter are pooled among the servers in a farm by default. Therefore, you do not need to assign licenses to individual servers.

If you want to, you can assign activated product or connection licenses to servers. Licenses that you assign will not be available to other servers in the farm.

Select the type of license to assign:

● Connection

○ Product

These licenses are no longer pooled for use by servers in the server farm. If you click the Connection or Product tab, you will see the Assigned and Assigned In Use columns, reflecting the assignments you just put into effect. Only those licenses that have been activated can be assigned.

Now that we have discussed the finer points of licensing, we are going to move on to other areas of interest within the Citrix Management Console nodes. Our next topic is a brief introduction to the Load Evaluators node.

## The Basics of Load Evaluators

This section and the section on printer management are very brief since we will cover these topics in greater detail in Chapters 7, "Load Management," and 13, "Printing." When we reach Chapter 7, we will discuss load evaluators and how to work with load management within the server farm.

The Load Evaluators node allows you to control which aspect of the servers is used when determining the load on the server. When you create the load evaluator, many rules are available. Once you've created the evaluator and assigned rules to it, you can attach the evaluator to a server or a published application. As clients create sessions, the server sends load information, based on the evaluator's rules, to the data collector for the zone. The data collector assigns a value to the server or the application and uses that number to direct users to the server with the lightest load. This method of load balancing is very effective, allowing the administrator to maintain the load on each server.

## The Basics of Printer Management

Printing has matured greatly since MetaFrame 1.8. Due in part to the new print drivers of Windows 2000, printing is not nearly the headache that it had been in the past. Citrix has also added more functionality to the printing subsystem. Now available are the abilities to replicate a print driver to other servers, import print servers that are not members of the server farm, and limit the amount of bandwidth consumed by print jobs.

Printing and printer management are the focus of Chapter 13. When we reach that point, we will look at printing in great detail. Until then, let's move on to the next chapter and take a look at the rest of the administrative tools.

## Summary

In this chapter, we took a look at the Citrix Management Console and saw how to use it to manage server farms and the servers within those farms. Server farms have many configuration options, so an administrator needs to know how to work with the Citrix Management Console to effectively and accurately control all those options.

We looked over each of the icons and tabs that are available in the Citrix Management Console, and then we made a detailed analysis of the nodes available. We discussed the importance of adding accounts to the Citrix Administrators and showed how to perform the task. We also covered installing and activating licenses, as well as publishing applications. Now we are going to move on to other administrative tools in the next chapter.

# Exam Essentials

**Understand the Citrix Administrators node and the implications of adding accounts to this node.** Adding an account to this node provides that account with the ability to run the Citrix Management Console.

**Understand how to restrict the accounts that have Citrix Administrator privileges.** Accounts can have either Read-Write or Read-Only abilities once they are added to the Citrix Administrators node.

**Know the icons that appear in the Citrix Management Console.** The icons that appear in the Citrix Management Console give the administrator quick access to important functions within it.

**Know the tabs available in the Citrix Management Console nodes and objects.** These tabs contain the configuration objects and detailed information for all the nodes and objects in the Citrix Management Console.

**Understand the ramifications of changing settings at the Server Farm node.** Changes made at the server farm affect the entire farm and all servers that are configured to inherit the properties of the farm.

**Understand how to configure server objects to override the farm properties.** Server settings override the farm settings if changes are made to the properties of the server.

**Know the steps and ramifications to publishing an application, and know how to change the properties of the application once it is published.** Using the Application Publishing Wizard and the Applications node, you can set and control published application properties.

**Understand licensing and the steps necessary to activate licenses.** Licenses may be added to a server farm and used for a short period of time. Once activated, the licenses are available for use without time restrictions.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Applications node

Citrix Administrators node

Connection tab

Contents tab

current sessions

Farm node

ICA browser

interoperability

Licenses node

Load Evaluators node

Load Manager Monitor

Log tab

Printer Management node

processes

Processes tab

product code

Product tab

publish applications

Servers node

Usage Reports tab

users

Users tab

zones

# Exercises

In the first exercise, we will add a Citrix Administrator account, make that account Read-Only, attempt to delete the original Citrix Administrator account, and then delete the account we just added.

**EXERCISE 5.1**

### Using Citrix Management Console to Add Administrators

1. Open Citrix Management Console either by clicking the Citrix Management Console button on the ICA Administrator toolbar or by choosing Start ➢ Programs ➢ Citrix ➢ Citrix Management Console to open the Log On To Citrix Farm dialog box.

**EXERCISE 5.1 *(continued)***

2. Verify that the account you entered during setup appears in the User Name field and that the name of the server appears in the Citrix Server field. Enter your password in the Password field and click OK.
3. In Citrix Management Console, click the Citrix Administrators node.
4. Open the Add Citrix Administrator dialog box by clicking the Add Administrator icon or by right-clicking the Citrix Administrator node and selecting Add Administrator from the context menu.
5. From the Domain pull-down list, select the server or domain where your account is located.
6. Select the Show Users check box.
7. From the Available Accounts list, select a user to add, and then click the Add button.
8. From the Assign Privileges To The Configured Accounts pull-down list, select Read-Write.
9. Click OK.
10. Right-click the account you just added and select Properties.
11. From the Privilege pull-down list, select Read-Only.
12. Click OK.
13. Select the account you made a Citrix Administrator during setup.

    Warning: Make sure the account you just added is set to Read-Only; otherwise, in the next steps you will delete the original Citrix Administrator!
14. Choose to delete the account by right-clicking the account and selecting Delete Citrix Administrator from the context menu or by clicking the Delete Citrix Administrator icon.
15. Click Yes when prompted whether you want to delete the account.

**EXERCISE 5.1 *(continued)***

16. When the warning message pops up, read it and click OK.

    Note: Since there were no other Citrix Administrators with Read-Write privileges, you are not allowed to delete this account. However, if there were any other accounts with Read-Write privileges, the account would be deleted.

17. Select the new account you made a Citrix Administrator in this lab.
18. Choose to delete the account by right-clicking the account and selecting Delete Citrix Administrator from the context menu or by clicking the Delete Citrix Administrator icon.
19. Click Yes when prompted whether you want to delete the account.
20. Verify that the account is not in the list of Citrix Administrators, and close Citrix Management Console.

In this next exercise, we will step through the process of adding a license to the server farm and then activate the license. To actually activate the license, you must purchase a license from Citrix.

**EXERCISE 5.2**

### Using Citrix Management Console to Add Licenses

1. Open Citrix Management Console either by clicking the Citrix Management Console button on the ICA Administrator toolbar or by choosing Start ➢ Programs ➢ Citrix ➢ Citrix Management Console to open the Log On To Citrix Farm dialog box.
2. Verify that the account you entered during setup appears in the User Name field and that the name of the server appears in the Citrix Server field. Enter your password in the Password field and click OK.
3. Select the Licenses node.
4. Open the Add License screen by one of these methods:
    - Right-clicking the Licenses node and selecting the Add License option.
    - Clicking the Add License icon.
    - Pressing the Insert key.

**EXERCISE 5.2 *(continued)***

5. Enter the serial number from the product packaging in the Serial Number entry box.

6. Select the License Numbers tab.

7. Select the license that you just entered.

8. Activate the license either by right-clicking the license and selecting the Activate option from the context menu or by clicking the Activate icon.

9. Click the Copy To Clipboard button to copy the license number to the Clipboard.

10. Open a web browser window and point the browser to `www.citrix.com/activate`.

11. Follow the steps on the website to log in and enter the license number for activation.

    Note: This step assumes that you have Internet connectivity from your server. If not, follow the steps in the text on how to copy the information to another computer.

12. Once the activation code appears, highlight it, right-click the highlighted text, and select Copy from the context menu.

13. Right-click in the Activation Code input box in the Activate License screen, and select Paste from the context menu.

14. Click OK.

15. Verify that the license appears with the status Active in Citrix Management Console.

# Review Questions

1. The centralized management tool used to manage and monitor your MetaFrame XP farm is:

   **A.** Citrix Server Administrator

   **B.** Citrix Management Console

   **C.** Citrix Management Administrator

   **D.** Citrix Connection Configuration

2. Citrix Management Console can be used to manage which of the following? (Choose all that apply.)

   **A.** License information

   **B.** Printer drivers

   **C.** MetaFrame 1.8 servers

   **D.** Published applications

3. If you want to add a Citrix Administrator who will have full control over the network, you should give this user which rights?

   **A.** Read-Only

   **B.** Read-Execute

   **C.** Read-Write

   **D.** Full Control

4. You are planning to install a new software application to your Metaframe XP server. Everyone is logged off the server and you want to make sure nobody else connects to that server while you are running the setup program. What would be the best way to do this?

**A.** Right-click the server name in Citrix Management Console and select Disable New Logons from the menu.

**B.** Unplug the network cable and take the system offline. There is no way to dynamically disable logons.

**C.** Right-click the server name in Citrix Management Console and select Properties. In the Metaframe Settings tab, remove the check from the box labeled Enable Logons To This Server and click OK.

**D.** Right-click the server farm name and select Properties. In the Metaframe Settings tab, remove the server from the list in the Active Servers window.

**5.** If you have configured the ICA Display options to Reduce Resolution, and you have a client that runs an application in a seamless window, what will happen if the required resolution from the client is too high?

**A.** The connection will fail.

**B.** The application will automatically reduce the resolution of the session to match what the server can handle.

**C.** The application will launch in a remote desktop instead of a seamless window.

**D.** You will be prompted as to whether you would like to downgrade the resolution.

**6.** The MetaFrame XP server in the zone that stores information about the servers and published applications is known as what?

**A.** ICA browser

**B.** IMA browser

**C.** Data collector

**D.** Zone master

7. The Applications node of the Citrix Management Console allows you to do which of the following? (Choose all that apply.)

   A. Create HTML and ICA files for published applications.

   B. Assign load evaluators to one or more published applications.

   C. Identify the connection type being used by the published application.

   D. Identify the state of the ICA session currently accessing the application.

8. Which node or nodes in the Citrix Management Console allow you to set bandwidth limits for client printing? (Choose all that apply.)

   A. Servers node

   B. Printers node

   C. Printer Management node

   D. Client Connections node

9. What must be installed before the Load Evaluators node will show up in the Citrix Management Console?

   A. Load balancing, purchased separately

   B. A load-management license

   C. A Citrix MetaFrame XPa or XPe license

   D. Citrix Advanced Services

10. What must be installed on a workstation in order for the Citrix Management Console to work?

    A. Java Runtime Environment version 1.3

    B. Java Runtime Engine version 1.3

    C. Citrix MetaFrame XP

    D. Microsoft Management Console

**11.** If you already have an instance of the Java Runtime Environment installed on your computer that is not compatible with the Citrix Management Console, what will happen when the version of the Java Runtime Engine that is required by the Citrix Management Console is installed?

**A.** The current Java Runtime Environment will be overwritten with the version required by the Citrix Management Console.

**B.** The installation of the Citrix Management Console will stop. The installation of the console will not succeed until the other version of the Java Runtime Environment is uninstalled.

**C.** The Citrix Management Console will not run properly. You will receive an error message about the Java Runtime Environment.

**D.** The version of the Java Runtime Environment required by the Citrix Management Console will be installed and will not affect any other instances of the Java Runtime Environment.

**12.** If a client system is using a legacy ICA Client and you have selected the Disable Local Time Estimation check box, what is affected?

**A.** The client's time information is not synchronized with the MetaFrame XP server.

**B.** The timestamp for the files saved on the server will use the client's local time.

**C.** The server will use Greenwich Mean Time when saving the file.

**D.** The server's time will be used.

**13.** The Subnet License Allocation section of the Interoperability tab on the server farm Properties sheet is not visible. What is the most likely cause?

**A.** Your Citrix Administrator account has not been granted the Read-Write privilege.

**B.** The server farm is in mixed mode.

**C.** The server farm is in native mode.

**D.** You have not activated any connection licenses.

**14.** After installing the first MetaFrame XP server in a new zone, what is its data collector preference set to?

**A.** Most Preferred

**B.** Preferred

**C.** Default Preference

**D.** Not Preferred

**15.** What is the command used to change the XML port?

**A.** `icaport`

**B.** `chgxml`

**C.** `ctxxmlss /`*`rnnn`*

**D.** `xmlport`

**16.** When you access a server's properties, the Interoperability tab is not available. What is the most likely cause?

**A.** Your Citrix Administrator account has not been granted the Read-Write privilege.

**B.** The server farm is in mixed mode.

**C.** The server farm is in native mode.

**D.** You have not activated any connection licenses.

**17.** You purchase an upgrade license pack to upgrade your server from MetaFrame XPa to XPe, install the additional software, and enter the serial number in the Licenses node, but your server does not show the Citrix Installation Manager node. What is the reason?

**A.** You have the Read-Only privilege in the server farm.

**B.** Installation Management Services is an add-on that does not ship with the upgrade pack.

**C.** You did not add the product code from the upgrade license to the server.

**D.** You have not activated the licenses.

**18.** A user with a stand-alone terminal is attempting to open a published application, but is unable to do so. Other applications run from the terminal device. When the same user moves to a Windows-based PC, the application starts normally. What is the most likely cause of the application not starting on the terminal device?

**A.** The user does not have permissions to run the published application.

**B.** The Client Requirements options are set to require something the client device does not have available.

**C.** The published application has been disabled.

**D.** The client device is not configured to access the appropriate server.

**19.** You just finished publishing an application to two servers in your farm. When you look at the sessions in the Servers node, you notice that only one server is running the application sessions. Other applications are running on that server. What would cause this?

**A.** The published application path was not the same on the two servers.

**B.** The second server has the application disabled.

**C.** Logons are disabled for that server.

**D.** The second server did not have Installation Manager loaded.

**20.** You have installed MetaFrame XP on a new server and entered your original licenses from MetaFrame 1.8 into the pool. The Connection tab of the Licenses node does not show any of these licenses being used. What is the most likely cause?

**A.** The connection migration license was not added.

**B.** The upgrade license was not added.

**C.** The licenses are not assigned to any servers.

**D.** The licenses are not activated.

# Answers to Review Questions

1. B. Citrix Management Console is a centralized management and administration tool used to monitor and manage many aspects of MetaFrame XP operation from single-server to multiple-server farms.

2. A, B, D. Citrix Management Console takes the place of many utilities that were separate entities in MetaFrame 1.8. Many of these utilities are incorporated in Citrix Management Console, such as published applications, license information, etc. You cannot, however, manage or monitor MetaFrame 1.8 servers with Citrix Management Console.

3. C. The two options for rights levels are Read-Only and Read-Write. An administrator whom you wish to have full administrative control over the network should be given Read-Write rights.

4. C. To disable new logons to a MetaFrame XP server, right-click the server and select Properties from the menu. In the MetaFrame Settings tab, remove the check from the box labeled Enable Logons To This Server and click OK. This will only affect users trying to connect to that server. Direct connections to the server will be refused. Load-balanced published applications will not direct user sessions to that server.

5. C. If required resolution size from the client is too high and you have selected Reduce Resolution, the application will launch in a remote desktop instead of a seamless window.

6. C. Data collectors in the zone store information about the servers and published applications in the farm. The data collector knows the address of each server and applications that are available on each server in the zone.

7. A, B, C, D. From the Applications node of the Citrix Management Console, you can create HTML and ICA files and assign load evaluators to published applications. Use the tabs in the Applications node to see information about which published applications are being accessed.

8. A, C. Printer bandwidth can be set in two places: the Printer Management node and the Servers node.

9. C. Options available with Citrix MetaFrame XPa or XPe are not available in the Citrix Management Console until you install a license for them.

10. A. The Citrix Management Console can be installed on workstations by using the MetaFrame XP CD-ROM. Workstations must have the Java Runtime Environment version 1.3 installed.

11. D. The Citrix Management Console requires the Java Runtime Environment version 1.3. If another version is already installed on the workstation, but it is not a compliant version, the installation of the Citrix Management Console will install version 1.3. This will not affect the previous version, and they can both run simultaneously.

12. D. If this option is selected, any legacy ICA Clients that cannot report their local time will have all files timestamped with the server's time instead of the server attempting to estimate the client's time by using the client's time zone information.

13. C. In native mode, the servers do not have to allocate licenses to each subnet, as all of the licenses are available to all servers in the farm. If the server farm is in mixed mode, this section appears for the administrator to configure the license allocation.

14. A. The first server in the zone is configured as Most Preferred. All other servers are configured as Default Preference as they are installed.

15. C. When changing the port number used by the XML service, you need to use the `ctxxmlss` command and specify the port number you wish to change to.

16. C. When the server farm is in native mode, there are no MetaFrame 1.8 servers to communicate with, so the Interoperability tab is not available. In mixed mode, this tab is available so that the server can communicate with the ICA browser service.

17. C. Once you install the upgrade license pack, you must change the server's product code so that the server will use the MetaFrame XPe product license and activate the additional services.

18. B. The most likely cause of the problem is that the client device does not have a required option. For example, if the published application requires sound and the device does not have a sound card, the application will not start.

**19.** A. When an application is published to a server, the application path has to be correct or the server will not be able to start the session. You can modify the application's path by opening the application's properties and selecting the Edit Configuration button on the Servers tab.

**20.** A. Until you add a connection migration license, the original legacy license is not available for use by a MetaFrame XP server.

Chapter 6

# Other Administrative Tools

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **5. Additional Management Tools**

- 5a. Identify features of Citrix Server Administration
- 5b. Shadowing with the Shadow Taskbar
- 5c. Creating connections with the Citrix Connection Configuration
- 5d. Configure SpeedScreen Latency Reduction Manager

In the previous chapter, we discussed the new Citrix Management Console and how to use it. Citrix Management Console provides nearly all of the functionality we need in order to control our MetaFrame XP server farm. This centralized management tool cannot perform all of the functions we require as administrators, however. Very few implementations utilize a native-mode server farm from the outset; most have MetaFrame 1.8 servers and server farms in their environment until they are able to migrate to MetaFrame XP.

Since we need to be able to interoperate with these legacy systems, Citrix provided the tools to monitor and manage mixed-mode server farms. We will start this chapter with a discussion of one of these tools, *Citrix Server Administration*. Be forewarned that this tool should be used only with MetaFrame 1.8 and earlier; MetaFrame XP servers and server farms should be configured using Citrix Management Console.

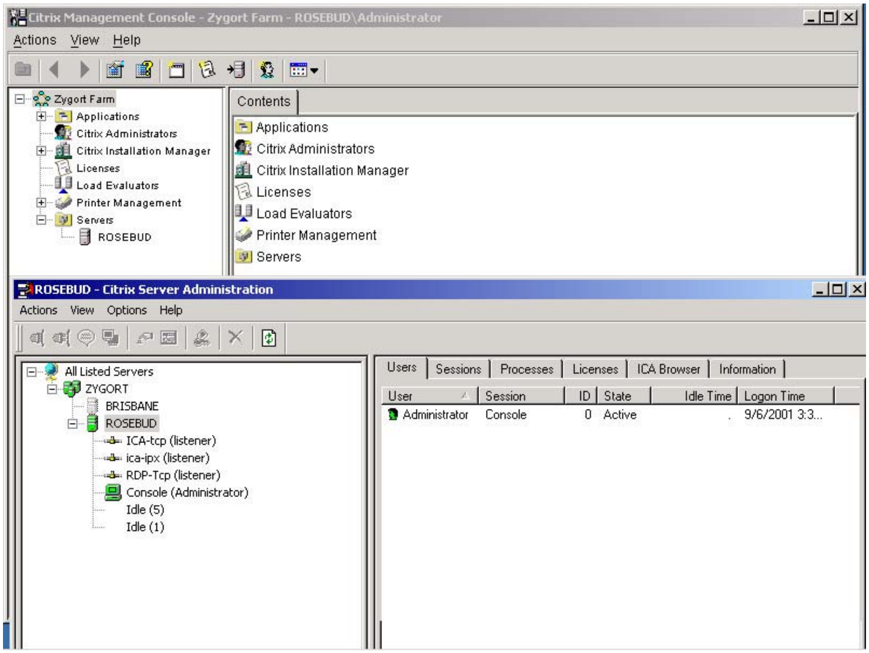
After the discussion of Citrix Server Administration, we will delve into the ever-popular topic of *shadowing*. You already know you like it—now we are going to discuss the finer details of this popular tool. After shadowing, the focus changes to a discussion of connections and how to control them. If you want to control all of the users connecting to a server, this is where you will need to pay attention, as global settings can be very powerful.

Finally, we will take another look at *SpeedScreen*, which we introduced in Chapter 2, “Underlying Citrix MetaFrame XP Technologies.” It will be a more thorough look this time, with emphasis on the server-side control of this tool. The client-side control is discussed in Chapter 11, “Program Neighborhood.” Until then, let’s start our chapter with the Citrix Server Administration tool.

# Identifying Citrix Server Administration Features

Citrix Server Administration is the tool used to control the server features of MetaFrame 1.*x* and WinFrame servers. The functionality of Citrix Server Administration is still alive and well, even when using MetaFrame XP, since it has been incorporated into the Citrix Management Console. As a matter of fact, after having read the previous chapter, you will see many similarities between the Servers node in the Citrix Management Console and Citrix Server Administration. For a comparison of the two utilities, see Figure 6.1.

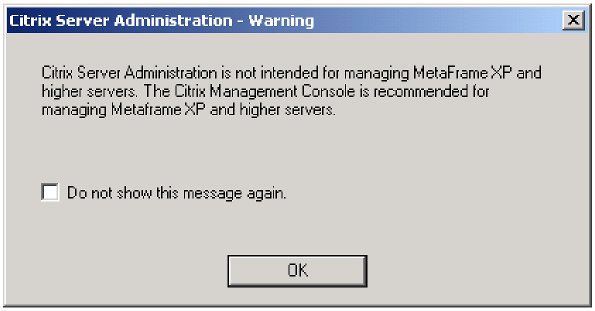
**FIGURE 6.1** Citrix Management Console and Citrix Server Administration



| User | Session | ID | State | Idle Time | Logon Time |
|---|---|---|---|---|---|
| Administrator | Console | 0 | Active | . | 9/6/2001 3:3... |

To start Citrix Server Administration, point to Start ➢ Programs ➢ Citrix ➢ MetaFrame XP ➢ Citrix Server Administration. Unless you have previously disabled the warning message, you will see the warning message shown in Figure 6.2.

**FIGURE 6.2** The Citrix Server Administration – Warning screen



Citrix Server Administration - Warning

Citrix Server Administration is not intended for managing MetaFrame XP and higher servers. The Citrix Management Console is recommended for managing Metaframe XP and higher servers.

☐ Do not show this message again.

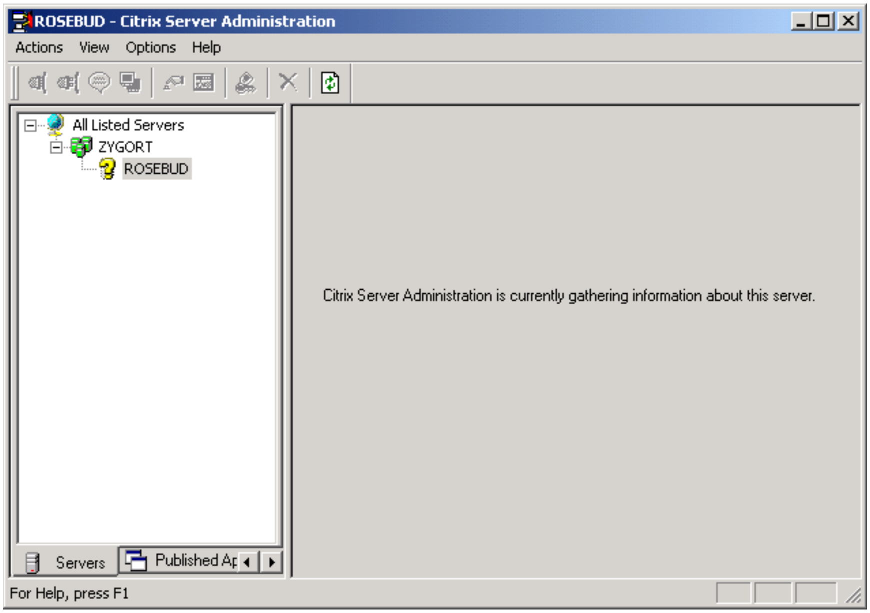
While this tool will run on any of the MetaFrame XP servers within your MetaFrame XP server farm, you should not use it to configure your MetaFrame XP servers. It is added to the installation by default because Citrix Systems knows that most of the server farms will be used in mixed mode and administrators will want to have the tool installed at their point of administration. Do heed this warning screen, however. While most administrators are familiar with Citrix Server Administration, there are many functions that are specific to MetaFrame XP that you cannot configure with this tool. You will need to become familiar with the Citrix Management Console when working with MetaFrame XP server farms.

The first time Citrix Server Administration opens, it tries to enumerate the servers in the server farm. Figure 6.3 shows the initial view as CSA contacts the ICA master browser for server information. As it gathers each server's information, the question mark beside the server name changes to a server icon.

Once a server is available to work with, you can perform the following functions from within Citrix Server Administration:

- Display information about servers, sessions, published applications, users, and processes.
- Connect and disconnect sessions.
- Log off users from a session.
- Shadow Citrix ICA sessions (but only if you are in a session when you open the Citrix Server Administration tool).
- Send messages to users.
- Reset sessions.
- Display status information about a session.
- Terminate processes.

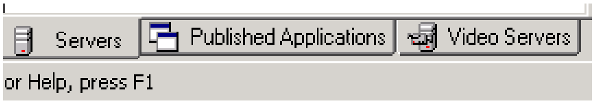
**FIGURE 6.3** Discovering the servers



Citrix Server Administration is currently gathering information about this server.

Citrix Server Administration divides the information that you will need to work with into three separate sections. Notice the three tabs shown partially at the bottom of the left-hand pane in Figure 6.3 and shown in more detail in Figure 6.4: Servers, Published Applications, and Video Servers. The first tab is the most used. It holds information about the server farm and all of the servers and sessions. When you select the second tab, you will see information about the published applications in the server farm. The final tab is used with the VideoFrame product that was released for MetaFrame 1.8. Since this tab is beyond the scope of this book, we will not be reviewing it. We'll take a closer look at options available in these tabs in the following sections.

**FIGURE 6.4** The Citrix Server Administration control tabs



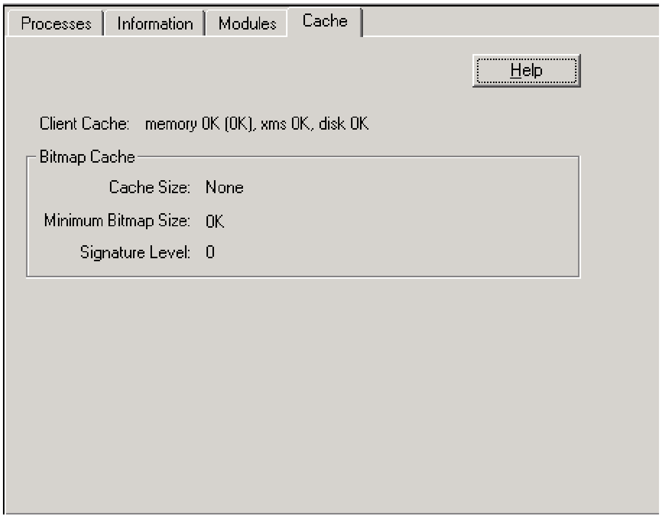
## The Servers Configuration Tabs

Each of the configuration levels in the Servers control tab has many tabs that display information and allow us to manage our MetaFrame environment. We are going to take a look at each of the tabs in alphabetical order. We will identify where each tab may be found and what is available on each one.

### Cache Tab

Displayed at the Session level, the *Cache tab* details the cache information for the client, as shown in Figure 6.5. It includes information about the amount of cache used on the client as well as the amount of cache available for use by the client.

**FIGURE 6.5** The Cache tab



Client Cache: memory 0K (0K), xms 0K, disk 0K

Bitmap Cache

Cache Size: None

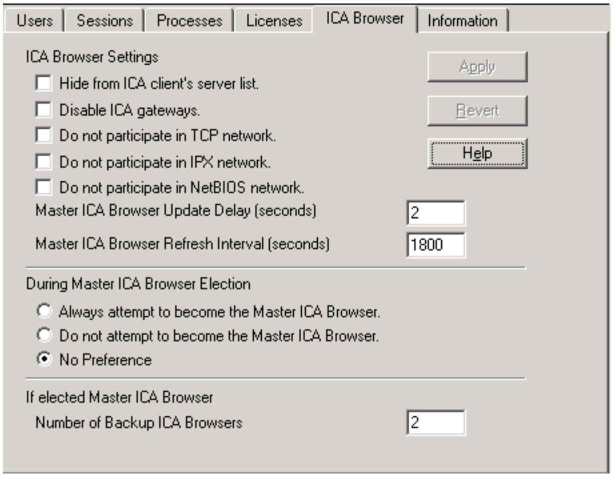
Minimum Bitmap Size: 0K

Signature Level: 0

### ICA Browser Tab

This tab contains a screen of ICA browser configuration options, as shown in Figure 6.6. If the server is running in mixed mode, this tab allows you to configure how the server will work with the ICA browser. By default, the ICA browser function is taken over by a MetaFrame XP server once the server farm is put in mixed mode.

**FIGURE 6.6** The ICA Browser tab



ICA Browser Settings

- □ Hide from ICA client's server list.
- □ Disable ICA gateways.
- □ Do not participate in TCP network.
- □ Do not participate in IPX network.
- □ Do not participate in NetBIOS network.

Master ICA Browser Update Delay (seconds) 2

Master ICA Browser Refresh Interval (seconds) 1800

During Master ICA Browser Election

- ○ Always attempt to become the Master ICA Browser.
- ○ Do not attempt to become the Master ICA Browser.
- ● No Preference

If elected Master ICA Browser

Number of Backup ICA Browsers 2

If you do not want clients to see the server, but see only the published applications on the server, you can select the Hide From ICA Client's Server List option in the ICA Browser Settings section. This option allows you to use the server to host published applications but does not allow clients to use it to start a desktop session, unless they know the IP address of the server, in which case they can start a desktop session by contacting the server via its IP address. The second option in this section allows you to disable the ICA gateway function on the server. In a mixed-mode server farm, this option does nothing since the gateway function is taken over by a MetaFrame XP server.

Three check boxes on this tab control which protocols the browser will use to communicate. If you select any of these three options, you will disable the browser function on the specified protocol. Once you select the option, the server will no longer appear in a client's server list and the client will not be able to connect to the published applications on the server. One other point to note: If the protocol you select is the only protocol on the server, the server will no longer participate in the server farm and will not take advantage of pooled licenses.

To control the ICA browser updates and refreshes, you can enter values in the Master ICA Browser Update Delay (Seconds) and Master ICA Browser Refresh Interval (Seconds) fields. The update option specifies how long you want to wait after a client connects or disconnects to the server until the ICA browser on this server updates the master ICA browser of the connection or disconnection. The refresh interval is the length of time the ICA browser will wait before updating the master ICA browser of its current status.

The middle section of this tab controls the election criteria for the ICA browsing service. Don't confuse this with the data collector election. The ICA browser is used only in a mixed-mode server farm, and then only so that legacy clients can find servers and published applications. The higher the setting, the more likely a server will become the master ICA browser should the original fail. The Always Attempt To Become The Master ICA Browser setting will cause the server to always force an election when it is rebooted. The Do Not Attempt To Become The Master ICA Browser setting will keep the server from participating in elections. No Preference is the default setting, so the server will try to become the master ICA browser only when no other servers are configured to Always Attempt.

At the bottom of the tab is the Number Of Backup Master ICA Browsers input box. When a server is elected as a master ICA browser, it needs to determine the license allocation for the server farm. The new master ICA browser collects farm information from all the MetaFrame servers. Then it receives the information that the backup browsers had from the original master browser. Using that information, the new master ICA browser sends out its farm information to the backup browsers. By entering a number here, you can control the number of backup ICA browsers that collect and send the license information.

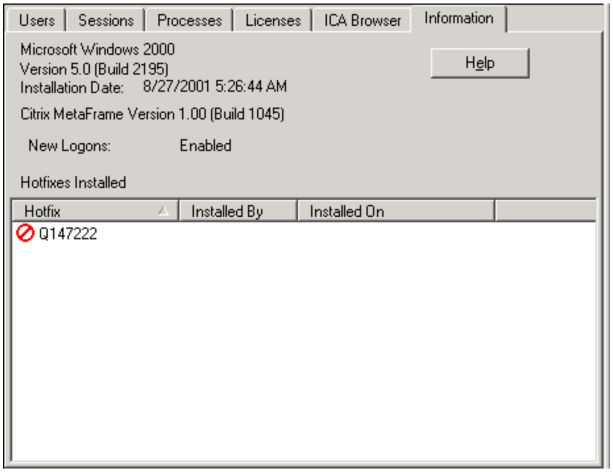
## ICA Gateways Tab

This tab is found at the root level, All Listed Servers. In mixed mode, this tab serves no function since a MetaFrame XP server performs the gateway function.

## Information Tab

This tab contains exactly what it sounds like—information about the server. Found at the Servers and Session levels, the information contained on this tab includes the operating system on which MetaFrame is installed, the installation date, whether access is allowed to the server, the MetaFrame build number, and any hotfixes that are applied to the server. See Figure 6.7 for a view of this tab.

**FIGURE 6.7** The Information tab



Microsoft Windows 2000
Version 5.0 (Build 2195)
Installation Date: 8/27/2001 5:26:44 AM

Citrix MetaFrame Version 1.00 (Build 1045)

New Logons: Enabled

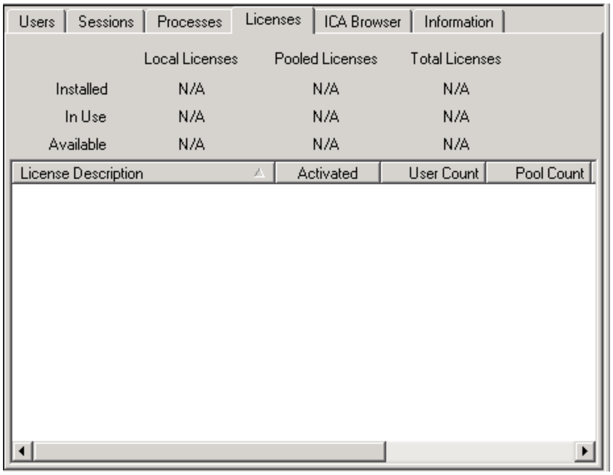
Hotfixes Installed

| Hotfix | Installed By | Installed On |
|---|---|---|
| Q147222 | | |

## Licenses Tab

Found on the All Listed Servers, Server Farm, and Server levels, the Licenses tab, shown in Figure 6.8, displays information about the licenses installed on a server and those pooled in the server farm. At the All Listed Servers level, it shows the number of pooled licenses by subnet and those assigned to servers. The Server Farm level displays the license numbers that are installed within the farm, while the Server level shows the licenses that are available to be pooled within the farm and the licenses that are assigned to the server.

**FIGURE 6.8** The Licenses tab



| | Local Licenses | Pooled Licenses | Total Licenses |
|---|---|---|---|
| Installed | N/A | N/A | N/A |
| In Use | N/A | N/A | N/A |
| Available | N/A | N/A | N/A |

| License Description | Activated | User Count | Pool Count |
|---|---|---|---|

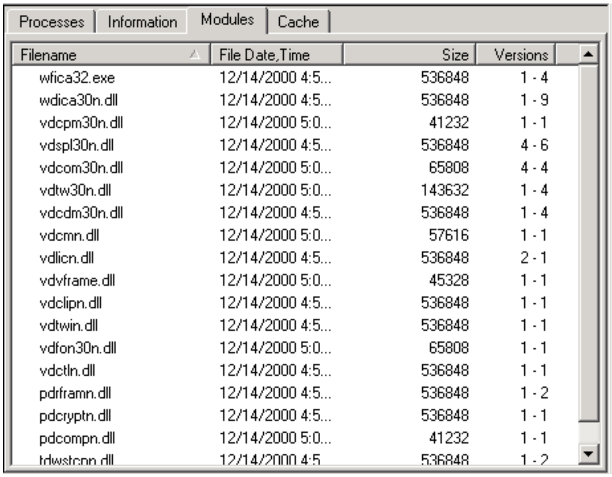
The following columns are available:

| Column | Function |
|---|---|
| Server | Shows the server where the license is installed. |
| License Description | Indicates the type of license installed. |
| Activated | Shows whether the license is activated or not. |
| User Count | Indicates the number of user licenses available. |
| Pool Count | Indicates the number of user licenses allocated to the pool. |
| License Number | Provides the serial number of the license. |

## Modules Tab

Found only when a session is selected, the *Modules* tab provides information about the software modules that are used for session creation, processing, and communication. See Figure 6.9 for a view of this tab.

**FIGURE 6.9** The Modules tab



| Filename | File Date,Time | Size | Versions |
|---|---|---|---|
| wfica32.exe | 12/14/2000 4:5... | 536848 | 1 - 4 |
| wdica30n.dll | 12/14/2000 4:5... | 536848 | 1 - 9 |
| vdcpm30n.dll | 12/14/2000 5:0... | 41232 | 1 - 1 |
| vdspl30n.dll | 12/14/2000 4:5... | 536848 | 4 - 6 |
| vdcom30n.dll | 12/14/2000 5:0... | 65808 | 4 - 4 |
| vdtw30n.dll | 12/14/2000 5:0... | 143632 | 1 - 4 |
| vdcdm30n.dll | 12/14/2000 4:5... | 536848 | 1 - 4 |
| vdcmn.dll | 12/14/2000 5:0... | 57616 | 1 - 1 |
| vdlicn.dll | 12/14/2000 4:5... | 536848 | 2 - 1 |
| vdvframe.dll | 12/14/2000 5:0... | 45328 | 1 - 1 |
| vdclipn.dll | 12/14/2000 4:5... | 536848 | 1 - 1 |
| vdtwin.dll | 12/14/2000 4:5... | 536848 | 1 - 1 |
| vdfon30n.dll | 12/14/2000 5:0... | 65808 | 1 - 1 |
| vdctln.dll | 12/14/2000 4:5... | 536848 | 1 - 1 |
| pdrframn.dll | 12/14/2000 4:5... | 536848 | 1 - 2 |
| pdcryptn.dll | 12/14/2000 4:5... | 536848 | 1 - 1 |
| pdcompn.dll | 12/14/2000 5:0... | 41232 | 1 - 1 |
| tdwstcpn.dll | 12/14/2000 4:5 | 536848 | 1 - 2 |

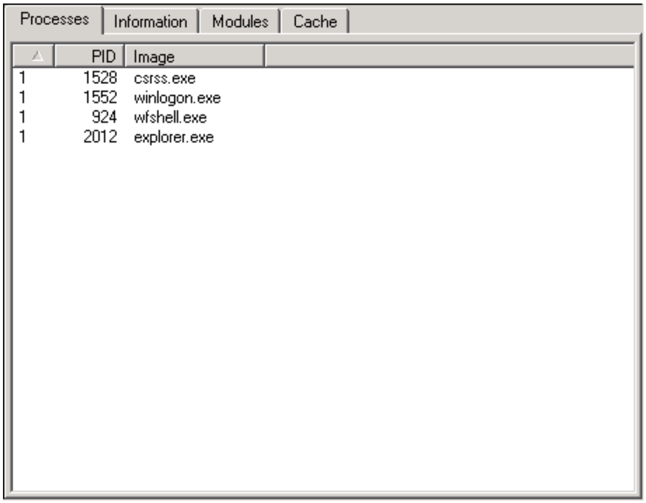
The following columns are available:

| Column | Function |
|---|---|
| Filename | Shows the name of the module loaded. |
| File Date, Time | Indicates the creation date and time of the module. |
| Size | Indicates the file size of the module. |
| Versions | Lists software versions that can use the module. |

## Processes Tab

The *Processes* tab, found at all levels, displays the processes that are running on the server and the sessions that are using each process. See Figure 6.10 for a view of this tab.

**FIGURE 6.10** The Processes tab



```
      PID  Image
1    1528  csrss.exe
1    1552  winlogon.exe
1     924  wfshell.exe
1    2012  explorer.exe
```

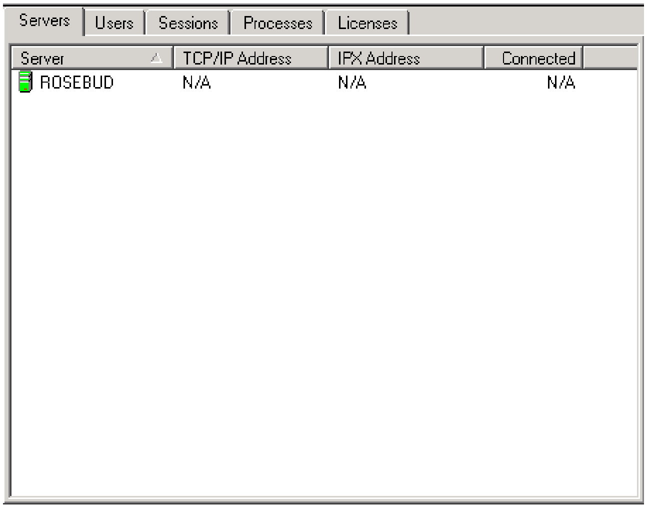
The following columns are available:

| Column | Function |
|---|---|
| User | Shows the username that is accessing the session using the process. |
| Session | Shows the session that is using the process. |
| ID | Indicates the session ID. |
| PID | Indicates the ID number assigned to the process by the operating system. |
| Image | Provides the filename of the process. |

## Servers Tab

Found on the All Listed Servers and Server Farm levels, this tab displays information about the server installed in the server farm. See Figure 6.11 for details.

**FIGURE 6.11** The Servers tab



| Server | TCP/IP Address | IPX Address | Connected |
|---|---|---|---|
| ROSEBUD | N/A | N/A | N/A |

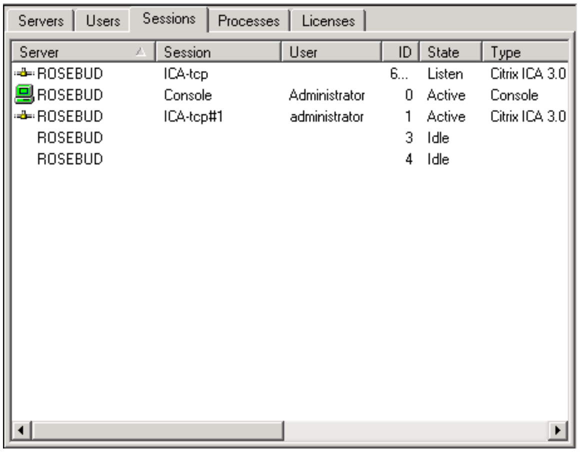
The following columns are available:

| Column | Function |
|---|---|
| Server | Shows the name of the server. |
| TCP/IP Address | Provides the TCP/IP address of the server, if applicable. |
| IPX Address | Provides the IPX address of the server, if applicable. |
| Connected | Indicates the number of sessions connected. |

## Sessions Tab

This tab is found on the All Listed Servers, Server Farm, and Server levels and contains information about each of the sessions started. See Figure 6.12 for details.

**FIGURE 6.12** The Sessions tab



| Server | Session | User | ID | State | Type |
|---|---|---|---|---|---|
| ROSEBUD | ICA-tcp | | 6... | Listen | Citrix ICA 3.0 |
| ROSEBUD | Console | Administrator | 0 | Active | Console |
| ROSEBUD | ICA-tcp#1 | administrator | 1 | Active | Citrix ICA 3.0 |
| ROSEBUD | | | 3 | Idle | |
| ROSEBUD | | | 4 | Idle | |

The following columns are available:

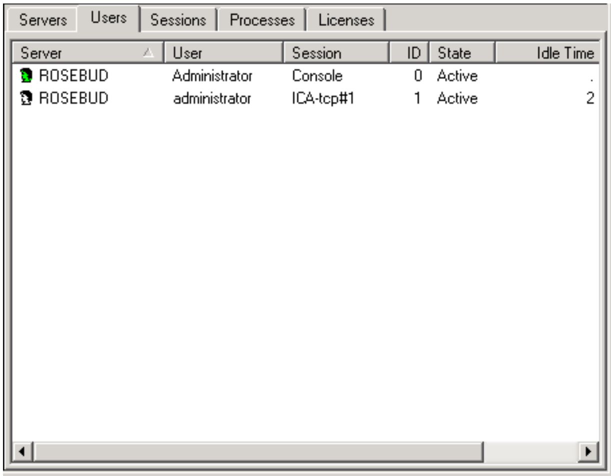
| Column | Function |
|---|---|
| Server | Shows the name of the server. |
| Session | Shows the name of the connected session on the server. |
| User | Shows the name of the user connected to the session on the server. |

| Column | Function |
|---|---|
| ID | Provides the session ID. |
| State | Indicates the state of the session. |
| Type | Indicates the type of session, usually client or console. |
| Client Name | Shows the client name of the session, if applicable. |
| Idle Time | Shows the number of minutes since the last keyboard or mouse input at the session. |
| Logon Time | Indicates the time at which the user logged on, if applicable. |
| Comment | Contains additional information about the session, such as its location. This field is optional. |

## Users Tab

Found at all of the levels with the exception of the Session level, the Users tab displays all of the users who have initiated sessions. The information presented on this screen, shown in Figure 6.13, allows an administrator to view the users who are connected to MetaFrame servers and indicates the current state of the connection.

**FIGURE 6.13** The Users tab



| Server | User | Session | ID | State | Idle Time |
|---|---|---|---|---|---|
| ROSEBUD | Administrator | Console | 0 | Active | . |
| ROSEBUD | administrator | ICA-tcp#1 | 1 | Active | 2 |

The following table describes the columns available:

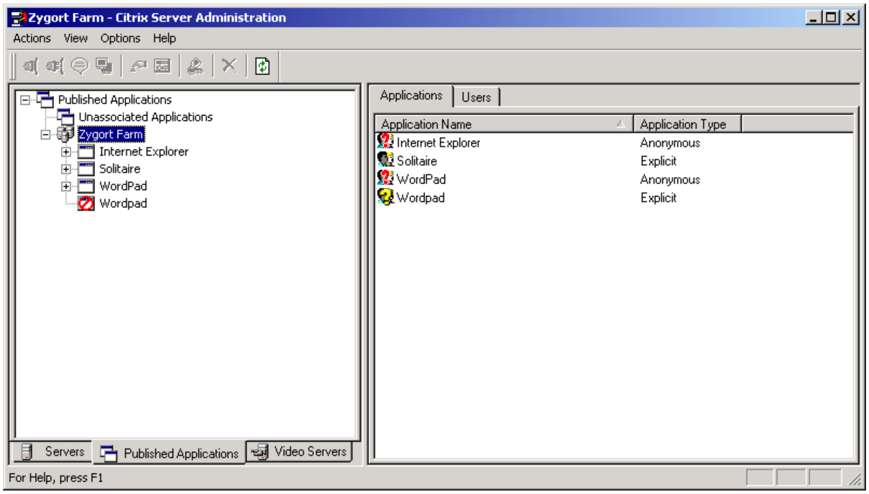
| Column | Function |
|---|---|
| Server | Shows the name of the server. |
| User | Shows the account used to start the session and access the published application. |
| Session | Identifies the connection used. This is a combination of the connection type and the ICA session ID. |
| ID | Displays the unique number assigned to the connection. |
| State | Indicates whether the session accessing the published application or remote desktop is in an Active or Disconnected state. |
| Idle Time | Indicates the amount of time the session has been in an Idle state. |
| Logon Time | Displays the time the session was started. |

These tabs in the Servers section see the most use when you administer MetaFrame 1.8 servers within your server farm. The other section, Published Applications, is not used nearly as much, but it still sees a lot of action. Let's take a look at the tabs available when working with it.

## The Published Applications Configuration Tabs

The three levels discussed in this section represent the applications in use depending upon what is encompassed at each level. The top level, *Published Applications*, displays all applications published within every farm. The second level, *Unassociated Applications*, displays those applications that are published under NT Domain scope within a MetaFrame 1.*x* server farm. The final level, *Server Farm*, shows the applications that are published within the farm itself. Two tabs are available for viewing information at this level, Applications and Users, as shown in Figure 6.14.

**FIGURE 6.14** The Published Applications configuration tab showing the Applications tab



| Application Name | Application Type |
|---|---|
| Internet Explorer | Anonymous |
| Solitaire | Explicit |
| WordPad | Anonymous |
| Wordpad | Explicit |

## Applications Tab

This tab displays the application that is published and indicates whether the application is published explicitly or anonymously. The following columns are available:

| Column | Function |
|---|---|
| Application Name | Shows the name of the published application. |
| Application Type | Indicates explicit or anonymous access. |

## Users Tab

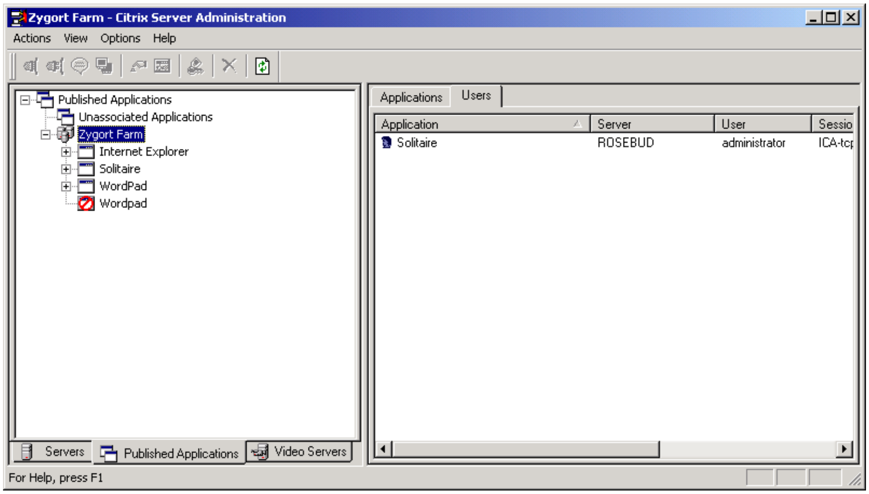
The Users tab displays information about the users running published application sessions. See Figure 6.15 for details.

The following columns are available:

| Column | Function |
|---|---|
| Application | Gives the name of the published application. |
| Server | Gives the name of the server on which the published application session is running. |

| Column | Function |
|---|---|
| User | Indicates the account that is running the application. |
| Session | Provides the Session ID of the session used to run the published application. |
| ID | Identifies the session. |
| State | Indicates whether the session is in an Active, Disconnected, Idle, etc. state. |
| Idle Time | Shows the amount of time the session has been idle. |
| Logon Time | Indicates when the session became active. |

**FIGURE 6.15** The Published Applications configuration tab showing the Users tab



| Application | Server | User | Sessio |
|---|---|---|---|
| Solitaire | ROSEBUD | administrator | ICA-tcp |

These tabs are very useful when the administrator needs to determine the published application usage. You can view the information concerning individual users and their application access, find out which applications are not in use, and decide which applications you may need to reset because they are not functioning. In the next section, we will discuss some of the functionality built into these configuration tabs.

## Configuration Options

Right-clicking an object to bring up its context menu allows you to perform functions based on the object selected, as shown in Figure 6.16. If you right-click an object from any of the tabs, you are presented with the options Connect, Disconnect, Send Message, Shadow, Reset, Status, Logoff, Enable New Logons, and Disable New Logons. The options available vary depending on the object selected. For example, selecting a server brings up the following options:

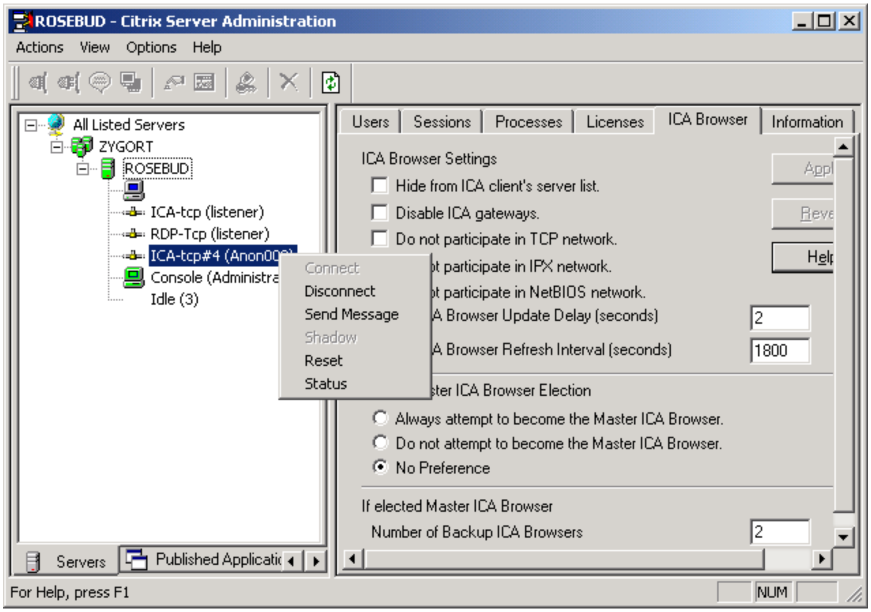
**Connect** Allows you to connect to a server and gather information about it.

**Disconnect** Disconnects Citrix Server Administration from the server.

**Enable New Logons** Allows the server to accept session requests from clients.

**Disable New Logons** Stops new sessions from being created on the server while existing sessions may continue.

**FIGURE 6.16** A sample context menu



ICA Browser Settings

☐ Hide from ICA client's server list.

☐ Disable ICA gateways.

☐ Do not participate in TCP network.

☐ ...t participate in IPX network.

☐ ...t participate in NetBIOS network.

...A Browser Update Delay (seconds) 2

...A Browser Refresh Interval (seconds) 1800

...ter ICA Browser Election

○ Always attempt to become the Master ICA Browser.

○ Do not attempt to become the Master ICA Browser.

● No Preference

If elected Master ICA Browser

Number of Backup ICA Browsers 2

The options in the context menu are also available from icons at the top of the Citrix Server Administration screen. Most of these icons should appear familiar since they have been adopted into the Citrix Management Console. Table 6.1 shows each icon and its function.

**TABLE 6.1** Citrix Server Administration Icons

| Icon | Function |
|---|---|
| | Connects to a server session. |
| | Disconnects from a server session. |
| | Sends a message to the selected user. |
| | Initiates shadowing of a session. |
| | Resets a session. |
| | Views the status of a session. |
| | Logs off a user's session. |
| ✕ | Ends a process. |
| | Refreshes the Citrix Server Administration information. |

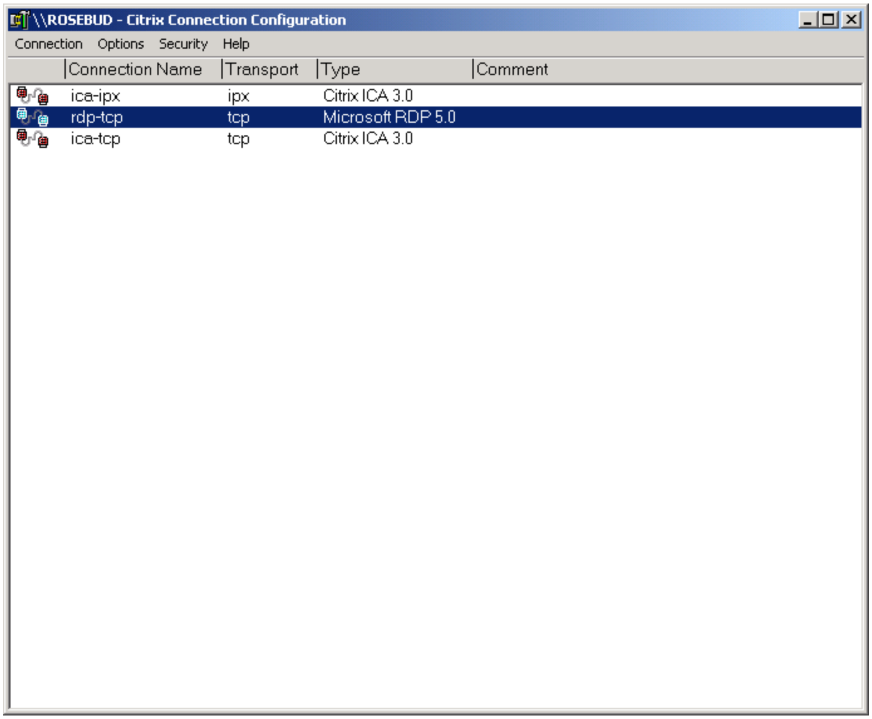
Now that we have examined the Citrix Server Administration utility, we need to move on to other management utilities found within the MetaFrame tools. The first tool we are going to look at is the Citrix Connection Configuration (CCC) utility.

# Using Citrix Connection Configuration

When you first open the Citrix Connection Configuration utility, it appears to be a rather unassuming tool, as shown in Figure 6.17. It reminds us of the Terminal Server Connection Configuration tool found in Windows NT Server 4.0, Terminal Server Edition (TSE) or the Terminal Server Configuration tool found in Windows 2000 Server when Terminal Services are added. However, this utility has additional functionality to allow you to control ICA connections.

You can control each of the connection types appearing in this screen by right-clicking the connection and choosing one of the options found on the context menu or by using the menu items at the top of the screen. The only option that is not available from the context menu is the ability to create a new connection. The other options, Copy, Delete, Edit, Rename, Enable, Disable, and Permissions, are easily accessible.

**FIGURE 6.17** The Citrix Connection Configuration utility



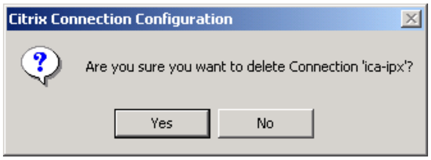
| Connection Name | Transport | Type | Comment |
|---|---|---|---|
| ica-ipx | ipx | Citrix ICA 3.0 | |
| rdp-tcp | tcp | Microsoft RDP 5.0 | |
| ica-tcp | tcp | Citrix ICA 3.0 | |

**Copy** Copy creates another connection based on the currently selected connection. If you add another network adapter to your server, you may want to copy the information from the original connection to a new connection, allowing the same level of control over the new adapter.

**Delete** Take one guess at what happens when you choose the Delete option. Of course, the obvious, but there is a warning that appears, giving you the option of allowing the connection to be deleted or not, as shown in Figure 6.18. If you are deleting the only connection for a given protocol, you will be presented with a warning also.

**Edit** When you choose this option, the Edit Connection dialog box appears, allowing you to configure the connection properties. We will take a look at all of the options available from this dialog box in the "Edit Connection" section.

**FIGURE 6.18** The deletion warning message

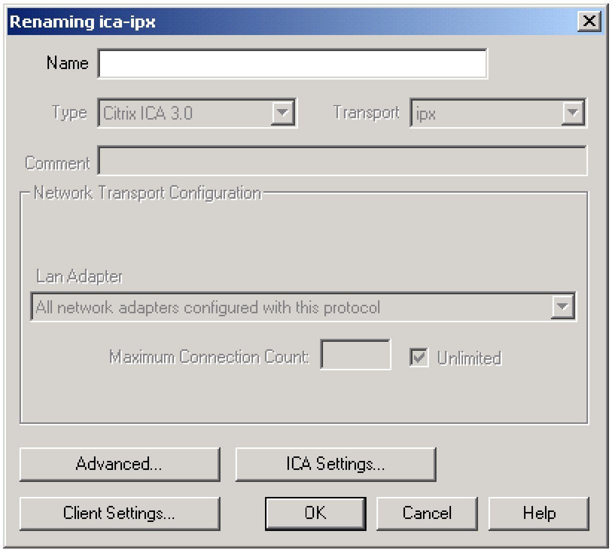


Citrix Connection Configuration

Are you sure you want to delete Connection 'ica-ipx'?

**Rename** If you choose this option, you will see the dialog box shown in Figure 6.19. You can change the connection name, but the default options are self-explanatory.

**FIGURE 6.19** The Rename option



Renaming ica-ipx

Name

Type Citrix ICA 3.0

Transport ipx

Comment

Network Transport Configuration

Lan Adapter

All network adapters configured with this protocol

Maximum Connection Count: ☑ Unlimited

**Enable** You can change any connection that is disabled to allow connections by selecting this option. Once selected, the connection icon appears in color.

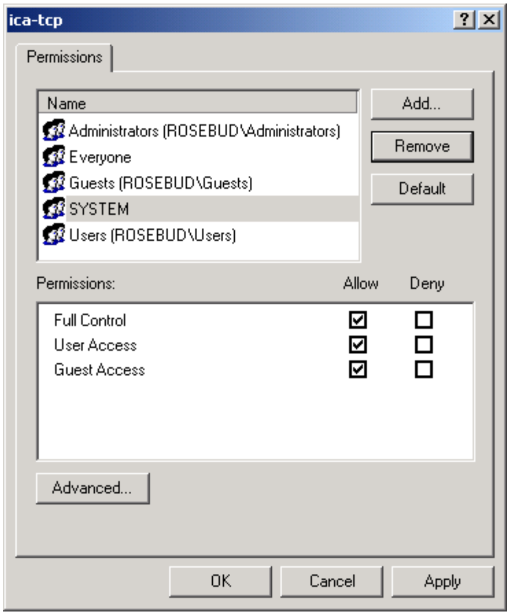
**Disable** You can change any connection that is enabled to not allow connections by selecting this option. Once selected, the connection icon appears grayed out.

**Permissions** The last option on the menu opens a dialog box that allows you to assign permissions to users or groups. The following section details the options available from the Permissions menu item.

## Connection Permissions

When you choose to set permissions on a connection, the screen shown in Figure 6.20 appears. The upper window shows the names of the accounts that have been added to the access control list. The lower window displays the level of permissions granted to those accounts. As with any permissions list, the accounts added to the list may be groups or users. In order to make administration easier, you should always assign permissions to group accounts and add the user accounts to the groups.

**FIGURE 6.20** The connection's Permissions dialog box


ica-tcp

Permissions

Name
Administrators (ROSEBUD\Administrators)
Everyone
Guests (ROSEBUD\Guests)
SYSTEM
Users (ROSEBUD\Users)

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | ☑ | □ |
| User Access | ☑ | □ |
| Guest Access | ☑ | □ |

Three permission options, known as the standard permissions, are available at this point. These permissions are actually combinations of multiple permissions. Assigning permissions in this manner is easier than assigning individual permissions, since the most commonly used permissions are grouped together.

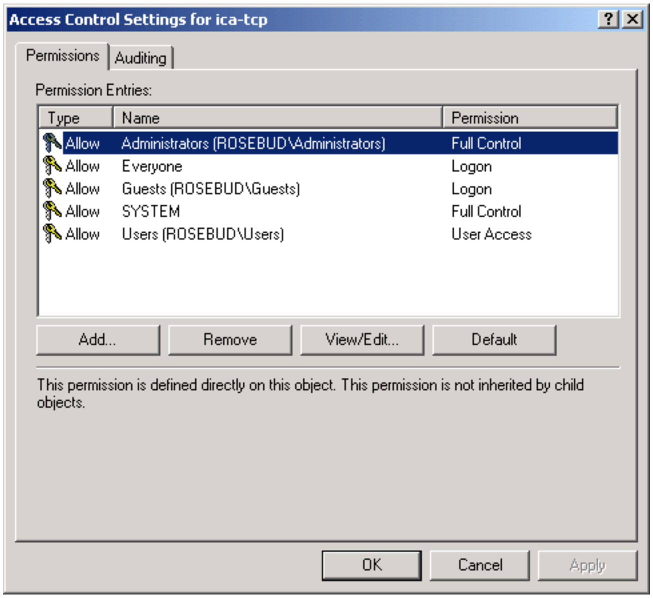
**Full Control** In effect, all permissions are assigned. An account with the Full Control permission assigned has complete control over the connection and may modify the connection if granted the proper level of administrative control from within Citrix Management Console.

**User Access** An account with the User Access level of permission can access information about the session, log on to a session, send messages, and connect to the session if the session is in a Disconnected state.

**Guest Access** Accounts granted Guest Access will be able to log on to a session but will be unable to perform any other function with the connection.

These standard permissions are adequate for most situations; however, there may be special occasions when these groupings of permissions do not meet your needs. If you deem it necessary to use special permissions for an account, click the Advanced button to see the dialog box shown in Figure 6.21.

**FIGURE 6.21** Advanced permissions



| Type | Name | Permission |
|---|---|---|
| Allow | Administrators (ROSEBUD\Administrators) | Full Control |
| Allow | Everyone | Logon |
| Allow | Guests (ROSEBUD\Guests) | Logon |
| Allow | SYSTEM | Full Control |
| Allow | Users (ROSEBUD\Users) | User Access |

This permission is defined directly on this object. This permission is not inherited by child objects.

The Permissions tab in the Access Control Settings dialog box displays the accounts for which you have already granted permissions and the level of permission assigned. From this tab, you can add and remove accounts or change the permissions on existing accounts. The following buttons allow you to perform these functions:

**Add** Allows an administrator to add accounts into the access control list and assign permissions to the account.

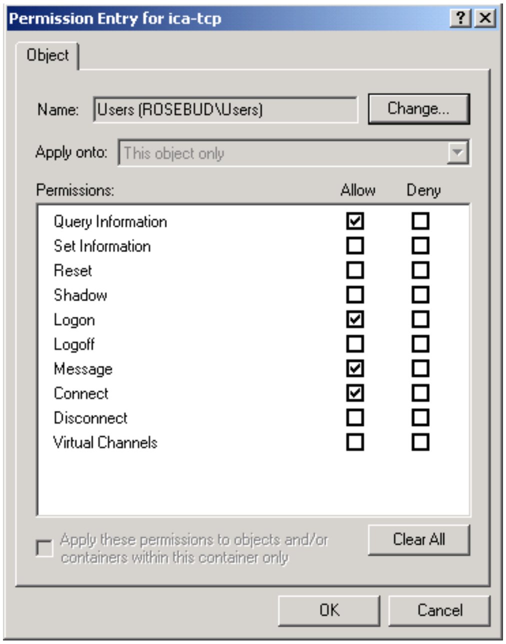
**Remove** Allows an administrator to delete accounts from the access control list, thus implicitly denying the account access to the connection.

**View/Edit** Allows an administrator to view the permissions assigned to accounts and modify those permissions if necessary.

**Default** Changes the access control list to the default list provided by MetaFrame XP.

To modify the permissions, select the account you need to modify and click the View/Edit button. This brings up the special permissions access control list shown in Figure 6.22. Essentially, this dialog box looks like the standard permissions version, but this list contains more permission options.

**FIGURE 6.22** Special permissions access control list



Name: Users (ROSEBUD\Users)

Apply onto: This object only

| Permissions: | Allow | Deny |
|---|---|---|
| Query Information | ☑ | ☐ |
| Set Information | ☐ | ☐ |
| Reset | ☐ | ☐ |
| Shadow | ☐ | ☐ |
| Logon | ☑ | ☐ |
| Logoff | ☐ | ☐ |
| Message | ☑ | ☐ |
| Connect | ☑ | ☐ |
| Disconnect | ☐ | ☐ |
| Virtual Channels | ☐ | ☐ |

☐ Apply these permissions to objects and/or containers within this container only

The special permissions and what they allow an account to do are shown here:

| Permission | Ability |
|---|---|
| Query Information | Query information about the session. |
| Set Information | Modify connection parameters. |
| Reset | Reset the session. |

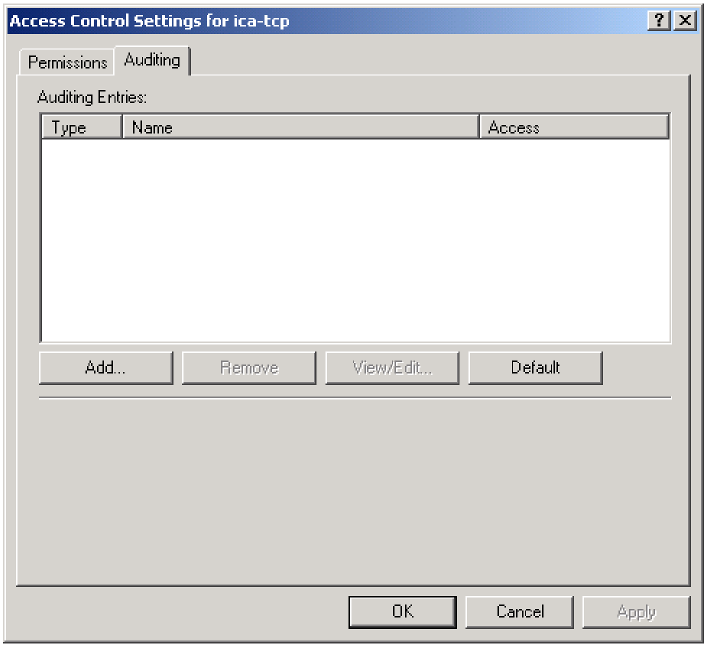
| Permission | Ability |
|---|---|
| Shadow | Shadow a session. |
| Logon | Log on to a session. |
| Logoff | Remotely log off another session. |
| Message | Send messages to sessions. |
| Connect | Connect to a disconnected session. |
| Disconnect | Disconnect a session remotely. |
| Virtual Channels | Disable the use of virtual channels. |

The other tab that is available from the Advanced section is Auditing, shown in Figure 6.23. From this tab, you can log information about the accounts that have access to the connection. This Auditing tab offers the same functionality as any Auditing tab within Windows 2000. Click the Add button and select the account you would like to monitor. This is a very handy place to select the Everyone group so that you are able to watch every type of access on the connection.

Once you select the account you wish to *audit*, you are presented with the permissions. Select those permissions you need to watch. For example, if you wish to view all logons on the connection, you can specify that the success of the logon be audited. Then any successful logon will be noted in the Security log. The same may be applied to failures. If your server does not allow logons during certain times of the day, you may want to select the failure option to record any failed attempts in the Security log.

One rule of thumb, however: You should audit only those items that need to be watched. Auditing does consume resources. The more auditing that goes on, the more processing is performed for auditing, taking away from the processing of sessions. Now let's look at the configuration options available when you choose Edit from the connection's context menu.

**FIGURE 6.23** The Auditing tab

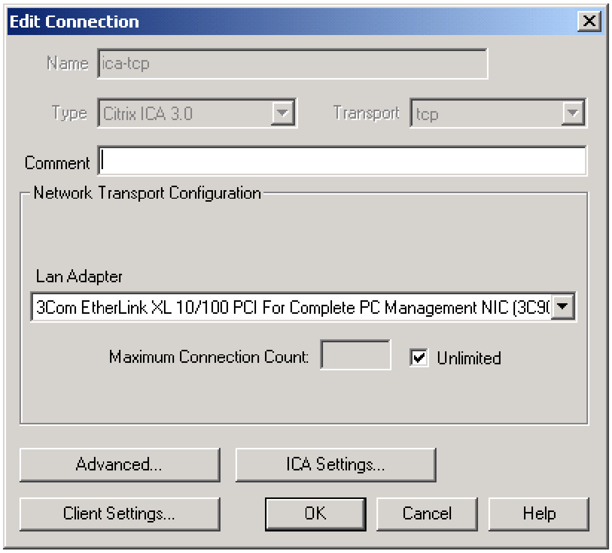


## Edit Connection

Each connection can be fine-tuned and controlled from the Edit Connection dialog box, shown in Figure 6.24. From here, the administrator can configure connection settings to allow global control over all of the clients using the connection. The opening screen allows you to insert a comment concerning the connection, which will then show up in the Citrix Connection Configuration window, change the adapter used for the connection, and set the number of connections allowed at any one time. You can also achieve a finer level of control through the buttons at the bottom of the screen.

If you change the adapter, a warning dialog will appear, explaining that all sessions currently using that adapter will be disconnected. The default number of users is Unlimited. If you have a reason to limit the number of sessions running over this connection, deselect the check box and enter the number of users you would like to allow on the connection.

**FIGURE 6.24** Edit Connection dialog box



Edit Connection

Name: ica-tcp

Type: Citrix ICA 3.0

Transport: tcp

Comment:

Network Transport Configuration

Lan Adapter: 3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C9(

Maximum Connection Count: ☑ Unlimited

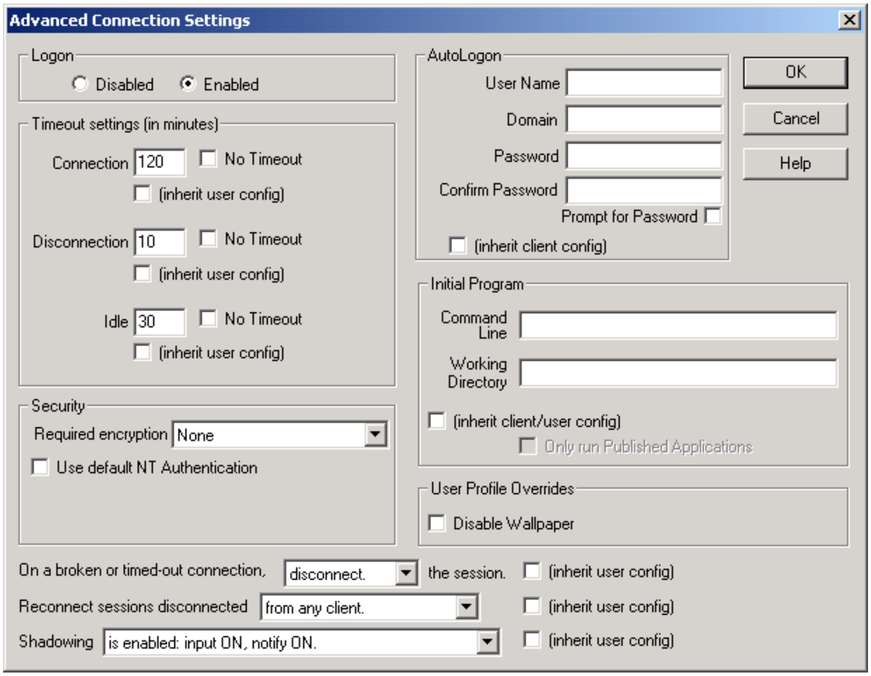
The Advanced, ICA Settings, and Client Settings buttons are the primary means of configuring the connection. When you click each button, you can control exactly what is allowed on the connection via the options that appear. Let's start with the Advanced button.

## Advanced Settings

When you click the Advanced button, you will see the screen shown in Figure 6.25. Notice that most of the options are grayed out. This is because the connection adopts the settings configured from within the client's settings. In most cases, this is the way most connections should be configured. When the client attempts to start a connection, the user's settings are applied to the connection, and the session is created using those settings. You can then tailor each user's session according to the user's individual needs.

Changing the default settings at this point will force the settings on every user, effectively overriding the user's configuration settings. This option is very useful if you want to limit the abilities or the session usage on an individual server.

**FIGURE 6.25** Advanced Connection Settings dialog box



Advanced Connection Settings

Logon: ○ Disabled ● Enabled

Timeout settings (in minutes)

Connection 120 □ No Timeout □ (inherit user config)

Disconnection 10 □ No Timeout □ (inherit user config)

Idle 30 □ No Timeout □ (inherit user config)

Security

Required encryption None

□ Use default NT Authentication

AutoLogon

User Name

Domain

Password

Confirm Password

Prompt for Password □

□ (inherit client config)

Initial Program

Command Line

Working Directory

□ (inherit client/user config)

□ Only run Published Applications

User Profile Overrides

□ Disable Wallpaper

On a broken or timed-out connection, disconnect. the session. □ (inherit user config)

Reconnect sessions disconnected from any client. □ (inherit user config)

Shadowing is enabled: input ON, notify ON. □ (inherit user config)

Let's look at each of the sections shown on this screen starting at the upper left:

### Logon

The Logon section controls access to the connection. When you set this option to Disabled, the connection will not allow users to create sessions on the server. Other connections that are enabled will still allow session creation and logon if their Logon option is set to Enabled.

### AutoLogon

This AutoLogon section allows you to configure an account that is used to start a session from this connection. You would usually use this option only when you have a special application that users run from the server and you may not need them to authenticate to the server. After deselecting the (Inherit Client Config) check box, you can enter the username that you want to use for the logon, the domain you want the account to authenticate to, and the password necessary to authenticate. If you want to add a little security to this option, you can check the Prompt For Password option. If you select this check box, then any user connecting across the connection will have to supply the password shown here.

### Timeout Settings (In Minutes)

Each of the options in the Timeout Settings (In Minutes) section is set to (Inherit User Config) by default. You can change any of these options by deselecting the check box. When you do, the next default setting of No Timeout is shown. Of course, if you want to limit any of the settings, you will need to deselect this check box also. The settings you can configure here are as follows:

**Connection** Indicates the amount of time a session may remain connected across this connection.

**Disconnection** Indicates the amount of time a disconnected session may remain on the server before it is terminated.

**Idle** Indicates the amount of time a session will remain active when no processing occurs.

### Initial Program

If a user initiates a session and the Initial Program option is selected, that application will be the only one able to run. Once the application starts, it appears as an application only; no desktop is displayed. When the user exits the application, the session shuts down. This is similar to having a seamless window except that you can control the program that is accessed from the connection.

If the (Inherit Client Config) check box is selected, the program that is selected as the user's default application will run. The Only Run Published Applications check box restricts the user to running only those applications that are published in the farm. Of course, deselecting the (Inherit Client/User Config) check box allows you to enter a program path and its working directory. This again limits all users on the connection to the same application.

### Security

If you want more information on the security levels, you should refer to Chapter 8, "Security." Within this section, you can turn off encryption by selecting None from the Required Encryption pull-down list, or you can choose the appropriate level of encryption for this connection.

The Use Default NT Authentication check box forces the connection to use Windows NT logon authentication even when a third-party authentication product is installed on your server.

### User Profile Overrides

The only option here is Disable Wallpaper. It does exactly what it says. If the user's profile has desktop wallpaper configured, or if the default desktop has desktop wallpaper defined, the wallpaper will not appear in the session if you select this check box. Use this option when you want to reduce the amount of information to be transmitted to the client, especially in a low-bandwidth environment.

The lower portion of this screen contains three other option settings that further control the processing of sessions on the connection. Again, these options are set to inherit the configuration of the user's account, but they can be overridden to make all connections conform to the rules applied here:

**On A Broken Or Timed Out Session** Use this option to choose how the server will treat the session if the connection to the client system is broken or it reaches a timeout limit. You can choose to disconnect the session if you want the user to reconnect and resume where they left off. Otherwise, you can choose to reset the connection, in which case all of the information in the session is lost.

**Reconnect Sessions Disconnected** This option specifies that when the user's session is disconnected, the user can reconnect to the session from any available client device or from the original client device only. Making the disconnected session available from any client device allows a user to reconnect in case their original client device fails, while allowing the connection from the original device only creates a security blanket. If the original device is the only device allowed to reconnect, the user's session cannot be remotely disconnected and then reconnected from another machine by someone wanting to steal information.

**Shadowing** We discuss shadowing later in this section, so we will not go into the details of the options contained in this pull-down list. However, the options set here control the shadowing of every session on the connection.

## ICA Settings

The only option available on the *ICA Settings* screen, Client Audio Quality, lets you change the quality of the audio stream sent from the server to the client device. Depending upon which option you select, the quality can be set to allow nearly all, or very little, of the sound spectrum to pass to the client. The three available settings are as follows:

**Low** All of the sound is compressed to the point where only 16Kbps is allowed to pass to the client. In a low-bandwidth environment, this may be the best setting since it sends very small amounts of data. This setting seriously degrades most sound transmissions, however.

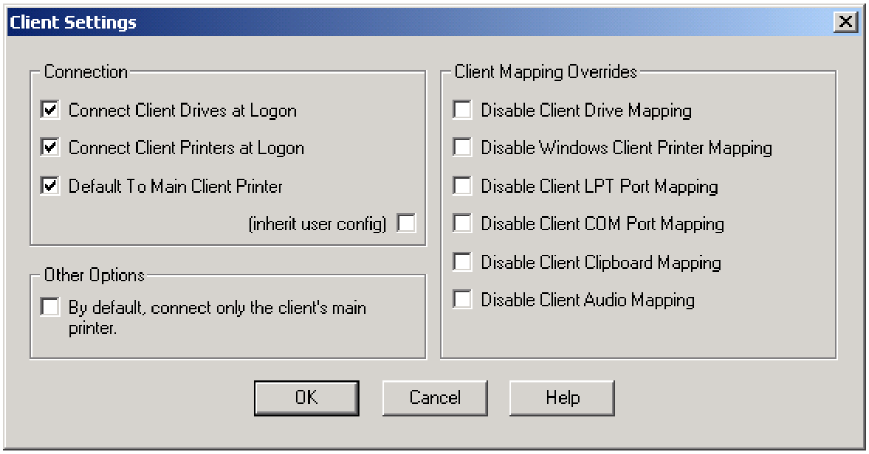
**Medium** This is the trade-off setting. Using this setting allows you to send better quality audio to the client while still maintaining control of the bandwidth used. All audio data is compressed to a maximum of 64Kbps.

**High** Use this setting when you have plenty of bandwidth available or you need the entire sound range of the application transmitted to the client. This setting utilizes more CPU and network bandwidth. However, since it allows up to 1.3Mbps of audio transmission, nearly every application can send its audio in a native state, uncompressed, and clear.

## Client Settings

The Client Settings screen, as shown in Figure 6.26, presents three areas for controlling the users' work environment when connected to a session: Connection, Client Mapping Overrides, and Other Options. Let's take a look at each.

**FIGURE 6.26** Client Settings screen



Client Settings

Connection

☑ Connect Client Drives at Logon

☑ Connect Client Printers at Logon

☑ Default To Main Client Printer

(inherit user config) ☐

Other Options

☐ By default, connect only the client's main printer.

Client Mapping Overrides

☐ Disable Client Drive Mapping

☐ Disable Windows Client Printer Mapping

☐ Disable Client LPT Port Mapping

☐ Disable Client COM Port Mapping

☐ Disable Client Clipboard Mapping

☐ Disable Client Audio Mapping

### Connection

The options in this section allow you to control which resources are available to the client during a session. The default is to inherit the user's configuration, but when you deselect the (Inherit User Config) check box, the connection settings will override the user's settings.

**Connect Client Drives At Logon** When you select this option, the user's drives are mapped to the session based on the server's drive mappings. When it is deselected, the user's drives are not automatically made available during the session. The drives may be mapped manually after the session is started.

**Connect Client Printers At Logon** When you select this option, the user's printers are mapped to the session. When it is deselected, the user's printers are not available during the session. The printers may be mapped manually after the session is started.

**Default To Main Client Printer** When you select this option, the printer selected as the default printer on the client is chosen as the default printer for the session. When it is deselected, the default printer on the server is chosen as the default printer for the session. This option is not available when the Connect Client Printers At Logon option is deselected.

### Client Mapping Overrides

All of the options in this section control the enabling or disabling of the client mapping functions. Use these functions to control the users' environment by restricting the use of certain features.

**Disable Client Drive Mapping** Once you select this option, all client drive-mapping abilities are disabled. The drives will not be mapped as the session initiates, and the user will not be able to map a client drive during the session. When this option is selected, the Connect Client Drives At Logon option in the Connection section of this screen is not available.

**Disable Windows Client Printer Mapping** When you select this option, the client's printers are not available through client mappings. If the client system has the printers shared for network access, the printer may still be used through standard printer mappings. When this option is selected in conjunction with the Disable Client LPT Port Mapping option, the Connect Client Printers At Logon and Default To Main Client Printer options of the Connection section and the By Default, Connect Only The Client's Main Printer option of the Other Options section of this screen are unavailable.

**Disable Client LPT Port Mapping** When you select this option, the client's LPT ports are not available for mapping from within a session. When it is selected in conjunction with the Disable Windows Client Printer Mapping option, the Connect Client Printers At Logon and Default To Main Client Printer options of the Connection section and the By Default, Connect Only The Client's Main Printer option of the Other Options section of this screen are unavailable.

**Disable Client COM Port Mapping** When you select this option, the client's COM ports are not available for mapping from within a session.

**Disable Client Clipboard Mapping** When you select this option, the client's Clipboard is not available for mapping from within a session.

**Disable Client Audio Mapping** When you select this option, the client's audio device is not available for mapping from within a session.

### Other Options

When you select the By Default, Connect Only The Client's Main Printer option, the default printer on the client device is the only printer mapped during the session. Other printers may be mapped manually. If this check box is deselected, all of the client's printers are mapped and available during the session.

So there you have it—the Citrix Connection Configuration and all of the options available for you to configure. We are now going to move on to everyone's favorite utility, shadowing.

## The Shadow Knows: Shadowing and the Shadow Taskbar

In Chapter 3, "Planning the Installation of MetaFrame XP," and Chapter 4, "Installing MetaFrame XP," we presented information about the shadowing options that are available during the installation of MetaFrame XP. Any options that are set at that point, such as disabling shadowing on the server, take precedence, and any options that we discuss here are limited to the selections you make during the install. With that disclaimer in mind, let's discuss those options that are available to configure if you leave the default settings alone during the installation of MetaFrame XP.

Shadowing is available in three different utilities: the Citrix Management Console, Citrix Server Administration, and the *Shadow Taskbar*. The options available to you depend upon which tool you decide to use. Citrix Management Console is the most versatile of the three, while Citrix Server Administration does not afford control over multiple sessions.

When you use the Citrix Management Console to start shadowed sessions, the administrator who is initiating the session will consume only one connection license regardless of the number of sessions that are shadowed. This is a great benefit when multiple sessions need to be shadowed at a time. Consider the help desk employee who needs to help multiple users with problems. The help desk administrator can start multiple shadowed sessions, one for each of the users whom they are helping, and assist them or fix their problems. This person consumes only one connection license, making the rest of the licenses available for use with other sessions.

Conversely, Citrix Server Administration allows only one shadowed session at a time. This is due to limitations in earlier versions of MetaFrame that did not allow the shadowing of multiple sessions at once. Citrix Server Administration was not updated for use with MetaFrame XP since the Citrix Management Console took over its functionality.

The final method of initiating a shadowed session is to use the Shadow Taskbar. Again, this is a tool that originated with an earlier version of MetaFrame, thus it has limitations. While it does allow the shadowing of multiple sessions, it does so at the expense of using multiple licenses, one for each session shadowed. Many administrators found this an unfair compromise—having the ability to shadow more than one user but consuming a license for each. They felt that the only license that should be consumed was the license used by the actual owner of the session. Now with the new technology in MetaFrame XP, the ability to use only one connection license per user is available, but the Shadow Taskbar was not updated to take advantage of this new feature.

NOTE

While the Shadow Taskbar is supposed to consume one license for every connection that is shadowed, in reality it appears that it consumes only one license no matter how many connections are shadowed. Know the "book" answer for the test, but understand that the "book" answers are not always correct in real life.

So you have the tradeoff: You can use the tools that you may be familiar with from the previous versions of MetaFrame, or you can use the new Citrix Management Console and take advantage of the new licensing model. Generally, when it comes to the tradeoff between licensing and training, training a user how to use the new tools is far more cost-effective. Let's take a look at some of the restrictions and benefits of shadowing.

## Capabilities and Considerations

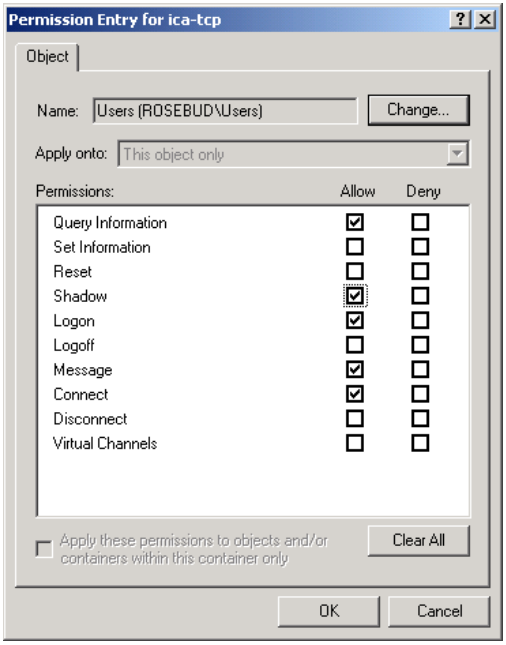
When you first install MetaFrame, the only account that has the ability to perform shadowing is the account you specify as the Citrix Administrator. Every other account added into the Citrix Administrator node with Read-Write privileges has the ability to shadow sessions. Of course, having these privileges may be too generous for some users. The user may need to shadow other sessions, but you do not want them to be able to control any of the other aspects of your MetaFrame environment. To control the users who may need to shadow, you can assign them permission to shadow within the Citrix Connection Configuration utility.

As seen in the Citrix Connection Configuration section earlier in this chapter, once you choose the connection and select the Permissions option, the accounts with permissions to the connection are displayed. By clicking the Advanced button, you can edit the permissions, and from the Permission Entry screen, you can select the Shadow permission, as shown in Figure 6.27.

Enabling this permission gives the account you are editing the ability to shadow other sessions on the connection. Ideally, this is the preferred method of assigning an account to shadow, since no other permissions or rights are assigned at the same time. The account does not have the power to change any of the connection options or assign any other account permission to the connection.

Audio cannot be transmitted to a shadowed session. This limitation is in place to reduce the amount of data transmitted on the network. It is also partially due to the fact that the audio is transmitted to the original client's audio device mapping, and the shadow session may not have the same audio setup. If you are shadowing a client to try to resolve an audio problem, you will be able to make configuration changes but will have to rely on the user to give you feedback as to whether or not the change is effective.

**FIGURE 6.27** Selecting the Shadow permission



Name: Users (ROSEBUD\Users)

Apply onto: This object only

| Permissions: | Allow | Deny |
|---|---|---|
| Query Information | ☑ | □ |
| Set Information | □ | □ |
| Reset | □ | □ |
| Shadow | ☑ | □ |
| Logon | ☑ | □ |
| Logoff | □ | □ |
| Message | ☑ | □ |
| Connect | ☑ | □ |
| Disconnect | □ | □ |
| Virtual Channels | □ | □ |

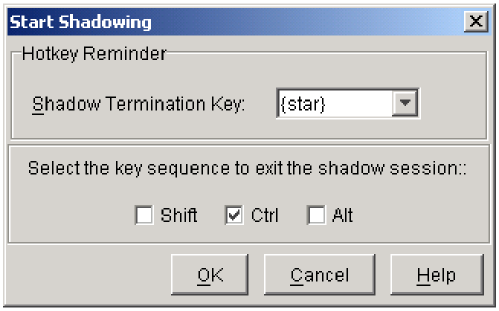
□ Apply these permissions to objects and/or containers within this container only

An administrator can shadow any number of users at one time within the limitations of the utility used to shadow (Citrix Management Console and Shadow Taskbar can shadow multiple sessions, while Citrix Server Administration can shadow only one session). Conversely, multiple administrators can shadow a single user's session. This functionality allows an administrator to work with multiple users at the same time, while allowing another administrator to aid in diagnosing a problem.

Shadowing is available across all of the servers within your server farm. In mixed mode, that includes MetaFrame 1.8 and MetaFrame XP servers. The administrator can shadow users on either platform at the same time while using a single connection license. The only restriction is that you can shadow sessions only on servers within the server farm where you are currently logged on.

With Citrix Management Console or Citrix Server Administration, when the shadowed session starts, the Start Shadowing dialog box appears, which allows you to set the key combination that will end the shadowed session, as shown in Figure 6.28. By default, the Ctrl+* key combination is used. However, you can specify combinations of the Shift, Ctrl, and Alt keys in conjunction with nearly every other key on the keyboard.

**FIGURE 6.28** Hotkey selection screen



Start Shadowing

Hotkey Reminder

Shadow Termination Key: {star}

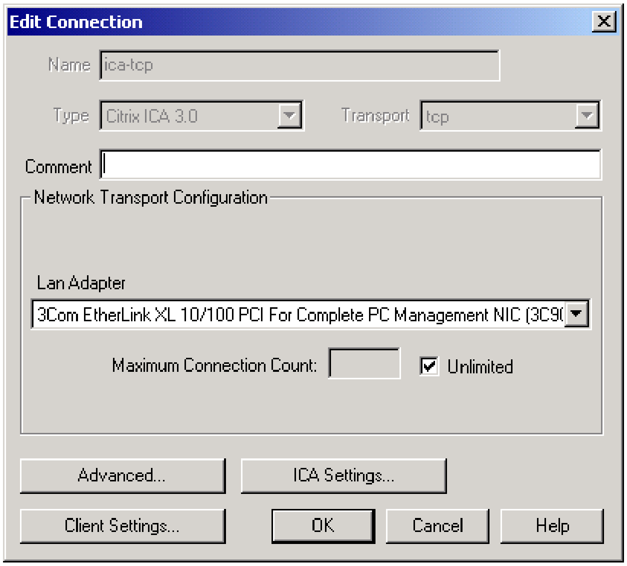
Select the key sequence to exit the shadow session::

□ Shift ☑ Ctrl □ Alt

If the user's session supports a video resolution that is higher than that used by the administrator to shadow the session, the shadow session will fail. There is no warning message telling you that the resolution is incompatible—the shadow session simply stops. Once you reconfigure the administrator's resolution properties, the shadowing will work, barring any other configuration issues.

Since the shadowing settings are applied individually at the server instead of globally at the server farm, you should set any settings that must be enforced on all servers during installation of the server. You configure connection settings in the Citrix Connection Configuration utility by selecting the connection, right-clicking it, and choosing Edit from the context menu. When the Edit Connection screen shown in Figure 6.29 appears, click the Advanced button. The shadow configuration options are available at the bottom of the Advanced Connection Settings screen, shown in Figure 6.30. If the default setting of (Inherit User Config) is selected, the Remote Control settings of the user's properties, shown in Figure 6.31, are used for shadowed sessions. If the Enable Remote Control check box is deselected, the user cannot be shadowed. If it is selected, the other options become available. Require User's Permission enables notification messages to the user when a shadow session starts. The radio buttons within the Level Of Control section specify whether the administrator may interact with the session or simply view what is occurring.

**FIGURE 6.29** Edit Connection screen



Edit Connection

Name: ica-tcp

Type: Citrix ICA 3.0 Transport: tcp

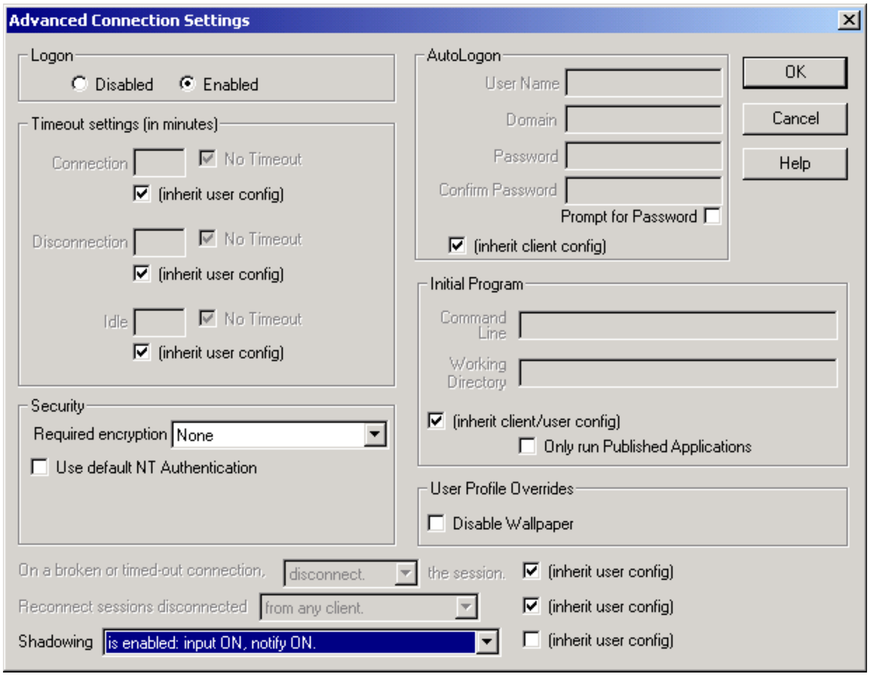
Comment:

Network Transport Configuration

Lan Adapter: 3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C9(

Maximum Connection Count: ☑ Unlimited

**FIGURE 6.30** Advanced Connection Settings screen



Advanced Connection Settings

Logon: ○ Disabled ● Enabled

Timeout settings (in minutes)

Connection: ☑ No Timeout
☑ (inherit user config)

Disconnection: ☑ No Timeout
☑ (inherit user config)

Idle: ☑ No Timeout
☑ (inherit user config)

Security

Required encryption: None

☐ Use default NT Authentication

AutoLogon

User Name:

Domain:

Password:

Confirm Password:

Prompt for Password ☐

☑ (inherit client config)

Initial Program

Command Line:

Working Directory:

☑ (inherit client/user config)

☐ Only run Published Applications

User Profile Overrides

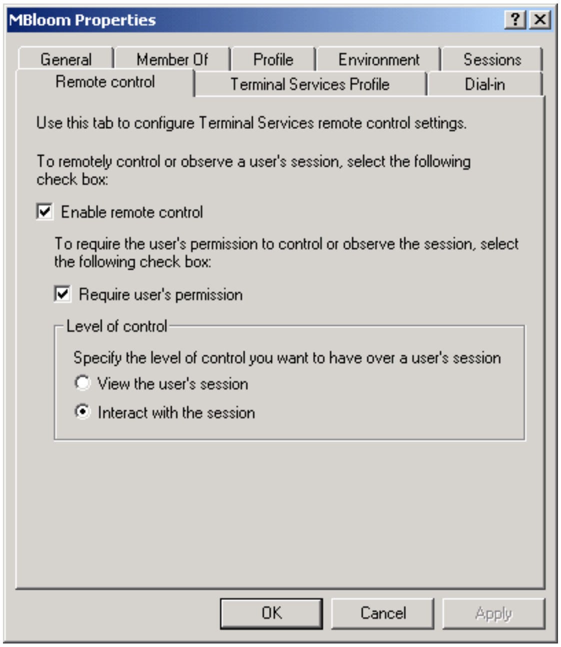
☐ Disable Wallpaper

On a broken or timed-out connection, disconnect. the session. ☑ (inherit user config)

Reconnect sessions disconnected from any client. ☑ (inherit user config)

Shadowing: is enabled: input ON, notify ON. ☐ (inherit user config)

**FIGURE 6.31** Remote Control settings



Use this tab to configure Terminal Services remote control settings.

To remotely control or observe a user's session, select the following check box:

☑ Enable remote control

To require the user's permission to control or observe the session, select the following check box:

☑ Require user's permission

Level of control

Specify the level of control you want to have over a user's session

○ View the user's session

● Interact with the session

Once the check box next to (Inherit User Config) is deselected, the Shadowing pull-down menu becomes available, as shown in Figure 6.32. Three options display initially, but if you click the scroll arrows, you will see the remainder of the options. These options are as follows:

**Is Disabled** No shadowing is available on this connection on this server.

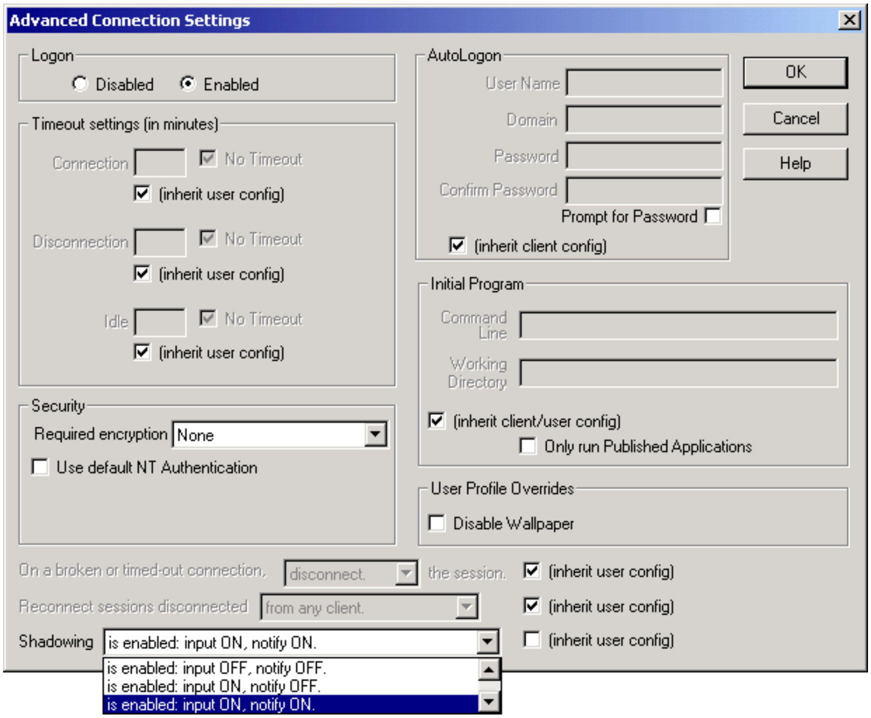
**Is Enabled, Input OFF, Notify ON** The administrator can shadow but cannot take control of the session. The user is notified that the session is being shadowed.

**Is Enabled, Input OFF, Notify OFF** The administrator can shadow but cannot take control of the session. The user is not notified that the session is being shadowed.

**Is Enabled, Input ON, Notify OFF** The administrator can shadow and take control of the session. The user is not notified that the session is being shadowed.

**Is Enabled, Input ON, Notify ON** The administrator can shadow and take control of the session. The user is notified that the session is being shadowed.

**FIGURE 6.32** The Shadowing pull-down menu



Advanced Connection Settings

Logon
○ Disabled ● Enabled

Timeout settings (in minutes)
Connection ☑ No Timeout
☑ (inherit user config)
Disconnection ☑ No Timeout
☑ (inherit user config)
Idle ☑ No Timeout
☑ (inherit user config)

Security
Required encryption None
□ Use default NT Authentication

AutoLogon
User Name
Domain
Password
Confirm Password
Prompt for Password □
☑ (inherit client config)

Initial Program
Command Line
Working Directory
☑ (inherit client/user config)
□ Only run Published Applications

User Profile Overrides
□ Disable Wallpaper

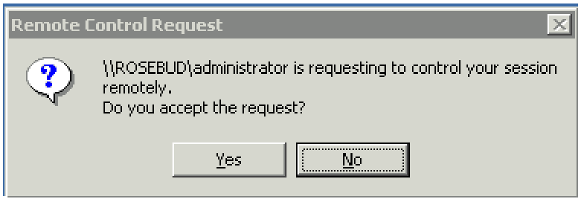
On a broken or timed-out connection, disconnect the session. ☑ (inherit user config)
Reconnect sessions disconnected from any client. ☑ (inherit user config)
Shadowing is enabled: input ON, notify ON. □ (inherit user config)

is enabled: input OFF, notify OFF.
is enabled: input ON, notify OFF.
is enabled: input ON, notify ON.

After you've configured the shadowing settings for the user and/or the connection, you can initiate a shadowed session. When using Citrix Management Console, you can navigate to any of the Users tabs to locate the session you want to shadow, right-click it, and select Shadow. Alternatively, you can select the session and click the Shadow icon. The Hotkey Reminder screen will appear, followed by the logon screen.

If notification has been enabled, the user will receive a remote control request, asking whether the session can be shadowed, as shown in Figure 6.33. If the user selects No, the shadow session is not allowed to run. If the user selects Yes, the *Shadow Indicator*, a small window displaying a shadowing notification message, appears in the upper-left side of the user's session, as shown in Figure 6.34. The user or the shadower can minimize this indicator, and the user can click the Stop Shadowing button if desired. The shadower can use the hotkey chosen at the start of the shadowing session request or click the Stop Shadowing button to stop shadowing. If notification is not enabled, neither the warning message nor the shadow indicator will appear to the user.

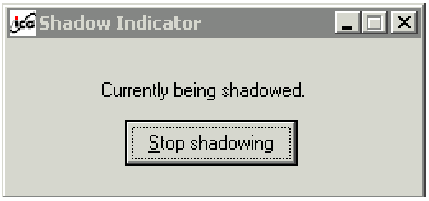
**FIGURE 6.33** Remote Control Request dialog box



Remote Control Request

\\ROSEBUD\administrator is requesting to control your session remotely.
Do you accept the request?

**FIGURE 6.34** Shadow Indicator dialog box



Shadow Indicator

Currently being shadowed.

Another way to initiate a shadow session is to use the Shadow Taskbar. This utility allows you to start multiple shadowed sessions and maintain them from a single taskbar that resides on your desktop. Just like the Start menu or Citrix Administrator taskbars, the Shadow Taskbar can be positioned anywhere on the screen, and the settings for autohide and stay-on-top are available.

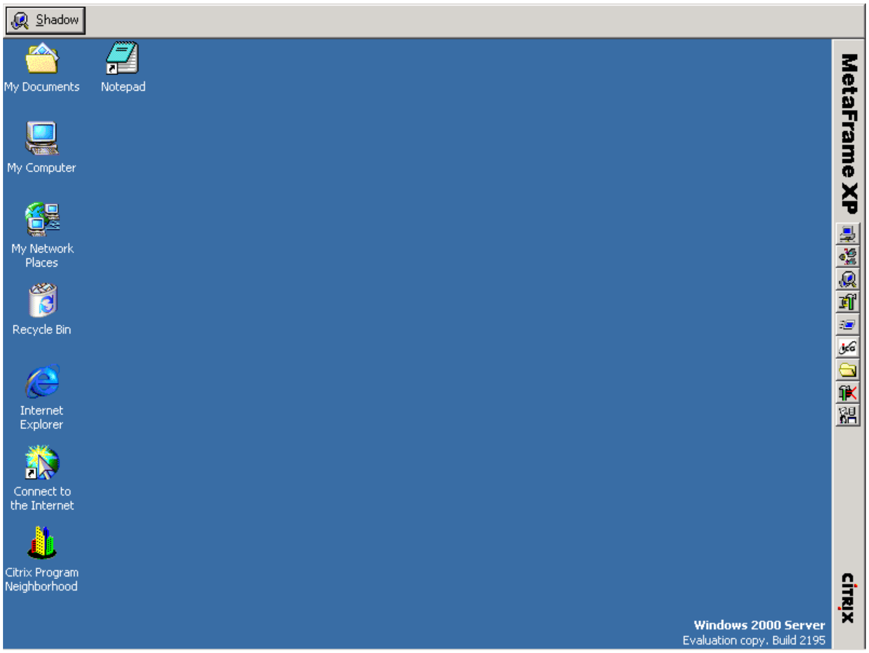
To start the Shadow Taskbar, choose Start ➢ Programs ➢ Citrix ➢ MetaFrame XP ➢ Shadow Taskbar, or select the Shadow Taskbar from the ICA Administrator toolbar. Once started, it will sit unassumingly at the top of the screen, as in Figure 6.35. If you click the Shadow button, you will see a window that allows you to choose the session that you want to shadow. These sessions are separated into three groupings within the Available Users list: Servers, Applications, and Users.

**Servers** This group displays the servers within the server farm and each session running on the server. If you double-click the session's username, the name of the client device used to access the session is displayed.

**Applications** Within this group, all servers that the application is published on are listed. Beneath the server, the session's username is displayed, along with the client device used to access the session.

**Users** This group displays the users with a session running on a server and the client devices used to access the session.

**FIGURE 6.35** Shadow Taskbar



Choose the sessions you wish to shadow and click the Add button. Once you've selected all of the sessions you want, click the OK button. The shadow session will be created, and you will see the same notification messages that we worked with previously. All of the sessions will appear on the Shadow Taskbar. This allows you to quickly choose which session you want to work with or view. You can even stop shadowing by right-clicking a session and choosing Stop Shadow, as shown in Figure 6.36. To quickly stop shadowing all of the sessions, you can right-click the Shadow button and select Stop All Shadowed Sessions from the context menu, shown in Figure 6.37.

Now that you know how to shadow user sessions, let's take a look at our final topic within this section on shadowing, logging the shadowed sessions.

**FIGURE 6.36** Choosing Stop Shadow

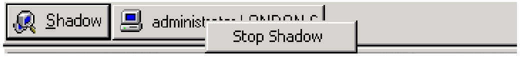
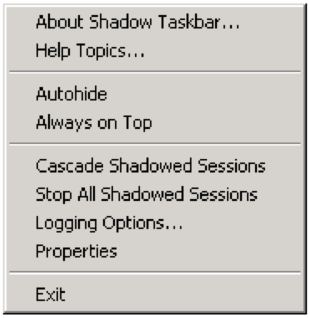


**FIGURE 6.37** Stop All Shadowed Sessions option

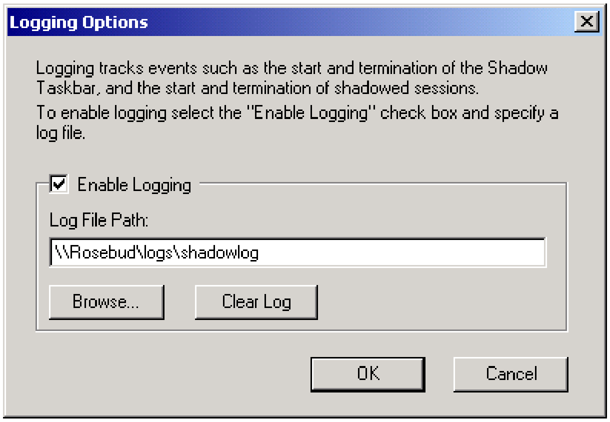


## Logging

*Logging* of shadowed sessions is not a new feature; it was introduced with the Shadow Taskbar in MetaFrame 1.8. However, logging functions differently in the two main utilities. The Shadow Taskbar allows you to create a log file anywhere on the server, while the Citrix Management Console allows you to start logging events to an event viewer.

Starting with the Shadow Taskbar, you enable logging by right-clicking the Shadow button. This brings up a menu with the Logging Options choice. The screen shown in Figure 6.38 shows the options available. Once you select the Enable Logging check box, you can make an entry in the Log File Path field. This can be a directory on the local computer or a shared directory on a server within your network. Citrix was nice enough to include the Browse button to allow you to locate the directory where you want to place the file. The Clear Log button does exactly what it says: It clears all entries from the log file.

**FIGURE 6.38** Logging Options from the Shadow Taskbar


Logging Options

Logging tracks events such as the start and termination of the Shadow Taskbar, and the start and termination of shadowed sessions.

To enable logging select the "Enable Logging" check box and specify a log file.

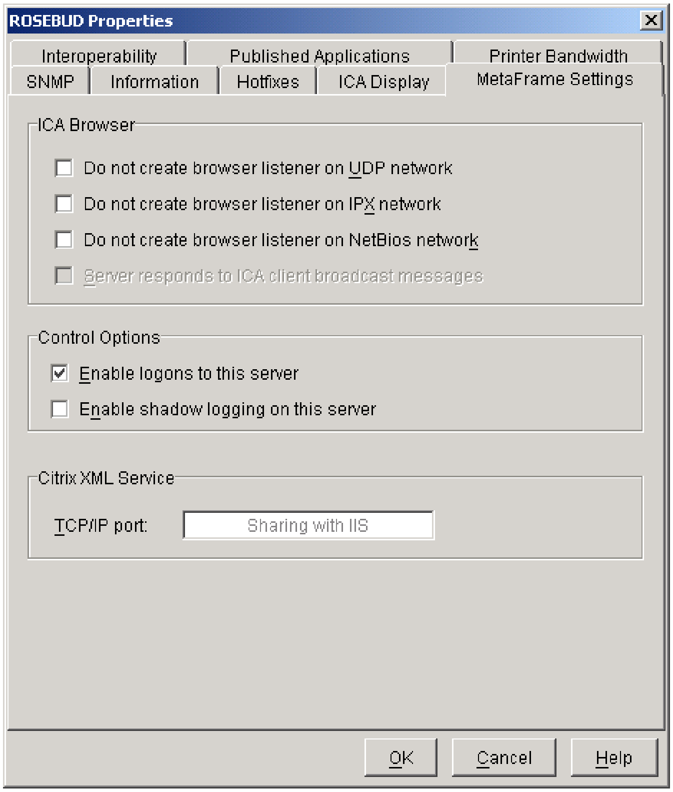
☑ Enable Logging

Log File Path:

\\Rosebud\logs\shadowlog

Citrix Management Console has added more functionality to the logging of shadowed sessions. Once logging is enabled, the entries are placed in the event viewer logs. To enable logging, open the properties of the server where you want to log the shadowing, and select the MetaFrame Settings tab, as shown in Figure 6.39. Select the Enable Shadow Logging On This Server check box.

**FIGURE 6.39** Logging from the Citrix Management Console



ICA Browser

□ Do not create browser listener on UDP network

□ Do not create browser listener on IPX network

□ Do not create browser listener on NetBios network

□ Server responds to ICA client broadcast messages

Control Options

☑ Enable logons to this server

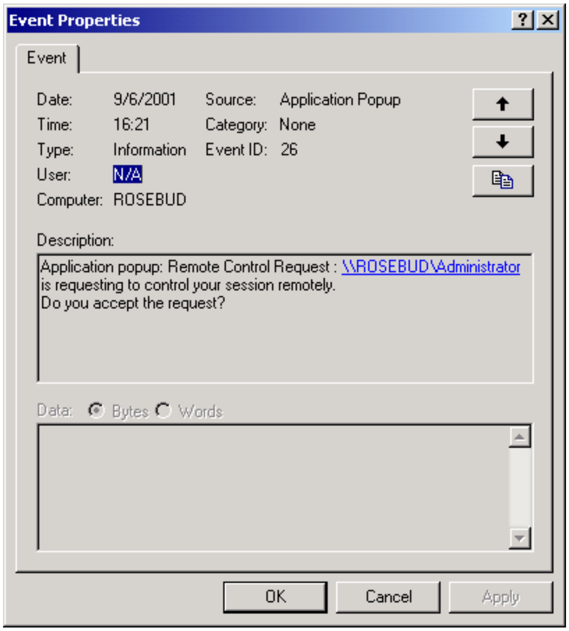
□ Enable shadow logging on this server

Citrix XML Service

TCP/IP port: Sharing with IIS

Once logging is enabled, logged shadow events will appear in two of the event logs. Requests sent to users informing them of the intent to shadow are sent to the *System log* as Application Popup events with an Event ID of 26, as shown in Figure 6.40. All other shadow logging is sent to the *Application log*, which displays the start of a shadowed session with an Event ID of 1000 and the end of a shadowed session with an Event ID of 1001. See Figures 6.41 and 6.42 for these events.

**FIGURE 6.40** Application Popup in the System log



Event Properties

Event

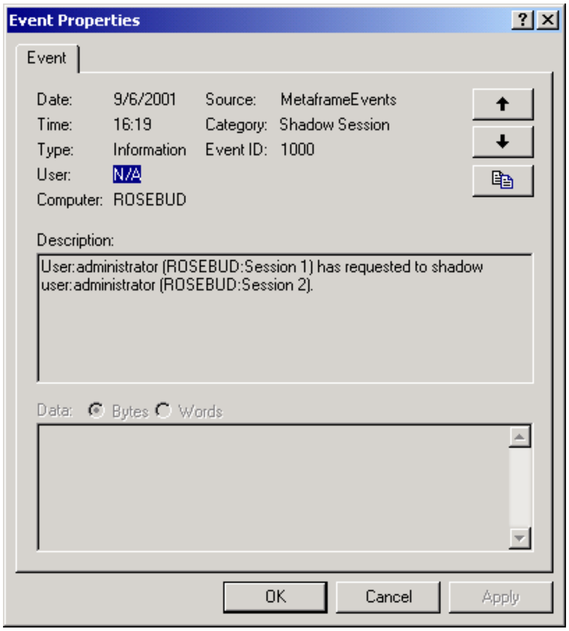
Date: 9/6/2001 Source: Application Popup
Time: 16:21 Category: None
Type: Information Event ID: 26
User: N/A
Computer: ROSEBUD

Description:

Application popup: Remote Control Request : \\ROSEBUD\Administrator is requesting to control your session remotely.
Do you accept the request?

Data: ● Bytes ○ Words

**FIGURE 6.41** Start of shadowing logged to the Application log



Event Properties

Event

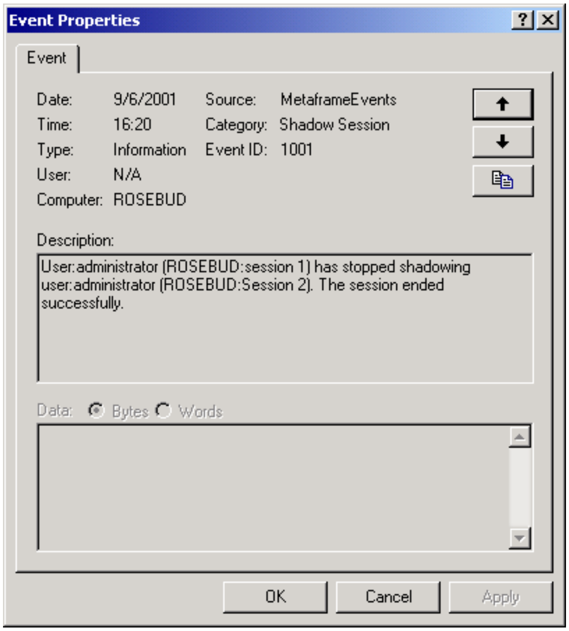
Date: 9/6/2001 Source: MetaframeEvents
Time: 16:19 Category: Shadow Session
Type: Information Event ID: 1000
User: N/A
Computer: ROSEBUD

Description:

User:administrator (ROSEBUD:Session 1) has requested to shadow user:administrator (ROSEBUD:Session 2).

Data: ● Bytes ○ Words

**FIGURE 6.42** End of shadowing logged to the Application log



Date: 9/6/2001 Source: MetaframeEvents
Time: 16:20 Category: Shadow Session
Type: Information Event ID: 1001
User: N/A
Computer: ROSEBUD

Description:
User:administrator (ROSEBUD:session 1) has stopped shadowing user:administrator (ROSEBUD:Session 2). The session ended successfully.

Data: ● Bytes ○ Words

So there you have it. All of the information you could ever want on shadowing. Plenty to peruse and work with. Study this section well, as the exam will cover points on shadowing that you may not be familiar with. From here we move on to making our sessions more user friendly with the SpeedScreen Latency Reduction Manager.

## Working with SpeedScreen

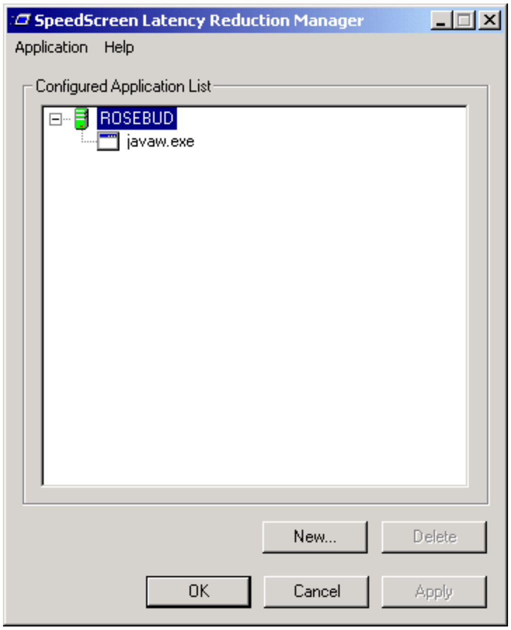
Not all connections are created equal. With that in mind, Citrix strove to create a technology to optimize the data sent to a client in order to update the display information. Originally, SpeedScreen was a set of algorithms used to determine the display information that had changed and needed to be sent to the client device. If a portion of the screen was not updated, the data would be suppressed, thus cutting down on the amount of data sent to the client.

For the most part, this system was adequate and worked quite well, but there are some inherent issues with terminal services technologies. All of the processing is performed on the server, thus causing a slight delay in the transmission of screen updates to the client. In Chapter 2, "Underlying Citrix MetaFrame XP Technologies," we discussed the new technologies introduced in MetaFrame XP: mouse click feedback and local text echo. These two technologies help alleviate the problem of the server updating information and the client having to wait for the screen update.

At the server, we can configure applications to take advantage of these new features by using the *SpeedScreen Latency Reduction* Manager. To start the SpeedScreen Latency Reduction Manager, either click the icon on the ICA Administrator toolbar or choose Start ➤ Programs ➤ Citrix ➤ MetaFrame XP ➤ SpeedScreen Latency Reduction Manager.

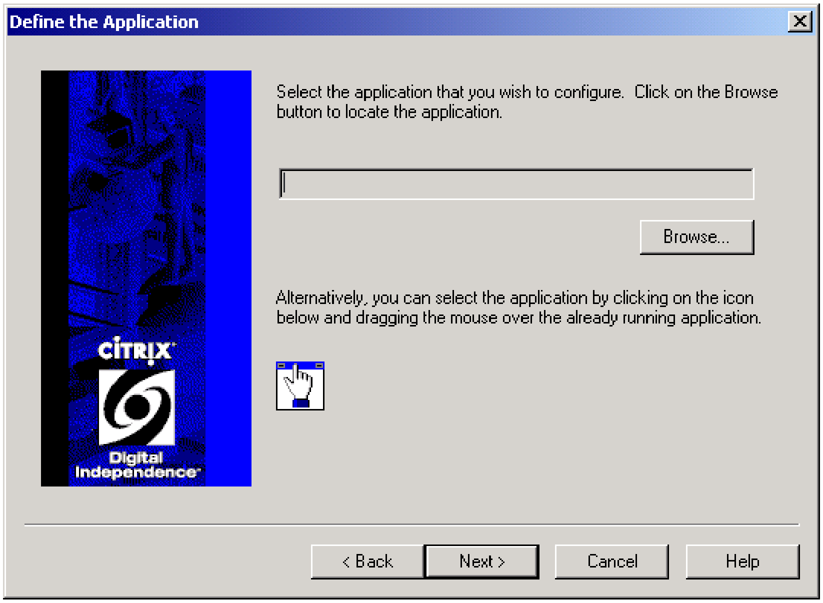
This unassuming utility, shown in Figure 6.43, allows us to configure applications to utilize the new SpeedScreen functionality. Configuring the applications here allows them to use *mouse click feedback* and *local text echo*, but the client device cannot take advantage of these features unless it is configured to use them. When we discuss the client features in Chapter 11, we will go into detail on how to set the options.

**FIGURE 6.43** SpeedScreen Latency Reduction Manager screen


SpeedScreen Latency Reduction Manager
Application
Help
Configured Application List
ROSEBUD
javaw.exe
New...
Delete
OK
Cancel
Apply

Click the New button to start the SpeedScreen Wizard: Add New Application Wizard. The splash page details what the wizard does. Click Next to move on, and you will see the Define The Application screen, shown in Figure 6.44. From here, you can browse for the application you wish to configure, or you can drag the Pointer icon onto an application that is already running on the server. This will identify the application and enter the path into the application path entry line. Click Next to continue.

**FIGURE 6.44** Define The Application screen



Define the Application

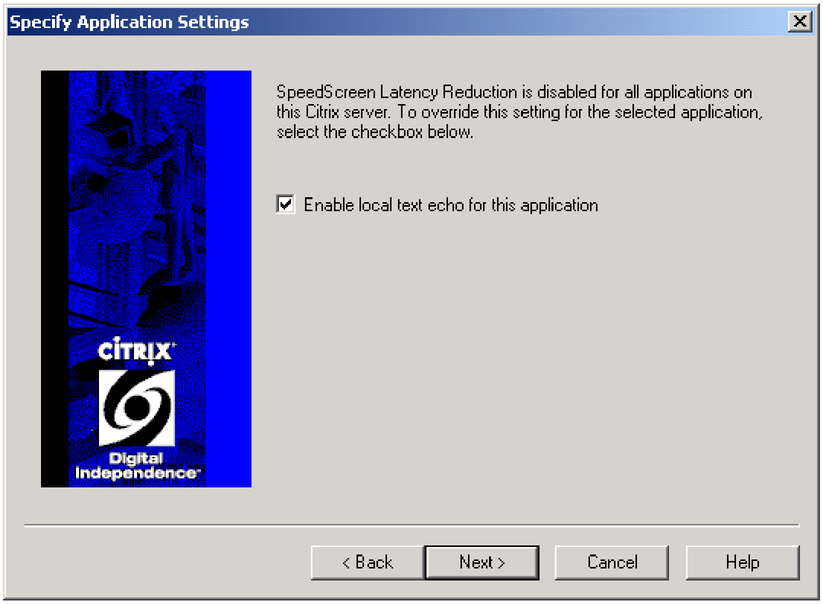
Select the application that you wish to configure. Click on the Browse button to locate the application.

Alternatively, you can select the application by clicking on the icon below and dragging the mouse over the already running application.

The Specify Application Settings screen, shown in Figure 6.45, allows you to change the application's settings to allow local text echo. If you do not want local text echo for this application, deselect the check box. Click Next to move on.

On the Specify Configuration Options screen, shown in Figure 6.46, you can select whether to apply the settings to all installations of this application or only to the instance that you selected on the Define The Application screen. If you choose to apply it to all instances, the executable name is registered, and all instances of the executable will have the settings applied. If you choose only the selected application, then the entire path to the executable will be used when applying the settings and no other instances will be affected by the settings.

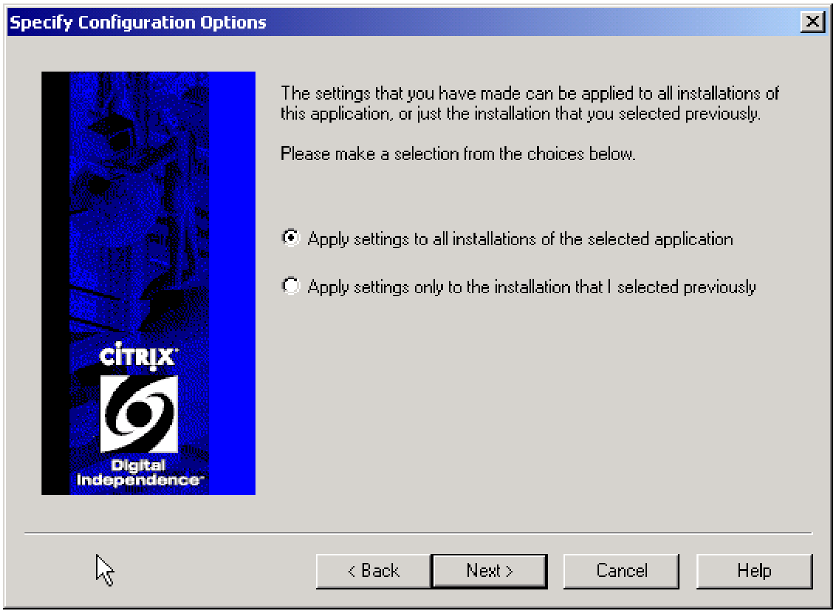
**FIGURE 6.45** Specify Application Settings screen



SpeedScreen Latency Reduction is disabled for all applications on this Citrix server. To override this setting for the selected application, select the checkbox below.

☑ Enable local text echo for this application

**FIGURE 6.46** Specify Configuration Options screen



The settings that you have made can be applied to all installations of this application, or just the installation that you selected previously.

Please make a selection from the choices below.

● Apply settings to all installations of the selected application

○ Apply settings only to the installation that I selected previously

Click Next to display the Finish Adding The Application screen. If you are not sure that you entered the correct information, you can always click the Back button and review the settings. Once you click Finish, the application will be configured to use the new technologies.

The server and the applications that are configured for SpeedScreen Latency Reduction appear in the SpeedScreen Latency Reduction Manager window. If you right-click an application, you will see a menu with the options Delete and Application Properties. The first option is self-explanatory, so we will concentrate on what happens when you select the properties option.

Two tabs are available in the Application Settings screen: Application Properties and Input Field Configuration. These two tabs allow you to configure how the local text echo affects the user's session.

## Application Properties

This tab, shown in Figure 6.47, provides information about the application you just selected and allows you to configure the local text echo properties for all aspects of the application. In the top section, Application Name And Location, the name of the application and the path to the application executable are shown. If this is the only instance of the application that SpeedScreen Latency Reduction is configured for, the application path is displayed. If all instances of the application are configured, the message shown in Figure 6.48 will be present.

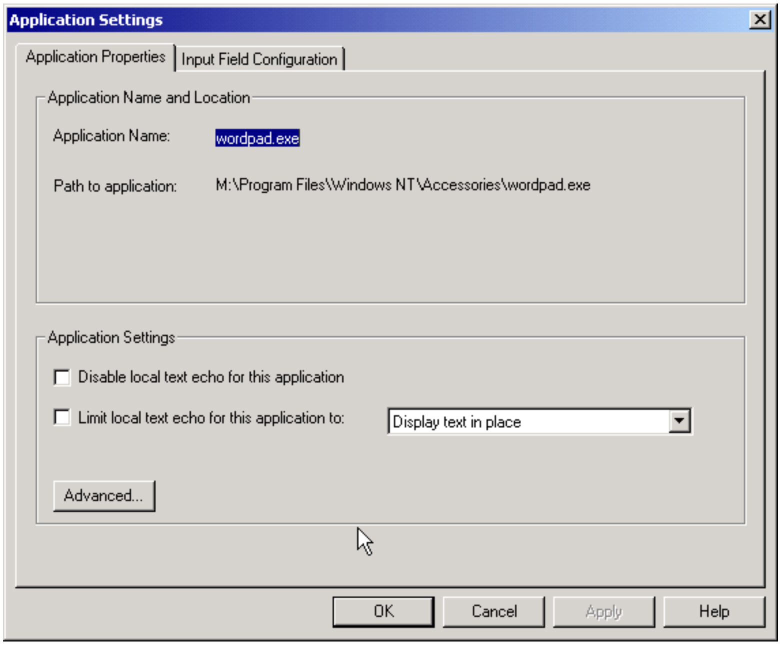
The lower section of this tab, Application Settings, allows you to configure the settings that are applied to all of the text fields of the application. The following options are configurable:

**Disable Local Text Echo For This Application** Select this check box to completely disable all local text echo when the application is used.

**Limit Local Text Echo For This Application To:** You can specify that the default configuration for the text fields is either to display text in the text window or to display text within a text bubble that overlays the text field.

Clicking the Advance button gives you the option Force SpeedScreen To Treat All Input Fields In This Application In Native Mode. If selected, this option reduces the functionality of SpeedScreen by not taking advantage of mouse click feedback and local text echo.

**FIGURE 6.47** Explicit application properties



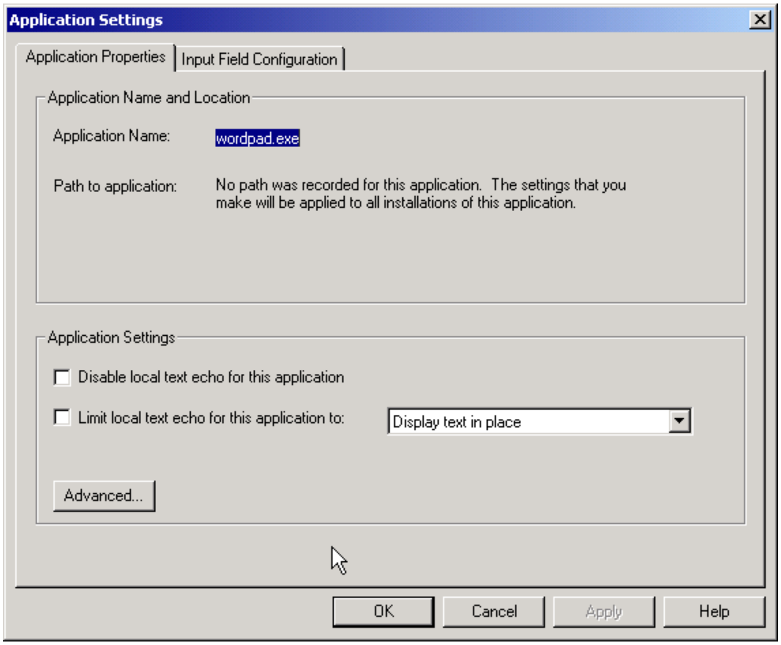
Application Name: wordpad.exe

Path to application: M:\Program Files\Windows NT\Accessories\wordpad.exe

□ Disable local text echo for this application

□ Limit local text echo for this application to: Display text in place

**FIGURE 6.48** All instances of an application included



Application Name: wordpad.exe

Path to application: No path was recorded for this application. The settings that you make will be applied to all installations of this application.

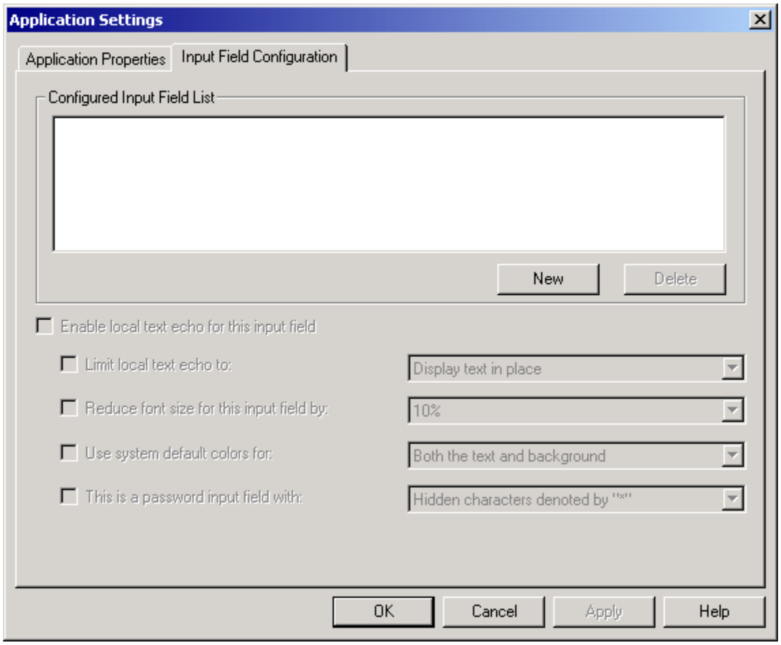
□ Disable local text echo for this application

□ Limit local text echo for this application to: Display text in place

## Input Field Configuration

The true power of SpeedScreen Latency Reduction lies in the Input Field Configuration tab. From this tab, shown in Figure 6.49, you can configure every text field within the application to react according to the specifications you choose. If the text fields within the application do not function as you want them to, you can step through the SpeedScreen Latency Reduction Manager Wizard to change the default behavior of the text fields. This is especially useful for password fields since the password is displayed when local text echo is turned on.

**FIGURE 6.49** Input Field Configuration tab



□ Enable local text echo for this input field

□ Limit local text echo to: Display text in place

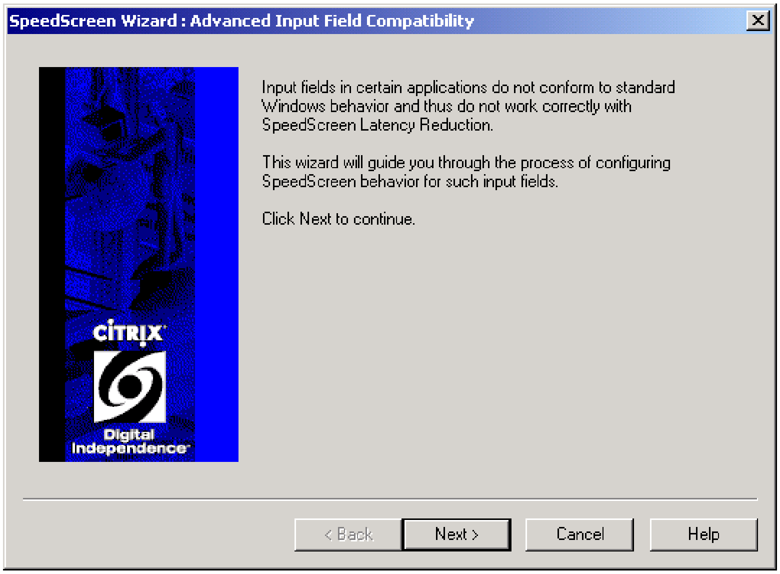
□ Reduce font size for this input field by: 10%

□ Use system default colors for: Both the text and background

□ This is a password input field with: Hidden characters denoted by "*"

When you click New, the wizard appears, as shown in Figure 6.50, and allows you to choose the fields within the application for which you want to modify the behavior. Once you click the Next button, you are presented with the screen seen in Figure 6.51. Before going any further, you must make sure that the application you are configuring is running on the server.

**FIGURE 6.50** SpeedScreen Wizard: Advanced Input Field Compatibility screen

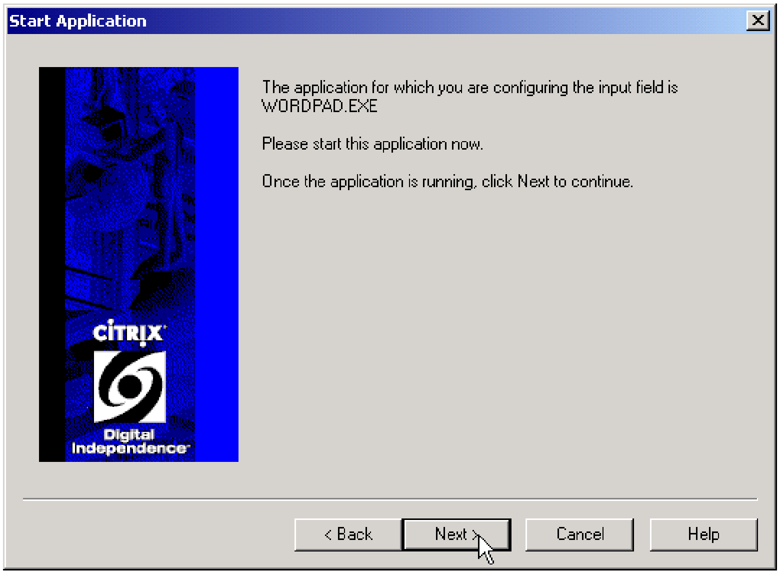

SpeedScreen Wizard : Advanced Input Field Compatibility

Input fields in certain applications do not conform to standard Windows behavior and thus do not work correctly with SpeedScreen Latency Reduction.

This wizard will guide you through the process of configuring SpeedScreen behavior for such input fields.

Click Next to continue.

**FIGURE 6.51** Start your apps!


Start Application

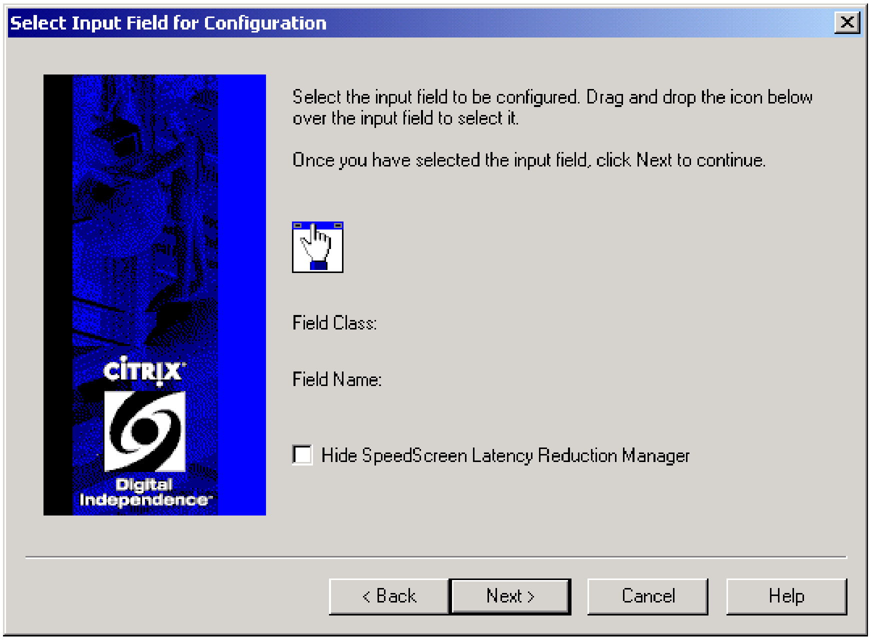
The application for which you are configuring the input field is WORDPAD.EXE

Please start this application now.

Once the application is running, click Next to continue.

Once the application is running, click Next in the wizard to move to the Select Input Field For Configuration screen shown in Figure 6.52. At this point, it is a good idea to make sure the application you want to configure and the wizard you are running are positioned so that both screens are completely visible. You may have to change the screen display to do this. A check box is provided to hide the SpeedScreen Latency Reduction Manager from view if it is interfering with your ability to see the fields you wish to configure.

**FIGURE 6.52** Select Input Field For Configuration screen


Select Input Field for Configuration

Select the input field to be configured. Drag and drop the icon below over the input field to select it.

Once you have selected the input field, click Next to continue.

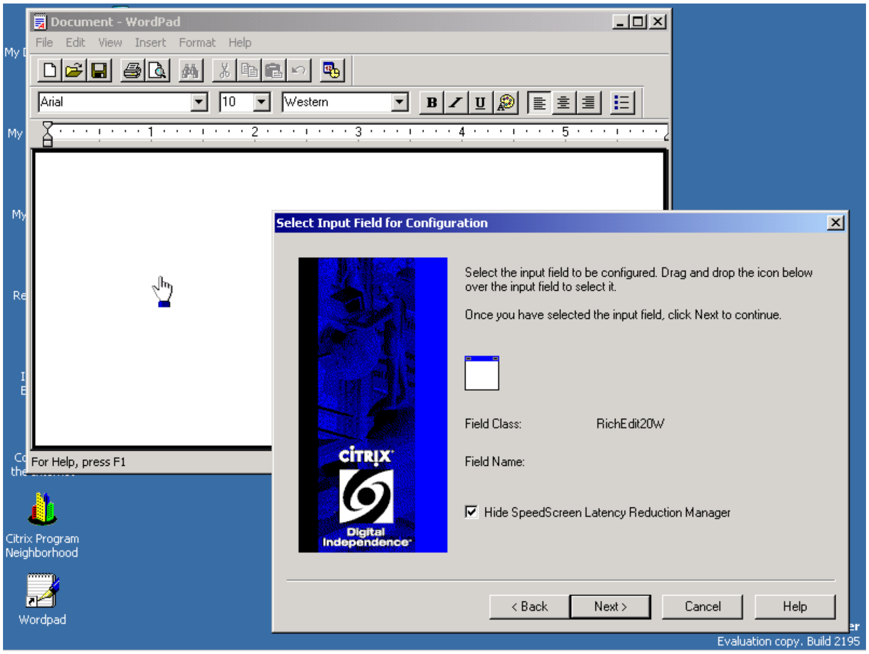
Field Class:

Field Name:

□ Hide SpeedScreen Latency Reduction Manager

After you have started the application and positioned the windows, drag the icon to the text field on the application, as shown in Figure 6.53. As you move over the field, the Field Class and Field Name information will appear in the wizard. After dropping the icon on the field, click the Next button to move to the next screen of the wizard.

**FIGURE 6.53** Selecting the field



Select Input Field for Configuration

Select the input field to be configured. Drag and drop the icon below over the input field to select it.

Once you have selected the input field, click Next to continue.

Field Class: RichEdit20W

Field Name:

☑ Hide SpeedScreen Latency Reduction Manager

The wizard assumes that since you are configuring the text field, the default settings did not work correctly for some reason and you need to make changes to the default behavior. The slider on the Input Field Compatibility screen, shown in Figure 6.54, allows you to make generic changes to the field's settings.

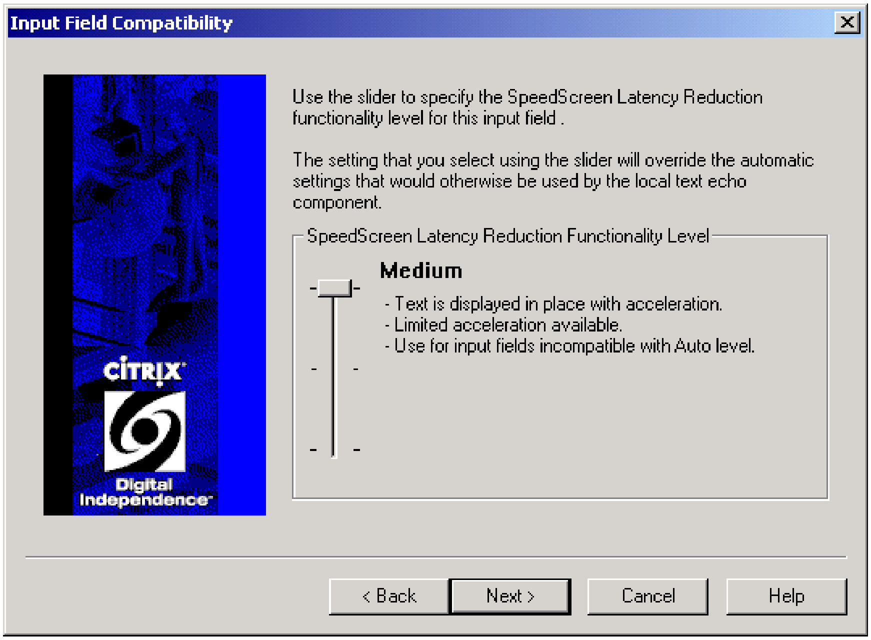
**Medium** This should be your first choice when configuring the input field. This setting will still use the text window, but not at the full acceleration that the default settings would use.

**Low** When the input field does not display the text in a readable form, use this setting to display the text in a text bubble.

**Off** When none of the settings work, this setting disables local text echo.

Later, after the wizard is complete, you will have better control over each aspect of the text field. Move the slider to the setting you need and click Next to move to the Finish Configuring the Input Field screen. If you are sure the options you chose are the settings you want, click Finish. Otherwise, click Back and modify the settings.

**FIGURE 6.54** Input Field Compatibility slider



Use the slider to specify the SpeedScreen Latency Reduction functionality level for this input field .

The setting that you select using the slider will override the automatic settings that would otherwise be used by the local text echo component.

SpeedScreen Latency Reduction Functionality Level

**Medium**

- Text is displayed in place with acceleration.
- Limited acceleration available.
- Use for input fields incompatible with Auto level.

Once you complete the wizard, the text field will show in the Configured Input Field List of the Application Settings screen, shown in Figure 6.55. To change the settings that were applied during the wizard, you can select the Enable Local Text Echo For This Input Field check box. When you do, four other options become available:

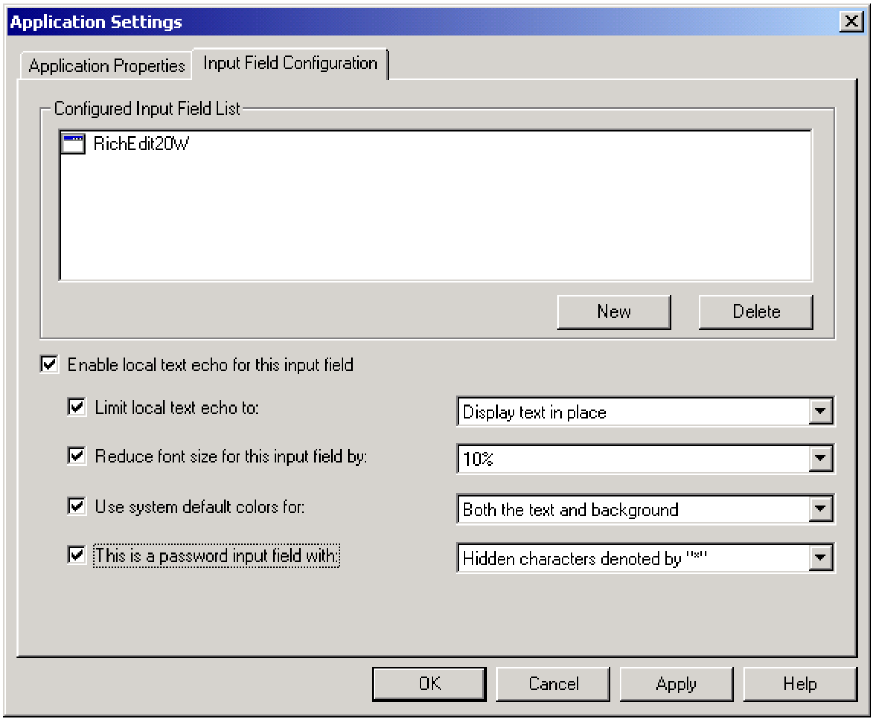
**Limit Local Text Echo To** The two choices available for this selection are Display Text In Place, which uses the text field to display the information, and Display Text In A Floating Bubble, which displays the text in a bubble before the information is entered into the text field.

**Reduce Font Size For This Input Field By** If the text does not appear correctly within the text field, you can reduce the font size by 10%, 20%, or 30%.

**Use System Default Colors For** You can choose the color of the font and the displayed background from this option, and you also have the choice of using just the background color or both the text and background colors.

**This Is A Password Input Field With** Use this option to hide the password being entered into a password field with either a space or an asterisk.

**FIGURE 6.55** Input Field Configuration tab



RichEdit20W

☑ Enable local text echo for this input field

☑ Limit local text echo to: Display text in place

☑ Reduce font size for this input field by: 10%

☑ Use system default colors for: Both the text and background

☑ This is a password input field with: Hidden characters denoted by "*"

You may need to test the application while making adjustments. The optimal solution is to have the application appear as though it is running on the user's local system. However, that may not be entirely possible. Work with each of these settings until the application appears as close to the native behavior as possible.

After you've configured the application, the settings are saved on the server in the `%systemroot%\system32\ss3config` directory. If all of the servers in your server farm need the same configuration settings, you can copy this entire directory to the other servers to save time. If you are going to copy the settings to another server, you should configure the application path to include all instances of the application; otherwise, if another server has the application installed in a different directory, that application will not inherit the SpeedScreen settings.

There you have the SpeedScreen Latency Reduction Manager and the options it allows you to configure. This concludes our chapter covering the additional administration tools. There are a few other tools available that allow us to work with our servers, and we will cover them in later chapters. The SSL Relay Configuration tool is covered in Chapter 8, "Security." ICA Client Creator, ICA Client Distribution Wizard, and ICA Client Update Configuration are discussed in Chapter 10, "ICA Client Software." ICA Client Printer Configuration is covered in Chapter 13, "Printing." For now, we will advance to Chapter 7 and the next topic, "Load Management."

## Summary

With this chapter, we close the book on the major administrative tools that are available at the server to control sessions. After detailing the finer points of the Citrix Server Administration, we have given you the information necessary to control the sessions on MetaFrame XP as well as MetaFrame 1.8 servers. Add in the Citrix Connection Configuration utility to control access to the system, and you have the ingredients for a very powerful administrative pie.

We also took a look at shadowing and showed how to configure the shadowing options. Using the Citrix Management Console or the Shadow Taskbar, you have the power to shadow multiple users at the same time. Each of these tools has it benefits, such as the Citrix Management Console using only one connection license no matter how many users are shadowed, and the Shadow Taskbar organizing all of your shadowed sessions in a nice, neat, orderly fashion on the taskbar.

Then we wrapped everything up with the SpeedScreen Latency Reduction Manager and the options available for controlling the look and feel of applications. With this tool, you can improve the user's experience while running a session. In the chapter to follow, we will look at load management and how to control the utilization of servers in your server farm.

## Exam Essentials

**Know when to use Citrix Server Administration.** Citrix Server Administration should be used only to administer MetaFrame 1.8 servers in your server farm. To administer MetaFrame XP servers, use Citrix Management Console.

**Know the tabs in Citrix Server Administration.** The tabs found at all of the levels of the Citrix Server Administration hierarchy contain the configuration and control information for the MetaFrame 1.8 servers.

**Know how to control the sessions from Citrix Server Administration.** Right-clicking a session from within Citrix Server Administration will bring up a menu with the control options. These options include Connect, Disconnect, Send Message, Shadow, Reset, Status, and Logoff.

**Understand how to create a connection using Citrix Connection Configuration.** Citrix Connection Configuration allows you to create a connection or delete a connection when a protocol is added or removed from the system.

**Know how to control the connection with the configuration options in Citrix Connection Configuration.** The Edit option brings up the Edit Connection dialog box. From here, you can modify the settings for the connection, including the number of connections allowed, the shadow settings, the client mapping settings, and the audio settings.

**Understand how to configure connection settings.** Right-clicking a connection and choosing Permissions displays the Permissions dialog, where you can set the level of permissions available to users and groups.

**Understand the implications of shadowing with the various administrative utilities.** Shadowing consumes licenses, but the utility you use dictates the number of licenses used. Citrix Server Administration consumes one license for the shadowed session but lets you shadow only one session at a time. Citrix Management Console and the Shadow Taskbar allow you to shadow multiple sessions, but only Citrix Management Console uses a single connection license. The Shadow Taskbar consumes one license for every session shadowed.

**Understand how to configure applications for SpeedScreen Latency Reduction.** The SpeedScreen Latency Reduction Manager lets you configure an application for local text echo. When you configure the application, the entire application can have the same settings, or you can specify that certain fields behave according to rules you set.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Application log

audit

Cache tab

Citrix Server Administration

ICA Settings

local text echo

logging of shadowing

modules

mouse click feedback

processes

published applications

server farm

Shadow Indicator

Shadow taskbar

shadowing

SpeedScreen

SpeedScreen Latency Reduction

System log

unassociated applications

# Exercises

For this first exercise, you will need two computers, one with MetaFrame XP installed and the other acting as a client, with the ICA Client installed. This exercise assumes that you already have a client installed. If not, refer to Chapter 10, "ICA Client Software," for the steps to install the client software.

## EXERCISE 6.1

### Shadowing

From the MetaFrame XP server, perform the following:

1. Open the Citrix Connection Configuration by either clicking the Citrix Connection Configuration icon on the ICA Administrator toolbar or choosing Start ➢ Programs ➢ Citrix ➢ MetaFrame XP ➢ Citrix Connection Configuration.

**EXERCISE 6.1 *(continued)***

2. Right-click the ica-tcp connection and choose Edit.
3. Click the Advanced button.
4. Deselect the (Inherit User Config) check box next to Shadowing at the bottom of the screen.
5. From the Shadowing pull-down menu, select the option Is Enabled: Input ON, Notify ON.
6. Click OK to close the screen.
7. Click OK again to close the Edit Connection Screen.

Perform the following steps from the client:

1. Choose Start ➢ Programs ➢ Citrix ICA Client ➢ Program Neighborhood.
2. Double-click the WordPad icon.
3. Click OK to dismiss any warning messages.

Perform the following from the MetaFrame XP server:

1. Open the Citrix Management Console by clicking the Citrix Management Console icon on the ICA Administrator toolbar or by choosing Start ➢ Programs ➢ Citrix ➢ MetaFrame XP ➢ Citrix Management Console.
2. Double-click the Servers node.
3. Select your server.
4. Right-click the session you want to shadow and click Shadow.
5. Set the key combination that will end the shadowed session, unless you want to keep the default Ctrl+* key combination. Click OK.
6. Enter your Citrix Administrator credentials.
7. Wait for the client to allow you to shadow.

Perform the following functions from the client:

1. When the Shadow Authorization window pops up, select Yes.
2. Minimize the Shadow Indicator.

**EXERCISE 6.1 *(continued)***

Perform the following from the MetaFrame XP server:

1. Type a message into the WordPad program.
2. Restore the Shadow Indicator.
3. Click the Stop Shadowing button.
4. Verify that WordPad on the client machine has been updated with the message you entered in step 1.

In this exercise, we are going to add the NWLink protocol and then create an ICA connection where users can establish IPX sessions.

**EXERCISE 6.2**

### Creating Connections

First, let's add NWLink to the server:

1. Open Network And Dial Up Connections by choosing Start ➢ Settings ➢ Control Panel and then double-clicking the Network And Dial Up Connections icon or by right-clicking the My Network Places icon.
2. Right-click the Local Area Connection icon and select Properties.
3. Click the Install button.
4. Select Protocol from the list of components and click the Add button.
5. Select NWLink IPX/SPX/NetBIOS Compatible Transport Protocol and click OK.
6. Click Close on the Local Area Connection Properties dialog box.

Next, let's add the IPX ICA connection:

1. Open the Citrix Connection Configuration by clicking the Citrix Connection Configuration icon on the ICA Administrator Toolbar or by choosing Start ➢ Programs ➢ Citrix ➢ MetaFrame XP ➢ Citrix Connection Configuration.

**EXERCISE 6.2** ***(continued)***

2. From the Connection menu, select New.
3. When the New Connection dialog box appears, enter the following information:
   a. In the Name box, enter **ica-ipx.**
   b. From the Transport pull-down list, select ipx.
   c. From the Device pull-down list, select your network card.
4. Click the OK button to finish creating the connection.

# Review Questions

1. Which utility must you use if you want to manage MetaFrame 1.8 servers in mixed mode?

   A. Citrix Management Console

   B. Citrix Server Administration

   C. Citrix Server Console

   D. Terminal Server Administrator

2. Which of the following can you *not* do with Citrix Server Administration?

   A. Display data about MetaFrame 1.8 and XP servers in your farm.

   B. Log off users.

   C. View print drivers that are being used on a server.

   D. Display information about published applications.

3. Which of the following is true regarding session shadowing?

   A. You can shadow the console and you can shadow sessions from the console.

   B. You can shadow the console, but you cannot shadow sessions from the console.

   C. You can shadow sessions from the console, but you cannot shadow the console.

   D. You cannot shadow the session console or shadow sessions from the console.

4. Which of the following utilities allows you to shadow more than one session at a time? (Choose all that apply.)

   A. Citrix Server Administration

   B. Citrix Management Console

   C. Shadow Taskbar

   D. Citrix Connection Configuration

**5.** Which of the following are true about licensing during shadowing sessions? (Choose all that apply.)

**A.** Shadowing done through the Citrix Management Console uses a single connection license regardless of the number of ICA sessions being shadowed.

**B.** Shadowing done through the Shadow Taskbar uses a single connection license regardless of the number of ICA sessions being shadowed.

**C.** Shadowing done through the Citrix Management Console uses a connection license for each ICA session being shadowed.

**D.** Shadowing done through the Shadow Taskbar uses a connection license for each ICA session being shadowed.

**6.** Which of the following items are true? (Choose all that apply.)

**A.** Multiple administrators can shadow a single user.

**B.** Multiple users can be shadowed at the same time.

**C.** During a shadow session, all mouse movement, keystrokes, video, and audio can be transmitted to administrator doing the shadowing.

**D.** The shadow request will fail if the shadower's session is not capable of supporting the video resolution of the user's session being shadowed.

**7.** Which utility would you use to change the shadowing restrictions?

**A.** Citrix Management Console

**B.** Shadow Taskbar

**C.** Citrix Connection Configuration

**D.** Citrix Server Administration

**8.** You are a Citrix administrator and want to change the shadowing settings. When you load the Citrix Connection Configuration, the settings you want to change are grayed out. What could be the problem?

**A.** You are at a MetaFrame XP console and are trying to change shadowing settings on a MetaFrame 1.8 server.

**B.** The Citrix administrator does not have shadowing permissions.

**C.** Shadowing restrictions were set during installation and cannot be changed.

**D.** The farm is set to mixed mode. To set shadowing permissions in the Citrix Connection Configuration utility, the server farm must be operating in native mode.

**9.** Your company has just merged with another company. The users from the new company need access to your MetaFrame server. They run IPX only. After you add the IPX protocol to your server, what must you do next for the users to connect to the MetaFrame server?

**A.** Add an IPX connection to the server using Citrix Connection Configuration.

**B.** Add an IPX connection to the server using Citrix Management Console.

**C.** Do nothing. MetaFrame XP by default installs a connection for TCP/IP, IPX, and async.

**D.** In Citrix Connection Configuration, check the box labeled IPX/SPX in the Supported Connections tab.

**10.** Where does SpeedScreen Latency Reduction Manager save the configuration settings file (`ss3config`) for an application?

**A.** `%systemroot%\`

**B.** `%systemroot%\system32\ss3`

**C.** `%systemroot%\system32\ss3config`

**D.** `%systemroot%\system32`

**11.** You have enabled local text echo on the server, but when you run one application, you notice that the local text is not being echoed back to the screen. What could be the problem?

**A.** The application does not have local text echo enabled.

**B.** The connection is fast enough that local text echo is not needed.

**C.** The connection is not fast enough to allow local text echo.

**D.** The server's ICA connection does not allow local text echo.

**12.** With SpeedScreen Latency Reduction Manager, you can configure latency reduction settings for which of the following? (Choose all that apply.)

**A.** An application

**B.** All applications on a server

**C.** All servers in a farm

**D.** An input field within an application

**13.** A user mentions to you that when they type their password into a custom in-house application, the letters of the password show up in the password field in normal text. You do some research and find that local text echo is enabled for that application. How would you change this setting so that normal text does not show up when a password is typed?

**A.** In the Input Field Configuration tab of the application's Properties window, place a check in the check box labeled This Is A Password Field.

**B.** In the Input Field Configuration tab of the application's Properties window, click the Advanced button, select This Is A Password Field With, and define which character you would like to appear when data is typed into the field.

**C.** Turn off local text echo.

**D.** The application cannot be used in a session if password fields are used.

**14.** You want to end a user's session. From which level in the Citrix Server Administration hierarchy can you find the Users tab so that you can do this? (Select all that apply.)

**A.** The All Listed Servers level

**B.** The Server Farm level

**C.** The Server level

**D.** The Session level

**15.** When granting access permissions, which of the following individual permissions are assigned when the User Access permission is used? (Choose all that apply.)

**A.** Query Information

**B.** Set Information

**C.** Shadow

**D.** Logon

**E.** Logoff

**F.** Message

**G.** Connect

**H.** Disconnect

**16.** From which configuration button on the Connection Properties sheet can you configure the amount of time before a disconnected session is terminated?

**A.** Advanced

**B.** Client Settings

**C.** Connection Settings

**D.** ICA Settings

**17.** From which configuration button on the Connection Properties dialog box can you configure audio quality?

**A.** Advanced

**B.** Client Settings

**C.** Connection Settings

**D.** ICA Settings

**18.** From which configuration button on the Connection Properties dialog box can you disable client drive mappings?

**A.** Advanced

**B.** Client Settings

**C.** Connection Settings

**D.** ICA Settings

**19.** From which configuration button on the Connection Properties dialog box can you disable a connection?

**A.** Advanced

**B.** Client Settings

**C.** Connection Settings

**D.** ICA Settings

**20.** You selected the option Disable Windows Client Printer Mapping in the Client Settings screen, yet some clients still have printer mappings appear. Why?

**A.** You need to disable the option on the client device.

**B.** You need to disable the LPT port mapping also.

**C.** You need to disable printer mappings in the client's user account properties.

**D.** This option is not supported under MetaFrame XP.

# Answers to Review Questions

1. B. The Citrix Management Console can monitor and manage only MetaFrame XP servers. If you are in a mixed-mode environment, you must use Citrix Server Administration to manage the MetaFrame 1.8 servers.

2. C. With Citrix Server Administration, you can view information about MetaFrame 1.8 and MetaFrame XP servers. You can use Citrix Server Administration to view information about MetaFrame XP servers, but the added functionality of the Citrix Management Console will not be available. From Citrix Server Administration, you can log off users, reset and terminate processes, and view information about published applications.

3. C. Sessions can be shadowed from the console within MetaFrame XP, but the console itself cannot be shadowed. This is a change from MetaFrame 1.*x* where the console was not allowed to shadow; you had to start another session to shadow other sessions.

4. B, C. Citrix Server Administration allows you to shadow only one session at a time. The Citrix Management Console and the Shadow Taskbar allow a Citrix administrator to shadow more than one session at a time.

5. A, D. The Citrix Management Console uses a single connection license when a Citrix administrator shadows multiple sessions. One license is used regardless of the number of ICA Clients that are being shadowed. The Shadow Taskbar uses a connection license for each ICA session being shadowed.

6. A, B, D. Multiple administrators can shadow a single connection, and multiple connections can be shadowed by a single connection. The video resolution must be compatible or the shadow session will fail. Audio cannot be transmitted over a shadow session.

7. C. The Citrix Connection Configuration utility is used to configure the shadowing settings. Edit an ICA connection and click the Advanced button.

8. C. Shadowing restrictions set during installation cannot be changed. If shadowing policies were set during MetaFrame XP setup, the ICA sessions might not be able to be shadowed, or the shadowing capabilities may be restricted.

9. A. Use the CCC to add ICA connections for transport protocols, network adapters, and asynchronous connections that were not created during MetaFrame XP installation.

10. C. SpeedScreen Latency Reduction Manager saves the configuration settings to the `%systemroot%\system32\ss3config` folder on the MetaFrame XP server. Other servers can deploy the configuration settings by copying the entire directory and its contents to each server in the farm.

11. A. If an application does not use the server settings for SpeedScreen Latency Reduction, then its own settings will override the server settings for all applications.

12. A, B, D. SpeedScreen Latency Reduction Manager can configure latency reduction settings for a server, an application, or even an input field within an application.

13. B. This Is A Password Input Field With specifies whether an asterisk or a space should be used to denote a locally echoed character. You should select this option if hidden characters, such as those used in a password input field, appear as normal text when they are locally echoed.

14. A, B, C. This tab is found at the top three levels, making it easy for you to find a user within the server farm or connected to a server.

15. A, D, F, G. These four permissions are granted so that a user can discover information about the server, log on to a session, send messages to the server, and connect to their own previously disconnected session.

16. A. The Advanced button brings up the settings for connection timeouts, autologon, security encryption level requirements, reconnection restrictions, shadowing, and user profiles.

17. D. The ICA Settings button brings up the settings for the audio quality level allowed over the connection: low, medium, or high.

18. B. The Client Settings button brings up the options to control the client mappings, including those for drive mappings, printer mappings, Clipboard mappings, and port mappings.

19. A. The Advanced button is used to enable or disable a connection. Alternatively, you can enable or disable a connection from the context menu when you right-click the connection.

20. B. Printers that are connected to LPT ports that use a non-Windows printer driver may still be mapped if the Disable Client LPT Port Mapping option is not selected.

Chapter 7

# Load Management

**THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:**

✓ **6. Load Management and Security**

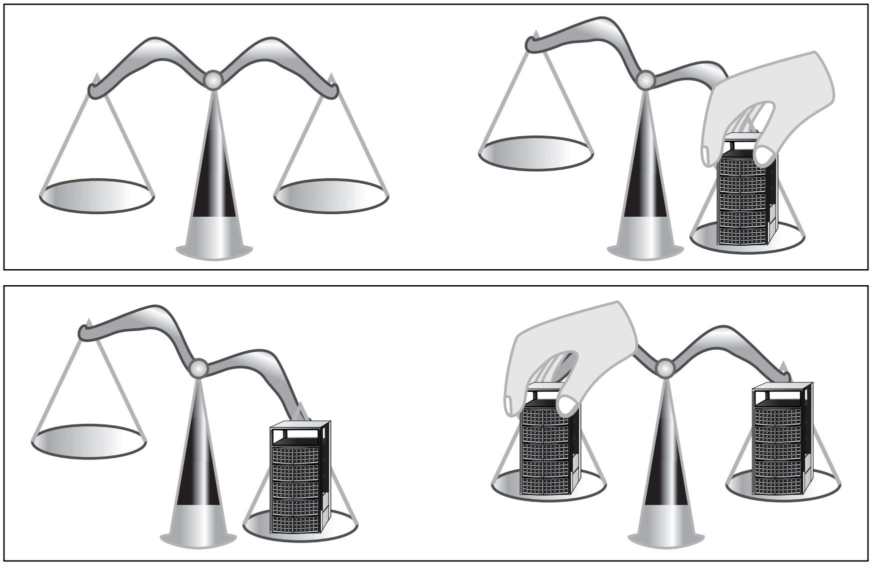
- 6a. Analyzing Load with Load Manager

Up until this point, we have been concentrating on installing and configuring the server to allow users to start and interact with sessions. In this chapter, we will discuss how to control sessions so that when a user initiates an ICA connection, they are directed to a server that is not overloaded, and each server bears an equal amount of the server farm load.

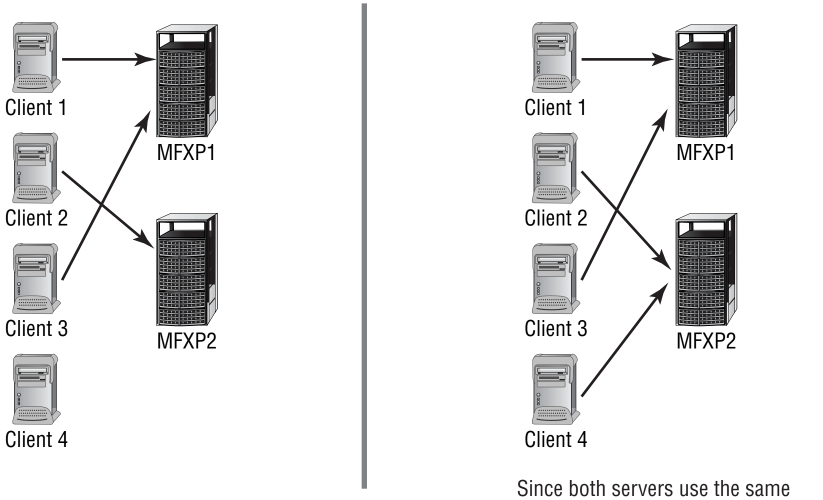
## What Is Load Balancing?

One of the benefits of adding MetaFrame XPa or XPe on top of Terminal Services is the enterprise-level management tools that are available. *Load balancing* is one of these tools, which is not available on Windows 2000 Server, Windows NT Server 4.0, Terminal Server Edition, or MetaFrame XPs. When running Microsoft's Terminal Server or MetaFrame XPs, you do not have the ability to truly load-balance sessions across the server farm. While some administrators try to even the load by directing a certain number of clients to each of their servers, this is not true load balancing. Clients are simply directed to a server for a published application. There are no mechanisms in place to determine whether another server's resources are available to more efficiently handle the request.

The load-balancing component changes all this. When we think of load balancing, we think of a scale that has two large pans on which we can add weight to either side. When weight is added on one side, as in the first graphic below, the pan drops, causing the opposite side to rise. We know that we have to add weight to the opposite side to equalize everything. If we then add an equal amount of weight to the second pan, as in the second graphic, the two will move to the same horizontal level.



The same holds true with load balancing in a MetaFrame XP environment. When a client initiates an ICA session, the data collector for the zone is contacted. The data collector holds information about the current load limit on each of the servers in the server farm. From this information, the data collector determines which server has the most resources available and directs the client to use that server. The data collector is then updated with the new load limit on the server and uses that information to determine which server to send the next client request. The following graphic shows the clients connecting to the servers equally.



Since both servers use the same load evaluator, Client 4 is directed to MFXP2 because it has the lightest load.

While this is a simplification of the process, it does visually represent what happens during the load-balancing process. Later in this chapter after we discuss the components of load balancing, we will take a look at the full process and see how everything works together to give our users a better experience with MetaFrame. To start off, let's take a look at the requirements necessary to implement load balancing.

NOTE

Please note that load balancing is not a fault-tolerant solution. The ICA connections route to the XP servers during the initial access of the application. No dynamic rebalancing of active ICA connections occurs between XP servers if the server hosting the application goes down.

## Requirements

You can determine whether your system can handle the service by examining the requirements. In the case of load management, there are two separate sets of requirements: one for the server and one for the server farm.

The server itself requires that the base operating system be either Windows NT Server 4.0, Terminal Server Edition or one of the Windows 2000 Server family members. Of course, this is also the minimum requirement for Citrix MetaFrame XP, so that point should be easy to remember. As for MetaFrame itself, you must use either MetaFrame XP Application (XPa) Server or MetaFrame XP Enterprise (XPe) Server. The standard edition of MetaFrame XP (XPs) has no additional services.

As soon as MetaFrame XPa or XPe is installed, load balancing is enabled as part of the license for those two products. You do not have to perform any other actions to get it up and running. All servers will have a *load evaluator* assigned to them and they will start reporting their current load to a data collector.

Since load balancing is a part of MetaFrame XPa and XPe, you cannot uninstall or disable load management from those products. If you don't want load balancing, you can either purchase MetaFrame XPs or assign a MetaFrame XPs product code to the server. Once a server is associated with a MetaFrame XPs product code, the load-balancing service is not authorized to start and the server will not participate in the load-balancing game.

Load balancing is also available in a MetaFrame 1.8 environment. Since MetaFrame 1.8 and MetaFrame XP can interoperate, there is a need for load balancing between the platforms. The load-balancing component for MetaFrame 1.8 relies on the ICA browser to collect load information from servers and directs the clients to the appropriate server. When the server farm is in mixed mode, MetaFrame XP takes over the functions of the ICA browser, thus allowing all of the servers to participate.

Combining the two products for load balancing does limit the load-balancing mechanisms, however. In a MetaFrame 1.8 environment, only servers can be load-balanced. With MetaFrame XP, the functionality has been extended so that published applications may be load-balanced. Also, rules and evaluators do not exist in the load-balancing add-on for MetaFrame 1.8. Load evaluators created in the Citrix Management Console do not recognize MetaFrame 1.8 servers since the operating system was not designed to use the new tools. If load balancing is used in a mixed-mode server farm, MetaFrame XP switches to using Load Balancing Services 1.0, which is used by MetaFrame 1.8 server farms.

Taking all this into account, let's move on to the next topic: the components that make up load balancing in a MetaFrame XP environment.

## Components

Not all servers are created equal. More often than not, when you purchase a server, it does not have the same hardware installed as your existing servers. As newer, more powerful computers are produced, the memory, hard drives, CPUs, and other hardware come down in price. With the disparity between the hardware components of your servers, you may need to configure load balancing to allow servers with more available resources to carry a heavier load. After all, they are generally able to process more information and therefore run more sessions.

You may also have servers that perform more than one function. Data collectors are a prime example. If you have a data collector loaded with published applications, you may not want to overload the data collector with too many sessions since it must still perform the responsibilities of a data collector.

To control the session balancing among your servers, MetaFrame XP load balancing uses what is known as *load evaluators*. Load evaluators are tools that monitor the resource usage on a server and report the current load to the data collector for the zone. Servers are allowed only one evaluator assigned to them. Published applications, likewise, are allowed only a single evaluator assigned to them. If a published application has an evaluator assigned to it and that application is on a server that also has an evaluator assigned, the evaluator with the highest threshold is used to determine the load.

Each load evaluator is controlled by one or more *rules*. These rules specify the resources that are monitored when calculating the load on the server. Let's take a look at these two components in detail.

## Load Evaluators

There are two built-in load evaluators: Default and Advanced. These are installed when load balancing is activated. All of the servers are automatically placed under the watchful eye of the Default load evaluator.

### Default

The *Default evaluator* is the evaluator that is assigned to all servers by default. This evaluator cannot be deleted or changed. When you use this evaluator, the user load on the server determines the entire load. For example, if you set a limit of 100 users, when the 100-user limit is met, the server stops accepting connections. While it may seem like a good idea to have a load evaluator automatically assigned to the servers, the problem with this scenario is that the load is not realistic for all installations of MetaFrame. Most companies install several smaller systems instead of a few large systems. This evaluator is optimized for servers running quad processors, 2–4GB of RAM, and dual RAID controllers. Not every system has that configuration. Since you cannot change the Default evaluator, if you have other hardware, you will need to create your own load evaluator based on the limits you want to set.

### Advanced

The *Advanced evaluator* is optimized for single-CPU systems with 192MB of RAM and a single SCSI Ultra Wide controller, and it cannot be altered. If your system is configured differently than this, you will need to create your own evaluator to meet your needs. This evaluator uses three resources to calculate the load on your server: CPU utilization, memory usage, and the number of page swaps.

## Rules

The Load Manager feature included with MetaFrame XPa and XPe allows administrators to combine individual rules into load evaluators for highly customized load management. If neither of the two built-in evaluators meets your needs, you can create your own evaluator using the rules provided.

The rules are based on one of four logical criteria: *Moving Average, Moving Average Compared To High Value, Incremental,* and *Boolean*. The first of these, Moving Average, is based on the percentage of the resource in use. CPU utilization is a good example of Moving Average. You can configure the high and low load values according to the CPU usage percentage. The low value determines when the server is considered as having no load placed on it, whereas the high value determines when the server is seen as having a full load. All Moving Average rules are based on a 0–100 range, with 100 equaling 100 percent of the resource being used.

The second rule type, Moving Average Compared To High Value, uses a percentage based on the values specified in the high and low threshold values. The values that can be used with this rule fall in the range 0–2,147,483,647. An example of this type rule is the *Disk Data I/O* rule. This rule uses disk I/O as the deciding factor when calculating the load. As an administrator, you would decide the threshold values for the server. If you choose a *Lower Threshold* of 0 and an *Upper Threshold* of 20,000, and the disk drives on the server are transferring 1200KB per second, the computed value would be 600. Since all of the rules are based on an arbitrary maximum number of 10,000, you would divide this arbitrary value by the upper threshold, yielding .5. The data stream from the drives is 1200KB per second. Multiplying the total KB per second by .5 yields 600, or 150/(10,000/20,000).

Incremental rules are based on an integer value that determines the maximum number that can be obtained for that rule. A good example of this rule would be the *Server User Load* rule. If this rule is configured with a 100-user limit, as soon as the 100th user connects to the server, the limit is reached and the server stops accepting connections. These rules are based on a maximum value of 10,000. Depending upon the value that is set, the server calculates the load by dividing the maximum value, 10,000, by the value configured in the rule. In the case of our Server User Load rule with a value of 100, each user that connects is calculated as 100 (10,000/100). When the total load reaches 10,000 as the 100th user connects, the server denies connections until one of the sessions ends.

The final rule type is Boolean. These rules either allow or disallow a connection based on whether the value entered in the rule is evaluated as True or False. These rules do not actually afford any type of load balancing but are used to explicitly allow or deny a connection. An example of this rule type is the *IP Range* rule. With this rule, you can specify the range of IP addresses that are allowed or not allowed to connect to a server.

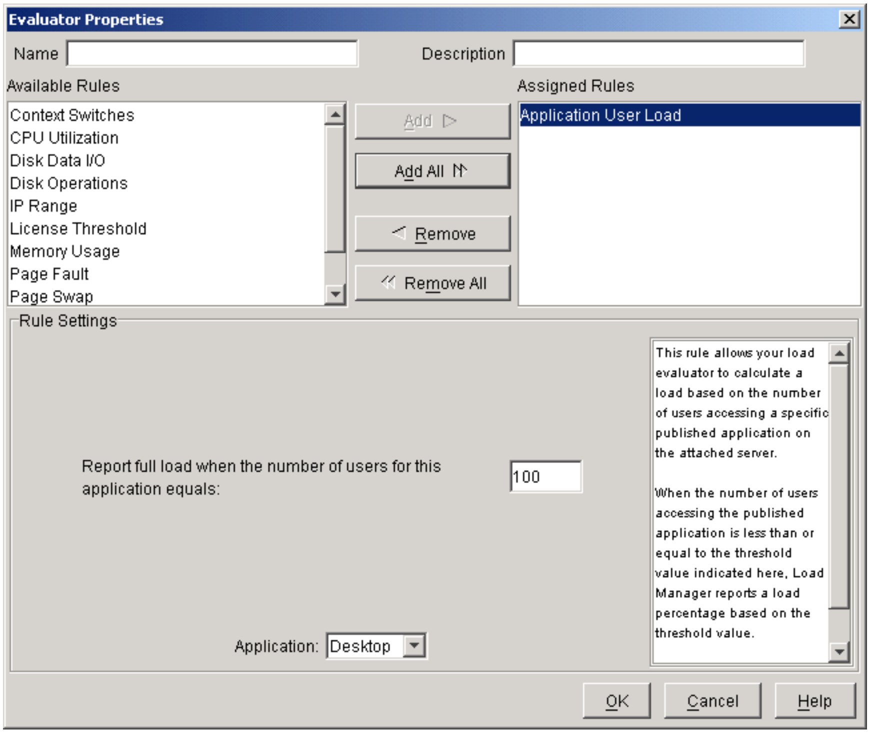
There are many rules available for inclusion in load evaluators, and you should know the implications of using each one. The following individual rules can be configured as part of a load evaluator:

**Application User Load** The *Application User Load* rule, shown in the Properties sheet in Figure 7.1, allows the load evaluator to calculate a load based on the number of users accessing a specific published application on the attached server. It is based on the Incremental criterion.

When the number of users accessing the published application is less than or equal to the threshold value indicated here, Load Manager reports a load percentage based on the threshold value.

The valid range for this rule is 1–10,000.

**FIGURE 7.1** Application User Load rule



Evaluator Properties

Name:

Description:

Available Rules: Context Switches, CPU Utilization, Disk Data I/O, Disk Operations, IP Range, License Threshold, Memory Usage, Page Fault, Page Swap

Assigned Rules: Application User Load

Rule Settings

Report full load when the number of users for this application equals: 100

Application: Desktop

This rule allows your load evaluator to calculate a load based on the number of users accessing a specific published application on the attached server.

When the number of users accessing the published application is less than or equal to the threshold value indicated here, Load Manager reports a load percentage based on the threshold value.

**Context Switches** The *Context Switches* rule, shown in Figure 7.2, allows the load evaluator to calculate a load based on the number of CPU context switches. A context switch occurs every time the operating system switches from one executing process to another. It is based on the Moving Average Compared To High Value criterion.

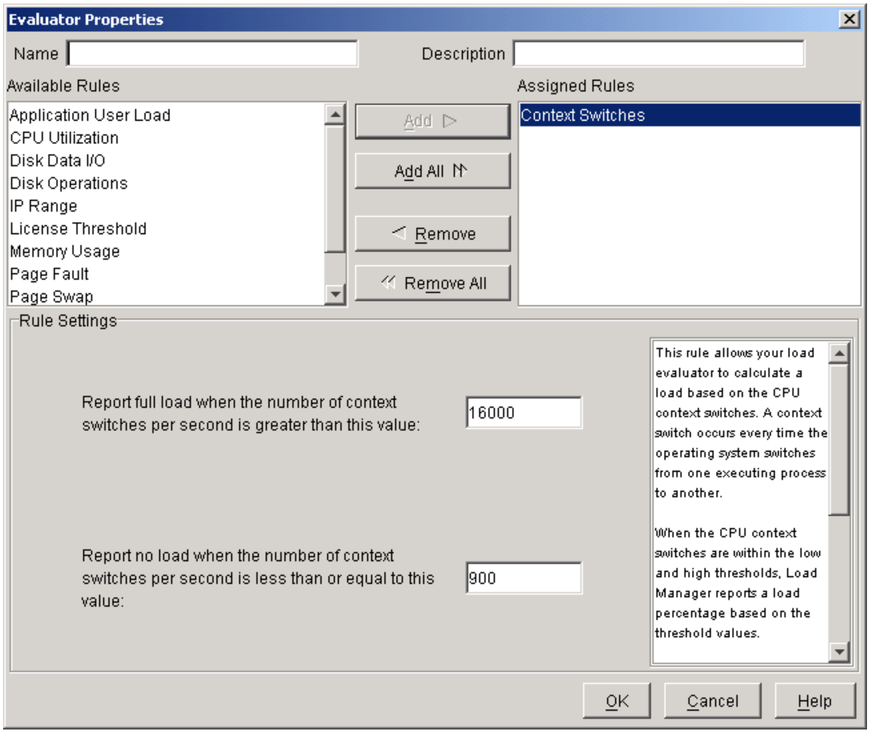
When the number of CPU context switches falls within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the number of CPU context switches exceeds the high threshold, Load Manager reports a full load.

When the number of CPU context switches is less than the low threshold, Load Manager reports no load.

The valid range for the low and high thresholds is 0–2,147,483,647.

**FIGURE 7.2** Context Switches rule



Evaluator Properties

Name

Description

Available Rules

Application User Load
CPU Utilization
Disk Data I/O
Disk Operations
IP Range
License Threshold
Memory Usage
Page Fault
Page Swap

Assigned Rules

Context Switches

Rule Settings

Report full load when the number of context switches per second is greater than this value: 16000

Report no load when the number of context switches per second is less than or equal to this value: 900

This rule allows your load evaluator to calculate a load based on the CPU context switches. A context switch occurs every time the operating system switches from one executing process to another.

When the CPU context switches are within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

**CPU Utilization** The *CPU Utilization* rule, shown in Figure 7.3, allows the load evaluator to calculate a load based on CPU utilization. It is based on the Moving Average criterion.

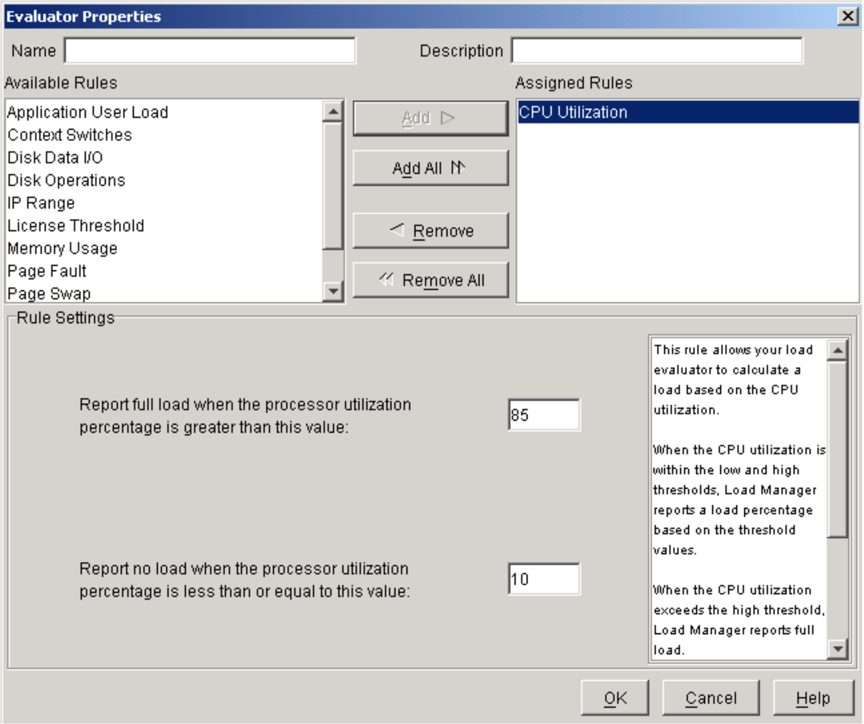
When the CPU utilization is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the CPU utilization exceeds the high threshold, Load Manager reports a full load.

When the CPU utilization is less than the low threshold, Load Manager reports no load.

The valid range for the high and low thresholds is 0–100.

**FIGURE 7.3** CPU Utilization rule



Report full load when the processor utilization percentage is greater than this value: 85

Report no load when the processor utilization percentage is less than or equal to this value: 10

This rule allows your load evaluator to calculate a load based on the CPU utilization.

When the CPU utilization is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the CPU utilization exceeds the high threshold, Load Manager reports full load.

**Disk Data I/O** The *Disk Data I/O* rule, shown in Figure 7.4, allows the load evaluator to calculate (in kilobytes) a load based on the disk I/O throughput. It is based on the Moving Average Compared To High Value criterion.

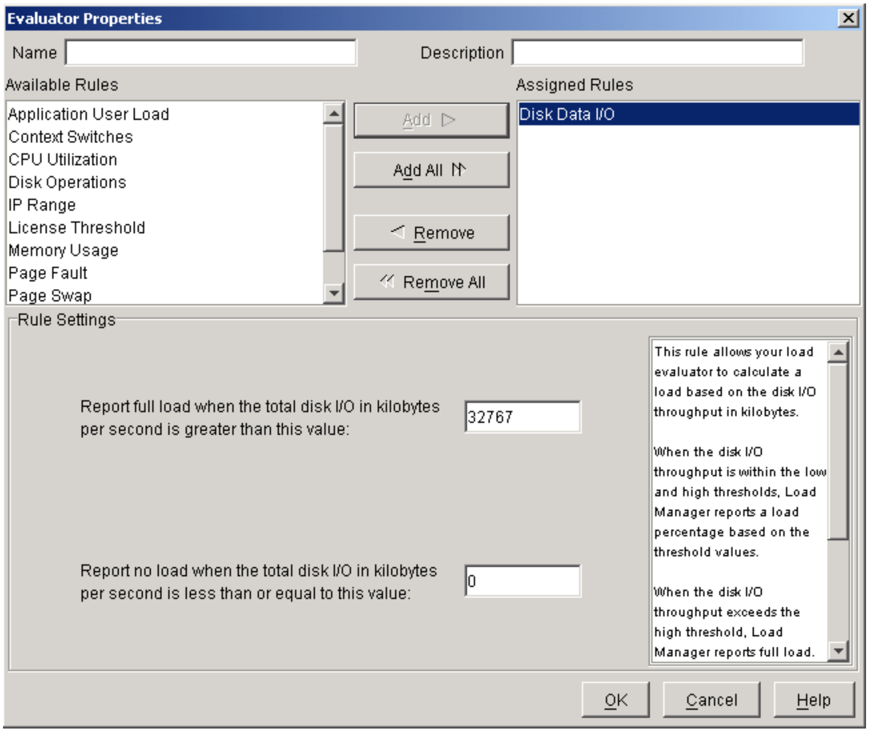
When the disk I/O throughput is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the disk I/O throughput exceeds the high threshold, Load Manager reports a full load.

When the disk I/O throughput is less than the low threshold, Load Manager reports no load.

The valid range for the high and low thresholds is 0–2,147,483,647.

**FIGURE 7.4** Disk Data I/O rule



Evaluator Properties

Name

Description

Available Rules

- Application User Load
- Context Switches
- CPU Utilization
- Disk Operations
- IP Range
- License Threshold
- Memory Usage
- Page Fault
- Page Swap

Assigned Rules

- Disk Data I/O

Rule Settings

Report full load when the total disk I/O in kilobytes per second is greater than this value: 32767

Report no load when the total disk I/O in kilobytes per second is less than or equal to this value: 0

This rule allows your load evaluator to calculate a load based on the disk I/O throughput in kilobytes.

When the disk I/O throughput is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the disk I/O throughput exceeds the high threshold, Load Manager reports full load.

**Disk Operations** The *Disk Operations* rule, shown in Figure 7.5, allows the load evaluator to calculate a load based on the number of disk operations per second. It is based on the Moving Average Compared To High Value criterion.

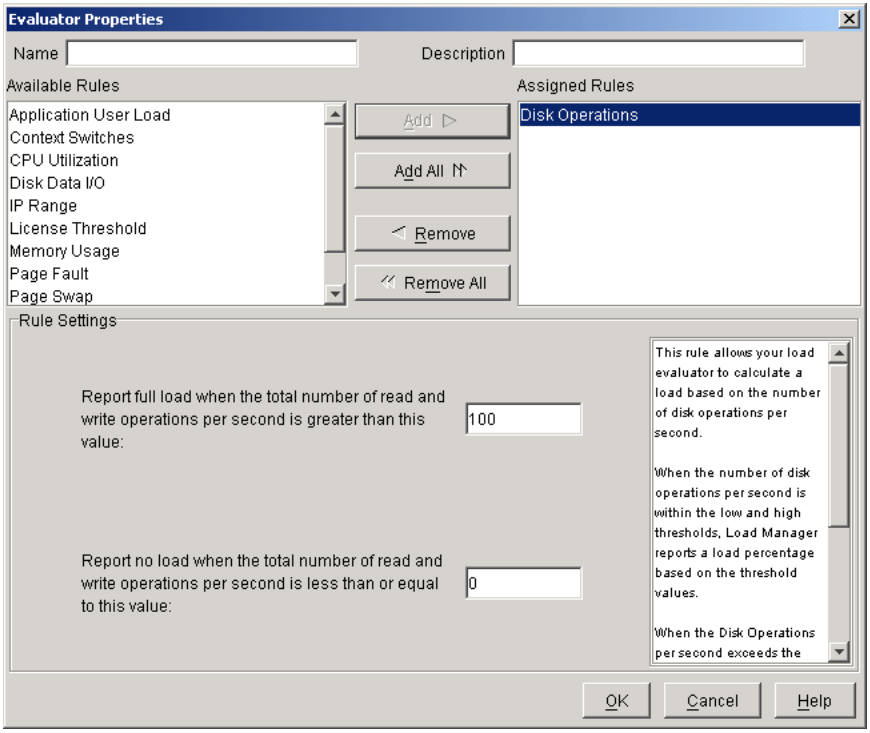
When the number of disk operations per second is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the number of disk operations per second exceeds the high threshold, Load Manager reports a full load.

When the number of disk operations per second is less than the low threshold, Load Manager reports no load.

The valid range for the high and low thresholds is 0–2,147,483,647.

**FIGURE 7.5** Disk Operations rule



Evaluator Properties

Name

Description

Available Rules

- Application User Load
- Context Switches
- CPU Utilization
- Disk Data I/O
- IP Range
- License Threshold
- Memory Usage
- Page Fault
- Page Swap

Assigned Rules

- Disk Operations

Rule Settings

Report full load when the total number of read and write operations per second is greater than this value: 100

Report no load when the total number of read and write operations per second is less than or equal to this value: 0

This rule allows your load evaluator to calculate a load based on the number of disk operations per second.

When the number of disk operations per second is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

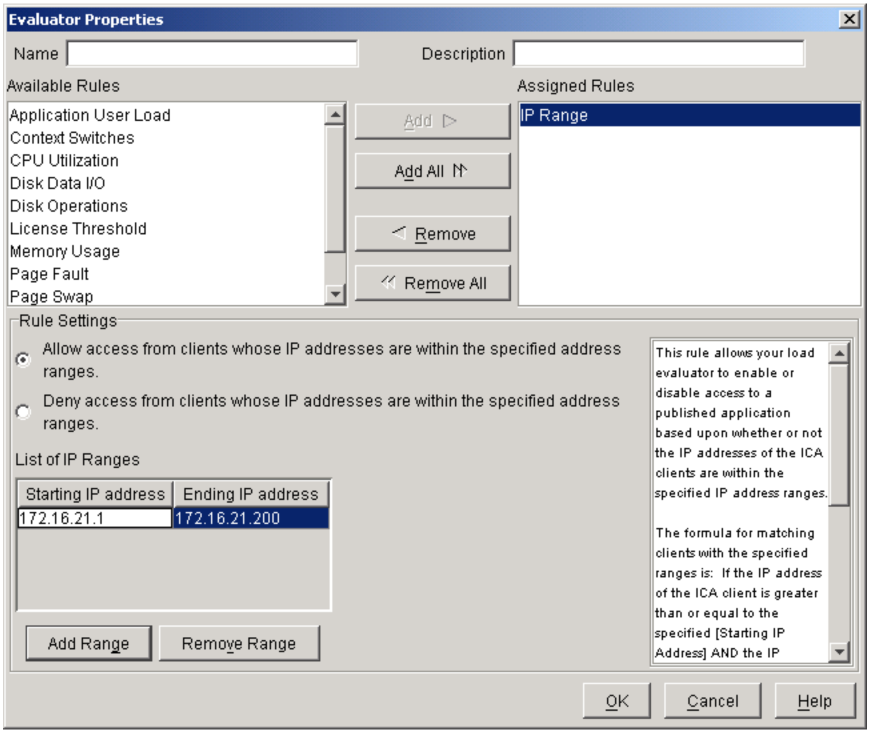
When the Disk Operations per second exceeds the

**IP Range** The *IP Range* rule, shown in Figure 7.6, allows the load evaluator to enable or disable access to a published application based upon whether or not the IP addresses of the ICA Clients are within the specified IP address ranges. It is based on the Boolean criterion.

The formula for matching clients with the specified ranges is as follows: If the IP address of the ICA Client is greater than or equal to the specified [Starting IP Address] *and* the IP address of the ICA Client is less than or equal to the specified [Ending IP Address], the client is considered to be a part of the specified range and action is taken depending on the inclusion or exclusion mode.

You must use this rule in conjunction with another rule. This rule will not load-balance connections by itself.

**FIGURE 7.6** IP Range rule



Assigned Rules: IP Range

● Allow access from clients whose IP addresses are within the specified address ranges.

○ Deny access from clients whose IP addresses are within the specified address ranges.

| Starting IP address | Ending IP address |
|---|---|
| 172.16.21.1 | 172.16.21.200 |

This rule allows your load evaluator to enable or disable access to a published application based upon whether or not the IP addresses of the ICA clients are within the specified IP address ranges.

The formula for matching clients with the specified ranges is: If the IP address of the ICA client is greater than or equal to the specified [Starting IP Address] AND the IP

**License Threshold** The *License Threshold rule*, shown in Figure 7.7, allows the load evaluator to calculate a load based on the number of assigned or pooled connection licenses used on each server. It is based on the Incremental criterion.

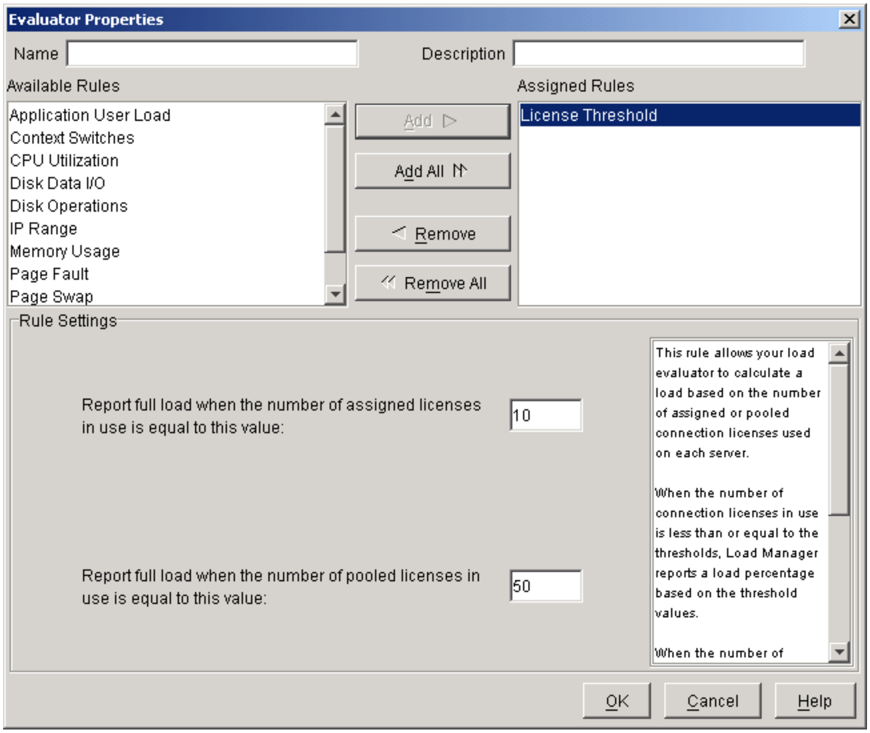
When the number of connection licenses in use is less than or equal to the thresholds, Load Manager reports a load percentage based on the threshold values.

When the number of connection licenses in use exceeds the high threshold, Load Manager reports a full load.

To indicate that a license type is to be ignored, enter a zero for the license type. You can enter a zero for only one of the license types.

The valid range for the high threshold is 0–9999.

**FIGURE 7.7** License Threshold rule



Report full load when the number of assigned licenses in use is equal to this value: 10

Report full load when the number of pooled licenses in use is equal to this value: 50

This rule allows your load evaluator to calculate a load based on the number of assigned or pooled connection licenses used on each server.

When the number of connection licenses in use is less than or equal to the thresholds, Load Manager reports a load percentage based on the threshold values.

When the number of

**Memory Usage** The *Memory Usage* rule, shown in Figure 7.8, allows the load evaluator to calculate a load based on memory utilization. It is based on the Moving Average criterion.

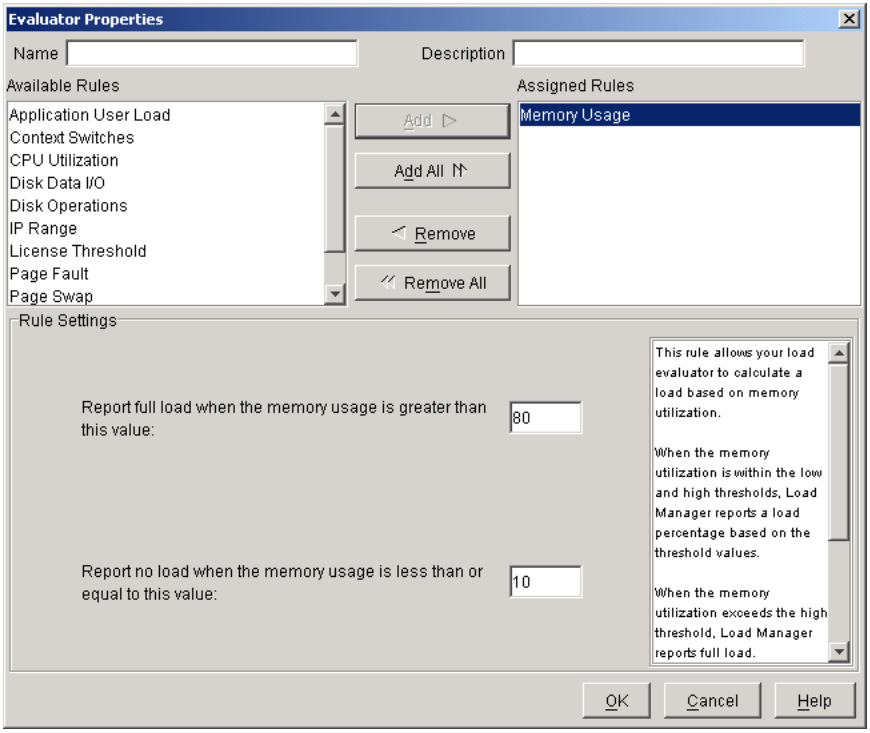
When the memory utilization falls within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the memory utilization exceeds the high threshold, Load Manager reports a full load.

When the memory utilization is less than the low threshold, Load Manager reports no load.

The valid range for the high and low thresholds is 0–100.

**FIGURE 7.8** Memory Usage rule



Evaluator Properties

Name

Description

Available Rules

- Application User Load
- Context Switches
- CPU Utilization
- Disk Data I/O
- Disk Operations
- IP Range
- License Threshold
- Page Fault
- Page Swap

Assigned Rules

- Memory Usage

Rule Settings

Report full load when the memory usage is greater than this value: 80

Report no load when the memory usage is less than or equal to this value: 10

This rule allows your load evaluator to calculate a load based on memory utilization.

When the memory utilization is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the memory utilization exceeds the high threshold, Load Manager reports full load.

**Page Fault** The *Page Fault* rule, shown in Figure 7.9, allows the load evaluator to calculate a load based on the number of page faults per second. A page fault occurs every time the operating system accesses physical memory that has been flushed to disk. It is based on the Moving Average Compared To High Value criterion.

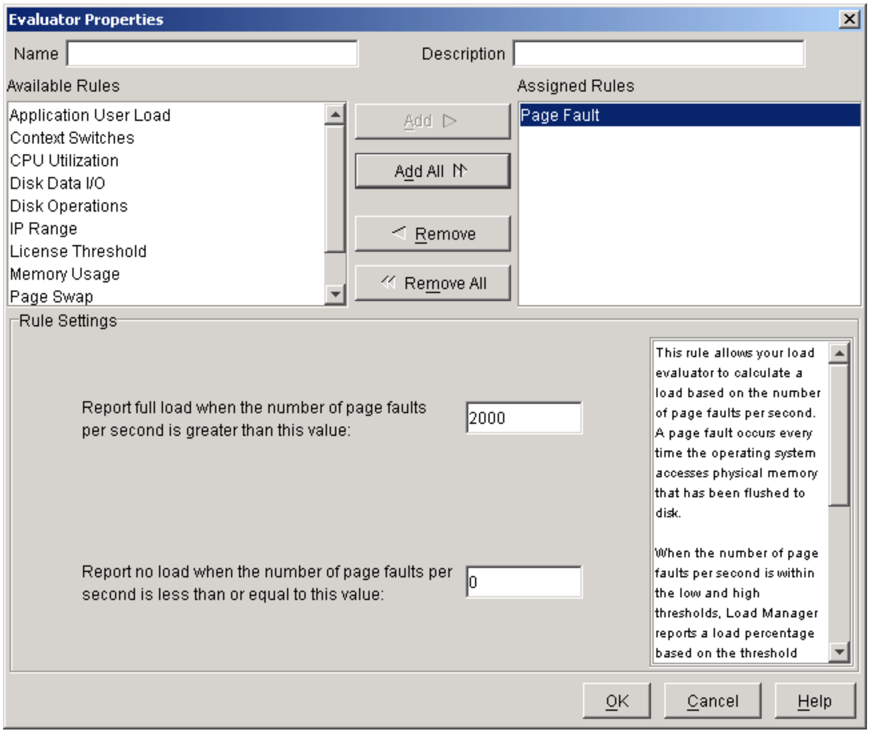
When the number of page faults per second falls within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the number of page faults per second exceeds the high threshold, Load Manager reports a full load.

When the number of page faults per second is less than the low threshold, Load Manager reports no load.

The valid range for the high and low thresholds is 0–2,147,483,647.

**FIGURE 7.9** Page Fault rule



Report full load when the number of page faults per second is greater than this value: 2000

Report no load when the number of page faults per second is less than or equal to this value: 0

This rule allows your load evaluator to calculate a load based on the number of page faults per second. A page fault occurs every time the operating system accesses physical memory that has been flushed to disk.

When the number of page faults per second is within the low and high thresholds, Load Manager reports a load percentage based on the threshold

**Page Swap** The *Page Swap* rule, shown in Figure 7.10, allows the load evaluator to calculate a load based on the number of page swaps per second. A page swap occurs every time the operating system swaps physical memory to virtual memory on disk. It is based on the Moving Average Compared To High Value criterion.

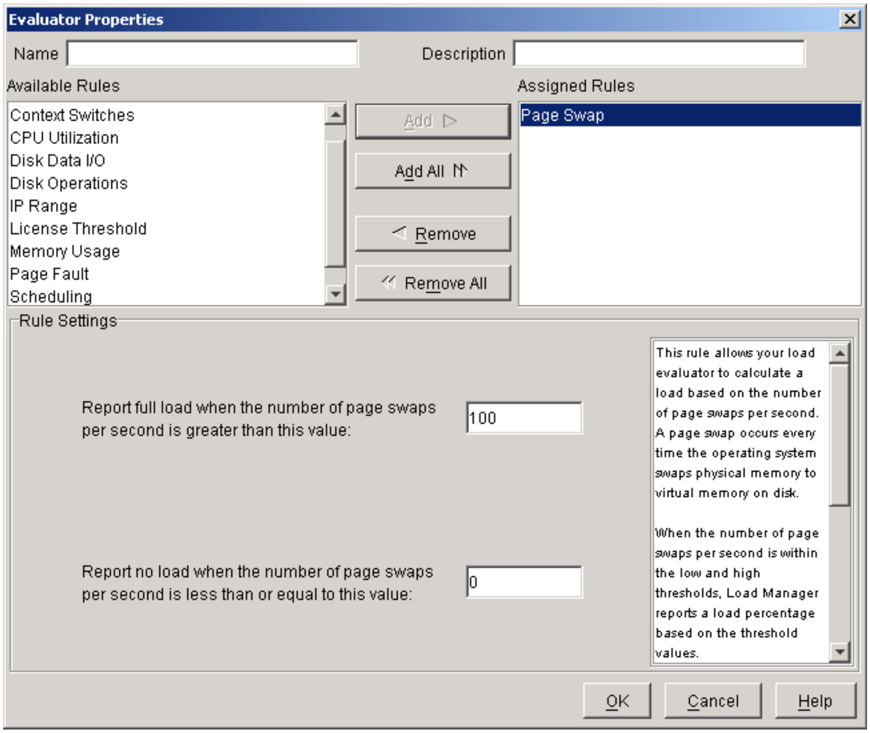
When the number of page swaps per second falls within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the number of page swaps per second exceeds the high threshold, Load Manager reports a full load.

When the number of page swaps per second is less than the low threshold, Load Manager reports no load.

The valid range for the high and low thresholds is 0–2,147,483,647.

**FIGURE 7.10** Page Swap rule



Evaluator Properties

Name

Description

Available Rules

- Context Switches
- CPU Utilization
- Disk Data I/O
- Disk Operations
- IP Range
- License Threshold
- Memory Usage
- Page Fault
- Scheduling

Assigned Rules

- Page Swap

Rule Settings

Report full load when the number of page swaps per second is greater than this value: 100

Report no load when the number of page swaps per second is less than or equal to this value: 0

This rule allows your load evaluator to calculate a load based on the number of page swaps per second. A page swap occurs every time the operating system swaps physical memory to virtual memory on disk.

When the number of page swaps per second is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

**Scheduling** The *Scheduling* rule, shown in Figure 7.11, allows the load evaluator to enable and disable the availability of a server or published application during certain days of the week and certain hours of the day. It is based on the Boolean criterion.

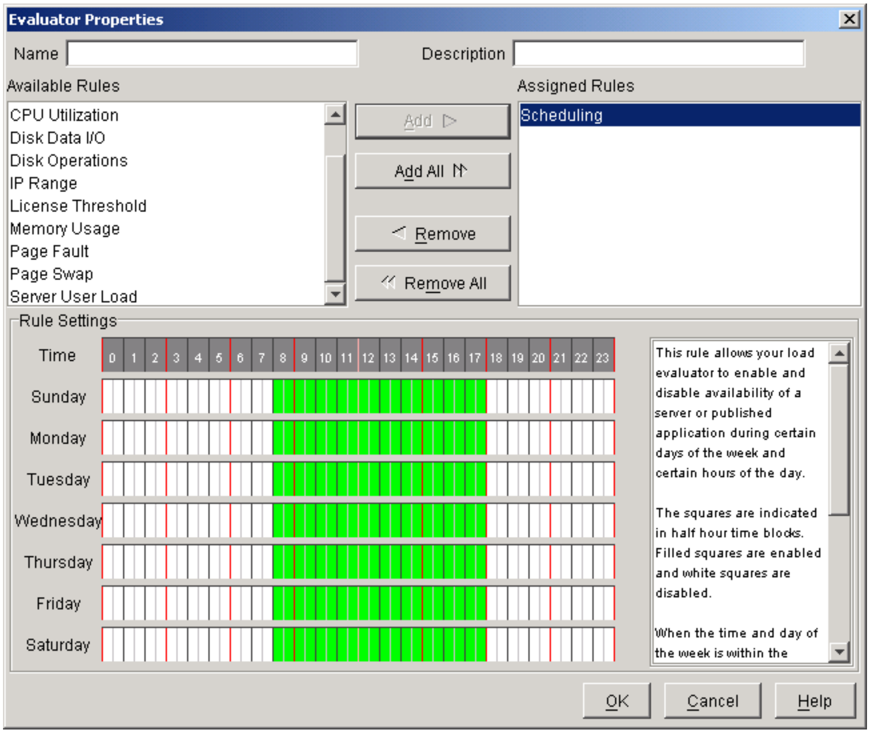
The squares are indicated in half-hour time blocks. Filled squares are enabled and empty squares are disabled.

When the time and day of the week fall within the specified time, Load Manager reports no load.

When the time and day of the week are outside the specified time, Load Manager reports a full load.

You must use this rule in conjunction with another rule. This rule will not load-balance connections by itself.

**FIGURE 7.11** Scheduling rule



Evaluator Properties

Name

Description

Available Rules

CPU Utilization
Disk Data I/O
Disk Operations
IP Range
License Threshold
Memory Usage
Page Fault
Page Swap
Server User Load

Assigned Rules

Scheduling

Rule Settings

| Time | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sunday | □□ | □□ | □□ | □□ | □□ | □□ | □□ | □□ | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | □□ | □□ | □□ | □□ | □□ | □□ |
| Monday | □□ | □□ | □□ | □□ | □□ | □□ | □□ | □□ | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | □□ | □□ | □□ | □□ | □□ | □□ |
| Tuesday | □□ | □□ | □□ | □□ | □□ | □□ | □□ | □□ | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | □□ | □□ | □□ | □□ | □□ | □□ |
| Wednesday | □□ | □□ | □□ | □□ | □□ | □□ | □□ | □□ | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | □□ | □□ | □□ | □□ | □□ | □□ |
| Thursday | □□ | □□ | □□ | □□ | □□ | □□ | □□ | □□ | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | □□ | □□ | □□ | □□ | □□ | □□ |
| Friday | □□ | □□ | □□ | □□ | □□ | □□ | □□ | □□ | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | □□ | □□ | □□ | □□ | □□ | □□ |
| Saturday | □□ | □□ | □□ | □□ | □□ | □□ | □□ | □□ | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | 🟩🟩 | □□ | □□ | □□ | □□ | □□ | □□ |

This rule allows your load evaluator to enable and disable availability of a server or published application during certain days of the week and certain hours of the day.

The squares are indicated in half hour time blocks. Filled squares are enabled and white squares are disabled.

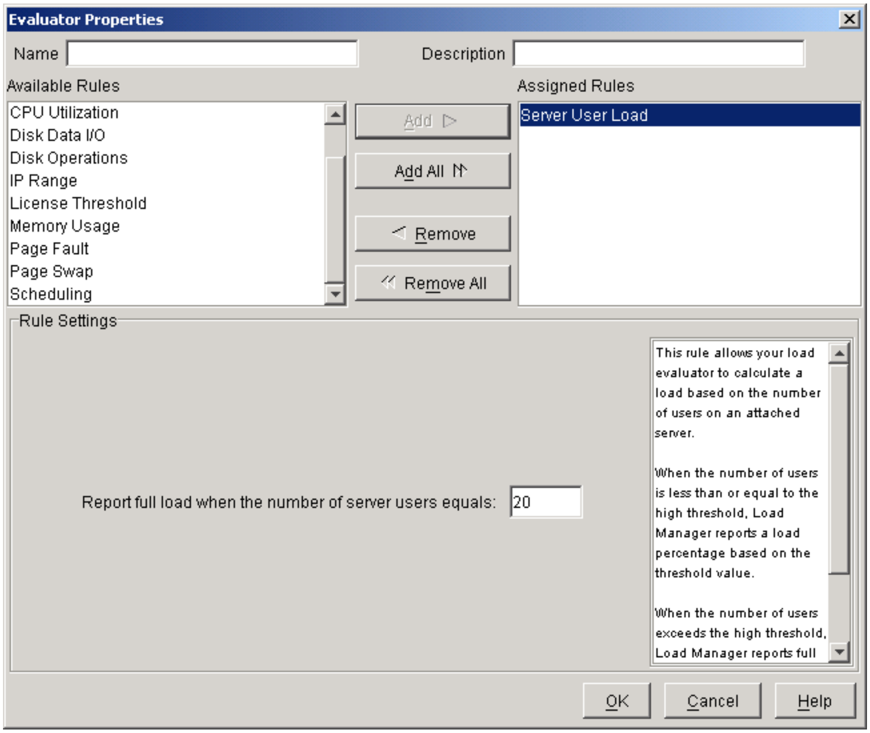
When the time and day of the week is within the

**Server User Load** The *Server User Load* rule, shown in Figure 7.12, allows the load evaluator to calculate a load based on the number of users on an attached server. It is based on the Incremental criterion.

When the number of users accessing the server is less than or equal to the threshold value indicated here, Load Manager reports a load percentage based on the threshold value.

The valid range for this rule is 1–10,000.

**FIGURE 7.12** Server User Load rule



Report full load when the number of server users equals: 20

This rule allows your load evaluator to calculate a load based on the number of users on an attached server.

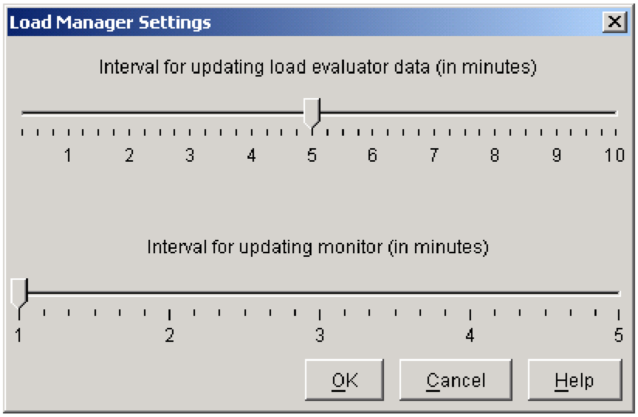
When the number of users is less than or equal to the high threshold, Load Manager reports a load percentage based on the threshold value.

When the number of users exceeds the high threshold, Load Manager reports full

MetaFrame XP's load balancing collects information periodically from the servers in the server farm. The data collector is responsible for maintaining the server load information and directing clients to the correct server. By default, servers report load information to the data collector every five minutes. This guarantees that any updates that may have been missed will be delivered. In the Load Manager Settings dialog box, shown in Figure 7.13, you can adjust this update interval if you want the data collector to receive updates more or less frequently. You can reach this screen by opening the Citrix Management Console and choosing Actions ➤ Load Manager ➤ Load Manager Settings.

MetaFrame XP servers report load information to the data collector when certain events trigger an update. Three *triggers* are designed to optimize the load-balancing process and control the number of sessions. The first of these triggers is *User Logon/Logoff*. When a user attempts to start a published application, the data collector evaluates the load on all servers and directs the client to connect to the server with the lightest load. The data collector then increments that server's load value by 200 so that the data collector can guess which server has the lightest load for the next client that wishes to connect. As the user logs on to the session, the server adjusts its load and sends an update to the data collector, which will modify the server's load information to reflect the correct load information. Having the data collector perform this guesstimate guarantees that the server will not receive multiple logins from an inaccurate load evaluation.

**FIGURE 7.13** Load Manager Settings



Load Manager Settings

Interval for updating load evaluator data (in minutes)

Interval for updating monitor (in minutes)

The next trigger we will look at is the *User Connect/Disconnect*. This trigger is very similar to the User Logon/Logoff trigger, but this trigger alters the load when the user's session is in a disconnected state. As a session is connected, the load information is updated on the data collector, and when the session is placed in a disconnected state, the data collector is informed and the load is reduced to reflect the change.

Finally, any fluctuations in the load of the server greater than a 5 percent change over a 30-second time frame are sent to the data collector. Take Excel, for instance. As you enter information into the spreadsheet, the application may not consume very much of the processor's power. However, after the data has been entered and you execute a macro against the data, the processor utilization increases. If this increase averages more than 5 percent over a 30-second time frame, the data collector will be notified and the server's load level will be updated accordingly. Unfortunately, you cannot change this rate. Of course, that can also be a benefit since you will not cause the servers to send too many, or too few, updates to the data collector.

Even if none of these triggers have initiated an update, the servers still perform an update. In a process known as the Specified Update Interval, each server sends updated load information to the data collector in order to keep the load information current. Take for instance a server that has not had enough of a load change to activate one of the aforementioned triggers. If the load has changed over the five-minute time frame but not enough during each of the 30-second intervals to warrant the server sending out an update, the current load information will be sent to the data collector. The default interval is set for five minutes but can be changed by navigating through Action ➢ Load Manager ➢ Load Manage Settings. Moving the slider on the setting screen shown previously in Figure 7.13, you can change the update time interval in 15-second increments. The maximum update interval is 10 minutes.

Issues may arise from events that bypass Load Manager's control. For example, instead of using the data collector to determine which server you will connect to, if you make a direct connection to a server in the server farm, the load management subsystem is bypassed and a session can be initiated on an already overused server. The same holds true for a disconnected session. While a server is sitting idle, you can start other sessions on the server, maximizing the server's resources. When a user reconnects to an existing session, the server loses efficiency. Session sharing can also cause problems. If a user starts additional seamless window applications, they will all share the same session, but the server may not have the horsepower to efficiently handle the additional load from the applications.

Another issue may arise when users connect to nearly loaded servers because the Load Manager subsystem is unable to efficiently handle a large number of connections at the same time. If connection requests come into the data collector faster than the servers can update the load information, the data collector could send the client to a fully loaded server instead of denying the connection. While this situation is rare, it could be an issue in an environment where numerous users log on to sessions at the same time. Take a multiple-shift organization with overlapping shifts, for example. With one shift already connected to sessions, the second shift arrives and attempts to log on at the same time. As the servers process information for the existing sessions, clients are requesting new sessions. If the data collector does not receive timely information from the load-balanced servers, the data collector could direct clients to the already loaded servers, causing them to overload and run very inefficiently.

Our goal is to configure our systems so that they will never get to the point that they become so loaded that they will not send out timely information to the data collector, yet will be able to run enough sessions so that the server is utilized to its fullest extent. In the next sections, we will look at how the Load Manager interface works, and then we will discuss how to effectively use the rules and evaluators.

# The Load Manager Interface

Load Manager is a component that is added to the Citrix Management Console. You will find two separate administrative tools within the Citrix Management Console when you use load management. In the list of nodes, notice the Load Evaluators node. This is where evaluators are created, edited, and deleted. This is not where you assign an evaluator to a server or published application. To perform that function, you need to expand the Servers node and identify the server where the evaluator will be assigned. For published applications, you need to expand the Applications node and identify the application that will be load-balanced. The other tool is the Load Manager Monitor, which we will look at later in this section. You will use this tool to visually monitor the effects of the evaluators as the servers are used.

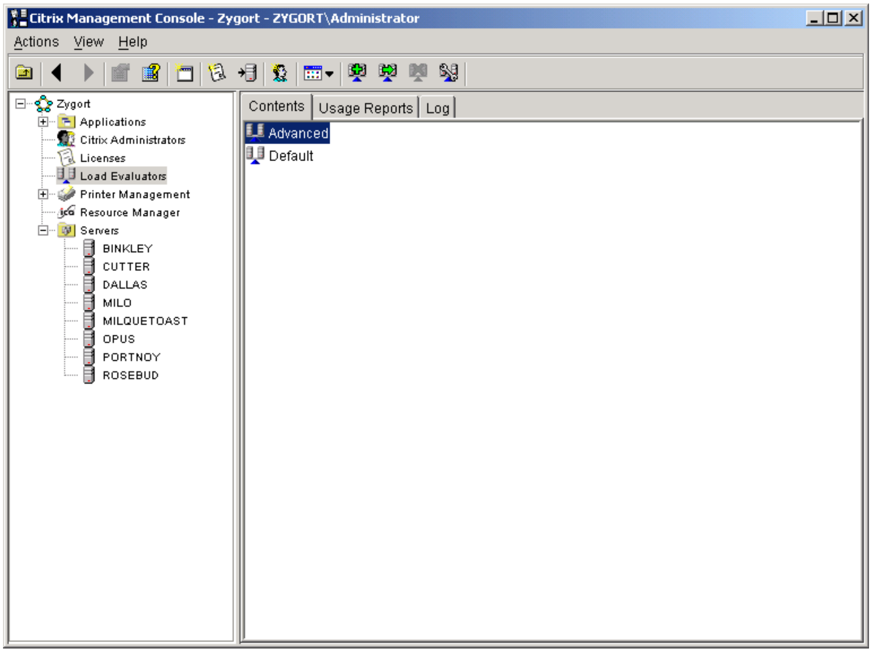
## Load Evaluators Node

First though, let's take a look at the *Load Evaluators node*. When you click the node, you are presented with three tabs: Contents, Usage Reports, and Log. This is where you can centrally control which evaluator is attached to a server or published application and view the long-term information. This node always contains at least two evaluators, Default and Advanced, and since the Default evaluator is attached to every server by default, the servers in your farm appear here also. Published applications appear in this node only if you have attached an evaluator to them. If you right-click this node in the left window, two options appear: Refresh Load Evaluators and New Load Evaluator. Selecting the first menu option forces the Citrix Management Console to display the latest information about this node just in case the autorefresh has not occurred. Now let's look at each of the tabs available from this node.

### Contents Tab

The first of the tabs, *Contents*, is shown in Figure 7.14. All of the evaluators that have been created are displayed here, along with the two built-in evaluators. From here, you can create new evaluators, modify existing evaluators, and delete those that are no longer needed.

FIGURE 7.14 The Contents tab



As shown in Figure 7.15, if you right-click an evaluator, you will see a menu that allows you to perform these actions. Most of these functions are also available from the icons at the top of the Citrix Management Console. Figure 7.16 shows the menu that appears when you right-click the Load Evaluators node. From either of these areas, you can choose the New Load Evaluator option to create an evaluator.

FIGURE 7.15 Evaluator options

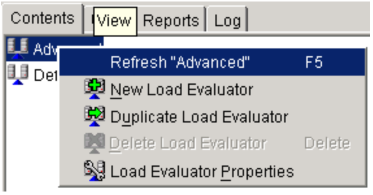
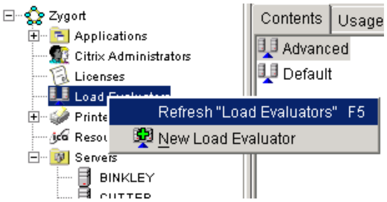
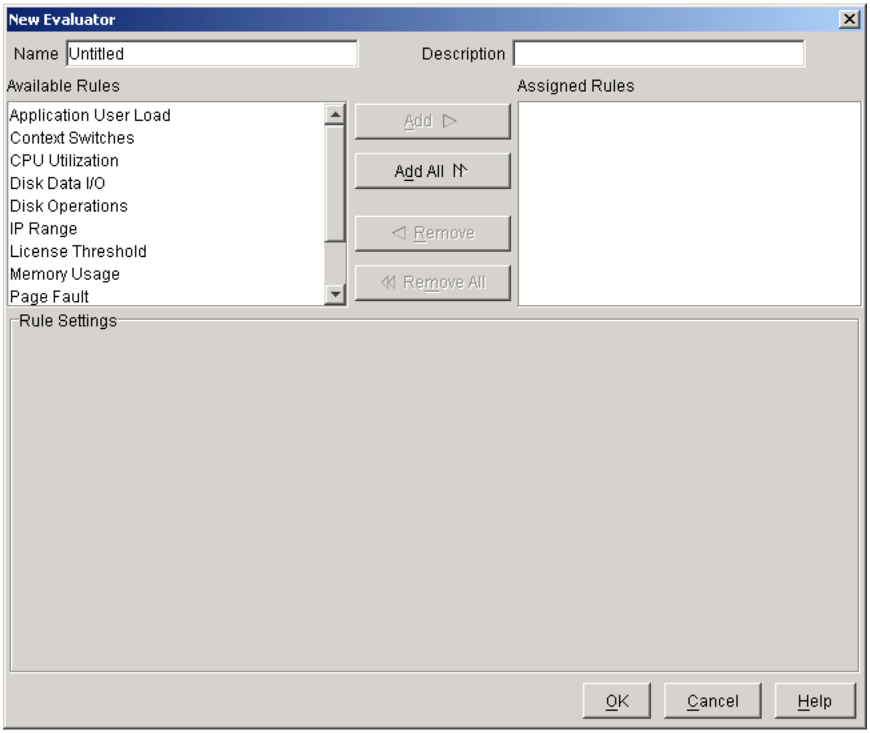


**FIGURE 7.16** Evaluator node options



Clicking this option brings up the New Evaluator screen shown in Figure 7.17. After you give the evaluator a name, you can choose the rules that you want applied. Select the rules from the Available Rules column and click the Add button to move them to the Assigned Rules column. If you decide that you do not want one or more of the rules assigned to the evaluator, you can select them from the Assigned Rules column and click the Remove button.

**FIGURE 7.17** New Evaluator screen


New Evaluator

Name: Untitled

Description:

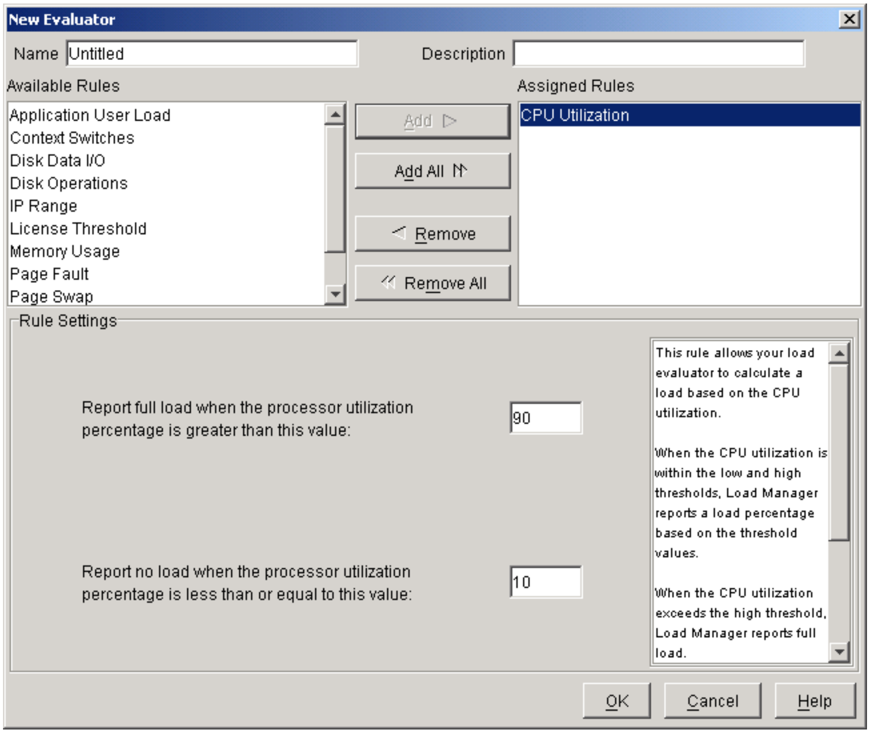
Available Rules
- Application User Load
- Context Switches
- CPU Utilization
- Disk Data I/O
- Disk Operations
- IP Range
- License Threshold
- Memory Usage
- Page Fault

Assigned Rules

Rule Settings

After you've added the appropriate rules, you can set limits by selecting the rule and configuring the options in the lower half of the screen. An explanation of the rule appears in this area also, so if you are unsure of the function of the rule, you can read it there. In Figure 7.18, the CPU Utilization rule has been selected, and its limits are displayed. These settings determine at what point the evaluator notifies the data collector that there is either no load on the server or a full load on the server, or they show the percentage of the load according to the processor activity. Select other rules to familiarize yourself with how they are used.

**FIGURE 7.18** Selecting a rule



New Evaluator

Name: Untitled

Description:

Available Rules

- Application User Load
- Context Switches
- Disk Data I/O
- Disk Operations
- IP Range
- License Threshold
- Memory Usage
- Page Fault
- Page Swap

Assigned Rules

- CPU Utilization

Rule Settings

Report full load when the processor utilization percentage is greater than this value: 90

Report no load when the processor utilization percentage is less than or equal to this value: 10

This rule allows your load evaluator to calculate a load based on the CPU utilization.

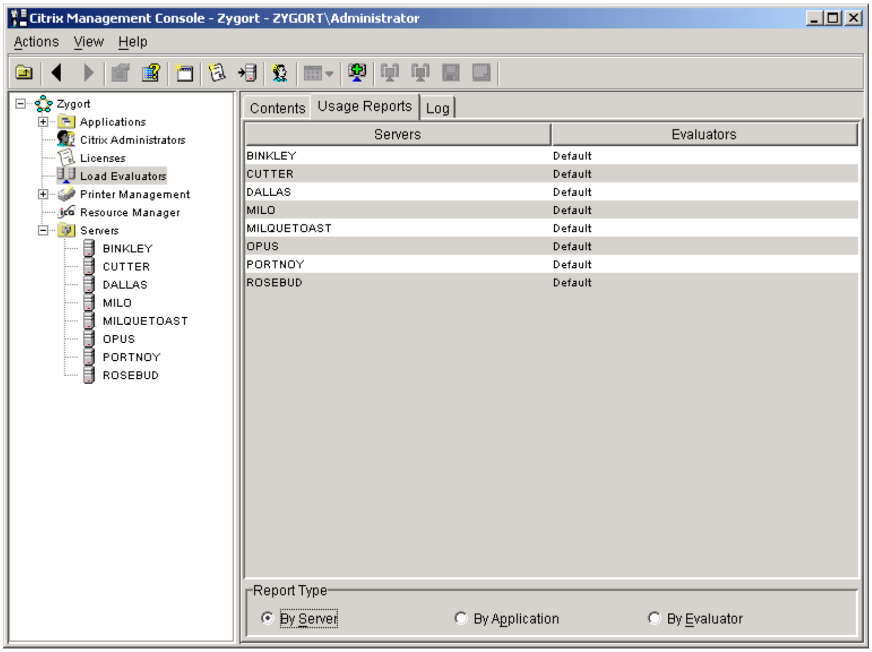
When the CPU utilization is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the CPU utilization exceeds the high threshold, Load Manager reports full load.

## Usage Reports Tab

The second tab, *Usage Reports*, displays the evaluators that are assigned to servers and published applications, as shown in Figure 7.19. From here, you can quickly view all of the evaluators and where they are attached. Three radio buttons at the bottom of this tab control which view is displayed: the servers and the evaluators assigned to them, the published applications and the evaluators assigned to each application, or a list of evaluators and all of the servers and applications to which the evaluator is attached.

**FIGURE 7.19** Usage Reports tab



| Servers | Evaluators |
|---|---|
| BINKLEY | Default |
| CUTTER | Default |
| DALLAS | Default |
| MILO | Default |
| MILQUETOAST | Default |
| OPUS | Default |
| PORTNOY | Default |
| ROSEBUD | Default |

Report Type

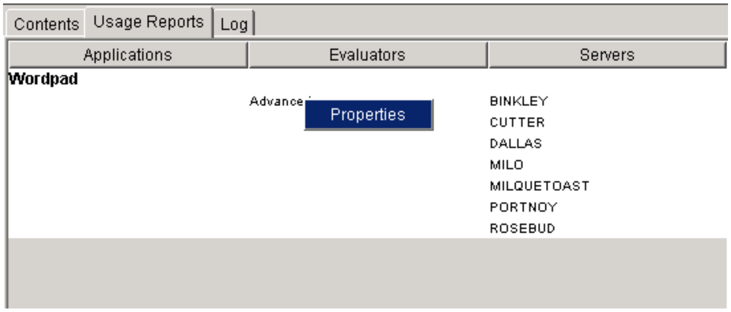
● By Server ○ By Application ○ By Evaluator

Select the By Server option to see every server in the server farm and its associated evaluator. With this view, you can quickly examine the different associations and compare the server's evaluators. You can also control the associations from here. If you right-click a server, the menu that appears has only one option available, Load Manage Server. Selecting this option displays the available evaluators. Selecting one and clicking OK associates the new evaluator with the server. Before changing evaluators, you should know the implications of making the change. If other servers in the same zone are using a different evaluator, the rules may not be compatible and load balancing will be effectively ruined.

Of course, the same can be said for the By Application option. Clicking this button displays all of the applications that have evaluators attached to them. You can change the evaluator that is attached to an application by right-clicking the application and selecting Load Manage Application.

From within either of these options, if you right-click the evaluator associated with a server or an application, you will be presented with the Properties menu option, as shown in Figure 7.20. From here, you can modify the rules that make up the evaluator.

**FIGURE 7.20** Right-clicking the evaluator



### Log Tab

The third and final tab is the *Log tab*. When logging is enabled, this tab displays information based on the events that trigger load changes. All of the messages that are generated during a session will be displayed here.

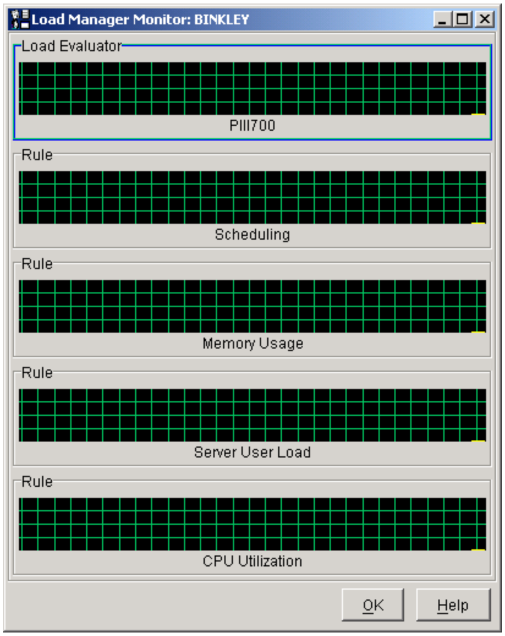
## Load Manager Monitor

If you want to view the current load on a server, you can use the *Load Manager Monitor* view to see a graphical representation of the server's load. Within this monitor, you will see the Load Evaluator graph at the top of the screen, as shown in Figure 7.21. This is the load that is reported to the data collector. Beneath that graph are separate graphs for all of the rules that make up the evaluator. Since each rule has its own individual graph, you can see how each rule is being utilized and how it is affecting the entire load.

This view comes in very handy when you want to see which resources are affecting the load. If a rule is causing a denial of connections, you will see the rule's results in a graphic format and can make decisions on modifying the rule for later use.

The monitor will refresh automatically, but it is not a real-time representation of the load. The default refresh rate is once per minute. Using this one-minute delay takes some of the load off the servers since they need not continually update the data sent to the monitor. If you want to change the update interval, open the Load Manager Settings screen from the Actions menu. If you look back at Figure 7.13, you will see the slider that is used to control the refresh rate. This slider is marked in 10-second intervals from one minute to five minutes.

FIGURE 7.21 Load Manager Monitor screen



Now that we have shown how to control the load on servers by using evaluators, let's move on to actually using the evaluators on servers in our farm. In the next section, we will create and manage evaluators on small servers in a server farm.

# Adjusting the Load

Let's now create a few evaluators and see how the rules work together to fine-tune the balance of sessions across the server farm. In the following examples, we will be using seven MetaFrame XP servers in our server farm, each with single Pentium III 700MHz processor and 512MB of RAM.

If you remember the description for the Default load evaluator, you know that the configuration of these servers does not quite meet those lofty expectations. Instead, we have moderately sized servers handling client sessions. Configuring multiple servers in this fashion may actually prove to be a better solution than trying to support all of your users on one large server. If only one server is used to host the sessions, all of the users go down if the server fails. In the environment we are presenting here, if one server fails, the other servers are still able to support the users connected to them. Only those connected to the failed server lose their sessions. And since load balancing dispersed them equally across the servers, only a minimum number of users are affected by the outage. As a bonus, those users can attempt to start another session and will more than likely be able to connect to one of the remaining servers to continue their processing.

**Real World Scenario**

### Balancing Act

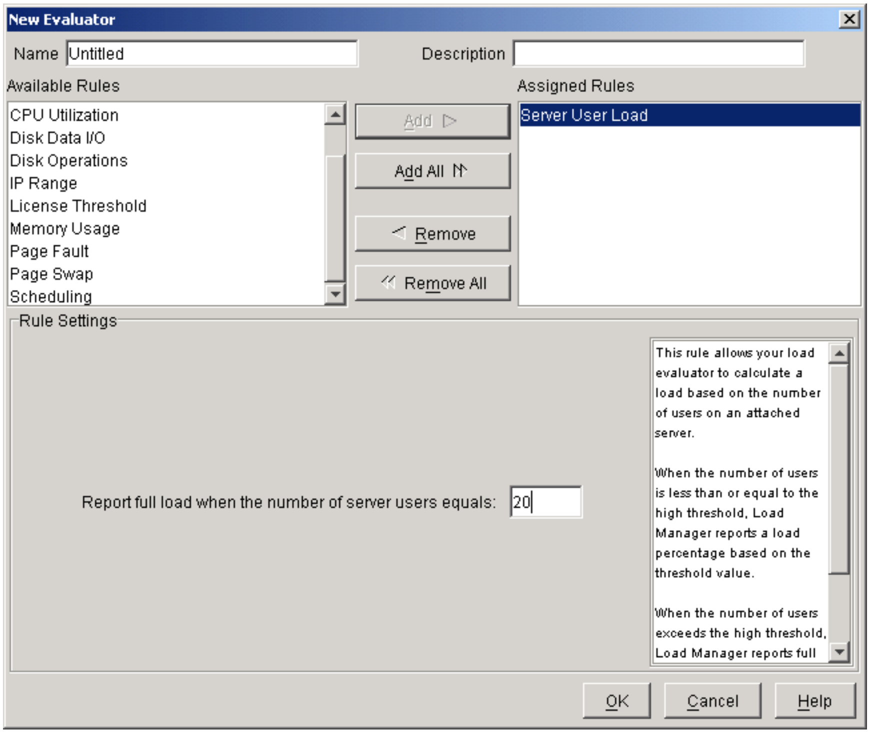
Josh has a Citrix MetaFrame farm, which consists of six MetaFrame XP servers. He purchased all of his servers at the same time and configured all of them identically with Quad 1GHz processors, 512MB of RAM, and three 18GB SCSI hard drives. Since he wanted the servers to be load balanced, he purchased MetaFrame XPa and left the servers configured to use the Default load evaluator.

As the company has grown, Josh has found that the existing servers are reaching capacity. Josh gained approval to purchase another server, and since memory prices had dropped dramatically, he was able to purchase a server that was identical with the exception of 1GB of RAM instead of the 512MB the other servers were configured with.

After adding the server to the farm, Josh noticed that the new server accepted the same number of connections as the other servers. He wanted the new server to be utilized more efficiently since it had more memory and could handle more sessions than the other servers. He decided to create an evaluator that would include the Memory Usage rule. This rule would then report the percentage of memory consumed on the server. As clients requested connections, the new server began to accept more connections than the original servers since the percentage of memory used on the new server increased more slowly than that of the original servers.

We need to create an evaluator that is optimized for the servers we are using. Since all of our servers have identical configurations, we will need to create only one evaluator and assign it to all of the servers. Looking back on the rules listed earlier in this chapter, we need to identify those that will work for our environment. One rule that can be applied in nearly any environment is the Server User Load rule, as shown in Figure 7.22. This rule stops any connections above the number specified in the rule. If we determine that the servers can handle 20 users each, we could enter 20 as the number at which the rule would report a full load to the data collector, prohibiting any further connections. Of course, you could enter a lower number than this if you do not want the server to reach the maximum load, effectively allowing the server to process more efficiently.

**FIGURE 7.22** Adding the Server User Load rule



Name: Untitled

Description:

Available Rules:
CPU Utilization
Disk Data I/O
Disk Operations
IP Range
License Threshold
Memory Usage
Page Fault
Page Swap
Scheduling

Assigned Rules:
Server User Load

Report full load when the number of server users equals: 20

This rule allows your load evaluator to calculate a load based on the number of users on an attached server.

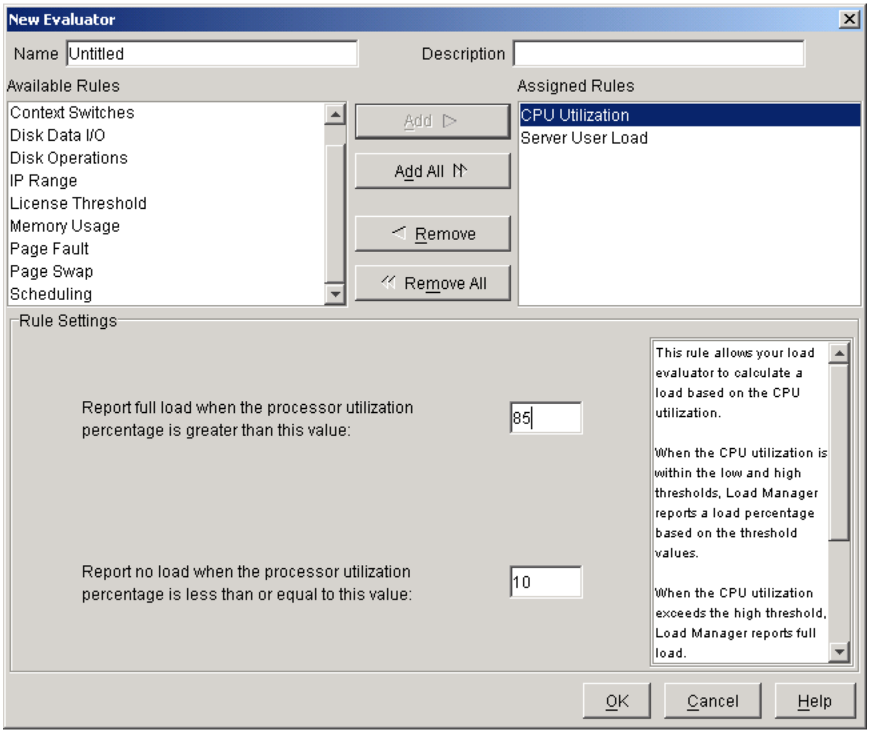
When the number of users is less than or equal to the high threshold, Load Manager reports a load percentage based on the threshold value.

When the number of users exceeds the high threshold, Load Manager reports full

The only problem with the Server User Load rule is that it does not take into account the amount of resource consumption. If users start more applications than originally determined, they could effectively overload the server even though they have not reached the maximum number of users specified in the rule. To take this into consideration, we can add other rules to the evaluator. These additional rules will work in conjunction with the first rule we put in place.

Now we need to decide which additional rules we would like to include and the limits we want to place on them. One rule to consider is the CPU Utilization rule, shown in Figure 7.23. With this rule, we can specify the percentage of the CPU that is consumed on the server. If you do not want additional users to connect when the processor reaches 85 percent utilization, you can indicate that amount in the full-load entry. Now with the two rules we have put in our evaluator, the maximum number of users that the server will allow is 20 as long as the processor has not reached more than 85 percent utilization.

**FIGURE 7.23** Adding the CPU Utilization rule



New Evaluator

Name: Untitled

Description:

Available Rules:
- Context Switches
- Disk Data I/O
- Disk Operations
- IP Range
- License Threshold
- Memory Usage
- Page Fault
- Page Swap
- Scheduling

Assigned Rules:
- CPU Utilization
- Server User Load

Rule Settings

Report full load when the processor utilization percentage is greater than this value: 85

Report no load when the processor utilization percentage is less than or equal to this value: 10

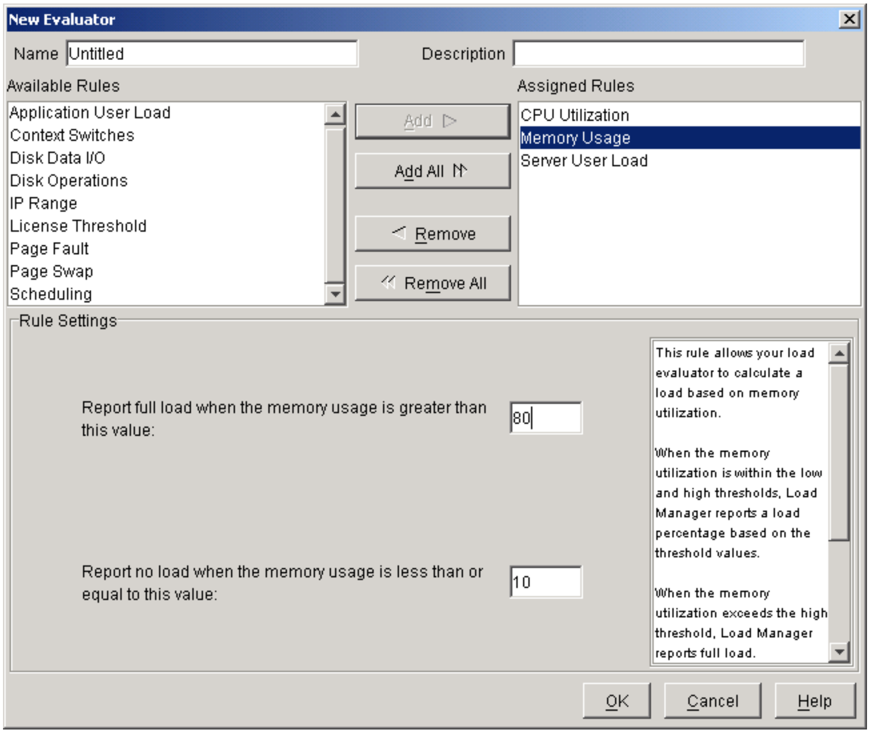
This rule allows your load evaluator to calculate a load based on the CPU utilization.

When the CPU utilization is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the CPU utilization exceeds the high threshold, Load Manager reports full load.

One other resource that is vitally important on a MetaFrame XP server is memory. While the processor works diligently to process all of the data from the sessions, memory is needed for every session that is started on the server. The more applications that are started, the more memory is consumed. When adding the Memory Usage rule shown in Figure 7.24, you can specify the maximum percentage of memory that Load Manager will allow to be used before denying connections.

**FIGURE 7.24** Adding the Memory Usage rule



New Evaluator

Name: Untitled

Description:

Available Rules:
- Application User Load
- Context Switches
- Disk Data I/O
- Disk Operations
- IP Range
- License Threshold
- Page Fault
- Page Swap
- Scheduling

Assigned Rules:
- CPU Utilization
- Memory Usage
- Server User Load

Rule Settings

Report full load when the memory usage is greater than this value: 80

Report no load when the memory usage is less than or equal to this value: 10

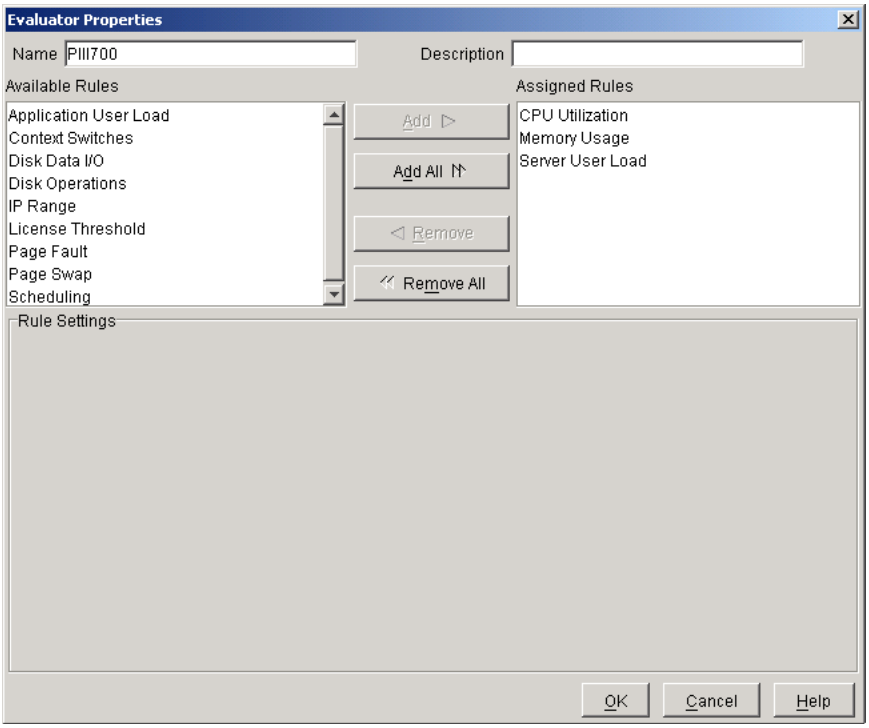
This rule allows your load evaluator to calculate a load based on memory utilization.

When the memory utilization is within the low and high thresholds, Load Manager reports a load percentage based on the threshold values.

When the memory utilization exceeds the high threshold, Load Manager reports full load.

All of these rules control the connections to the server. As connections are made to the server and resources are consumed, the rules are used to determine the load on the server—the rule with the highest load is the rule that determines the load information sent to the data collector. Since we have added the rules to our evaluator, let's save the evaluator so that it is ready to be assigned to our servers. Figure 7.25 shows the name PIII700 used to identify the evaluator. Click OK to save the evaluator.

**FIGURE 7.25** Naming the evaluator



Evaluator Properties

Name: PIII700

Description:

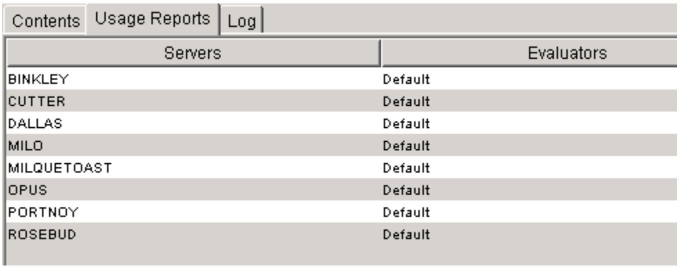
Available Rules:
- Application User Load
- Context Switches
- Disk Data I/O
- Disk Operations
- IP Range
- License Threshold
- Page Fault
- Page Swap
- Scheduling

Assigned Rules:
- CPU Utilization
- Memory Usage
- Server User Load

Rule Settings

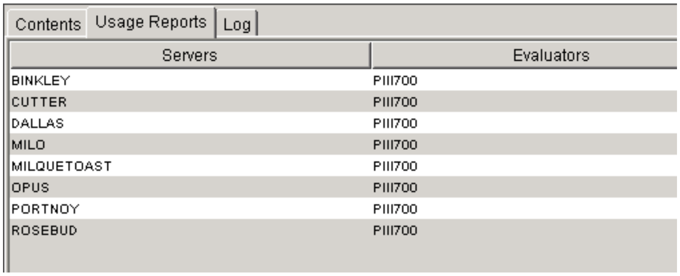
Figure 7.26 shows the Usage Reports tab, which displays the servers and their associated evaluators. To assign the newly created evaluator to the servers, right-click the server and choose Load Manage Server. From the dialog box that appears, choose the evaluator you want to assign to the server. For our scenario, we will choose the PIII700 evaluator and click OK. Once you have performed this action on all servers where you need to apply the evaluator, the Usage Reports tab should look like Figure 7.27.

**FIGURE 7.26** Before assigning evaluators to servers



| Servers | Evaluators |
|---|---|
| BINKLEY | Default |
| CUTTER | Default |
| DALLAS | Default |
| MILO | Default |
| MILQUETOAST | Default |
| OPUS | Default |
| PORTNOY | Default |
| ROSEBUD | Default |

**FIGURE 7.27** After assigning evaluators to servers

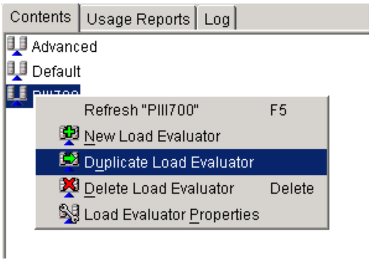


| Servers | Evaluators |
|---|---|
| BINKLEY | PIII700 |
| CUTTER | PIII700 |
| DALLAS | PIII700 |
| MILO | PIII700 |
| MILQUETOAST | PIII700 |
| OPUS | PIII700 |
| PORTNOY | PIII700 |
| ROSEBUD | PIII700 |

So what happens when you want to control which clients are allowed to access a server? Take, for example, the scenario where you have decided to make three servers available for one group of clients while the other four are available to another group of clients. Using the evaluator we created previously, Load Manager would send the clients to any of the seven servers, which we do not want. However, the rules that we have already added are sufficient to control the client connections to the servers.

In order to create evaluators that will work for us, we will first make duplicates of our PIII700 evaluator, one for each of the server groups. Right-click the PIII700 evaluator and select the Duplicate Load Evaluator option, as shown in Figure 7.28. Enter a new name for the evaluator; for our example, we will use **Group 1**. Perform this process again and name the next one **Group 2**.

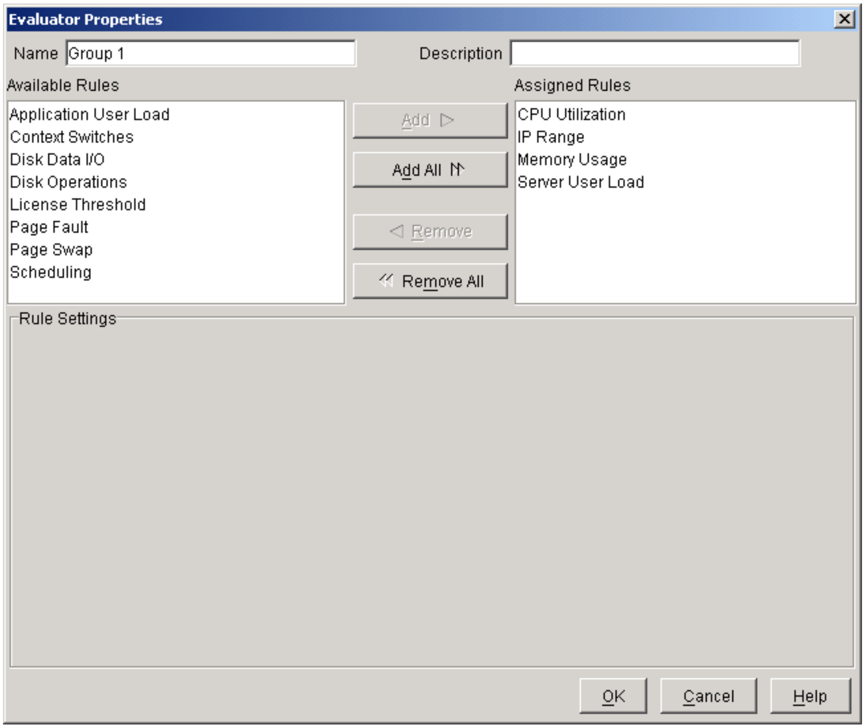
**FIGURE 7.28** Duplicating an evaluator



Look back at the descriptions of the rules that are available to add, and you will notice the IP Range rule, shown previously in Figure 7.6. This rule controls the connections to the servers based on the IP address of the client attempting to make a connection. Of course, you will have to have the IP addresses of the clients mapped out well so that this scheme will work correctly, but this is a very efficient way to control the clients. Clicking Add

Range allows you to add in the IP address range of the clients you want to control. The radio buttons directly above the List Of IP Ranges section control whether the addresses that are added to the rule are allowed or denied connections. Figure 7.29 shows that we have added the IP Range rule to the evaluator.

**FIGURE 7.29** The IP Range rule added to an evaluator



Evaluator Properties

Name: Group 1

Description:

Available Rules:
- Application User Load
- Context Switches
- Disk Data I/O
- Disk Operations
- License Threshold
- Page Fault
- Page Swap
- Scheduling

Assigned Rules:
- CPU Utilization
- IP Range
- Memory Usage
- Server User Load

The other rules that are available can help you further fine-tune your environment. For example, if you want to load-balance your servers during only a specific time of the day, you could use the Scheduling rule. Or if you want to limit the number of licenses used from the pool by a server, you could use the License Threshold rule. Make sure you understand the rules and the consequences of using them, especially when combining them in an evaluator. Fine-tuning the evaluators and controlling the access to your servers enables you to give your users the best experience using terminal services.

From load balancing, we move on to the topic of security. Very few organizations have the luxury of not needing any type of security. MetaFrame XP provides its own security features on top of Windows 2000 Server's built-in security. So let's move on to Chapter 8, "Security."

# Summary

Load balancing is one of those services that makes Citrix shine. This feature, which is available in MetaFrame XPa and XPe, distributes users' sessions across the servers so that no one server is overloaded while others sit relatively idle.

To configure load balancing, you assign load evaluators to servers and published applications. These load evaluators are made up of rules that monitor certain aspects of the server and control the connections made to the server. Load balancing can be very beneficial to an organization since the resources are utilized more efficiently.

# Exam Essentials

**Understand what load balancing provides.** Load balancing allows MetaFrame servers to manage the client connections so that no server bears the brunt of the session loads.

**Know the requirements for implementing load balancing.** Only the XPa and XPe versions of MetaFrame XP have load balancing available.

**Know the components that monitor the load.** Load evaluators, which consist of rules, are assigned to computers. Data collectors control where the clients are directed when they attempt to start a session.

**Know the two built-in evaluators.** When load management is activated, the two evaluators that are included are Advanced and Default.

**Understand the types of rules.** Rules are either Boolean, Incremental, Moving Average, or Moving Average Compared To High Value.

**Know what causes the evaluators to report a load change.** There are triggers that force the evaluator to report a load change to a data collector. They are User Logon/Logoff, Session Connect/Disconnect, Specified Time Interval (every five minutes by default), and a load variance greater than 5 percent over a 30-second period.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

advanced evaluator

Application User Load

Boolean

Contents

Context Switches

CPU Utilization

default evaluator

Disk Data I/O

Disk Operations

Incremental

IP Range

License Threshold

load balancing

load evaluator

Load Evaluators node

Load Manager Monitor

Log tab

Lower Threshold

Memory Usage

Moving Average

Moving Average Compared To High Value

Page Fault

Page Swap

rules

Scheduling

Server User Load

triggers

Upper Threshold

Usage Reports

User Connect/Disconnect

User Logon/Logoff

# Exercise

Now we are going to experiment with some of the load-balancing settings that we discussed throughout this chapter. We will start with creating our own load evaluator, assign it to a server, and then view the effect of sessions running on the server by opening Load Manager Monitor.

**EXERCISE 7.1**

### Load Manager Configuration

In this exercise, we will work with the Load Manager interface to create a load evaluator, assign it to our server, and then view the load using Load Manager Monitor.

First, let's add a load evaluator:

1. Start the Citrix Management Console.
2. Log on as a Citrix Administrator.
3. Expand the Server Farm node.
4. Right-click Load Evaluators, and select New Load Evaluator from the context menu.
5. When the New Evaluator window appears, type **Test** in the Name field.
6. In the Description field, type **Test Evaluator**.
7. In the Available Rules section, select CPU Utilization and click Add. CPU Utilization now shows up in the Assigned Rules window.
8. Under Rule Settings, change the value listed in the Report Full Load When The Processor Utilization Percentage Is Greater Than This Value field to 75.
9. Click OK.

Next, we need to assign the new load evaluator to a server:

1. In the Citrix Management Console, expand the Servers node.
2. Right-click the server where you want to assign the new evaluator and select Load Manage Server. The Load Manage Server window now appears.
3. Select Test from the list of Available Load Evaluators. Notice that the Description and Rules Used By Evaluator windows now contain the information you provided in the last lab.
4. Click OK.

**EXERCISE 7.1 *(continued)***

Finally, let's view the settings for the load evaluator:

1. In Citrix Management Console, select the server if it is not already selected.
2. Click the Load Manager Monitor tab.
3. At the top of the window, you will see the evaluator that is in place. On the bottom, you will see each rule that is in place for that load evaluator.

# Review Questions

1. Load balancing may be used with which of the following products? (Choose all that apply.)

   A. MetaFrame XPs

   B. MetaFrame XPa

   C. MetaFrame XPe

   D. MetaFrame XP+

2. If you are running a published application and the server that you are running the application on goes down, what happens to your ICA session?

   A. The session is automatically rerouted to another load-balanced server.

   B. The connection is lost. When you reconnect to the published application running on another server, your session will be in the same place as when you were disconnected.

   C. The connection is lost. When you reconnect to the published application running on another server, you will start a new session, and the disconnected session will be lost.

   D. You will see a pop-up screen telling you to save your work and giving you an option to connect to another server.

3. You have two Citrix MetaFrame XP servers on your network. One is running the IPX protocol, and the users that connect to that server are using the IPX protocol only. The other server is running TCP/IP, and the users that are connecting to that server are running TCP/IP only. Which of the following steps must you do in order to implement load balancing? (Choose all that apply.)

A. Install TCP/IP on the workstations that are running IPX only. Now you can connect to each server, whether it is the server running IPX or the server running TCP/IP.

B. Install TCP/IP on the server that is running IPX. The workstations do not need to be configured. The servers that are running IPX will be able to connect to either server.

C. Install TCP/IP on the server that is running IPX. Install TCP/IP on the workstations that are running IPX only.

D. Install IPX on the server that is running TCP/IP. Install IPX on the workstations that are running TCP/IP only.

4. What utility would you use to monitor the application loads across the Citrix farm?

A. Load Balancing Manager

B. Citrix Load Balancing

C. Citrix Management Console

D. Citrix Load Management

5. What are the two preconfigured load evaluators that come with MetaFrame XPa and XPe? (Choose all that apply.)

A. Default

B. Standard

C. Advanced

D. Dynamic

6. The Default load evaluator will report a full load when how many users sessions are on the server?

A. 50

B. 75

C. 100

D. 500

7. The Default load evaluator is programmed to work best on which type of server?

   A. A four-way server with 2–4GB of RAM and two RAID controllers

   B. A single CPU, Pentium 400MHz with 192MB of RAM, and a SCSI Ultra Wide controller

   C. A dual processor, Pentium-class server with 256MB of RAM, and a SCSI Ultra Wide controller

   D. A four-way server with 1GB of RAM and one RAID controller

8. The Advanced load evaluator is programmed to work best on which type of server?

   A. A four-way server with 2–4GB of RAM and two RAID controllers

   B. A single-CPU, Pentium 400MHz with 192MB of RAM and a SCSI Ultra Wide controller

   C. A dual-processor, Pentium-class server with 256MB of RAM and a SCSI Ultra Wide controller

   D. A four-way server with 1GB of RAM and one RAID controller

9. Using the Advanced load evaluator, when will the server report that a server has a full load? (Choose all that apply.)

   A. When CPU utilization is greater than 90 percent

   B. When memory usage is greater than 85 percent

   C. When the number of page swaps per second is greater than 90

   D. When the number of page swaps per second is greater than 100

10. Which load evaluator is assigned to a published application by default?

   A. Default.

   B. Advanced.

   C. Dynamic; Load Manager will determine what kind of server you are running and will automatically assign the load evaluator that will work best with your system.

   D. None.

**11.** You have a server farm with five load-balanced servers. All five servers are identical in hardware setup. You now add another server to the farm that has 1GB more RAM than the other servers. You want to change the load evaluators so that the load will be more evenly distributed among the servers. Which of the following rules should you take into consideration? (Choose all that apply.)

**A.** Memory Usage

**B.** Context Switches

**C.** Disk Data I/O

**D.** Page Swap

**12.** You want to change the Default load evaluator so the server will report a full load when the user number reaches 75. When you load the Default evaluator and try to change the numbers, they are grayed out. Why are the settings grayed out?

**A.** You are not logged on as a Citrix Administrator.

**B.** The load evaluator is not assigned to a published application.

**C.** The Default load evaluator cannot be changed.

**D.** Another load evaluator is currently in place on that server.

**13.** You have four MetaFrame XP servers and two MetaFrame 1.8 servers. You create load evaluators and assign them to all the servers. You notice that the load is not distributed evenly across the servers. What could be the problem?

**A.** Load evaluators created in the Citrix Management Console do not recognize MetaFrame 1.8 servers.

**B.** The farm is not running in interoperability mode.

**C.** The master browser is not one of the MetaFrame XP servers.

**D.** The IMA subsystem is not installed on the MetaFrame 1.8 servers.

**14.** Where is the load information stored?

**A.** On each server that hosts the published application

**B.** On the ICA browser

**C.** On the data collector

**D.** On the master zone collector

**15.** You have created a load evaluator that will report a full load when user sessions reach 75. All of your load-balanced servers are reporting 75 users. What will happen when the next user launches a published application?

**A.** The request will be denied.

**B.** The user will be directed to one of the load-balanced servers, using one of the five grace connections.

**C.** The user will receive a message asking if they would like to use one of the grace connections.

**D.** The data collector will accept the connection.

**16.** You have created a load evaluator and defined multiple rules for that evaluator. Which of the following statements is true about the interaction of the rules?

**A.** The rules will conflict. The rule that was created first will take precedence.

**B.** The rules will automatically work together to determine the overall server or published application load in the server farm.

**C.** The rules will conflict, but you can set values to the rules to determine which one has precedence.

**D.** The rules will work together. You can set values to the rules to determine the priority order in which to apply the rules.

17. Which rules are used by the Advanced load evaluator? (Choose all that apply.)

    A. CPU Utilization

    B. Memory Usage

    C. Page Fault

    D. Page Swap

18. Which of the following rule types have a value range encompassing the values 0–2,147,483,647?

    A. Moving Average

    B. Moving Average Compared To High Value

    C. Incremental

    D. Boolean

19. Which of the following is an example of a Boolean rule?

    A. CPU Utilization

    B. Server User Load

    C. Context Switches

    D. Scheduling

20. You have a network that is made up of three subnets, and you want to control access to your servers. Clients should only be able to connect to MetaFrame XP servers in their own subnet. Which of the following rules would allow you to control the connections in this manner?

    A. Context Switches

    B. IP Range

    C. License Threshold

    D. Scheduling

# Answers to Review Questions

1. B, C. Load balancing requires either a MetaFrame XPa or XPe license to be installed and activated before you can utilize this feature.

2. C. Load balancing is not fault-tolerant. If the server on which you are running an ICA session goes down, the session is lost. When you reconnect to the published application, it will start a new session and the previous session will be lost.

3. C, D. Load balancing requires that the same protocol be running on each MetaFrame server, whether it be TCP/IP or IPX. The workstations will also need to be configured to use the protocol you select.

4. C. Using Citrix Management Console, you can monitor loads on servers that contain published applications.

5. A, C. MetaFrame XPa and XPe come with two preconfigured load evaluators called Default and Advanced.

6. C. The Default load evaluator is based on the Server User Load rule. This rule reports a full load when the number of user sessions on the server exceeds 100. After 100 sessions, additional user sessions are not allowed on the server.

7. A. The Default load evaluator is programmed to work best on a four-way server with 2–4GB of RAM and two RAID controllers. If a server does not meet this configuration, you can create another load evaluator that specifies a smaller number of user sessions.

8. B. The Advanced load evaluator is configured to function best on a single-CPU, Pentium 400MHz system with 192MB of RAM and a SCSI Ultra Wide controller.

9. A, D. CPU utilization, memory usage, and page swap are all resources used with the Advanced load evaluator. CPU utilization is considered full when 90 percent load has been reached. Memory usage reports a full load when the memory usage is greater than 90 percent. Page swap reports a full load when the number of page swaps per second is greater than 100.

10. D. By default, no load evaluator is attached to a published application.

**11.** A, D. The Memory Usage rule calculates a load based on memory utilization. The Page Swap rule allows the load evaluator to calculate a load based on the number of page swaps per second. A page swap occurs every time the operating system swaps physical memory to virtual memory on disk. A system with less RAM will exhibit more page swaps than one with more RAM.

**12.** C. The Default load evaluator is assigned to all load-balanced servers by default, and the rules that are included cannot be changed.

**13.** A. Because the architecture of the two products is different (browser versus IMA), MetaFrame XP reverts to using Load Balancing Services 1.0 to manage loads. Load evaluators created in the CMC do not recognize MetaFrame 1.8 servers.

**14.** C. Each server calculates its load and sends values for all possible load evaluation criteria to the data collector for the zone. When a user launches a load-balanced published application, the data collector is queried, and the session then goes to the server with the lightest load.

**15.** A. If all servers hosting the published application are at their maximum load, as specified by their local evaluator rules, the request is denied.

**16.** B. When several rules exist in a single load evaluator, the rules work together to determine the overall server or published application load in the server farm.

**17.** A, B, D. The Advanced load evaluator is based on the following rules:

CPU Utilization, which reports a full load when processor utilization is greater than 90 percent and no load when the processor utilization is less than 10 percent.

Memory Usage, which reports a full load when memory usage is greater than 90 percent and no load when memory usage is less than 10 percent.

Page Swap, which reports a full load when the number of page swaps per second is greater than 100 and no load when the number of page swaps per second is equal to 0.

**18.** B. Moving Average Compared To High Value uses a percentage based on the values specified in the high and low threshold values. The values that can be used with this rule type fall in the range 0–2,147,483,647. A rule that is an example of this type is the Disk Data I/O rule.

**19.** D. Boolean rules either allow or disallow a connection based on whether the value entered in the rule is evaluated as True or False. These rules do not actually afford any type of load balancing but are used to explicitly allow or deny a connection.

**20.** B. The IP Range rule allows the load evaluator to enable or disable access to a published application based upon whether or not the IP addresses of the ICA Clients are within the specified IP address ranges.

Chapter

8

# Security

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **6. Load Management and Security**

- 6b. Identify Encryption Strengths and Performance

Probably no other subject raises so much discussion as the topic of *security*. And for good reason—the data held by a company is as vital as any product or service they are trying to market. From personnel records to secret ingredients to the data on a website, companies rely on accurate information and the ability to keep that information safe. If a user's account and password are compromised, the data the user has access to is no longer safe. If communication between a client computer and a server is intercepted, company secrets may be discovered.

While we could go into a long dissertation on securing resources, protecting passwords, and auditing access to the resources in an organization, those topics are covered in greater depth in other study guides. In this chapter, we are going to concentrate on securing the communication channels between the MetaFrame XP server and the ICA Clients, the encryption levels available, how and when to implement the SSL Relay Configuration tool, and how to allow clients to communicate through firewalls. So let's start with a discussion of client/server communication security.

## Client/Server Communication Encryption

The information that travels between MetaFrame XP servers and the client devices accessing sessions consists primarily of keystroke data, mouse movements, mouse clicks, and screen refreshes. Since the processing of the session is performed at the server, we do not have to worry about important files crossing the network between the server and the client. This does not mean that the data traveling between the two machines should be freely shared. Password information is transmitted to the servers, and the screen update information could theoretically be trapped and redisplayed on another user's terminal.

To limit the possibility of another individual gaining access to the data transmitted between the server and clients, Citrix has included software that encrypts the data. This encryption scheme was introduced with MetaFrame 1.*x* as a product called *Secure ICA*. With MetaFrame XP, this functionality is built into the client and all of the server products. Let's examine how this works to keep our data safe.

## How Encryption Works

The communication between our clients and servers needs to be secure from those miscreants who would intercept or damage the data transferred. This must be done in the most efficient manner possible. Our clients and servers have a finite amount of processing power available to them, so we need to balance the encryption level with the hit we take on resources. If the *encryption* and *decryption* of data consume too many resources, the sessions will appear slow to the clients and the overall experience using terminal services will be disappointing.

There are two encryption technologies that are used with MetaFrame XP: symmetric and asymmetric encryption. *Symmetric encryption* uses the same key for encryption and decryption. The main advantage of this encryption scheme is fast, efficient processing. The sender encrypts the data using the key, and the recipient uses the same key to decrypt the data once it is received. There is a definite drawback to this scheme, however. If anyone intercepts the key as it is shared between the two systems or the key is somehow compromised, all of the communication between the two is unsafe.

*Asymmetric encryption* uses different *keys* at the sender and receiver. Better known as *public key encryption*, the sender holds a *private key* that is not shared with any other entity, and the receiver has the *public key* that can be delivered to any of the intended recipients. The public key is then used to encrypt the information sent to the holder of the private key. Due to the mathematical algorithm used to generate the keys, only the private key can decrypt messages encrypted with the public key. To secure communications in both directions, each system needs to have the other system's public key. The largest drawback to this encryption scheme is the load it places on the resources of the systems communicating with one another.

MetaFrame XP takes advantage of both of these encryption schemes to make the communication not only secure, but also efficient. As a client requests a session on a MetaFrame XP server, both the client and the server generate a private/public key pair. The private keys are held on the client/server that generated the key, and the public key is passed to the partner system. Using the information contained in the public and private keys, the two systems generate a session key that is used for the remainder of the session to encrypt communication. This key is a symmetric key that will cause little performance degradation during the session. This dynamic generation of the secret key used between the two sessions safeguards the key since the key is never transmitted over the network.

NOTE To generate the secret key on each system, MetaFrame XP uses the *Diffie-Hellman key agreement algorithm*. Once the key is generated, it is used in conjunction with the *RSA RC5 algorithm* to encrypt the data. For more information concerning either of the algorithms and how they work, go to `www.rsa.com`.

# Encryption Levels

Depending upon the settings specified on the connection and at the client, different levels of encryption strength are available with MetaFrame XP. Choosing the appropriate encryption strength depends on certain factors. First, you must take the sensitivity of the data into account. The more bits used in the encryption algorithm, the harder it is for someone to decrypt the data. Second, the location of the client or the server dictates the strength of encryption allowed. All levels of encryption are allowed in the United States, but other countries may have export laws and restrictions governing cryptography. Finally, the server's processing power and available resources may dictate what level you can apply. The higher the encryption strength, the more processing power is required to encrypt and decrypt the data.

The following encryption strengths are available with MetaFrame XP:

**None** This disables any encryption across the connection.

**Basic** The default level of encryption using Base64 encoding is *Basic*.

**RC5 (128 bit) logon only** *RC5 (128 bit) logon only* is used to protect the authentication data, but the session data is encrypted as *Basic*.

**RC5 (40 bit)** *RC5 (40 bit)* uses RC5 secret key generation with a 40-bit encryption. It is available for domestic use and for export to all countries.

**RC5 (56 bit)** *RC5 (56 bit)* uses RC5 secret key generation with a 56-bit encryption. It is available for domestic use and for export to most countries, but you should check the export laws before implementing this level outside the United States.

**RC5 (128 bit)** *RC5 (128 bit)* uses RC5 secret key generation with a 128-bit encryption. It is available for domestic use and for export to some countries, but you should check the export laws before implementing this level outside the United States.

Now let's see how to configure connections and published applications to take advantage of these encryption levels.

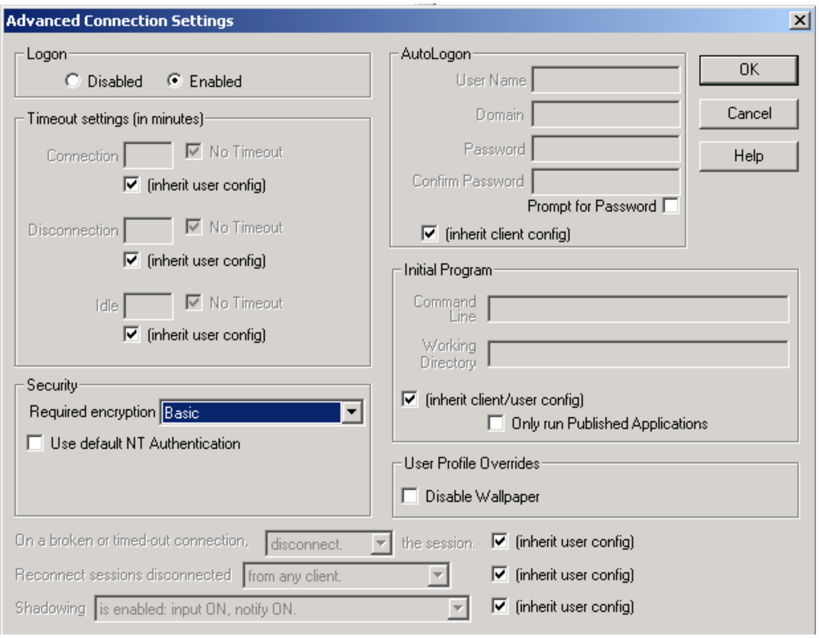
## Configuring the Encryption Level for the Connection

To ensure that all of the sessions communicating on a connection are using encryption, you can configure the connection to require a specified level of encryption. This has a two-fold advantage: Only clients that are using the encryption strength required by the connection can start a session, and all sessions using the connection are encrypted. You should configure encryption at the connection level when you have a special application that processes only from that server or when you want to secure all transactions on the server. Remember, however, that all clients requesting sessions from the server are required to use the level of encryption you have specified.

To set the encryption level for the connection, open Citrix Connection Configuration, right-click the connection you wish to configure, and select Edit from the context menu. When the Edit Connection screen appears, click the Advanced button to bring up the Advanced Connection Settings screen shown in Figure 8.1. The Required Encryption field in the Security section of this screen includes a pull-down menu that contains the available encryption levels.

All of the encryption levels presented earlier are available from this pull-down menu. Select the level of security that you deem necessary for the connection. Now let's take a look at setting the encryption level for a published application.

**FIGURE 8.1** The connection encryption options



Advanced Connection Settings

Logon
○ Disabled ● Enabled

Timeout settings (in minutes)
Connection ☑ No Timeout
☑ (inherit user config)
Disconnection ☑ No Timeout
☑ (inherit user config)
Idle ☑ No Timeout
☑ (inherit user config)

Security
Required encryption: Basic
□ Use default NT Authentication

AutoLogon
User Name
Domain
Password
Confirm Password
Prompt for Password □
☑ (inherit client config)

Initial Program
Command Line
Working Directory
☑ (inherit client/user config)
□ Only run Published Applications

User Profile Overrides
□ Disable Wallpaper

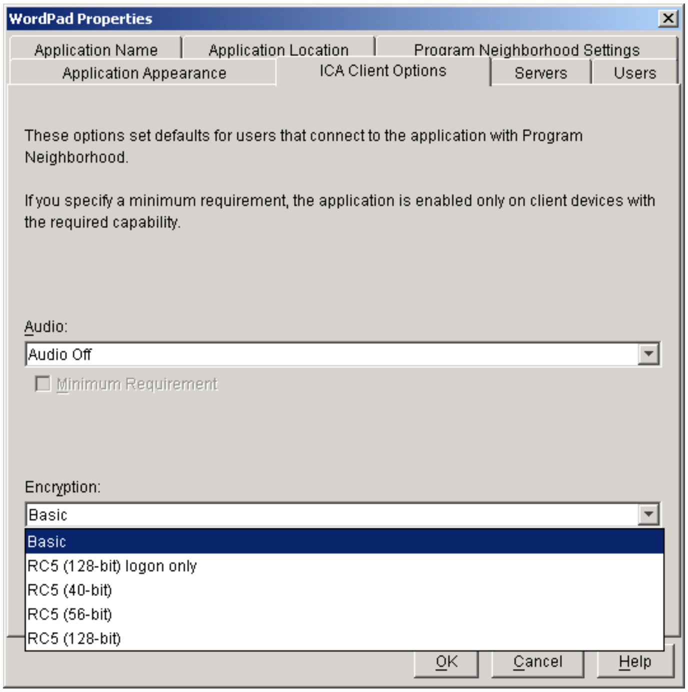
On a broken or timed-out connection, disconnect the session. ☑ (inherit user config)
Reconnect sessions disconnected from any client. ☑ (inherit user config)
Shadowing is enabled: input ON, notify ON. ☑ (inherit user config)

## Configuring the Encryption Level for a Published Application

There may be instances when you will want to enforce an encryption level based on the application the user is accessing instead of on a connection. Connection-based encryption is adequate for securing communication to a certain server, but having the ability to control the encryption when a user starts a published application may actually be more beneficial. Since published applications may be accessed from multiple servers and other applications may not require encryption, this may be the primary method used to implement encryption.

When you publish an application, or after the application has already been published, you have the option of setting the encryption level. Open Citrix Management Console and double-click the Applications node. Right-click the published application, and choose Properties from the context menu. Click the ICA Client Options tab of the Properties page, and you will see the Audio and Encryption options, as shown in Figure 8.2. From the Encryption pull-down menu, you can set the level of encryption you want for the application. This setting will be applied to all instances of this application on the servers in your farm.

**FIGURE 8.2** The published application encryption options



These options set defaults for users that connect to the application with Program Neighborhood.

If you specify a minimum requirement, the application is enabled only on client devices with the required capability.

Audio:

Audio Off

□ Minimum Requirement

Encryption:

Basic

- Basic
- RC5 (128-bit) logon only
- RC5 (40-bit)
- RC5 (56-bit)
- RC5 (128-bit)

Notice that the None option is not available from the Published Application Properties screen. This is to ensure that the application has at least the Basic level of encryption applied. From here, we will move on to the SSL Relay Configuration tool.

# SSL Relay Configuration Tool

*Secure Socket Layer (SSL)* has become an Internet standard for encrypting data transmitted between a client's web browser and a web server. You have probably used SSL in the past when connecting to a website that requests you to enter information about yourself, especially credit card information. When using Internet Explorer, you will see a small lock icon in the lower right-hand side of the browser's status frame.

SSL performs two primary functions: First, it verifies that the web server you are connecting to is truly the server you tried to contact. Second, it allows data to be encrypted between the client and the web server. Both of these functions are performed through the use of certificates that are issued through a *Certificate Authority*, usually a company such as VeriSign or CertiSign. Entities on the Internet request a certificate from one of these authorities that, in turn, authenticate the entity when the website is accessed. Along with the certificate, a public key and a private key are issued to the entity. Once the entity's public key is delivered to the client, any data that is passed to the server is encrypted using the public key.

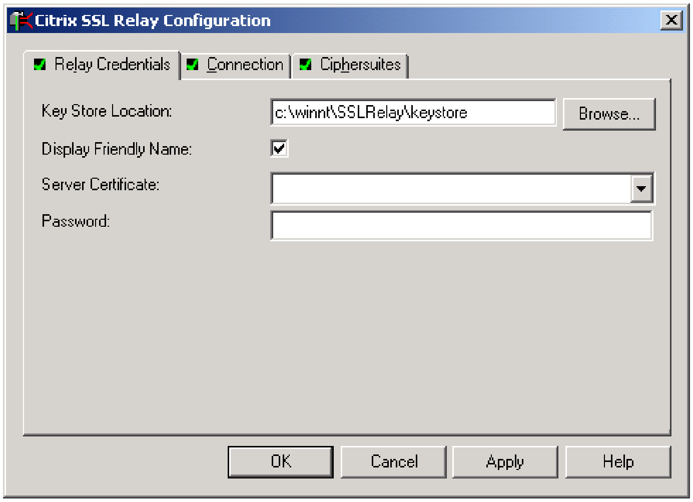
When the server that you are using as your NFuse server is the same server that is running IIS, SSL communication is used directly on the server and there is no need to configure any other options. However, if you are running NFuse on one server and IIS on another, you will need to redirect and translate the SSL data. Citrix has provided a utility that allows the SSL information that is destined for NFuse to be encrypted using SSL, even though the standard communication channel used by NFuse does not support it. This utility is known as the SSL Relay Configuration tool.

When configured, the SSL Relay Configuration tool decrypts the SSL data sent from a client and redirects the data to the MetaFrame XP server.

## The SSL Relay Configuration Tool Tabs

As shown in Figure 8.3, the SSL Relay Configuration tool has three configuration tabs: *Relay Credentials*, *Connection*, and *Ciphersuites*. We'll look at each tab in detail.

FIGURE 8.3 The SSL Relay Configuration tool



Key Store Location: c:\winnt\SSLRelay\keystore

Display Friendly Name: ☑

Server Certificate:

Password:

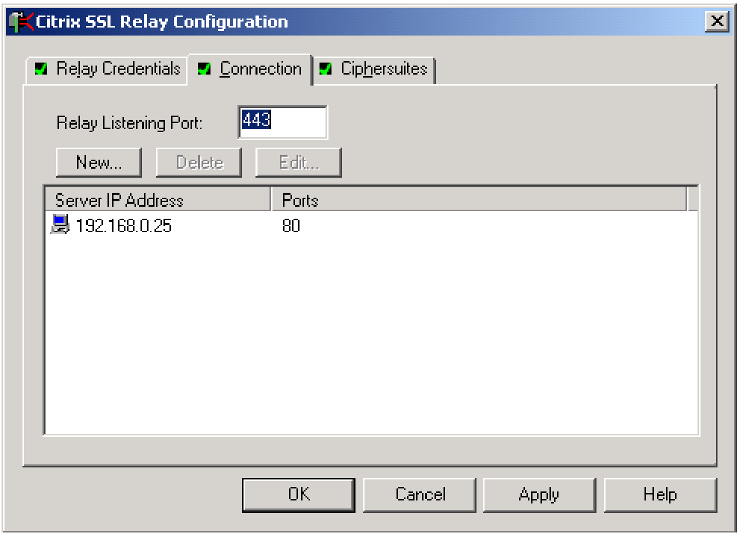
**Relay Credentials** From this tab, shown in Figure 8.3, you can enter the server certificate information. The configurable fields are as follows:

> **Key Store Location** The *Key Store Location* text box specifies the location of the certificate used to validate the identity of the relay to web servers that are NFuse-enabled. The default location of the certificate store is `%systemroot%\SSLRelay\keystore`.
>
> **Display Friendly Name** The *Display Friendly Name* check box toggles the display of the information found in the Server Certificate pull-down menu. If you check this option, the certificate's friendly name is displayed. If the friendly name is not available, the common name is displayed. If this option is not checked, the certificate's subject name is displayed.
>
> **Server Certificate** The *Server Certificate* field displays the server certificates used to identify the relay.
>
> **Password** Use the Password field to enter the password required by the server certificate chosen in the Server Certificate field.

**Connection** When the SSL Relay Configuration tool is enabled, it relays information to the XML service on the same computer running the relay. You may configure the relay service to relay SSL-encrypted data to other servers in your server farm by making changes to the Connection tab shown in Figure 8.4. You can configure the following information on this tab:

> **Relay Listening Port** The *Relay Listening Port* is used for SSL communication. By default, port 443 is used, but you can modify this port if necessary in your environment. Once you change it, all of the devices used in the communication path must have the same port available, including clients, NFuse web servers, and firewalls.
>
> **Server IP Address** The *Server IP Address* field shows the addresses of the servers that will have the data relayed to them after the SSL packets have been decrypted.
>
> **Ports** By default, port 80 is used to send data to the XML service. If you changed the port number during installation of MetaFrame XP (or the port was changed after installation using the `ctxxmlss` command), you will need to enter the appropriate port in the *Ports* field.

**FIGURE 8.4** The Connection tab



Relay Listening Port: 443

| Server IP Address | Ports |
|---|---|
| 192.168.0.25 | 80 |

Modifying the list of servers to relay information to is as easy as clicking one of the buttons on this tab. When you click the New button, the following options are available:

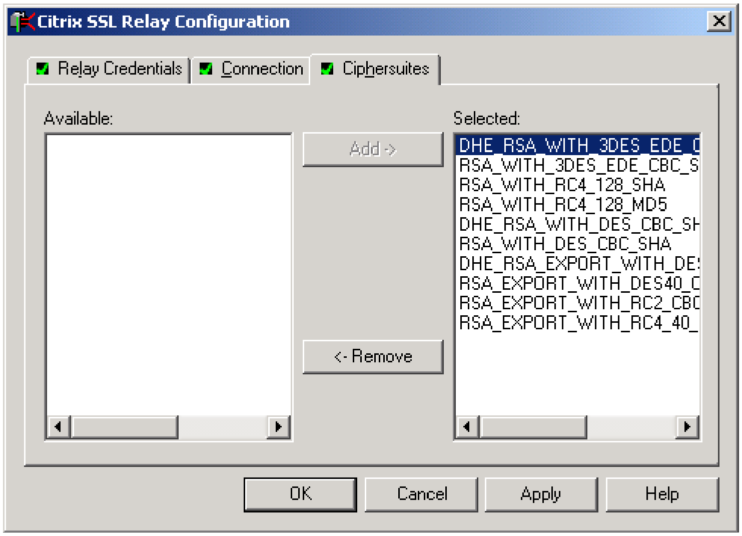
> **Server IP Address** Lists the address of the server to which the SSL-encrypted data is to be sent.
>
> **Destination Port** Indicates the port used on the target server. To determine the port number for the server, check the Registry entry `HKeyLocalMachine\System\CurrentControlSet\Services\CxtHttp\TcpPort`.

**Ciphersuites** Ciphersuites are encryption/decryption algorithms used with SSL communications. Citrix has included 10 of the most popular ciphersuites available today. When SSL communication is initiated, the sender and receiver negotiate the strongest encryption level that both support. This tab contains two windows, Available and Selected, as shown in Figure 8.5.

> **Available** This window displays the ciphersuites that are available for use but are not selected to be used with the relay. When you select a ciphersuite from this list and click the Add button, the ciphersuite moves to the Selected window.

**Selected** This window displays the ciphersuites that the relay may use during an SSL session. When you select a ciphersuite from this window and click Remove, the ciphersuite moves to the Available window and is not used during SSL sessions.

**FIGURE 8.5** The Ciphersuites tab



Selected:

DHE_RSA_WITH_3DES_EDE_C
RSA_WITH_3DES_EDE_CBC_S
RSA_WITH_RC4_128_SHA
RSA_WITH_RC4_128_MD5
DHE_RSA_WITH_DES_CBC_SH
RSA_WITH_DES_CBC_SHA
DHE_RSA_EXPORT_WITH_DE
RSA_EXPORT_WITH_DES40_C
RSA_EXPORT_WITH_RC2_CBC
RSA_EXPORT_WITH_RC4_40_

When configuring ciphersuites for use, you may remove the ciphersuite from the Selected list, but that does not delete the ciphersuite from the system. Also, you cannot add any new ciphersuites to the server.

Now that we have discussed the encryption technologies, let's move on to connection security and how to secure access to our local resources.

# Configuring External Access

Many companies have clients that need to use their MetaFrame servers from outside the organization's network. The organization's chief concern in this area is to prevent unauthorized access to the internal resources of the company. The most popular tools used to block access to these internal resources are *firewalls*, *proxy servers*, and *Network Address Translation (NAT) devices*. All of these tools hide the internal network from outside clients. Only those clients that are configured with the proper settings are allowed past any of these devices to the MetaFrame servers on the internal network. Let's start our discussion with firewalls.

## Firewalls

Firewalls may actually perform all three of the functions we will be discussing in this section, but for this example we will look at the port-blocking features they provide. The ability to block access to TCP/IP addresses and ports allows the administrator to control the access available to outside clients. Typically, port 80 is open on most firewalls to allow access to web servers. If a firewall is in place, certain ports will need to be opened for clients to initiate and run sessions on the MetaFrame XP servers.

The most widely used of the ports when MetaFrame XP is employed on your network is port 1494. This port provides access to MetaFrame XP servers and allows clients to initiate sessions, for either remote desktops or published applications. This port is also used by the clients when they make connections to the servers and published applications that are available in the farm. In addition, port 1494 is used for load-balancing information so that a client knows which server has the lightest load.

Other ports need to be opened for communication between servers when networks are separated with firewalls. Table 8.1 lists the ports that are used by MetaFrame XP servers.

**TABLE 8.1** Ports Used by MetaFrame XP Servers

| Port | Use |
|---|---|
| 80 | Used by ICA clients using TCP/IP+HTTP to communicate with MetaFrame XP servers. This port must be open for inbound traffic. Use the command `ctxxmlss/r`*nn* to change the port the client uses, where *nn* is the port number you would like to use. |
| 139, 1433, 443 | Used by MetaFrame XP to communicate with Oracle or SQL. If Oracle or SQL is used as the data store, these ports must be open for inter-server communication. |
| 443 | Used by Secure Socket Layer (SSL) Relay. SSL Relay is used to secure communications between an NFuse-enabled web server and the MetaFrame XP server farm. |

**TABLE 8.1** Ports Used by MetaFrame XP Servers *(continued)*

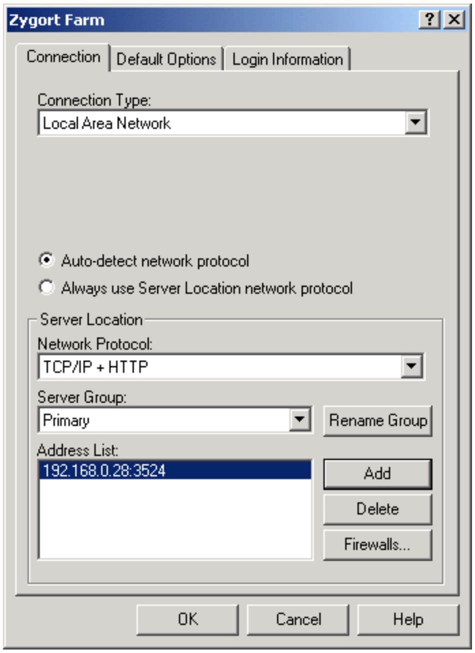
| Port | Use |
|---|---|
| 1494 | Used by clients using TCP to connect and communicate with the MetaFrame XP farm. This port must be open for inbound traffic. Use the command `icaport:`*xxxxx* to change the port number, where *xxxxx* is the number of the new port. |
| 1604 | Used by ICA Clients to communicate with the ICA browser service. Used only if MetaFrame XP is set to mixed mode or if the broadcast options are enabled in the MetaFrame Settings tab of the server in the server farm. Not used if the ICA Client is connecting with the TCP/IP+HTTP protocol. |
| 2512 | Used for server-to-server communication in a MetaFrame XP server farm. You can make data store port number modifications in the Registry of the server that accesses the data store: `HKeyLocalMachine\Software\Citrix\IMA\Runtime\ImaPort`. Servers using an indirect connection to the data store through the server with the direct connection store the port number in their Registry at `HKeyLocalMachine\Software\Citrix\IMA\PsServerPort`. |
| 2513 | Used by the Citrix Management Console to access MetaFrame XP servers in a server farm. This port is not configurable. |

Clients send and receive data from the MetaFrame XP server over TCP/IP port 1494 by default. If you do not want to use this port, or another application already uses this port, you may change the port assignment using the command `ICAPORT /port:`*`xxxxx`*, where *`xxxxx`* is a port number between 0 and 65535. Be careful not to use an already allocated port address when assigning the port number.

If you change the port number using the `ICAPORT` command, that port will have to be opened on the firewall, and the clients will need to know which port to use when trying to access the server. You can accomplish this by one of two methods. When configuring the ICA file for a published application that will be accessed through a web page, the administrator can change the `TcpBrowserAddress=` field to include the IP address of the MetaFrame XP server with the port number appended to it. For example, an entry for a server with the IP address of 192.168.0.28 using port 3524 for ICA sessions would use the entry `TcpBrowserAddress=192.168.0.28:3524`.

The other method is to include the port number in Program Neighborhood when configuring the server address used by the client to communicate with the server, as shown in Figure 8.6. For more information on configuring Program Neighborhood, see Chapter 11, "Program Neighborhood." Next up, we take a look at SOCKS proxy servers.

**FIGURE 8.6** Configuring the server port



Zygort Farm

Connection Type: Local Area Network

● Auto-detect network protocol

○ Always use Server Location network protocol

Server Location

Network Protocol: TCP/IP + HTTP

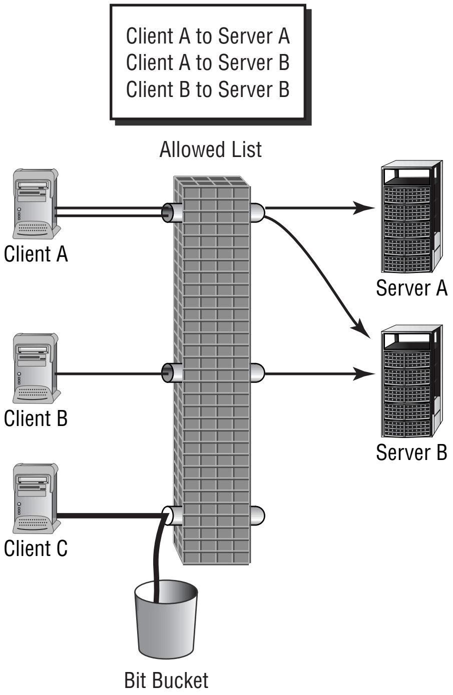
Server Group: Primary

Address List: 192.168.0.28:3524

## SOCKS Proxy Servers

A function most firewalls provide is SOCKS proxy. SOCKS, which stands for *Socket Secure*, forwards requests from external clients to internal resources. One of the main advantages of SOCKS proxy is that you can pick and choose the access allowed to certain servers according to a client's configuration. As a client makes a request for a resource, SOCKS proxy validates the destination address to make sure the requested resource is allowed access from a remote location and checks the identity of the client to make sure the client is allowed access to the resource.

For example, in the graphic that follows, three clients are attempting to access the MetaFrame servers on your network. The firewall protecting your servers from malicious attacks from the Internet has SOCKS proxy capabilities. The SOCKS proxy is configured to pass requests from Client A and Client B only. Client C, since it is not configured for access, is not allowed to access the servers. Furthermore, Client A is allowed to access Server A and Server B, while Client B is allowed to access only Server B.



Since these options need to be configured on a SOCKS proxy server, and all servers use different methods to configure the settings, you must refer to the server's documentation for how to configure the data to pass to the internal network and access the MetaFrame XP server. Now let's move on to Network Address Translation.

## Network Address Translation Servers

While a SOCKS proxy server authenticates users and identifies the clients and resources that are allowed to access the network, Network Address Translation (NAT) servers disguise the internal network by assigning addresses to a server or firewall connected to the Internet and then translate those addresses to another address on the internal network. While most NAT servers are intended to hide internal resources and allow internal clients to access external resources, most NAT servers and firewalls also allow you to configure filters that permit requests from outside the network to be forwarded to internal resources.

Once a NAT server is in place, the administrator can make a special mapping to associate an external public IP address with the IP address of an internal server, whether it is a web server or MetaFrame XP server. Clients that use the external IP address are forwarded to the internal resource. A problem arises when you use a NAT server in this manner to access MetaFrame XP servers. The servers return an address to the client, either their own internal IP address or the internal address of the zone's data collector. When the client attempts to access a server by using the internal address, the NAT server discards the request because it is configured to communicate using only the external addresses. The client does not gain access to the server and is unable to initiate a session.

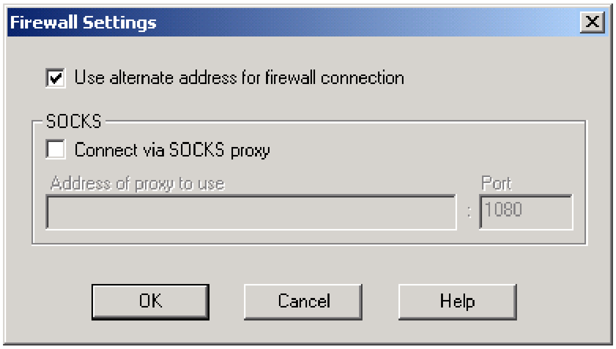
To alleviate this problem, the external address configured on the NAT server is identified on the MetaFrame XP server as an *alternate address*. When a client uses this alternate address, the NAT server can translate the request and pass it to the correct MetaFrame XP server, allowing the client to start a session. To ensure that the MetaFrame XP server identifies itself to clients correctly, you must assign the alternate address to the server using the *`ALTADDR`* command. The `ALTADDR` command allows the MetaFrame XP server to communicate with external clients using an IP address that the NAT server understands. The NAT server performs the translation needed to send the packets to the internal network where the MetaFrame XP server resides.

The syntax for the `ALTADDR` command is very simple: `ALTADDR /set` *`external_address`* configures a server with an alternate address, and `ALTADDR /delete` removes the entry. For example, if the MetaFrame XP server is configured with an internal address of 192.168.1.106 and the NAT server has a mapping associated with this server of 207.168.25.149, from a command line on the MetaFrame XP server you would enter **`ALTADDR /set 207.168.25.149`**. When the NAT server receives a request from an external client wanting to send a packet to 207.168.25.149, the NAT server accepts the request, translates the packets, and sends them to the server on IP address 192.168.1.106.

While this works well for a connection to a server when the client has requested the alternate address, if you attempt to start a published application session, the server will direct you to a data collector. When it does so, the server sends the client the internal address of the data collector. Unfortunately, as we already discussed, the client will be unable to resolve the data collector's address since the firewall will discard the packets or the packets will never make it to the firewall in the first place.

In order for clients to receive the alternate address of the data collector, the client must request that the MetaFrame servers return the alternate address of the data collector. You can accomplish this by configuring options at the MetaFrame server or the client. If the client needs to request the external address, you must configure Program Neighborhood to request the alternate address by editing the Firewalls entries. Right-click the icon of either the entire application set or a server connection and choose Properties. From the Connection tab, click the Firewalls button, and select the Use Alternate Address For Firewall Connection check box, as shown in Figure 8.7. When this option is selected, the MetaFrame servers will return the external address to the client, and the client can communicate with the data collector.

**FIGURE 8.7** Configuring the client to request an alternate address



☑ Use alternate address for firewall connection

SOCKS

☐ Connect via SOCKS proxy

Address of proxy to use:

Port: 1080

If you want to access a published application, you must edit the ICA file of the published application to include the following information:

```
TcpBrowserAddress=ipaddress
```

where `ipaddress` is the address of a MetaFrame XP server.

```
UseAlternateAddress=1
```

When you modify the ICA file in this manner, the server that is listed in the TcpBrowserAddress entry will return its external address to the client. If the published application is load balanced, the server will return the alternate address of the data collector to the client, and the client can connect to the data collector to gather load-balancing information. The data collector will then send the alternate address of the server with the lightest load.

This ends our discussion of security. The topics presented here are not an all-inclusive list of security topics, only a subset of those topics that are specific to a MetaFrame XP environment. While many other options are available to secure a MetaFrame XP environment, it would be too unwieldy to cover them in this book. So as we leave Chapter 8 behind, we move on to the topic of application support.

# Summary

Although this is a short chapter, the information contained here is vital to safeguarding the data transferred between ICA Clients and the MetaFrame XP server. Since the data that is transmitted between the client and server can be intercepted, we discussed the encryption algorithms available and reviewed the correlation between encryption strength and processing requirements.

After discussing encryption, we introduced the topic of Secure Socket Layer and illustrated how data traveling to an NFuse server can take advantage of this secure encryption method. Those servers that are not running NFuse on the server itself can use SSL Relay to decrypt the data and pass it to the appropriate XML service on the MetaFrame XP server.

Finally, we discussed accessing servers from outside the organization by allowing data to pass through proxy servers, NAT servers, and firewalls. Depending on the protection used to block access to the internal network, you can configure the client to pass through these firewall methods and start their sessions.

In the next chapter, we will discuss application-support issues. This is the final chapter that concentrates on the server side before we move on to client issues.

# Exam Essentials

**Understand the correlation between encryption strength and resource usage.** As the encryption strength increases, the amount of processing required to encrypt and decrypt the data also increases.

**Know the levels of encryption strength available.** The levels available are 40 bit, 56 bit, 128 bit, and 128 bit logon only.

**Know what the SSL Relay Configuration tool is used for.** For those MetaFrame servers that do not have IIS installed on them, the SSL Relay Configuration tool decrypts SSL-based data and forwards it to the correct server.

**Understand how to configure the SSL Relay Configuration tool.** The SSL Relay Configuration tool has three tabs that contain configurable information: Relay Credentials, Connection, and Ciphersuites.

**Know the ports required to allow access to MetaFrame XP servers through a firewall.** By default, port 1494 must be open for session information to pass through; others may be required as well, depending on your environment.

**Understand how to configure a client to access MetaFrame XP servers through a SOCKS proxy.** SOCKS proxy servers are configured to allow certain clients to access internal resources by specifying which clients are allowed through the firewall.

**Understand how to configure a client to access MetaFrame XP servers through a firewall using alternate addresses.** When the clients use a private IP address range on the private network and use a NAT server to access the Internet, external clients need to have the alternate IP addresses configured on the NAT server in order to gain access to the MetaFrame XP servers.

## Key Terms

Before you take the exam, be certain you are familiar with the following terms:

- `ALTADDR`
- alternate address
- asymmetric encryption
- Basic
- Certificate Authority
- Ciphersuites
- Connection
- decryption
- Diffie-Hellman key agreement algorithm
- Display Friendly Name
- encryption
- firewalls
- Key Store Location
- keys
- Network Address Translation (NAT) devices
- Ports
- private key
- proxy servers
- public key
- public key encryption
- RC5 (128 bit)
- RC5 (128 bit) logon only
- RC5 (40 bit)
- RC5 (56 bit)
- Relay Credentials
- Relay Listening Port
- RSA RC5 algorithm
- Secure ICA
- Secure Socket Layer (SSL)
- security
- Server Certificate
- Server IP Address
- Socket Secure
- symmetric encryption

## Exercises

In the first exercise, we will set the encryption level for a connection so that all clients connecting to the server using the connection will have their sessions encrypted.

## EXERCISE 8.1

### Configuring the Security Level of a Connection

1. Open the Citrix Connection Configuration by clicking the Citrix Connection Configuration icon on the ICA Administrator toolbar or by choosing Start ➢ Programs ➢ Citrix ➢ MetaFrame XP ➢ Citrix Connection Configuration.

2. Right-click the connection on which you want to configure the encryption, and select Edit from the context menu.

3. Click the Advanced button.

4. In the Security section of the Advanced Connection Settings screen, click the Required Encryption pull-down menu.

5. Select the RC5 (56 Bit) option.

6. Click OK to close the Advanced Connection Settings screen.

7. Click OK again to close the Edit Connection screen.

In this next exercise, we will set the encryption level for a published application so that all clients starting a session to run the application will have their sessions encrypted.

## EXERCISE 8.2

### Configuring the Security Level of a Published Application

1. Open the Citrix Management Console by either clicking the Citrix Management Console icon on the ICA Administrator toolbar or choosing Start ➢ Programs ➢ Citrix ➢ MetaFrame XP ➢ Citrix Management Console.

2. When prompted, enter the password for your account.

3. Double-click the Applications node to expand it.

4. Right-click a published application, and select Properties from the context menu.

5. Click the ICA Client Options tab.

## EXERCISE 8.2 *(continued)*

6. From the Encryption pull-down menu, select RC5 (56 Bit).
7. Click to select the Minimum Requirement check box.
8. Click OK.

In this third exercise, we will assume that the MetaFrame XP server is on a network protected by a firewall that has NAT capabilities. We will set an alternate address for the server.

## EXERCISE 8.3

### Setting an Alternate Address for a Server behind a Firewall or NAT Router

1. Open a command prompt by choosing Start ➢ Run and then typing **`cmd`**. Then click OK.
2. From the command prompt, type **`altaddr /set 10.10.65.12`**.
3. To verify that the address is configured on the server, from the command prompt type **`altaddr`**.
4. Verify that the IP address 10.10.65.12 is displayed in the Alternate Address column.
5. To delete the alternate address, from the command prompt type **`altaddr /delete`** and hit the Enter key.

# Review Questions

1. Where can you configure encryption levels? (Choose all that apply.)

   A. A published application in Citrix Management Console

   B. ICA connections in Citrix Connection Configuration

   C. The Applications node in Citrix Management Console

   D. A server object in Citrix Management Console

2. When you use the same key for encrypting and decrypting data, you are using what type of encryption?

   A. Asymmetric

   B. Bound

   C. Symmetric

   D. Static

3. When you use a different key to decrypt the data than was used to encrypt it, but the two keys are mathematically linked, what is the encryption type?

   A. Asymmetric

   B. Bound

   C. Symmetric

   D. Static

4. You are the administrator of an organization that has 30 sites throughout the United States. Several users dial in to start sessions on your MetaFrame XP servers. You want to use the highest level of encryption possible. Since your company is completely domestic and you have no overseas partners, which level of encryption would you select for the connections to your servers?

A. None

B. Basic

C. RC5 (128 bit) logon only

D. RC5 (40 bit)

E. RC5 (56 bit)

F. RC5 (128 bit)

5. Which of the following encryption levels are subject to international export laws? (Choose all that apply.)

A. RC5 (128 bit) logon only

B. RC5 (40 bit)

C. RC5 (56 bit)

D. RC5 (128 bit)

6. What does SOCKS stand for?

A. Standard Online Cryptography Key Solution

B. Secure Online Cryptography Key Standard

C. Secure Online Cryptography Key Solution

D. Socket Secure

7. In a MetaFrame XP server farm, when you configure the encryption level for a published application, which of the following administrative utilities do you use?

A. Citrix Connection Configuration

B. Citrix Management Console

C. Published Application Manager

D. Citrix Server Administration

**8.** When is the SSL Relay Configuration tool needed?

**A.** When the NFuse-enabled MetaFrame XP server is on the same server as IIS

**B.** When the NFuse-enabled MetaFrame XP server is not on the same server as IIS

**C.** When the NFuse-enabled MetaFrame server is not running the XML service

**D.** When the firewall is between the data collector for the zone and the NFuse-enabled MetaFrame XP server

**9.** What is the default port used by SSL for secure communications?

**A.** 80

**B.** 110

**C.** 119

**D.** 443

**10.** You have installed Windows 2000 Server using `D:\winnt` as the installation directory. You then installed MetaFrame XP using the default directory options. Where is the default key store located?

**A.** `D:\Program Files\Citrix\SSLRelay\keystore`

**B.** `D:\Program Files\SSLRelay\keystore`

**C.** `D:\Winnt\Citrix\SSLRelay\keystore`

**D.** `D:\Winnt\SSLRelay\keystore`

**11.** When configuring the SSL Relay Configuration tool, which tab would you use to enter the password for the server certificate?

**A.** Relay Credentials

**B.** Certificate Credentials

**C.** Connection

**D.** Ciphersuites

**12.** When configuring the ciphersuites for use with the SSL Relay Configuration tool, how can you add additional ciphersuites?

**A.** Ciphersuites can be added only with Service Releases to MetaFrame XP.

**B.** Ciphersuites can be added only when MetaFrame XP is installed.

**C.** Ciphersuites can be added by clicking the New button on the Ciphersuites tab.

**D.** Ciphersuites cannot be added to the system.

**13.** Which port needs to be open on a firewall to allow web clients to initiate a connection to a published application?

**A.** 80

**B.** 443

**C.** 1494

**D.** 1604

**14.** What does the acronym NAT stand for?

**A.** Network Address Translator

**B.** Network Address Translation

**C.** Network Adapter Translation

**D.** Network Adapter Transmission

**15.** What command can you issue to change the port used for communication between the client and the MetaFrame XP server?

**A.** `CFGPORT`

**B.** `ICAPRT`

**C.** `ICAPORT`

**D.** `ICACFG`

**16.** What command is used to set an alternate address on a MetaFrame XP server?

**A.** `ALTADDR` *`ipaddress`*

**B.** `ALTADDR /apply` *`ipaddress`*

**C.** `ALTADDR /config` *`ipaddress`*

**D.** `ALTADDR /set` *`ipaddress`*

**17.** What must you configure on a client in order for that client to request an alternate address?

**A.** In the Firewall section of the client, you must check the Use Alternate Address For Firewall Connections check box.

**B.** In the Firewall section of the client, you must enter the firewall's IP address.

**C.** In the client's ICA file, you must enter the firewall's IP address and the MetaFrame XP server's port number.

**D.** In the client's ICA file, you must enter the MetaFrame XP server's IP address and port number along with the `UseFirewall=1` entry.

**18.** What command will remove an alternate address entry on a MetaFrame XP server?

**A.** `ALTADDR`

**B.** `ALTADDR /delete`

**C.** `ALTADDR /delete` *`ipaddress`*

**D.** `ALTADDR /remove`

**19.** What command will display the alternate address assigned to a MetaFrame XP server?

**A.** `ALTADDR`

**B.** `ALTADDR /display`

**C.** `ALTADDR /show`

**D.** `ALTADDR /view`

**20.** What must you configure for a published application to return the alternate IP address of the data collector?

**A.** In the Firewall section of the published application, you must check the Use Alternate Address For Firewall Connections check box.

**B.** In the Firewall section of the published application, you must enter the firewall's IP address.

**C.** In the published application's ICA file, you must enter the MetaFrame XP server's IP address and include the `UseAlternateAddress=1` entry.

**D.** In the published application's ICA file, you must enter the MetaFrame XP server's IP address and include the `UseFirewall=1` entry.

# Answers to Review Questions

1. A, B. You can set the encryption level on a published application to control the encryption for that application on all of the servers in your server farm. You can also set the encryption level on a connection to control access to, and the encryption on, a connection on a server.

2. C. Symmetric encryption uses the same key to decrypt the data that was used to encrypt the data. Using this key type is more efficient as far as processing and resource usage is concerned, but not as secure as asymmetric encryption.

3. A. Asymmetric encryption uses two different, but mathematically linked, keys. One key, known as the public key, is used to encrypt the data, while the other, the private key, is used to decrypt the data. While this encryption scheme requires more system resources, it is much more secure than symmetric encryption.

4. F. Since all of the connections to the server are made from within the United States, you can use 128-bit encryption. If any of the connections were from clients based outside of the country, you would need to check the export laws governing the level of encryption allowed.

5. C, D. Of those listed, RC5 (40 bit) and (128 bit) logon only are the only ones that are not restricted by the export laws. For all other levels, you should check before using them on servers and clients outside of the United States.

6. D. Derived from Socket Secure, the SOCKS protocol allows an administrator to control the access into a network based on access rules, such as the protocol, ports, and addresses allowed.

7. B. You use the Citrix Management Console in a MetaFrame XP server farm to configure the encryption level of published applications. You do so by selecting the application from the Applications node and editing the Encryption entry on the ICA Client Options tab.

8. B. If the MetaFrame XP server that is running NFuse is not on the same server as IIS, the SSL Relay Configuration tool is needed to decrypt the data as it is sent on the SSL port and then redirect it to the MetaFrame server.

9. D. Port 80 is used for HTTP, 110 for POP3, 119 for NNTP, and 443 for SSL.

**10.** D. The default key store location for the certificates used in SSL communication is `%systemroot%\SSLRelay\keystore`. You can change this location from the Relay Credentials tab of the SSL Relay Configuration tool.

**11.** A. The Relay Credentials tab is used when configuring the server certificate for the SSL Relay Configuration tool. This tab includes the server certificate location, the certificate name, and the password.

**12.** D. Unfortunately, the last option is correct. Additional ciphersuites cannot be added to MetaFrame XP server's SSL Relay Configuration tool.

**13.** A. To initiate a connection to a published application, port 80 must be open. After HTTP makes the initial request, port 1494 must be open to allow the published application session to run.

**14.** B. Used to translate packets originating from a private address to a public address, Network Address Translation is used in many firewall products.

**15.** C. If you want to use another port besides the default port of 1494 to access the MetaFrame XP server from a client, the firewall must have the new port open. You must issue the command `ICAPORT /port:`*`xxxxx`* at a command prompt on the MetaFrame XP server to set the port number.

**16.** D. When configuring an external address that allows a client to access a MetaFrame XP server through a NAT server, you use the command `ALTADDR /set` *`ipaddress`*.

**17.** A. When you edit the properties of the client to select the Use Alternate Address For Firewall Connections check box, the client will request that the MetaFrame XP server's configured alternate address be returned.

**18.** B. When the external address of the client needs to be removed for any reason, the `ALTADDR /delete` command will do the trick.

**19.** A. Simply typing **`ALTADDR`** at a command prompt will cause the server to display the adapters using an alternate address and the alternate address used.

**20.** C. When the application is to return the alternate address to a client, the ICA file for the published application must include the fields `TcpBrowserAddress=ipaddress` and `UseAlternateAddress=1`.

Chapter 9

# Application Support

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **7. Applications**

- 7a. Installing, Uninstalling, and Migrating Applications
- 7b. Configuring Applications for use in a MetaFrame environment

In the preceding chapters, we have taken a look at the administrative tools available with MetaFrame XP. These tools allow us to control access to our MetaFrame servers and monitor how the system is running. None of these tools are very effective, however, if we do not have applications loaded onto the server. Without applications, the user has nothing to run and the server becomes a large paperweight.

This chapter presents some of the issues you will encounter when installing and maintaining applications. From the initial install to publishing those applications for user access, we detail the steps necessary to keep those apps running and your users happy.

## Benefits of Applications Running on MetaFrame XP

Imagine a perfect work environment. A new application is approved for your users' needs. It is up to you to install the application for all users. You obtain the software and install it one time, and voilà! All of the users who need access to the application have it at their fingertips. You now get to sit back and relax knowing that your job is complete. Later you discover that a service pack has been released for one of the applications you use. After downloading the files for the service pack and testing to make sure that there are no conflicts in your environment, you apply the service pack once, and all of the employees who utilize the application have the updated software.

While there are software packages that allow you to automatically install applications on clients' workstations, such as Microsoft's System Management Server and the Group Policy software installation functions, none are so easy to use as installing an application on a server running terminal services.

As discussed in Chapter 2, "Underlying Citrix MetaFrame XP Technologies," applications need only be installed once on a MetaFrame server, and every user who starts a session on that server has access to the application. If an application is upgraded or a service pack is applied, each user who starts the application will have the updated software. Everything is performed at the server; you needn't touch the client system. This is what every administrator wishes for: centralized control and access for all line-of-business software.

Of course, nothing is as easy as it seems. There are always some issues we must contend with as we install applications, one of which is loading applications on multiple servers. You can install the application on each server, but you will need to apply the same installation options for each server. Another feature that is available if you have purchased MetaFrame XPa or XPe is Installation Manager. With this product, you can install an application automatically on all of the servers where you wish it to be made available.

So let's go back to that idyllic environment we all dream of. Your users are clamoring for an application that will make their lives easier. This application will have to be loaded for more than 100 users. Since you already have MetaFrame XP servers in place, and they have enough horsepower to handle the additional load the application will place on them, you use Installation Manager to load the application on all servers. After loading the application, you publish the application for those users who require it and then use Load Manager to control the user load on each server. Now you have the application available for all users who need it, and the servers are used in an efficient manner.

With that in mind, we'll move forward and show you how you can install and manage applications on a MetaFrame XP server. We will discuss the steps needed to install an application, show how you can update the software when an upgrade or service pack is made available, teach you to use

Installation Manager to simplify installing on multiple servers, and explain what you need to do to make an application available for users once it is installed.

# Installing and Uninstalling Applications

Once again, we need to discuss the requirements for a service. As usual, certain items must be in place before an application is available for user access. On a Windows 2000 Server, you need to install Terminal Services in application mode and not remote administration mode. If Terminal Services is installed in remote administration mode, the server will allow only two connections and will not be optimized for applications running in the background. Also, the users who connect will need to be members of the Administrators group. If the server is in application mode, users will be able to connect using their domain or server account and run any application they have been given permission to use.

Most applications are installed for a specific user account on a computer. The settings are added to the user's profile so that the user has access to the application whenever they log on to their workstation. Whenever the user makes changes to the application, those changes are stored within the user's profile. The next time the user logs on, the application is configured the same way as when they used it last.

The problem with installing applications in this manner on a MetaFrame server is that whenever someone makes a change, it applies to all users of the application. This is not an ideal situation when you consider how many users want to change the look and feel of applications to meet their own desires or needs. To alleviate this problem, when you install an application, you need to put the server into a special software installation mode.

When you install an application using the Terminal Services installation methods, the application is installed in what is referred to as *install mode*. Installing the application for multiple users causes the server to track the application installation and prepare to distribute user-specific files and settings to users at runtime. This allows users to have application settings that they can change without affecting the other users' settings.

To install an application for multiple users on a MetaFrame XP server, you need to make sure that the server meets the minimum requirements listed in Chapter 3, "Planning the Installation of MetaFrame XP." You also need to be a member of the Local Administrators group. Without this level of permission, you will not be able to access the user account information when configuring the users who can run the application after it has been loaded.

Before actually performing the install, you should have all of the application installation data ready. One piece of this data might be a *transform file*. Transform files are files that Microsoft has introduced to modify installations of applications that conform to the *Windows Installer package* file specifications. These files allow you to uniquely configure an application during an automated installation. These files usually have an `.mst` extension, and you will need to have the transform file ready when installing the application.

### Checklist

Just as we prepared a checklist in the third chapter as we were planning to install the MetaFrame XP software, you should create a checklist for installing applications. This checklist should include options for the setup file location and name, any transform file that should be used, the application compatibility script if applicable, and an entry for disabling logons and ending all user sessions before proceeding.

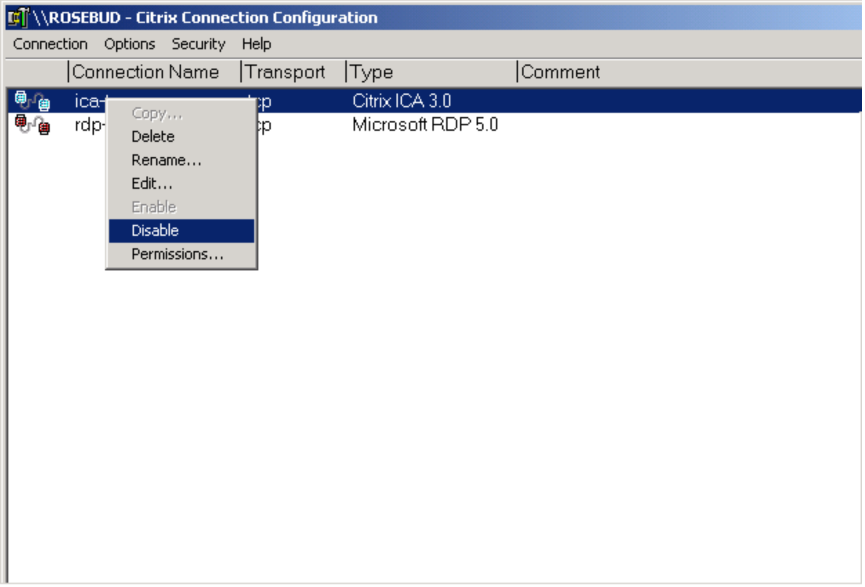
The other piece of the puzzle is an *application compatibility script*. These files are used to correct some inherent problems with applications that were not originally written for a multi-user environment. These scripts are written to modify configuration files and Registry entries of the specific application they were written for. You can find these files in the `Application Compatibility Script` folder under the `%systemroot%` folder. You should run a script only on the application that it was written for.

All users must log off the server before you can install an application. When the server is configured to install an application, it is switched to installation mode, which does not allow users to access their own sessions.

This limits most environments to specific timeframes for installing applications. You will need to plan when the applications can be installed and then follow the guidelines presented below.

First, you must make sure that new sessions cannot be created. To ensure this, go into Citrix Connection Configuration, right-click a connection, and select Disable, as shown in Figure 9.1. You will need to perform this step on all connections. This guarantees that no new sessions can be started on the server while you are installing an application.

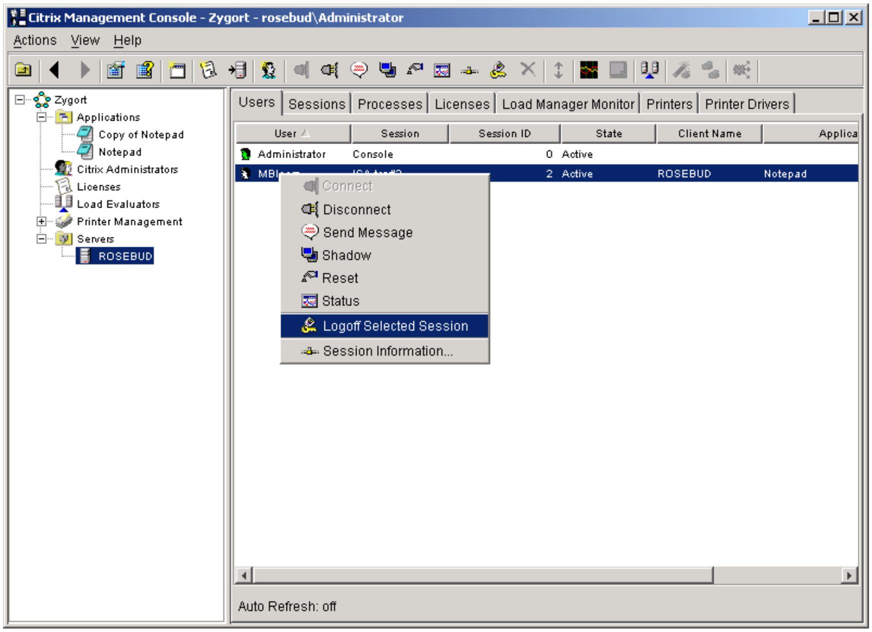
**FIGURE 9.1** Disabling connections



| Connection Name | Transport | Type | Comment |
|---|---|---|---|
| ica- | cp | Citrix ICA 3.0 | |
| rdp- | cp | Microsoft RDP 5.0 | |

You must also ensure that no one is connected to the server and running a session. There are several ways you can check to see if there are users remaining on your server, but the easiest method is to open Citrix Management Console and navigate to the Servers node. Once there, select the server where you want to install the application, and click the Users tab. From here you can right-click each of the users and choose Logoff Selected Session, as shown in Figure 9.2. Once you have determined that the server is devoid of any sessions, you are ready to install the application.

**FIGURE 9.2** Logging off users

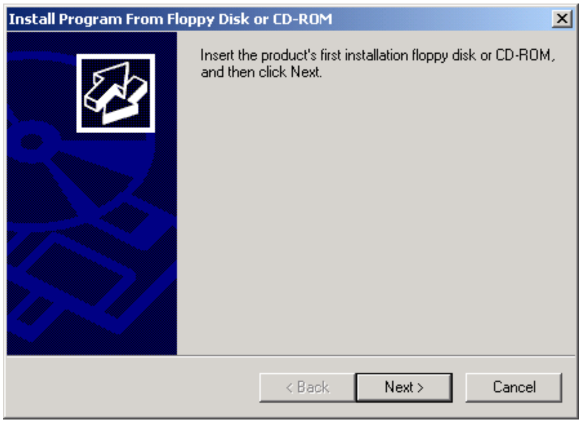


| User | Session | Session ID | State | Client Name | Applica |
|---|---|---|---|---|---|
| Administrator | Console | 0 | Active | | |
| MBl | [illegible] | 2 | Active | ROSEBUD | Notepad |

After you have collected all of the information you need for the application and all users are off the system, you are ready to start installing. There are two methods of placing the server into installation mode. The easier method is one that most administrators are already familiar with, the *Add/Remove Programs* utility in Control Panel. When Terminal Services has been installed in application server mode, this utility takes on a special function. Click the CD Or Floppy button in the Add New Program screen to start the Add New Program Wizard, shown in Figure 9.3. What you do not see is the server going into *application installation mode*. Once in this mode, the server monitors the installation progress and keeps track of user-specific application Registry entries and installation (INI) files.

Each of the user-specific entries is then used to modify the user's profile information when the user starts a session and uses the application. This way, each user is able to maintain unique configuration information for each of the applications. If the user changes any of the settings, those changes will be reflected in only that user's session and not in any other user's session.

**FIGURE 9.3** Add New Program Wizard

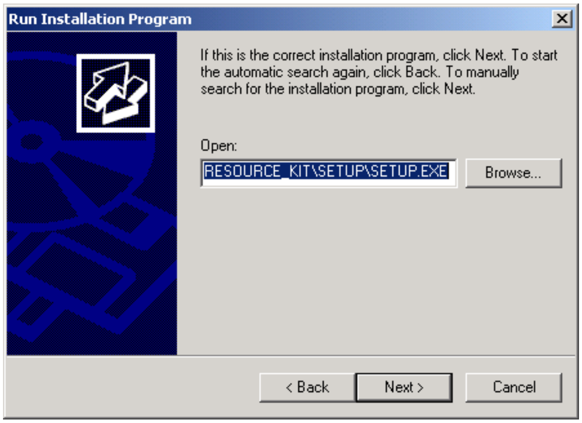


Install Program From Floppy Disk or CD-ROM

Insert the product's first installation floppy disk or CD-ROM, and then click Next.

Click the Next button to search the floppy and CD drives for a Setup program. If the wizard finds one, it will display the program path, as shown in Figure 9.4, and allow you to override the path if it is not the one you want. Once you've chosen the correct path, click Next to start the Setup program. When the application has finished installing, the wizard will again ask you to click Next. Once you do, the Finish Admin Install screen appears, stating that the install is complete. From here, you can click the Finish button to put the server back in application *execution mode*. You must make sure the application install has completed before clicking the Finish button. Once back in execution mode, the server will no longer be able to record the user-specific changes made by the install program. Click this button only when you are sure that the install has completed.

**FIGURE 9.4** Program path prompt



Run Installation Program

If this is the correct installation program, click Next. To start the automatic search again, click Back. To manually search for the installation program, click Next.

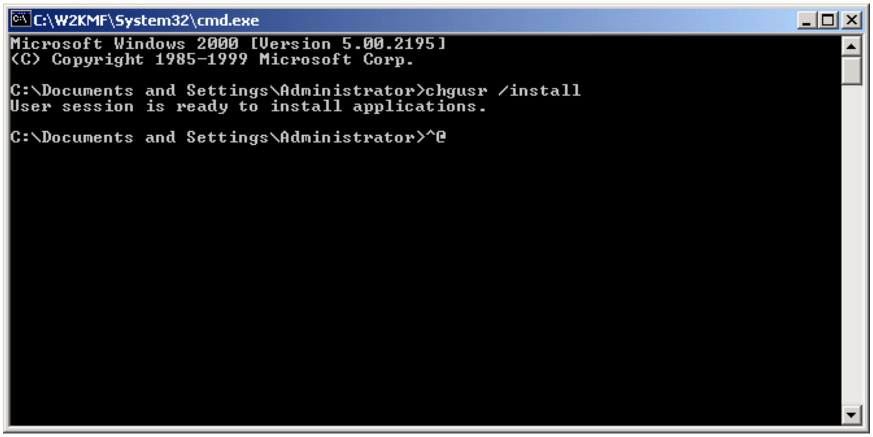
Open: RESOURCE_KIT\SETUP\SETUP.EXE

Some apps require a reboot after the installation is complete. Do not allow the application to reboot the server until you click Finish. Selecting Finish allows the system to complete its application tracking and safely record the changes. If the system reboots before you click the Finish button, some application settings may not be properly recorded and unpredictable results may occur. If the setup screen does not allow you to access the taskbar, you may need to press the Alt+Tab key combination to switch back to the wizard and click the Finish button.

After the application has been installed, you may need to run the application compatibility script that is associated with the application. This will ensure that any additional configuration of the application is complete. At this point, you've finished the install. Before allowing users to access the application, however, you should verify that the application is installed correctly and that it did install for multiple users and not for a single user.

The other method of placing the MetaFrame server in installation mode is to use a command-line command. While some administrators like to use the graphical user interface, many others like to control the system from the command line. Open a command line by choosing Start ➢ Run, typing **cmd**, and clicking OK or by choosing Start ➢ Programs ➢ Accessories ➢ Command Line. At the command prompt, type in the command **chgusr /install**, as shown in Figure 9.5.

**FIGURE 9.5** Preparing to install an application from the command line



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents and Settings\Administrator>chgusr /install
User session is ready to install applications.

C:\Documents and Settings\Administrator>^@
```

Once you've put the system in install mode, you can execute the Setup program for the application. As with the Add/Remove Programs utility, you should run any application compatibility script associated with it. When you've performed all of the install steps, you must put the system back into execute mode. Again, this is a command-line option: **`chgusr /execute`**. The same warning applies here as with clicking the Finish button—the application install must be complete before running this command. Otherwise, the system may not have all of the information required to apply to user sessions.

NOTE `chgusr /install` and `chgusr /execute` are actually shortcut versions of the `change user /install` and `change user /execute` commands. You can use either command, but most administrators take advantage of the shortcut command because it is easier to enter.

After you install the application on the server and change the options to allow users to connect to the server again, every user with permissions to the published application will be able to run it and make individual changes. The only drawback to this scenario is that the application is loaded on only one server. To have the application available on multiple servers, you will need to install it on each server. This can be time consuming, and if you install the application with different settings on other computers, the user will not enjoy a uniform work environment. In the next section, we will discuss the tool used to install the application across multiple servers at the same time.

# Automatic Application Installs

Let's take into consideration that most companies have multiple servers that host the same application for users to access. You, as the administrator, do not want to have to load the application on 20 computers over the course of the day. You have better things to do. Citrix Systems has included a utility with the MetaFrame XPe product that assists in automating the install of an application to multiple servers at once. This utility is known as Citrix Installation Manager.

With Citrix Installation Manager, you can create an installation package that can be pushed to servers within the server farm. This package is known as an *application deployment file*, which uses an extension of `.adf` to identify it. You can create this file from legacy applications that do not conform to the Windows Installer specifications, custom applications written by in-house development teams, compatibility scripts, software upgrade programs and service packs, and hotfixes.

Microsoft provides its own custom application installation files. Known as package files, they are used to automate and control the installation of software on client systems. These files can usually be identified by their `.msi` extension and are compatible with Citrix Installation Manager.

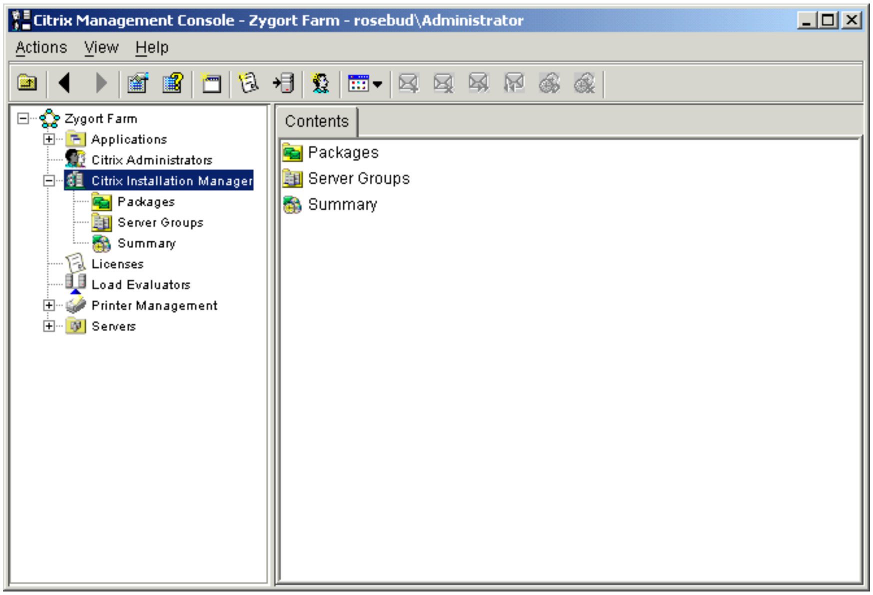
Citrix Installation Manager does not require that the ADF and MSI packages reside on the server with Installation Manager. It can access the application packages from a network share. This enables you to store the files on a file server within your network and run Installation Manager from a MetaFrame XP server, thus reducing the amount of resources you consume on the MetaFrame XP server.

Other administrative functions that Citrix Installation Manager performs include scheduling the installation of packages and controlling the packages that are included in the Installation Manager database. We will look at these functions as we go through the remainder of this section.

## Citrix Installation Manager Components

Three components make up Citrix Installation Manager. The first component is the *administrative plug-in* that is added to Citrix Management Console. The administrator can use this new node, Citrix Installation Manager, to view packages, change package properties, schedule installation jobs, and view a job's status, as shown in Figure 9.6.

**FIGURE 9.6** Administrative plug-in for Citrix Installation Manager



The second component is the *packager*. This is the tool that creates the software installation package that Installation Manager uses to install the application on the MetaFrame XP servers. After you install this component on a Windows 2000 Server or a Window NT Server 4.0 computer, it monitors an application install and tracks the changes made to the operating system. These changes are recorded in a script file. The script file contains commands that are used when the application is installed on a MetaFrame XP server. After the script file is created, you should save it with the application files on a server so that the MetaFrame XP servers that will be installing the application can access all of the required files.

The final component is the *installer service*. This is a service that should be added to every MetaFrame XP server in the server farm that will participate in the installation-management function. When you choose to have an application installed on a MetaFrame XP server, the installer service interprets the commands and the ADF or MSI file contained in the package and installs the software on the MetaFrame XP server.

All three of these components are used together to enable an administrator to automatically install an application to one or more servers at once. The packager creates the installation files; the administrative add-in allows you to control the packages, schedule the install, and select the server that the application will be installed to; and the installer service performs the installation based on the files generated from the packager according to the criteria set forth by the administrative add-in.

Here are some points to take into consideration when working with Installation Manager:

**Citrix Installation Manager installs applications but does not publish them.** When you use Citrix Installation Manager, the applications will be installed on the servers you specify, but the application will not automatically publish for users to access. To publish an application, you will need to use the utilities within the Applications node of Citrix Management Console.

**Deleting an application from Citrix Management Console does not uninstall it.** When you delete an application from the Applications node in Citrix Management Console, the application does not automatically uninstall from the servers where it is installed. Likewise, removing the server from the server list where the application is published does not uninstall the application from that server.

NOTE For more information on publishing applications, see the section "Configuring Applications for Client Use" later in this chapter.

**Do not use the Add/Remove Programs utility to uninstall an application that had been installed by Citrix Installation Manager.** Applications that are installed using Citrix Installation Manager should only be uninstalled using the administrative add-in in Citrix Management Console. If you use Add/Remove Programs, Installation Manager will not be able to maintain an accurate database of applications and where they are installed.

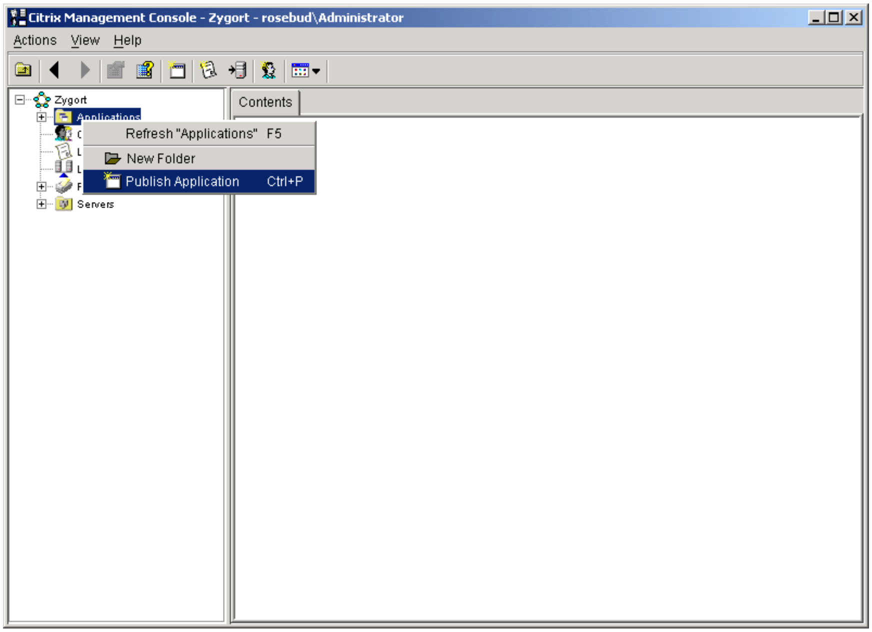
NOTE A complete discussion of Installation Manager is beyond the scope of this book and exceeds the needs of an administrator preparing for the Citrix Certified Administrator Exam. For more detailed information, read the "Citrix Installation Manager for MetaFrame XPe—Getting Started" white paper available from Citrix Systems' website.

Now that the applications are installed, we need a way for clients to access those applications. We can allow them to start a desktop session and run the applications from there, but in doing so we are limiting them to running applications installed on that server only. Instead, we want to allow the users to access applications from any server in the farm that is convenient. In the next section, we will discuss publishing those applications.

# Configuring Applications for Client Use

Now that the applications are installed on our MetaFrame XP servers, we need to configure them so that users can access them. In MetaFrame terms, this is known as *publishing* the applications. Of course, there is a wizard for performing this action. To access the Application Publishing Wizard, right-click the Applications node within Citrix Management Console and select Publish Application from the context menu, as shown in Figure 9.7. With this wizard, you can publish Win32, Win16, DOS, OS/2, and POSIX applications as well as publish a desktop for users to access in a load-balanced environment.

**FIGURE 9.7** Starting the Application Publishing Wizard

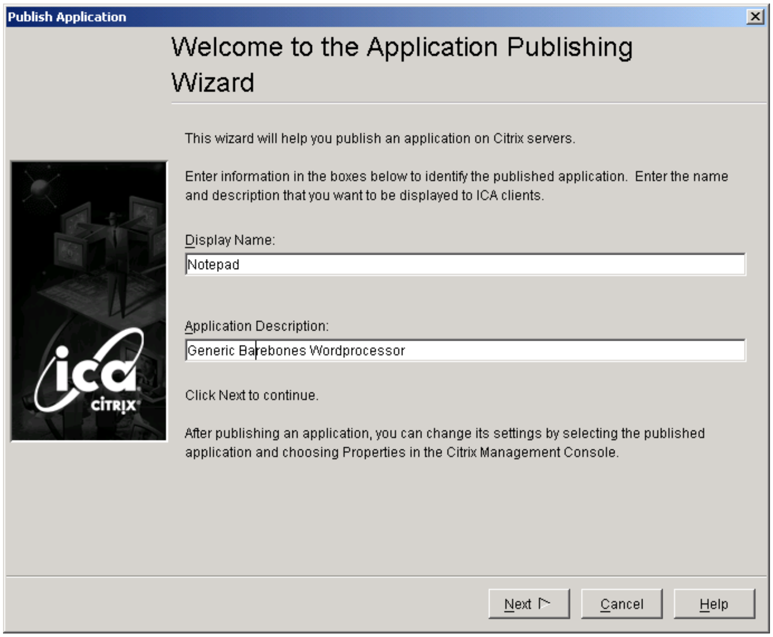

Citrix Management Console - Zygort - rosebud\Administrator
Actions
View
Help
Zygort
Applications
Servers
Contents
Refresh "Applications" F5
New Folder
Publish Application Ctrl+P

You can also start the Application Publishing Wizard by using the shortcut keys Ctrl+P or by clicking the Publish Application icon on the menu bar.

As shown in Figure 9.8, the first screen to appear when the wizard opens requests that you fill out the Display Name and Application Description fields. The first of these two entries, Display Name, is the name users see when they use Program Neighborhood. This name should be easily identifiable to the users. Of course, the text you enter in the Description field can further aid in the application's identification.

After entering the identifying information and clicking Next, you will be prompted to supply the path to the application and its working directory, as shown in Figure 9.9. Citrix Systems was nice enough to provide a Browse button so that you can search for the application's executable file instead of having to remember the path. If you use the Browse button to supply the path, the Working Directory entry will be filled in automatically. If you want to publish a desktop for your users to access, simply select the Publish Desktop radio button. Publishing a desktop allows your users to start a desktop session in a load-balanced environment instead of connecting directly to a MetaFrame server.

**FIGURE 9.8** Entering identifying information for the application



Welcome to the Application Publishing Wizard

This wizard will help you publish an application on Citrix servers.

Enter information in the boxes below to identify the published application. Enter the name and description that you want to be displayed to ICA clients.

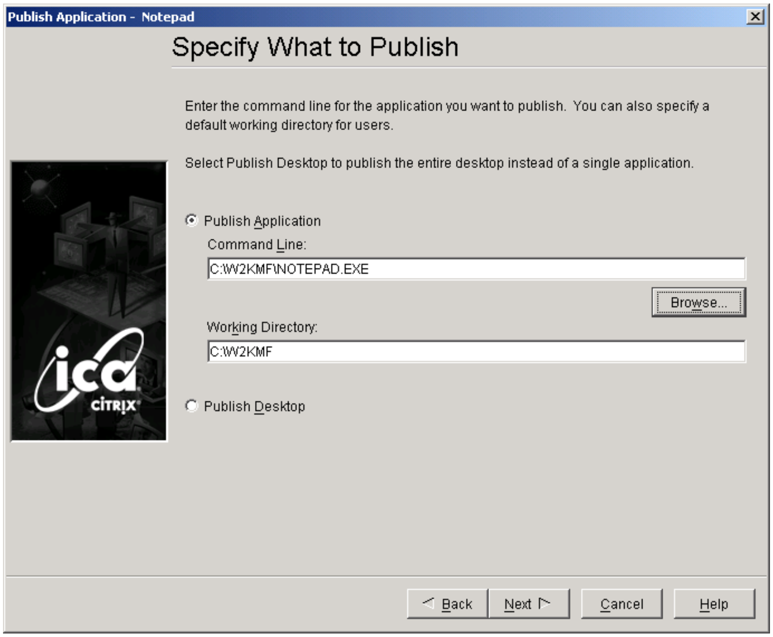
Display Name: Notepad

Application Description: Generic Barebones Wordprocessor

Click Next to continue.

After publishing an application, you can change its settings by selecting the published application and choosing Properties in the Citrix Management Console.

**FIGURE 9.9** Specifying the application path



Specify What to Publish

Enter the command line for the application you want to publish. You can also specify a default working directory for users.

Select Publish Desktop to publish the entire desktop instead of a single application.

● Publish Application

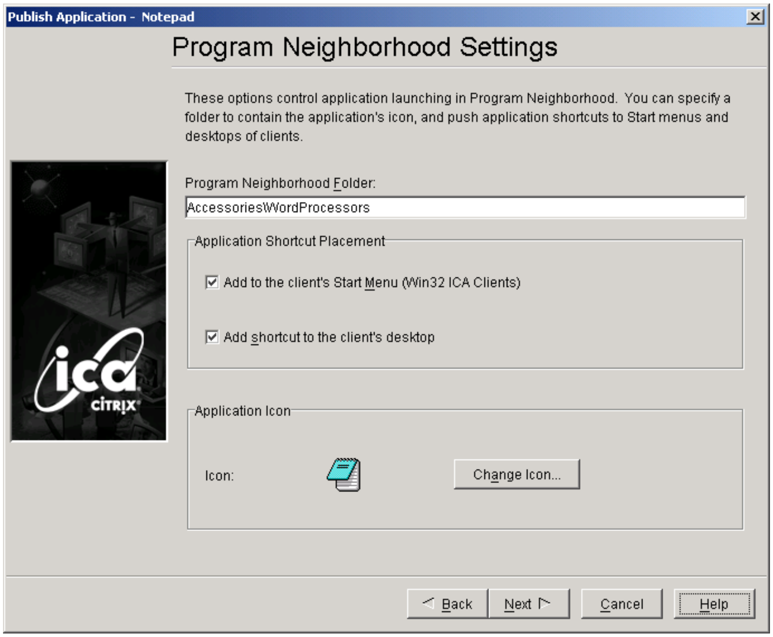
Command Line: C:\W2KMF\NOTEPAD.EXE

Working Directory: C:\W2KMF

○ Publish Desktop

The next screen, shown in Figure 9.10, allows you to control how users access the program. At the top of this screen is the Program Neighborhood Folder option. If you want the application to appear within a folder in the user's Program Neighborhood, you would specify the folder structure on this line. For example, if you want Notepad to appear in a folder named `Accessories`, you would enter **Accessories** on the line. If there are multiple levels of folders within Program Neighborhood, you can separate each level with a backslash (\). For example, if you want Notepad to appear in the folder `WordProcessors` under the `Accessories` folder, the entry would be **Accessories\WordProcessors**.

**FIGURE 9.10** Program Neighborhood Settings screen



Publish Application - Notepad

Program Neighborhood Settings

These options control application launching in Program Neighborhood. You can specify a folder to contain the application's icon, and push application shortcuts to Start menus and desktops of clients.

Program Neighborhood Folder: Accessories\WordProcessors

Application Shortcut Placement

☑ Add to the client's Start Menu (Win32 ICA Clients)

☑ Add shortcut to the client's desktop

Application Icon

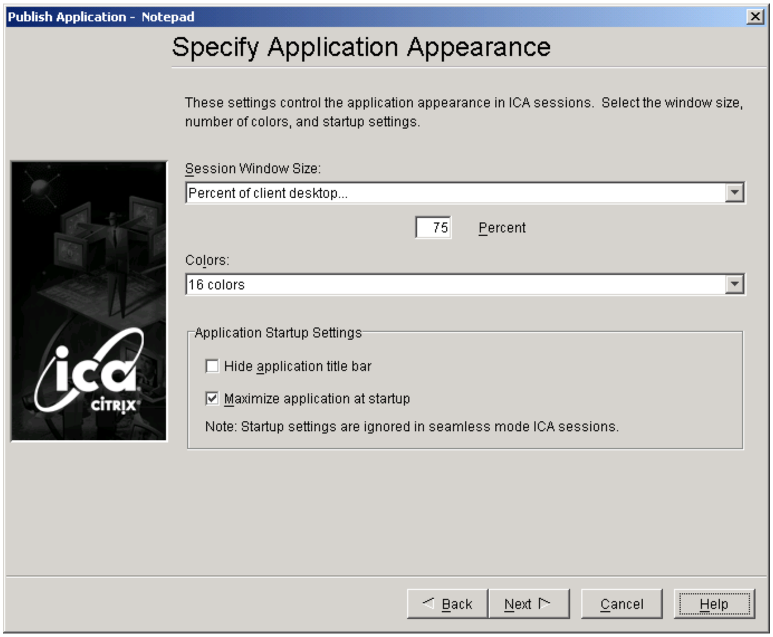
Icon:

The next section on this screen designates how the icon for the application will appear on a Win32 user's desktop. If you select the check box next to Add To The Client's Start Menu, an icon will appear on the user's Start menu when they connect to the MetaFrame XP server. Likewise, when you choose the other option, Add Shortcut To The Client's Desktop, a shortcut will appear on the user's desktop once they connect to the server.

The final option allows you to change the icon that appears within Program Neighborhood as well as what is pushed down to the user's desktop. If you do decide to change the icon, you should remember that users are generally familiar with the default icons for an application and therefore might be confused when they do not see the familiar icons.

Click Next to go to the Specify Application Appearance screen, shown in Figure 9.11. On this screen, you can set the default settings that an application will use if the user's settings within Program Neighborhood do not override them. The Session Window Size pull-down list provides options for sizing the application window from 640×480 up to 1600×1200 pixels. Three other options also exist on this pull-down list. Full Screen sizes the application so that it will consume the entire display area of your monitor. Custom allows you to configure the pixel size that you want the application to use, while Percent Of Client Desktop allows you to scale the application based on the user's current resolution settings.

**FIGURE 9.11** Appearance options



Specify Application Appearance

These settings control the application appearance in ICA sessions. Select the window size, number of colors, and startup settings.

Session Window Size: Percent of client desktop...

75 Percent

Colors: 16 colors

Application Startup Settings

□ Hide application title bar

☑ Maximize application at startup

Note: Startup settings are ignored in seamless mode ICA sessions.

The Colors pull-down list allows you to select the color depth that the application can use. Four choices are available from this menu: 16 Colors, 256 Colors, High Color (16 Bit), and True Color (24 Bit). When choosing the color depth, keep in mind that more colors equate to more bandwidth utilization and higher processor consumption.

Finally on this screen, you can configure how the application appears at startup and whether the title bar appears when the application is on-screen.

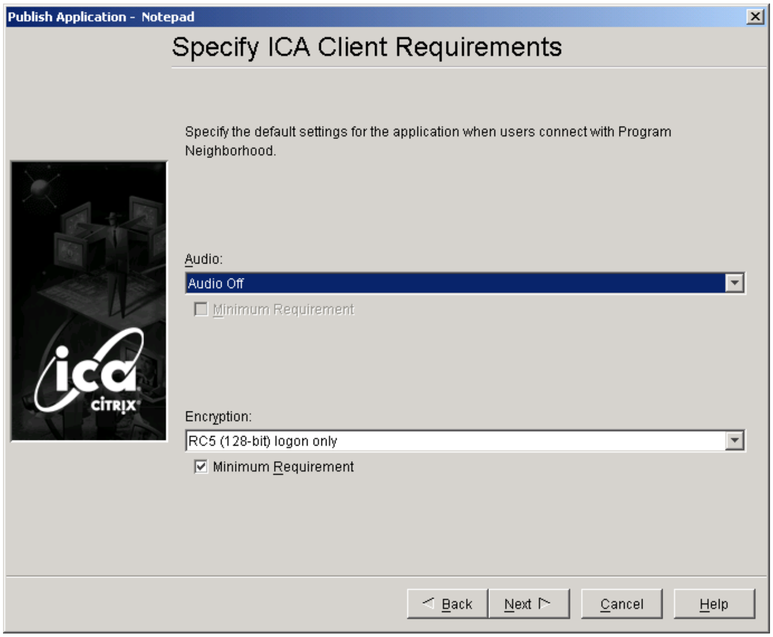
Both of these options are ignored if the application is started as a seamless window on a user's computer.

Audio and Encryption options are configured on the next screen, as shown in Figure 9.12. If you want the application to be able to send audio to the client's sound device, you can select the option Audio On under the Audio pull-down list. And you can select the level of encryption from the Encryption pull-down list. Notice the Minimum Requirement check box under both options. If this box is checked, the client will have to meet the requirement listed. If the client does not meet that requirement, they will not be allowed to start the application session.

NOTE

Only published applications can send sounds to client sessions. If you connect directly to a server to access an application, you will not be able to receive sounds in the client session.

**FIGURE 9.12** Specify ICA Client Requirements screen



Publish Application - Notepad

Specify ICA Client Requirements

Specify the default settings for the application when users connect with Program Neighborhood.

Audio: Audio Off

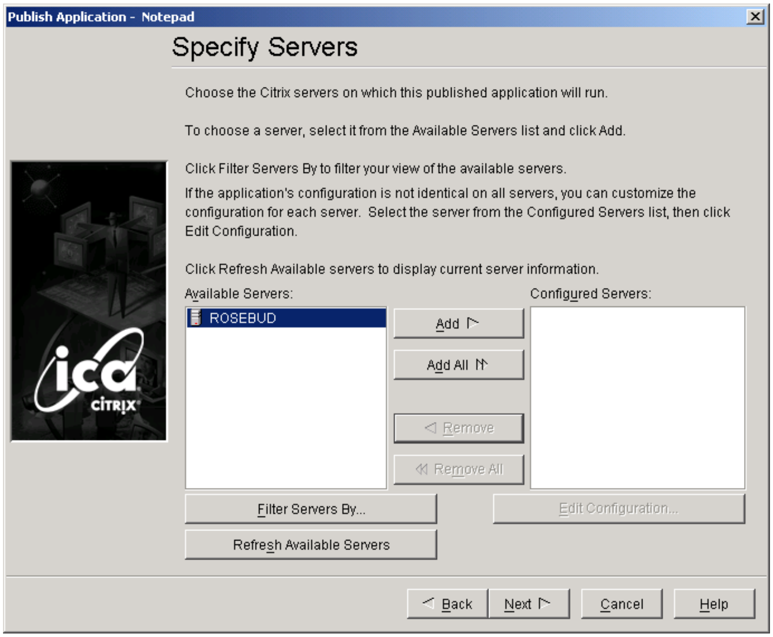
□ Minimum Requirement

Encryption: RC5 (128-bit) logon only

☑ Minimum Requirement

The next screen, Specify Servers, allows you to select on which servers the application will be published, as shown in Figure 9.13. When you select a server from the Available Servers list on the left side of the screen and click Add, the application will be published on that server. Most of the buttons on this screen are self-explanatory, so we will review only what the Filter Servers By button does. If you press this button, the screen shown in Figure 9.14 appears. The first option, Installation Management, specifies that the servers on which the application will be published must have the installer service installed in order to appear in the server list. The other two options specify the operating system level that is required before the server will appear in the list. Selecting any of these options turns on filtering, so any server that does not meet the requirements will not appear. Leaving all of the check boxes unchecked allows all MetaFrame servers to appear.

**FIGURE 9.13** Specify Servers screen



Publish Application - Notepad

Specify Servers

Choose the Citrix servers on which this published application will run.

To choose a server, select it from the Available Servers list and click Add.

Click Filter Servers By to filter your view of the available servers.

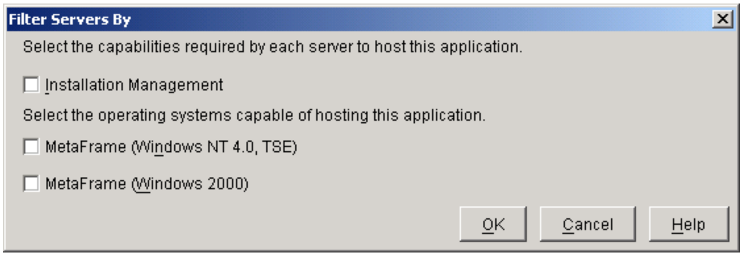
If the application's configuration is not identical on all servers, you can customize the configuration for each server. Select the server from the Configured Servers list, then click Edit Configuration.

Click Refresh Available servers to display current server information.

Available Servers: ROSEBUD

Configured Servers:

**FIGURE 9.14** Filter Servers By screen



Filter Servers By

Select the capabilities required by each server to host this application.

□ Installation Management

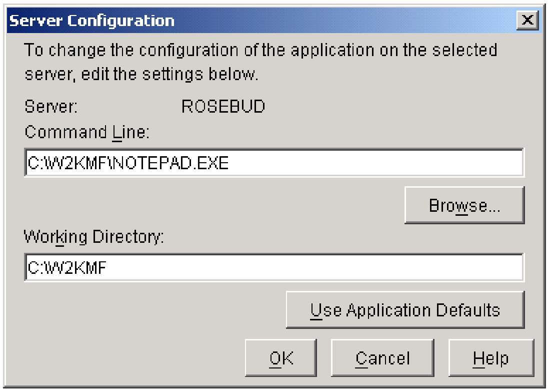
Select the operating systems capable of hosting this application.

□ MetaFrame (Windows NT 4.0, TSE)

□ MetaFrame (Windows 2000)

To make your life easier, you should attempt to install an application using the same directory path on all of your servers. If this is the case, you can select the servers on which you want to publish the application and click Next to choose which users can access the application. If you have servers where the application is installed using different directory paths, you will need to specify the path on each of those servers. To do this, select the server and click the Edit Configuration button. You will see the Server Configuration screen shown in Figure 9.15. Specify the appropriate path for the application and click OK. You will need to perform this step for every server that does not have the same path that you specified earlier in the wizard.

**FIGURE 9.15** Editing the application path



Server Configuration

To change the configuration of the application on the selected server, edit the settings below.

Server: ROSEBUD

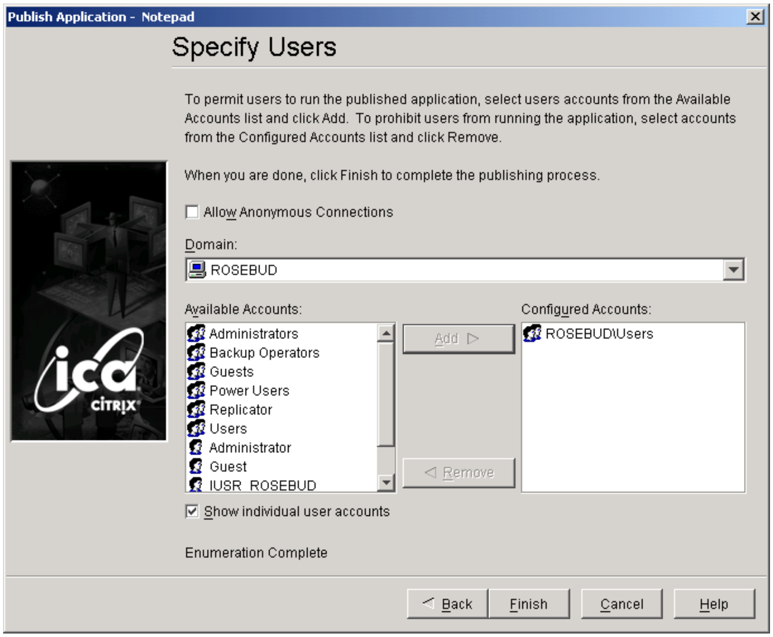
Command Line: C:\W2KMF\NOTEPAD.EXE

Working Directory: C:\W2KMF

We are finally at the last screen of the wizard. This is where you choose which users will be able to access the application once it is published. As in the Specify Servers screen shown previously, the Specify Users screen allows you to select users from the Available Accounts list and add them to the Configured Accounts list, as shown in Figure 9.16. Notice that you can choose from which domain to add the accounts. From the Domain pull-down list, you can select accounts from the local server, the domain in which the server resides, and any domain that has the appropriate trust relationship. Groups appear by default in this list since most administrators find it easier to administer their networks when they use groups and group permissions. If you want to add an individual user account, you will need to select the Show Individual User Accounts check box.

MetaFrame XP is smart enough to know when users are removed from the server or domain. When a user is removed from Active Directory Users and Computers or User Manager for Domains, the Configured Accounts list reflects the removal of the account. Likewise, if a user is added to or removed from a group that has access to the published application, they will automatically gain or lose permission to access the application.

**FIGURE 9.16** Assigning accounts



Publish Application - Notepad

Specify Users

To permit users to run the published application, select users accounts from the Available Accounts list and click Add. To prohibit users from running the application, select accounts from the Configured Accounts list and click Remove.

When you are done, click Finish to complete the publishing process.

□ Allow Anonymous Connections

Domain: ROSEBUD

Available Accounts:
- Administrators
- Backup Operators
- Guests
- Power Users
- Replicator
- Users
- Administrator
- Guest
- IUSR_ROSEBUD

Configured Accounts:
- ROSEBUD\Users

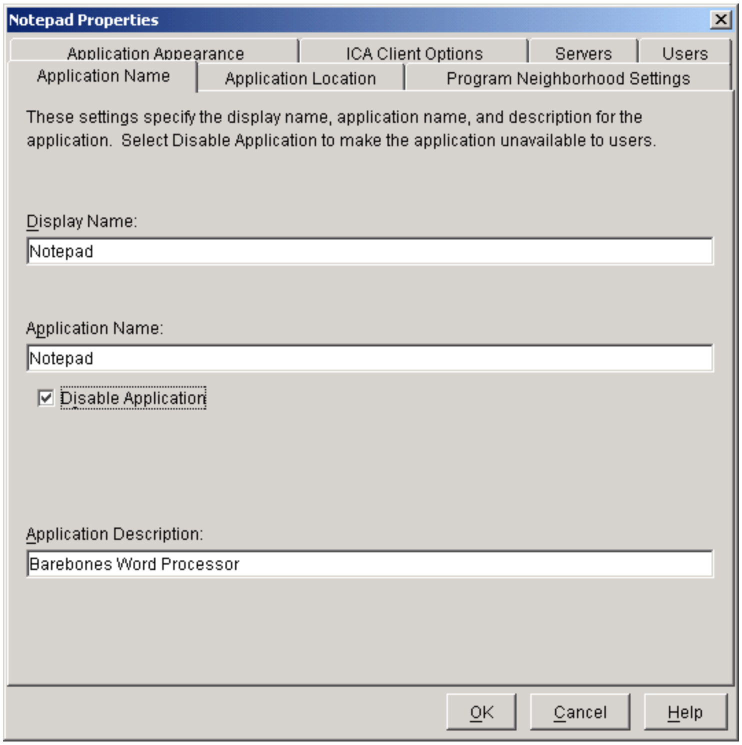
☑ Show individual user accounts

Enumeration Complete

The option at the top of the screen allows you to configure the application for anonymous connections. If you select this option, when a user attempts to start the application, a special *anonymous account* is used to create the session instead of the user's account. There are 15 anonymous accounts created when MetaFrame XP is installed on a member or stand-alone server. These accounts are named anon000–anon014.

Once you click Finish, the application is published on the servers selected in the wizard and appears in the Applications node. From there, you can modify the published application settings and control access to the application. If you right-click the published application and choose Properties, you can configure any of the options that were presented during the initial Application Publishing Wizard. There is one additional option included in the Properties sheet of the published application that was not available during the wizard, however, and that is the Disable Application check box on the Application Name tab, as shown in Figure 9.17. Selecting this check box turns off the application, preventing any user from starting the application until it is enabled again.

**FIGURE 9.17** Disabling an application



These settings specify the display name, application name, and description for the application. Select Disable Application to make the application unavailable to users.

Display Name: Notepad

Application Name: Notepad

☑ Disable Application

Application Description: Barebones Word Processor

Here are a few points to consider when publishing an application:

**Applications can be installed on all servers in the server farm.** Any application that you want to install can be installed on a single MetaFrame server if you want that server to be the only one to run the application, on multiple servers if you want to provide access to the application across multiple servers for load balancing, or on every server in your environment.

**Applications can be published on all servers where they are installed.** Any MetaFrame server that has the application installed can have the application published on it. The application does not have to be published on a server, but to be published it has to be installed.

**Applications published on MetaFrame XPs do not participate in load balancing.** MetaFrame XPs does not have the ability to participate in load balancing, so any client wanting to access the published application needs to connect directly to the server.

**Applications published on MetaFrame XPa or XPe servers participate in load balancing.** MetaFrame XPa and XPe take advantage of the load-balancing feature built into those products. Load evaluators are automatically assigned to servers, and the clients are directed to the server with the lightest load.

**You can create folders to organize published applications.** You can create folders within the Applications node of the Citrix Management Console and organize applications within the folders. If you have two applications that require the same display name, you will need to publish the applications and place them in different folders. You can move applications to a folder by dragging the application to the new folder. Folders are for administrative organizational purposes only and are not reflected in Program Neighborhood.

**Do not publish applications across WAN links.** If you want to minimize the amount of traffic consumed on your wide area network links, you should not publish applications so that they can be accessed across the WAN link.

**MetaFrame cannot publish video files.** VideoFrame was used with MetaFrame 1.8 to distribute video files to users. MetaFrame XP does not support VideoFrame and will not publish the files.

NOTE

For more information on restricting access to published applications in a load-balanced environment, see Chapter 7, "Load Management."

## Mixed-Mode Publishing

Server farms that are in mixed mode have special requirements, especially when it comes to publishing applications. The Citrix Management Console can publish applications only for MetaFrame XP servers. If you want an application available on both the MetaFrame 1.8 and MetaFrame XP platforms, you will need to publish the application twice, once for each platform. One item of note: You should publish the application on the MetaFrame 1.8 servers first. If it is published on the MetaFrame XP servers prior to being published on the MetaFrame 1.8 servers, Published Application Manager will not be able to publish the application in the farm using the same name as the MetaFrame XP published application. Management of the applications follows the same rules. Applications published on MetaFrame XP servers can be managed only from the Citrix Management Console, while those published on MetaFrame 1.8 servers must be managed using Published Application Manager.

## Managing Published Applications

Certain tasks can become tiresome for an administrator, and publishing applications using the Application Publishing Wizard is one of them. Most administrators would rather go directly to the Properties sheets of an object to configure it. Unfortunately, there is no option to create a blank object to configure the way you want the application to be. However, there is a nice shortcut that you can use when publishing an application: a template.

A *template* is a generic object that can be copied and configured for use. To create a template object, follow the steps of the Application Publishing Wizard to create a bogus object. Disable this bogus published application so that no one sees it in their Program Neighborhood. Once you have your template created, you can copy the template and use this copy for your published application. Simply right-click the template and choose Copy Published Application. If you were to copy your Notepad published application, you would see a Copy Of Notepad icon show up in the Applications node. You can then open the properties of the application and make the changes to the Properties sheets to reflect the new application. Make sure you enable the newly created published application when you have finished configuring it.

When a published application is no longer needed, you can unpublish it by deleting the entry. Once the entry has been deleted, the application will no longer be published on any server that the entry covered. To delete a published application, right-click the entry within Citrix Management Console, and select Delete Published Application or press the Delete key. Once it is deleted, any icons that were pushed down to the user's desktop will be removed the next time the user logs in to the server farm. Do note that the application files are not removed from the server; only the entry within the Citrix Management Console is removed. You can publish the application again at any time until the application files have been removed.

Now that we have installed our applications and published them for users to access, our MetaFrame XP servers are ready to allow users to start sessions. Since we have taken a good look at the server side of MetaFrame XP, we are ready to move on and examine the client's features. From here on out, we will be configuring and managing client software.

# Summary

In this chapter, we took a look at how to install and configure applications for users to access. From manual installs to using Installation Manager, we looked at the benefits of installing the applications on a MetaFrame system and showed how to streamline the process if multiple servers need to have the application installed on them.

Then we looked at publishing applications and controlling access to those published applications. In doing so, we allowed our users to access applications on all of the servers in our environment and allowed the applications to be load balanced when MetaFrame XPa or XPe is used.

Throughout the preceding chapters and including this one, we have concentrated on the server side of MetaFrame XP. In the following chapters, we will concentrate on the client side and show how to manage client sessions and perform troubleshooting.

# Exam Essentials

**Understand the benefits of installing and publishing applications on a MetaFrame XP server.** When an application is installed on a MetaFrame XP server, all users who can access the server will have access to the application if they have been given permissions to it. Also, any upgrades are performed at the server; upgrading once automatically upgrades all users.

**Know what is needed to install an application.** When installing an application, you need to make sure you have the application's setup software, any transform files, and application compatibility scripts.

**Know the difference between install mode and execute mode.** Install mode allows an administrator to install an application while the operating system monitors the changes made to the user environment. Execute mode allows users to run individual sessions on the server.

**Know the components of Citrix Installation Manager.** The packager is loaded onto a workstation to record changes to the system as an application is installed. It creates a file known as a package, which is used by the installer service to install the application automatically on multiple servers. The administrative add-in is a new node that appears in Citrix Management Console to be used to administer the packages and applications installed using this service.

**Know how to publish an application.** When an application is published, the servers that the application is loaded on are notified of how the application can be accessed as well as which users are allowed to access it.

**Understand what happens when a published application is deleted.** When a published application is deleted from the Citrix Management Console, the application software is not uninstalled; the application is simply no longer accessible from Program Neighborhood.

**Understand what a template is.** A template is a bogus published application that is used as a shortcut to create a published application. Most administrators find copying a template and configuring it with the appropriate settings faster than going through the Application Publishing Wizard.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

- Add/Remove Programs
- administrative plug-in
- anonymous account
- application compatibility script
- application deployment file
- application installation mode
- execution mode
- install mode
- installer service
- packager
- publishing
- template
- transform file
- Windows Installer package

# Exercise

In this exercise, we will install an application for multiple users and publish the application. Then we will give a group access to the published application.

## EXERCISE 9.1

### Installing an Application

To install an application for multiple users, follow these steps:

1. Download Adobe Acrobat Reader from `www.adobe.com` if you do not already have it installed.
2. Choose Start ➢ Settings ➢ Control Panel.
3. Run the Add/Remove Programs utility.
4. Choose Add New Programs from the left side of the window.
5. Click the CD Or Floppy button.
6. When the Install Program From Floppy Disk Or CD-ROM window appears, click Next. The Add/Remove Programs utility will automatically look for a program named `setup.exe` in the floppy drive

**EXERCISE 9.1 *(continued)***

and the CD-ROM drive. If it does not find a program named `setup.exe`, you can define a setup program by clicking Browse.

7. Since our setup program is not labeled `setup.exe`, click Browse and migrate to the directory where you downloaded the Adobe Acrobat Reader Setup program.

8. This portion of Add/Remove Programs also looks for a program named `setup.exe`. If the name of the setup program is something different, you will have to change the Files Of Type entry from Setup Program to Program.

9. When the name and path of the setup program appear in the Open dialog box, click Next.

10. The installation of Acrobat Reader begins. Install Reader, and when prompted for setup options, choose the install location and setup options you prefer. When the installation is complete, the After Install window appears. It is important to make sure the installation is complete before clicking the Next button.

11. Click Next to close the After Install screen.

12. Click Finish to close the Finish Admin Install screen.

To publish the application, follow these steps:

1. Start Citrix Management Console and log on as a Citrix Administrator.

2. Under the farm name, right-click the Applications node and select Publish Application to open the Application Publishing Wizard.

3. In the Display Name field, type **Acrobat Reader**.

4. In the Description field, type **Published Reader Application**.

5. Click Next.

6. Make sure the Publish Application radio button is selected, and type in the path to the executable or click Browse and browse to the executable.

7. Click Next.

8. On the Program Neighborhood Settings window, click Next.

**EXERCISE 9.1** ***(continued)***

9. On the Specify Application Appearance window, set the screen size and color depth to your preference and click Next.
10. On the Specify ICA Client Requirements window, click Next.
11. In the Specify Servers window, select your server from the list of available servers, click Add to add it to the list of Configured Servers, and then click Next.
12. In the Specify Users window, select the domain or server from the pull-down list containing the user accounts you would like to add.
13. Select the users or groups you would like to give access to the application, and click Add.
14. After you have added users and groups to the Configured Accounts section of the Specify Users window, click Finish.

Finally, to give a group access to the published application, follow these steps:

1. Start the Citrix Management Console, and log on as a Citrix Administrator.
2. Under the farm name, expand the Applications node.
3. Right-click the Acrobat Reader published application, and select Properties.
4. Select the Users tab of the Properties sheet.
5. In the Look In field, select your domain or server from the pull-down list.
6. In the Available Accounts window, place a check in the check box labeled Show Users.
7. In the Available Accounts window, select any group.
8. Click Add.
9. The group name should now appear in the Configured Accounts window.
10. Click OK to close the published application's Properties sheet.

# Review Questions

1. If you would like to install an application and let the users have application settings that they can change without affecting the other users' settings, how should you install the program?

   **A.** Navigate to the setup program for the application and double-click the program.

   **B.** Run the Add/Remove Programs utility in Control Panel.

   **C.** Use the Citrix Management Console to define the setup program.

   **D.** From the Start menu, choose Run. Then type the path of the setup program in the Run dialog box.

2. You installed an application on your MetaFrame XP server. Soon after that, you notice that the settings you defined the last time you ran the program are no longer there. What could be the problem?

   **A.** The application is a 16-bit program.

   **B.** An application compatibility script was not run for the application.

   **C.** The application was not installed using the Add/Remove Programs utility.

   **D.** The application was not published using the Citrix Management Console.

3. Which of the following must you do in order to install an application for multiple users? (Choose all that apply.)

   **A.** Make sure that Terminal Services on the Windows 2000 Server is configured to run in application server mode.

   **B.** Disable new logons to the MetaFrame server.

   **C.** Install the program using Installation Manager.

   **D.** Install the program using the Add/Remove Programs utility.

4. What is the name of the file that modifies the behavior of the Microsoft Software Installation (MSI) package?

   A. Microsoft transform file (MSF)

   B. Microsoft transfer file (MTF)

   C. Multiple transform file (MTF)

   D. Microsoft transform file (MST)

5. You are installing an application through the Add/Remove Programs utility. When the application completes, it asks you if you would like to reboot. What should you do at this step?

   A. Let the computer reboot. Installation will finish when the computer restarts.

   B. Choose to not reboot, and then click Finish.

   C. Choose to not reboot, but don't click Finish. Manually reboot the server, and the installation will finish when the computer restarts.

   D. Press Ctrl+Alt+Delete and end the Add/Remove Programs task. Then reboot the computer manually.

6. What is the name of the utility that automates the installation of applications to other servers in the farm?

   A. Installation Manager

   B. Application Manager

   C. Application Installation Manager

   D. Installation Configuration

7. If an application was installed on a server using Citrix Installation Manager, what is the best way to remove it from a server?

   A. Through the Add/Remove Programs utility

   B. Through the Application Publishing Wizard

   C. Through the Citrix Management Console

   D. Through the uninstall program that comes with the application

8. The Application Publishing Wizard can publish which of the following applications? (Choose all that apply.)

   A. Windows 32-bit applications

   B. POSIX applications

   C. OS/2 applications

   D. Macintosh applications

9. ICA Clients retrieve information from the Application Publishing Wizard about which of the following? (Choose all that apply.)

   A. Application location

   B. Type of application

   C. Servers that host the application

   D. Users with permission to access the application

10. In mixed mode, how are published applications handled between MetaFrame 1.8 and MetaFrame XP servers?

   A. Published applications are shared between all defined servers, whether they are MetaFrame 1.8 or MetaFrame XP servers. The published applications can be managed with Citrix Management Console.

   B. Published applications are not shared between servers. The applications should be published on both the MetaFrame 1.8 and MetaFrame XP servers. The published applications can be managed with Citrix Management Console.

   C. Published applications are shared between all defined servers, whether they are MetaFrame 1.8 or MetaFrame XP servers. Published Application Manager must be used to manage published applications on the MetaFrame 1.8 servers, and Citrix Management Console must be used to manage published applications on the MetaFrame XP servers.

   D. Published applications are not shared between servers. The applications should be published on both MetaFrame 1.8 and MetaFrame XP servers. Published Application Manager must be used to manage published applications on the MetaFrame 1.8 servers, and Citrix Management Console must be used to manage published applications on the MetaFrame XP servers.

**11.** Your network consists of four MetaFrame XP servers and two MetaFrame 1.8 servers. You want to publish a video file using Citrix VideoFrame. What is the best way to publish the video file among the different servers?

**A.** Publish the video file on the two MetaFrame 1.8 servers and two of the MetaFrame XP servers.

**B.** Publish the video file on the four MetaFrame XP servers only.

**C.** Publish the video file on all MetaFrame servers.

**D.** Publish the video file on the two MetaFrame 1.8 servers only.

**12.** If you publish an application with the Citrix Management Console while your server farm is in mixed mode, which utility can you use to manage the published application?

**A.** Citrix Management Console

**B.** Published Application Manager

**C.** Citrix Server Administrator

**D.** Citrix Connection Configuration

**13.** In the Properties sheet of a published application, which tab would you navigate to if you wanted to disable the application?

**A.** Program Neighborhood Settings

**B.** ICA Client Options

**C.** Application Name

**D.** Application Location

**14.** You want to add a published application's shortcut to a user's desktop. What is the best way of doing this?

- **A.** For each user, go to the user's desk, log on as that user, and open Citrix Program Neighborhood. Right-click the application and choose Create Desktop Shortcut.
- **B.** Shadow each user and open Citrix Program Neighborhood. Right-click the application and choose Create Desktop Shortcut.
- **C.** In the Program Neighborhood Settings tab of the application's Properties sheet, place a check in the Add Shortcut To Client's Desktop check box.
- **D.** In the Application Location tab of the application's Properties sheet, place a check in the Add Shortcut To Client's Desktop check box.

**15.** You receive a call from a user reporting that sound is not working with his ICA session. You check all of his settings and find that he has a direct connection to one of the application servers. You also check the Custom Connection Settings screen and see that the check box that enables sound is checked. Why is the user unable to receive sound?

- **A.** Direct server connections cannot receive sound; only published applications can receive sound.
- **B.** The Custom Connection Settings screen in Program Neighborhood has sound enabled, but the individual server connection does not.
- **C.** The published application is not configured for sound.
- **D.** The bandwidth connection is not sufficient.

**16.** You have a published application on your server called TimeLog. It is published on all of your servers, and the path on each server is `d:\apps\timelog`. Another administrator installs a new server into the farm and wants to add that server to the list of servers that host the application. The administrator installed the TimeLog application to `d:\program files\timelog`. How can you add the server to the list of servers that host the TimeLog application even though it points to a different location?

**A.** In the Application Location tab of the published application's Properties sheet, highlight the server in the Configured Servers list and click Edit Configuration. Then change the command line and working directory from there.

**B.** In the Servers tab of the published application's Properties sheet, highlight the server in the Configured Servers list and click Edit Configuration. Then change the command line and working directory from there.

**C.** Do nothing. The server will find all instances of the executable.

**D.** In the Application Name tab of the published application's Properties sheet, highlight the server in the Configured Servers list and click Edit Configuration. Then change the command line and working directory from there.

**17.** If you select Allow Anonymous Connections in the Users tab of the published application's Properties sheet, what account will be used for the anonymous user connections?

**A.** anon*XXX* (where *XXX* represents a number between 000 and 014)

**B.** guest

**C.** anon

**D.** guest*XXX* (where *XXX* represents a number between 000 and 014)

**18.** Which tab in the published application's Properties sheet would you use to access the Encryption settings for a published application?

**A.** Application Name tab

**B.** Encryption tab

**C.** ICA Client Options tab

**D.** Program Neighborhood Settings tab

19. A user is connecting to a published application that has a minimum requirement encryption setting of RC5 (56 bit). The user cannot make a connection and realizes that she only has RC5 (40 bit) encryption. How would you change it on the server so this user can connect? (Choose all that apply.)

    A. In the Encryption area of the ICA Client Options tab, uncheck the check box labeled Minimum Requirement.

    B. In the Encryption area of the ICA Client Options tab, choose a higher encryption setting.

    C. In the Encryption area of the ICA Client Options tab, choose a lower encryption setting.

    D. In the Encryption area of the ICA Client Options tab, check the box labeled Downgrade Encryption For Authenticated Users.

20. Your network consists of a Windows 2000 network and a Novell network. You have the Novell Client for NT installed on your MetaFrame server, and your Novell password is different from your Windows 2000 password. You have published an application that requires mappings to a drive on the Novell network. When you connect to the published application, your name and password used for Program Neighborhood are passed to the server and you are not getting your Novell network mappings. How can you make sure that your users receive the Novell login screen when you connect to the published application?

    A. In Citrix Management Console, right-click the application. Choose the Settings tab and place a check in the check box labeled Login To Server.

    B. In Citrix Management Console, right-click the application. Choose the Settings tab and remove the check from the check box labeled Use Program Neighborhood Username And Password.

    C. In the Citrix Connection Configuration utility, open the connection you want to change. Click the Advanced button. In the Auto Logon section of the window, place a check in the check box labeled Prompt For Password.

    D. In the Citrix Connection Configuration utility, open the connection you want to change. Click the Advanced button. In the Auto Logon section of the window, remove the check from the check box labeled Use Program Neighborhood Username And Password.

# Answers to Review Questions

1. B. Use the Add/Remove Programs utility in Control Panel to install the application. This utility puts the Windows 2000 Server in install mode and allows the server to keep track of user-specific application Registry entries and installation (INI) files.

2. C. If you do not install the application using the Add/Remove Programs utility, you install the application for a single user only. If you install an application for a single user, other users can run the application but will use the same copy of the application's settings. If the user changes an application setting in this configuration, the new setting will be used for all other users of the application.

3. A, B, D. The Windows 2000 Server must be in application server mode before you can install applications for multiple users. You must then disable new logons and use the Add/Remove Programs utility to install the program.

4. D. A transform file (MST) modifies the behavior of the MSI package so that an administrator can customize the installation.

5. B. Some apps require a reboot after the installation is complete. Do not allow the application to reboot the server until you select Finish. Selecting Finish allows the system to complete its application tracking and safely record the changes.

6. A. Citrix Installation Manager is an application installation product that simplifies the installation of applications and software components on MetaFrame XP servers in a server farm.

7. C. Do not use the Add/Remove Programs utility to uninstall an application installed by Citrix Installation Manager. Applications installed by Citrix Installation Manager can be uninstalled using the Citrix Management Console. Uninstalling the application using the Citrix Management Console allows the Citrix Installation Manager to keep track of its inventory.

8. A, B, C. The Application Publishing Wizard can publish Windows 32-bit, 16-bit, DOS, POSIX, and OS/2 applications, and server desktops.

9. A, C, D. The Application Publishing Wizard contains information about application location, servers supplying the application, users with permission to access the application, client settings, and minimum client requirements.

10. D. In mixed mode, load-balancing information and licensing information are shared between the server farms, but published applications are not. Applications should be published on both the MetaFrame 1.8 and XP servers. Citrix Management Console is used to manage published applications only on the MetaFrame XP server, and Published Application Manager is used to manage published applications only on the MetaFrame 1.8 server.

11. D. MetaFrame XP does not support VideoFrame 1.0. Video files cannot be published on a MetaFrame XP server. Videos can only be published on MetaFrame 1.8 servers using VideoFrame 1.0.

12. A. Applications published with the Citrix Management Console cannot be edited or deleted using the Published Application Manager, which is available in MetaFrame 1.8.

13. C. In the Application Name tab of the Properties sheet, place a check in the Disable Application check box when you want to prevent anyone from connecting to the application.

14. C. In the Program Neighborhood Settings tab of the published application's Properties sheet, placing a check in the Add Shortcut To The Client's Desktop check box adds a shortcut to the published application on the authenticated user's desktop.

15. A. In order for an application to receive sound, it must be a published application.

16. B. If you highlight a server in the Configured Servers list, you can edit the configuration. The Edit Configuration dialog box allows you to change the command line and working directory for the published application. This lets you publish applications on different servers that may have the same executable but in different locations.

17. A. Place a check in the box labeled Allow Anonymous Connections for the server to use one of the anon*XXX* accounts to run the application.

**18.** C. The settings in the ICA Client Options tab of the application's Properties sheet specify the encryption level to be used while you are connected via an ICA session. The options are Basic, RC5 (128 bit) logon only, RC5 (128 bit), RC5 (56 bit), and RC5 (40 bit).

**19.** A, C. If Minimum Requirement is selected on either of the two check boxes in the Encryption area of the ICA Client Options tab, an ICA Client must be able to run the minimum setting or the connection will be refused. If you remove the check mark, any connection will be accepted.

**20.** B. When you connect to a published application, the credentials that you entered to log in to Program Neighborhood are used. If you need to authenticate to another network that does not use the same username and password as the Program Neighborhood session, you must place a check in the check box labeled Prompt For Password in the Auto Logon section of the Advanced properties for the connection type.

Chapter

10

# ICA Client Software

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **8. Citrix ICA Client Software**

- 8a. Installing the Citrix ICA Client Software

Up to this point, we have concentrated on administering the MetaFrame XP servers. Starting with this chapter, we will be working with the client software and configuring the client to connect and work within a MetaFrame XP environment.

## Supported Clients

In Chapter 4, "Installing MetaFrame XP," we introduced a list of available clients for MetaFrame XP. If you look back at the list, you will notice that nearly every operating system that is still available for business use has client software. Those that do not have client software can take advantage of the web-based client.

While we are looking at the client software available, please note that not all features are available for all clients. All operating systems are not created equal and cannot perform the same functions. Take the Clipboard feature of the Windows family of operating systems, for example. This feature is not available from DOS-based workstations; thus Clipboard sharing is not available for that platform.

Tables 10.1 through 10.3 provide a comprehensive list of available features and all of the platforms at the time of the writing of this book. You should check Citrix Systems' website, `www.citrix.com`, for updated clients that may support features other than those listed here.

**TABLE 10.1** Protocols Available for Citrix Clients

| Protocol | DOS 32 | Win16 | Win32 | Win CE | Mac | Unix | Linux | EPOC | OS/2 | Java | IE | Netscape |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TCP/IP | × | × | × | × | × | × | × | × | × | × | × | × |
| IPX | × | × | × | | | | | | | | | |
| NetBIOS | × | × | × | | | | | | | | | |
| Serial | × | × | × | × | | | | | | | | |
| Modem | × | × | × | × | | | | | | | | |

**TABLE 10.2** ICA Client Redirection Features

| Feature | DOS 32 | Win16 | Win32 | Win CE | Mac | Unix | Linux | EPOC | OS/2 | Java | IE | Netscape |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Application Publishing | × | × | × | × | × | × | × | × | × | × | × | × |
| Audio Compression | × | × | × | × | × | × | × | × | | | | |
| Auto-Create Print Spooler | × | × | × | × | × | | | | | | × | × |
| Client Audio Mapping | × | × | × | × | × | × | × | × | | × | × | × |
| Client Auto-Update | × | × | × | | × | × | × | × | | | | |
| Client Clipboard Mapping | | × | × | × | × | × | × | × | × | × | × | × |
| Client COM Port Mapping | × | × | × | × | × | | × | × | × | × | | |
| Client Drive Mapping | × | × | × | ×[1] | × | × | × | × | × | × | × | × |
| Client LPT Mapping | × | × | × | × | | × | × | × | × | × | × | × |

**TABLE 10.2** ICA Client Redirection Features *(continued)*

| Feature | DOS 32 | Win16 | Win32 | Win CE | Mac | Unix | Linux | EPOC | OS/2 | Java | IE | Netscape |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Client Printer Creation | × | | | ×[2] | | | | | | | | |
| Client Spooler Mapping | × | × | × | ×[1] | × | × | × | × | × | | × | × |

[1] Win CE for Palm and HP
[2] Win CE for platforms other than Palm and HP

**TABLE 10.3** ICA Client Features

| Feature | DOS 32 | Win16 | Win32 | Win CE | Mac | Unix | Linux | EPOC | OS/2 | Java | IE | Netscape |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16-Color–Capable | × | × | × | × | × | × | × | × | | | × | × |
| 256-Color–Capable | × | × | × | × | × | × | × | × | | × | × | × |
| 16-Bit Color-Capable | | × | × | × | × | | ×[5] | | × | × | × | × |
| 24-Bit Color-Capable | | × | × | × | × | | ×[5] | | × | × | × | × |
| Basic Encryption | × | × | × | × | × | × | × | × | × | × | × | × |
| Client Auto-Reconnect | | | | ×[1] | | | | | | × | | |
| Data Compression | × | × | × | × | × | × | × | × | × | × | × | × |
| Floppy | × | × | × | × | ×[4] | × | × | | | | × | × |
| High Resolution | | × | × | × | × | | ×[5] | | × | × | × | × |
| Load Balancing | × | × | × | × | × | × | × | × | | × | × | × |

**TABLE 10.3** ICA Client Features *(continued)*

| Feature | DOS 32 | Win16 | Win32 | Win CE | Mac | Unix | Linux | EPOC | OS/2 | Java | IE | Netscape |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Multi-Session–Capable | | × | × | × | × | × | × | × | × | × | | |
| Panning | | | × | ×[1] | × | × | × | × | | | | |
| Persistent Cache | × | × | × | | × | × | × | | × | × | × | × |
| Printer Retention | × | × | × | × | | | | | | | × | × |
| Program Neighborhood | ×[3] | ×[3] | × | ×[3] | ×[3] | ×[3] | ×[3] | ×[3] | ×[3] | × | × | × |
| Remote Application Manager | × | × | | × | × | × | × | × | | | | |
| Scaling | | | × | ×[1] | | | | | | | | |
| Seamless Windows | | | × | | | | ×[5] | | | | | |
| Secure ICA | × | × | × | × | × | | ×[5] | | | × | × | × |
| Smart Card–Capable | × | × | × | | | | | | | | | |
| SOCKS-Capable | | × | × | ×[2] | × | | ×[5] | | | × | × | × |
| SpeedScreen Latency Reduction | | × | × | × | × | | ×[5] | | | × | × | × |
| Start Position Memory | | | × | | | | | | | × | × | × |
| TCP Browsing | | × | × | × | × | | ×[5] | | × | × | × | × |

[1] Win CE for Palm and HP.
[2] Win CE for platforms other than Palm and HP.
[3] Program Neighborhood is available through the ICA pass-through Client.
[4] PC floppy formatted with FAT is accessible if the Macintosh workstation has the appropriate extensions installed.
[5] Applicable only to Intel-based versions of Linux.

# Client Requirements

You should know the minimum hardware requirements for the client computers so that you are aware of the systems that can actually support the ICA Client software. Table 10.4 lists the minimum requirements for the client software based upon where it is installed. Review this list when you are determining which computer systems will be used as clients in a MetaFrame environment.

**TABLE 10.4** Minimum Client Requirements

| Client | Platform | Processor | Memory |
|---|---|---|---|
| Win32 | Windows 9*x*, Windows Me, Windows NT 3.5–4.0, Windows 2000 | 80386 or higher | Windows 9*x* - 8MB; 16MB for all others |
| Win16 | Windows 3.1 in enhanced mode, Windows for Workgroups version 3.11 | 80386 | 8MB |
| Macintosh | System 7.1[1] or later | 68030/040<br>PowerPC | 4MB |
| DOS* | DOS 16 and<br>DOS 32 | 80286[2]<br>386 DOS 32 | 2MB |
| Unix | [3] | [3] | 12MB |

* Extended memory required for DOS 16.
[1] Thread Manager must be added to System 7.1 systems.
[2] 80386 required for Secure ICA.
[3] Check individual operating system requirements in the *Citrix ICA Unix Client Administrator Guide*.

Of course, these are the minimum requirements. If you want the system to perform better, especially if you are attempting to run local applications while you are running sessions, you will want to increase all of the resources listed here. Now let's take a look at installing this software so your users will be able to access your MetaFrame servers.

# Client Software Installation

Various deployment methods are available for installing the client software on users' workstations. While each has its advantages, you will need to decide which one works best for your environment. We start this section with a discussion of the deployment methods, when you should use each one, and how to take advantage of each.

The files needed to install ICA Client software on a workstation can be found on the *ICA Client CD*. This CD ships with all of the versions of MetaFrame XP. The files can also be found on the Citrix Systems website. If you are looking for the most recent files, you should look to the website. Citrix Systems updates the site at regular intervals with any new versions of the client. Later in this chapter, we will look at the *ICA Client Update Database* and show how it can be used to keep our clients up-to-date with the latest client software.

You can also use this CD to install ICA Client software on workstations equipped with CD-ROM drives. While this is not the most efficient method of installing the client software, you do have all the different client types on one disk. If you are planning to copy the client installation files to the server using the ICA Client Distribution Wizard, you will need to have this CD available. Place the CD in the CD-ROM drive, and from the Start menu navigate to Programs ➤ Citrix ➤ MetaFrame XP ➤ ICA Client Distribution Wizard. When the wizard starts, it will prompt you to choose which client types you wish to include on the server. All of the files will be copied to the `%systemroot%\system32\Clients\ICA` directory of the MetaFrame server.

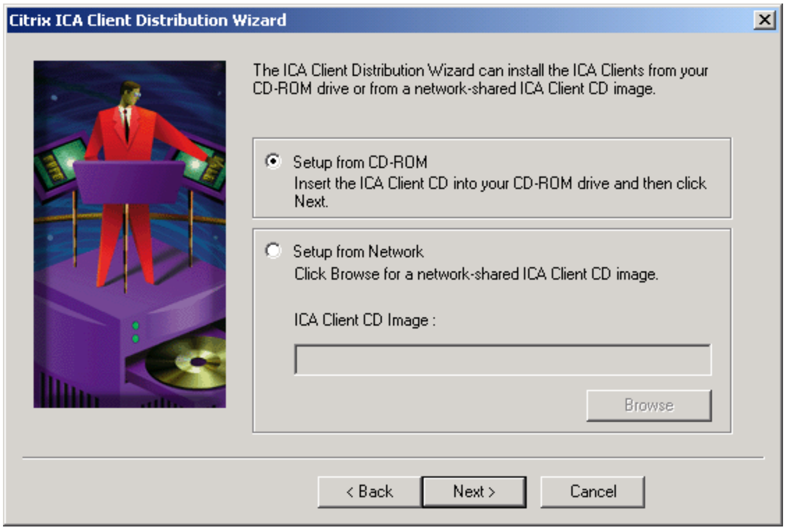
Figure 10.1 displays the second screen of the Citrix ICA Client Distribution Wizard. If you are using the ICA Client CD, you can leave the default option, Setup From CD-ROM, selected, which will copy the files directly from the CD. If you are upgrading the installation files or copying them from a shared network location, select the other option, Setup From Network, and specify the path to the files.

If you choose to copy the files from the CD, the next screen you are presented with lets you choose whether to perform a *Typical install* of the client files or a *Custom install*. If you choose Typical, then all of the clients will be added to the server, and the ICA Client Update Database will be installed with all of the clients added to it.

NOTE

Look for more information about the ICA Client Update Database later in this chapter.

**FIGURE 10.1** Selecting the source location for the client installation files



The ICA Client Distribution Wizard can install the ICA Clients from your CD-ROM drive or from a network-shared ICA Client CD image.

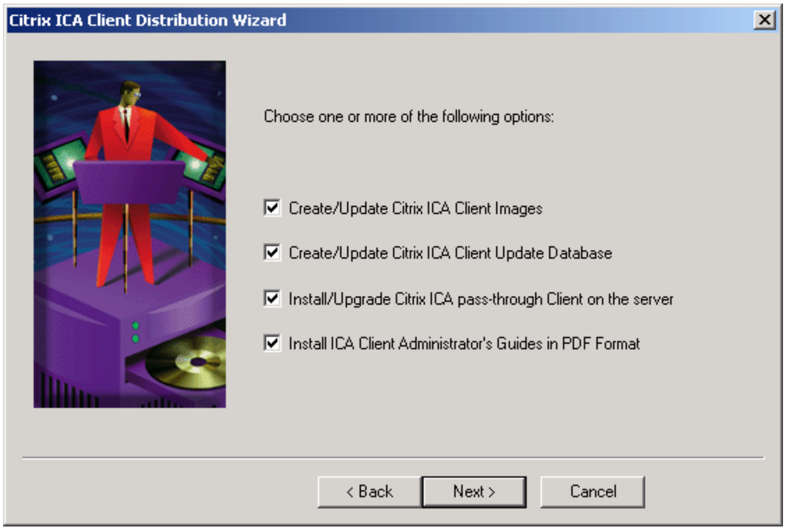
● Setup from CD-ROM
Insert the ICA Client CD into your CD-ROM drive and then click Next.

○ Setup from Network
Click Browse for a network-shared ICA Client CD image.

ICA Client CD Image :

If you choose a Custom install, you will be prompted for the options you wish to install. This option comes in very handy when you do not need to supply certain clients such as Unix clients. After selecting the Custom option and clicking Next, you will be presented with a screen telling you to choose which options you would like to configure, as shown in Figure 10.2.

**FIGURE 10.2** Custom install options



Choose one or more of the following options:

☑ Create/Update Citrix ICA Client Images

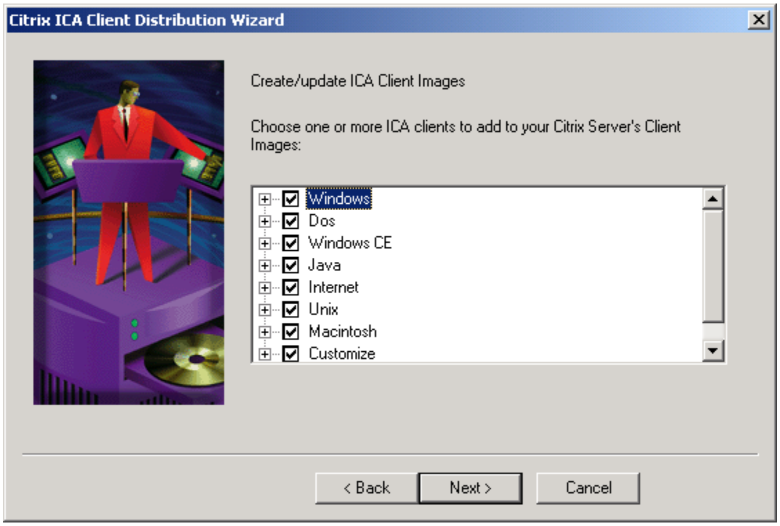
☑ Create/Update Citrix ICA Client Update Database

☑ Install/Upgrade Citrix ICA pass-through Client on the server

☑ Install ICA Client Administrator's Guides in PDF Format

Of the four options shown here, selecting either of the first two brings up further options. Checking the Create/Update Citrix ICA Client Images check box causes the screen found in Figure 10.3 to appear. From here, you can select only the ICA Client types you wish to install. If you check the second option, Create/Update Citrix ICA Client Update Database, the files necessary to create the database will be installed and you will be prompted to decide which ICA Clients to add to the database, as shown in Figure 10.4.

**FIGURE 10.3** Creating client images



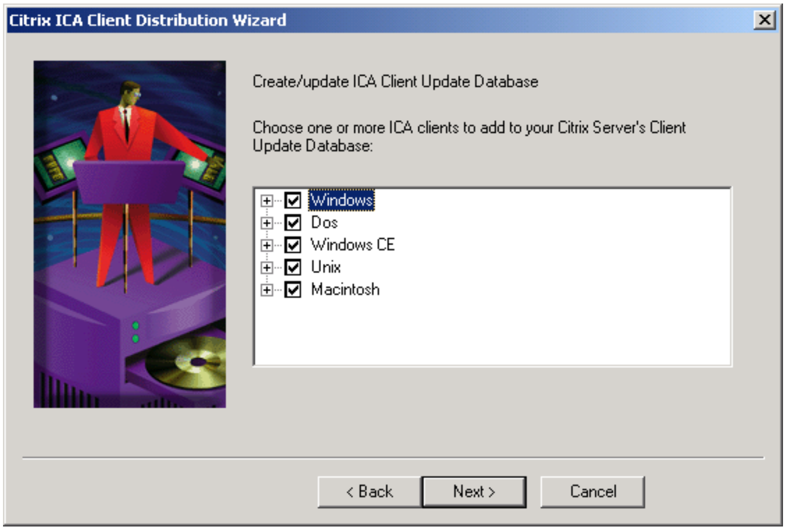
Create/update ICA Client Images

Choose one or more ICA clients to add to your Citrix Server's Client Images:

- ☑ Windows
- ☑ Dos
- ☑ Windows CE
- ☑ Java
- ☑ Internet
- ☑ Unix
- ☑ Macintosh
- ☑ Customize

If you choose a Typical install, or choose the Install/Upgrade Citrix ICA Pass-Through Client On The Server option while performing a Custom install, the *ICA pass-through Client* is installed on the MetaFrame server. This special client gives users access to the full range of benefits that Program Neighborhood has to offer, even if they do not have a client that has all of the functionality of Program Neighborhood. To take advantage of the ICA pass-through Client, Program Neighborhood is published just as if it were any other application. When a client starts a session to run Program Neighborhood, they will have access to all of the applications within the server farm that they have been given permission to use. The user will be able to take advantage of load-balanced applications in this manner also.

**FIGURE 10.4** Creating the Client Update Database



Create/update ICA Client Update Database

Choose one or more ICA clients to add to your Citrix Server's Client Update Database:

- ☑ Windows
- ☑ Dos
- ☑ Windows CE
- ☑ Unix
- ☑ Macintosh

NOTE For more information on Program Neighborhood, see Chapter 11, "Program Neighborhood."

Finally, if you select the last option, Install *ICA Client Administrator's Guides* In PDF Format, files with information concerning the modification and use of the different types of ICA Clients are installed on the server. These files are installed in the `C:\Program Files\Citrix\Documentation\ICA CLIENTS` directory by default. Share this directory if you want these files to be accessible from other computers. This way, you will have the documentation handy wherever you are. You will need Adobe's Acrobat Reader in order to view these files, so you may want to download the installation program and either publish the application from the server or install the Reader on the client workstations.

Once the files have been installed on the server, you are ready to deploy the ICA Clients to the users' workstations. There are various ways to perform the deployment. Let's examine the methods available.

## Deployment Methods

Citrix has created three deployment methods for installing the ICA Client software: using a web browser, downloading from a share point, and using installation disks. Of the three methods, most administrators are probably well versed in the latter two options but may not be familiar with the first option, using a web browser. Using a web browser can make it easier for an administrator of a large organization, or an organization that is providing Application Service Provider (ASP) functions, to deliver and install the client software. Let's take a look at the advantages of each of these methods and how the installation is performed.

## Installation Disks

Using *installation disks* is probably the most time-consuming method of the three. When you use this method, not only is the install slow due to the read time of the disk, but someone—usually the network administrator—has to deliver the disks to the workstation and perform the install. In a small network environment, this may not be an issue, but in larger networks, it becomes troublesome to take the time to visit each client workstation.

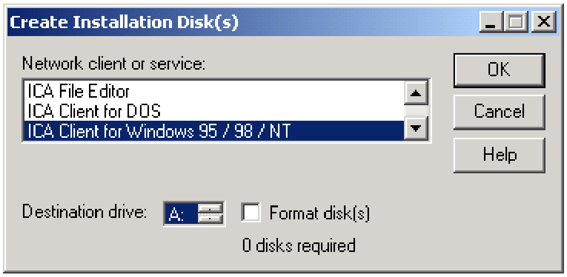
You create the installation disks by running the *ICA Client Creator* utility. Using this utility, you can create disks to install the client on the following platforms: DOS, Windows 3.*x*, Windows 9*x*, Windows Me, Windows NT 3.*x*/4.0, and Windows 2000. The client installation files for other platforms are also available, but you will have to access the files from the `%systemroot%\system32\clients\ica` directory.

For the files to be available in this directory and the ICA Client Creator utility to be available, you will need to run the ICA Client Distribution Wizard. This wizard steps you through copying the files from the ICA Client CD onto a MetaFrame XP server. Of course, you need to perform this step only if you did not install these files during the installation of the server. Once the files have been copied to the server, a shortcut will appear on the Start menu under Programs ➢ Citrix ➢ MetaFrame XP ➢ ICA Client Creator.

As you start the ICA Client Creator, you will be presented with a dialog box that displays the number of disks you will need depending on the client type you are installing. Figure 10.5 displays the information shown when the Win 95/98/NT client is selected. The dialog box also lets you select which drive you will use to create the disks. If you need to format the disks prior to having the client files copied to them, you can select the check box next to Format Disk(s).

Once you click OK, you will see prompts telling you to insert disks into the disk drive you specified. For each disk required, you will receive another prompt stepping you through the process. Once all of the disks are created, you can deliver them to the workstation where you want to install the ICA Client software.

**FIGURE 10.5** The Create Installation Disk(s) dialog box



## Download from a Network Share Point

One of the most beneficial aspects of having a network operating system is the ability to rather easily share information. You can take advantage of this capability and access the client installation files from a *network share*. If you installed the ICA Clients during the installation of MetaFrame XP, the files are already on the server. If you did not copy them, you can insert the Client CD and run the ICA Client Distribution Wizard.

Once the files are copied to the server, you can share each individual client type under the `%systemroot%\system32\clients\ica` folder. You will need to supply the path to the setup files for the appropriate client. For example, if you have shared the `ICA32` folder on the server Rosebud as `ICA32`, and you want to install the Win32 client on a Windows NT Workstation 4.0, you will need to navigate to `\\Rosebud\ICA32\disk1\setup.exe`. Table 10.5 shows each folder and the client types each one supports.

**TABLE 10.5** ICA Client Installation File Folders

| Folder | Client Type Supported |
|---|---|
| `ICA16` | Windows 3.*x* |
| `ICA32` | Windows 9*x*/Me/NT/2000 |
| `ICADOS32` | DOS clients |
| `ICAJAVA` | Java-based client for most operating systems |
| `ICAMAC` | Client for Macintosh operating systems |

**TABLE 10.5** ICA Client Installation File Folders *(continued)*

| Folder | Client Type Supported |
|---|---|
| `ICAUNIX` | Subfolders within this folder hold installation scripts for most Unix and Linux operating systems. |
| `ICAWEB` | Clients for most web browsers |
| `ICAWINCE` | Client files for Windows CE–based operating systems |

## Web Browser

While most administrators will take advantage of NFuse when they want to use MetaFrame in a web-based environment, you can still configure your own web server to dispense the web-based client files. You will need to know how to configure your own web server and design a web page so that your users can access the files. Sample pages are located on the NFuse CD in the *`WebInst` directory*. The client installation files are located in the *`icaweb` directory* on the ICA Client CD. If you have previously run the Citrix ICA Client Distribution Wizard, this directory will reside on your server.

If NFuse is installed in your environment, then most of the work required to create the website is done automatically for you. If you are using NFuse, you will need to place the clients in the web server's publishing directory. For example, if you have the English version of Win32, the directory that it would point to is `C:\Inetpub\WWWRoot\NfuseClients\en\ICA32`. The NFuse web page will detect if a client is already installed. If not, the default NFuse web page will detect the platform of the client device and the browser being used. The files will be downloaded and installed and the user will eventually be presented with the client software based on what was detected for the platform and browser type.

NOTE

For more information concerning NFuse, see Chapter 12, "Web Connectivity and NFuse."

Web-based installations are the easiest to control in a large environment. Users can simply connect to the web server to have the installation files delivered to their workstations. While the other two methods are still viable, they are not as flexible as this method. Most users understand how to connect to a web page since the Internet has become an integral part of our lives.

## Updating the ICA Clients

Unfortunately, the ICA Client software is just that, software. From time to time, software needs to be updated, either to correct a problem with the code or to allow the software to interact with new features. Therein lies the problem. As the software is updated, you must deliver it to your workstations. Citrix has provided a utility to assist in the delivery of updated client software—the *ICA Client Update Configuration*.

The primary tool used with the ICA Client Update Configuration is the Citrix ICA Client Update Database. If you performed a Typical installation of the ICA Client files or selected the option Create/Update Citrix ICA Client Update Database during a Custom install, the database will exist on the server and will contain the files from the ICA Client CD or the network share from which you installed them. As new client versions become available, you can add them to the database. Databases can be configured for an individual server or you can use the same database for multiple servers by specifying the path to the shared database on a server.

If this database exists, MetaFrame servers will use it to determine whether or not a user has the most recent version. Before the user is allowed to log on to a MetaFrame server, the server will query the user's ICA Client to determine which client version is in use. If the version in use by the client is different than the version in the database, and depending on the option set within the database, the user's software version can then be updated and the user can log on. If the update version was set to update only older clients, a client that has the same version or a newer version will receive no notification of any kind and will continue working like normal.

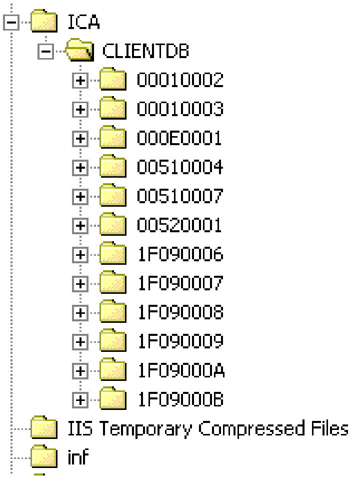
There are several options available to fine-tune the installation of the ICA Client software. You can control whether or not the user is notified that an update is about to be performed, you can indicate whether or not the user can proceed with their work while the new files are installed in the background, and you can even override a newer update version with an older version. All of these features work independently of the transport type in use by the client.

Citrix utilizes a hexadecimal identification scheme for the different versions of ICA Clients. Table 10.6 lists the clients for the various platforms and the product and model numbers for each. If you look at the directory structure that is created when the ICA Client Update Database is installed, you will see folders that mimic the product number/model number scheme presented here. Figure 10.6 shows the folder structure as viewed in Windows Explorer.

**TABLE 10.6** ICA Client Type, Product Number, and Model Number

| Client Type | Product Number | Model Number |
|---|---|---|
| 16-bit DOS | 1 | 1 |
| Win16 | 1 | 2 |
| Win32 | 1 | 3 |
| 32-bit DOS | E | 1 |
| Macintosh | 52 | 1 |
| Win CE *x*86 | 1F09 | 6 |
| Win CE SH3 | 1F09 | 7 |
| Win CE SH4 | 1F09 | 8 |
| Win CE MIPS | 1F09 | 9 |
| Win CE PPC | 1F09 | A |
| Win CE ARM | 1F09 | B |
| Linux | 51 | 7 |

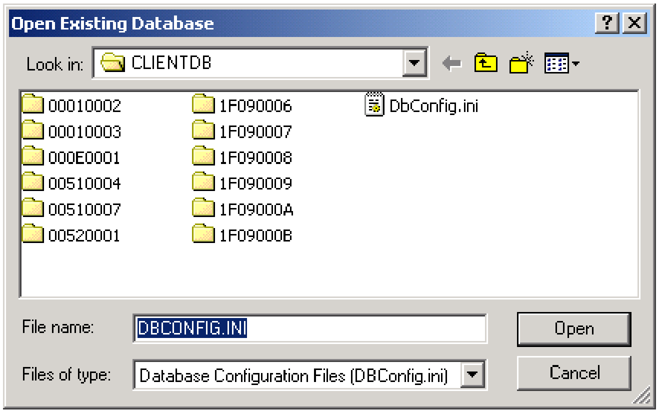
**FIGURE 10.6** The ICA Client Update Database file system folder location



## Configuring the Database

Let's take a look at this utility and see how we can configure it for our environments. To open the database, go to the Start menu and navigate to Programs ➢ Citrix ➢ MetaFrame XP ➢ ICA Client Update Configuration. When the utility opens, if you have not designated a default database, you will be prompted to specify the database. Figure 10.7 displays the dialog box that you are presented with. The default path for the database is `%systemroot%\ICA\ClientDB`. The file that the database is looking for is `DBConfig.ini`.

**FIGURE 10.7** Selecting the database



Open Existing Database

Look in: CLIENTDB

00010002
00010003
000E0001
00510004
00510007
00520001
1F090006
1F090007
1F090008
1F090009
1F09000A
1F09000B
DbConfig.ini

File name: DBCONFIG.INI

Files of type: Database Configuration Files (DBConfig.ini)

Figure 10.8 shows the utility after the database path has been selected. Note that all of the client types displayed here are those that were chosen when the ICA Client Distribution Wizard was run. Use the View menu to change the size and amount of information displayed in the window. We prefer to use the Details option since it provides the most information, but you may choose your own setting based on your preferences. Figure 10.9 shows the utility in Details view. In this view, all of the version information, along with the product and model number, is shown.

**FIGURE 10.8** The populated database

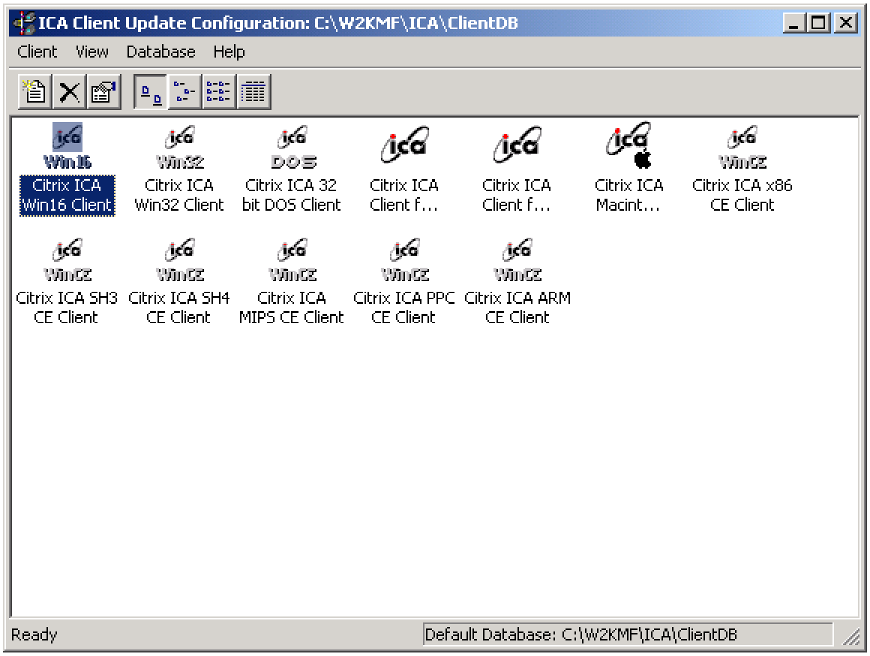
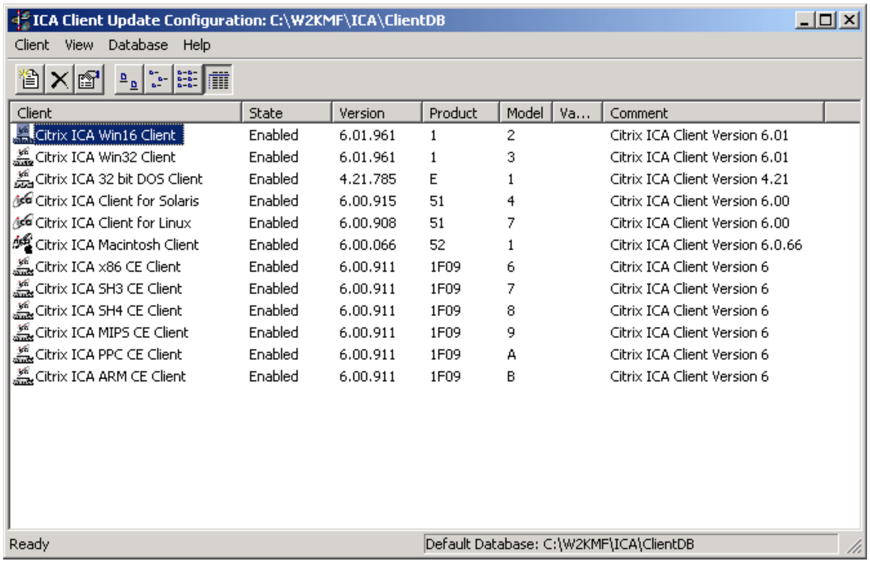


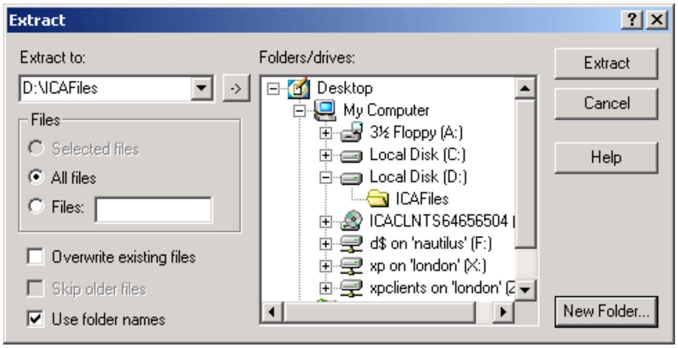
**FIGURE 10.9** The Details view of the database


ICA Client Update Configuration: C:\W2KMF\ICA\ClientDB
Client View Database Help

| Client | State | Version | Product | Model | Va… | Comment |
|---|---|---|---|---|---|---|
| Citrix ICA Win16 Client | Enabled | 6.01.961 | 1 | 2 | | Citrix ICA Client Version 6.01 |
| Citrix ICA Win32 Client | Enabled | 6.01.961 | 1 | 3 | | Citrix ICA Client Version 6.01 |
| Citrix ICA 32 bit DOS Client | Enabled | 4.21.785 | E | 1 | | Citrix ICA Client Version 4.21 |
| Citrix ICA Client for Solaris | Enabled | 6.00.915 | 51 | 4 | | Citrix ICA Client Version 6.00 |
| Citrix ICA Client for Linux | Enabled | 6.00.908 | 51 | 7 | | Citrix ICA Client Version 6.00 |
| Citrix ICA Macintosh Client | Enabled | 6.00.066 | 52 | 1 | | Citrix ICA Client Version 6.0.66 |
| Citrix ICA x86 CE Client | Enabled | 6.00.911 | 1F09 | 6 | | Citrix ICA Client Version 6 |
| Citrix ICA SH3 CE Client | Enabled | 6.00.911 | 1F09 | 7 | | Citrix ICA Client Version 6 |
| Citrix ICA SH4 CE Client | Enabled | 6.00.911 | 1F09 | 8 | | Citrix ICA Client Version 6 |
| Citrix ICA MIPS CE Client | Enabled | 6.00.911 | 1F09 | 9 | | Citrix ICA Client Version 6 |
| Citrix ICA PPC CE Client | Enabled | 6.00.911 | 1F09 | A | | Citrix ICA Client Version 6 |
| Citrix ICA ARM CE Client | Enabled | 6.00.911 | 1F09 | B | | Citrix ICA Client Version 6 |

If a new version of a client becomes available, you can download it from the Citrix Systems website at `www.citrix.com/downloads`. After downloading the compressed file, you can decompress it into a directory where it can be used to update the database. Figure 10.10 shows the files being decompressed using WinZip. After you have decompressed the client files, you are ready to add the new client to the database. To do this, select the New option from the Client menu. The dialog box that appears, shown in Figure 10.11, allows you to specify the path to the new client files, specifically the `update.ini` file. This file contains the information required to add the client files to the database.

**FIGURE 10.10** Decompressing the client files



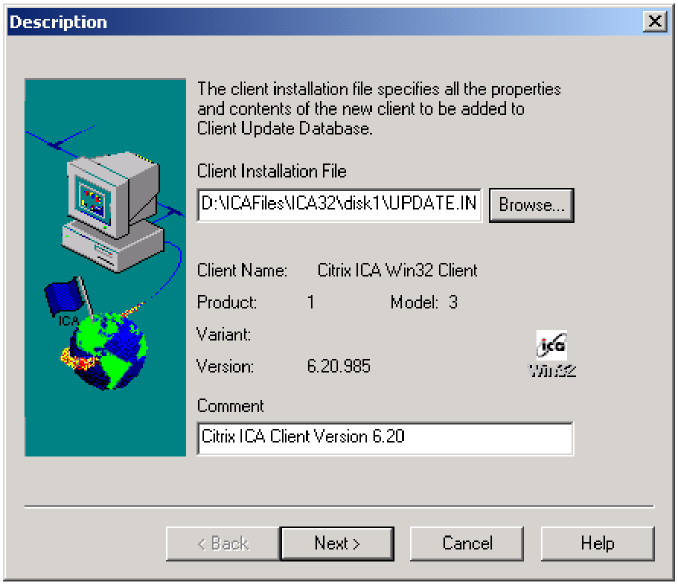
Extract to: D:\ICAFiles

Files
○ Selected files
● All files
○ Files:

☐ Overwrite existing files
☐ Skip older files
☑ Use folder names

Folders/drives:
Desktop
My Computer
3½ Floppy (A:)
Local Disk (C:)
Local Disk (D:)
ICAFiles
ICACLNTS64656504
d$ on 'nautilus' (F:)
xp on 'london' (X:)
xpclients on 'london' (Z

**FIGURE 10.11** Specifying the path to the `update.ini` file of the new client



Description

The client installation file specifies all the properties and contents of the new client to be added to Client Update Database.

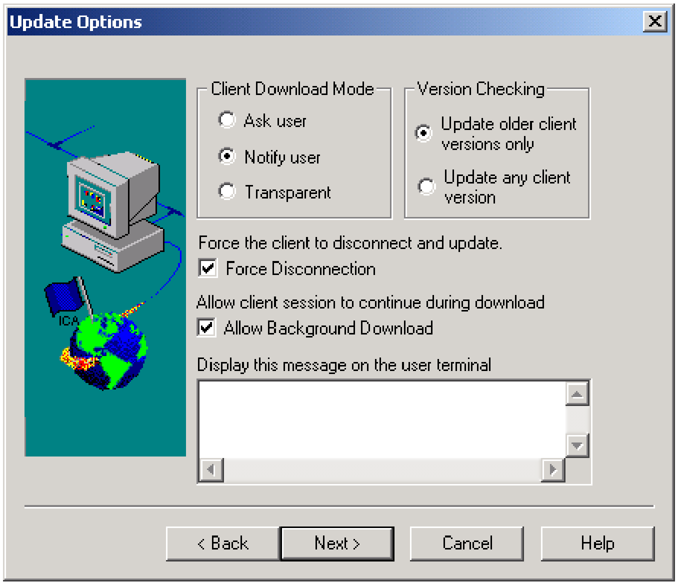
Client Installation File: D:\ICAFiles\ICA32\disk1\UPDATE.IN

Client Name: Citrix ICA Win32 Client
Product: 1 Model: 3
Variant:
Version: 6.20.985

Comment: Citrix ICA Client Version 6.20

After entering the path to the `update.ini` file and clicking Next, you will see options concerning how the client files will be processed, as shown in Figure 10.12. The *Client Download Mode* section allows you to specify how much interaction the user has with the update. If you choose the first option, Ask User, users will be given the option as to whether or not they want to upgrade the client immediately or postpone the installation until the next time they log on. Choosing Notify User will deliver a message to the users that the update is being performed. They will not have a choice; the update is mandatory with this setting. The last option is Transparent. When you select this option, the user is not notified and the update is performed before the users are allowed to log on.

**FIGURE 10.12** The Update Options dialog box



Update Options

Client Download Mode

○ Ask user

● Notify user

○ Transparent

Version Checking

● Update older client versions only

○ Update any client version

Force the client to disconnect and update.

☑ Force Disconnection

Allow client session to continue during download

☑ Allow Background Download

Display this message on the user terminal

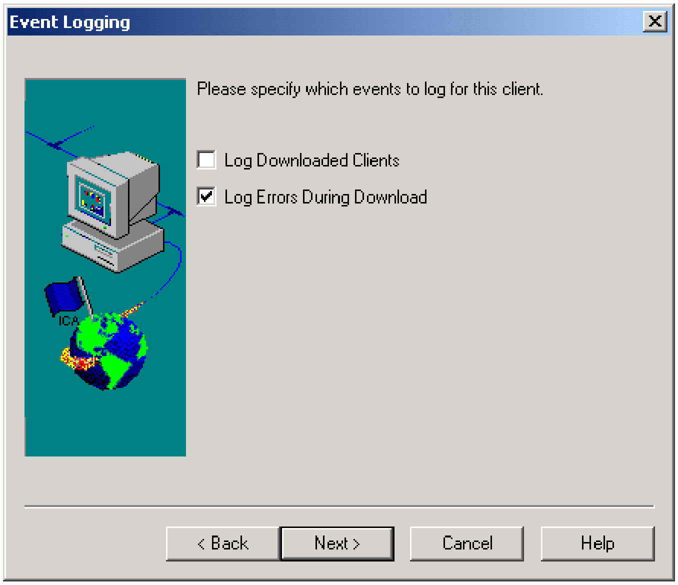
The *Version Checking* section determines how the clients will be updated. The default setting, Update Older Client Versions Only, will update client versions that are older than the database version that is enabled. If you need to replace a newer version of the client with a previous version, you can select the option Update Any Client Version. Be careful when selecting this option for it will replace both the older and newer versions of the client software.

The middle section of this screen contains two options that configure how the client update is to be processed. The client must be disconnected in order for the original files to be released and the new files to be activated. The first option, if selected, forces the client to disconnect after the files have been downloaded. The server will retain the session, and the user will start using the new client when they reconnect. The second option allows the files to be downloaded in the background as the user continues to work. Once the files have been downloaded, the user can disconnect and restart their session to take advantage of the new files. If both of these options are selected, the users will be disconnected and will have to reconnect to their session.

The last section of the Update Options page is the Display This Message On The User Terminal text area. You can enter any information or messages you wish the user to see when the client notification appears. The user can click the More Info button on the notification screen to see your message. Once you've chosen all of the desired options, click Next.

The *Event Logging* page appears next, as shown in Figure 10.13. From here, you can specify whether an event will be logged for every client downloaded by selecting the Log Downloaded Clients check box. Use this option only if you need to track which users have updated to the selected client. This option can put many entries into the event logs and could fill up those logs if they are not configured correctly. The second option, Log Errors During Download, should always be selected since you want to know when a client did not download completely or correctly. Click Next to reach the last page of the wizard.

**FIGURE 10.13** Event Logging options



Event Logging

Please specify which events to log for this client.

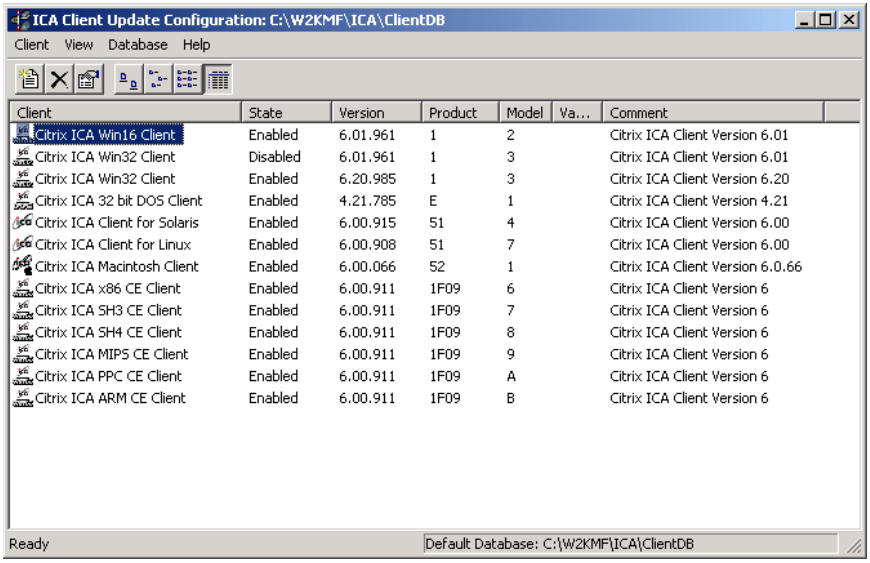
□ Log Downloaded Clients

☑ Log Errors During Download

Here you can choose to enable the client. Please note that if you select the Enable option, any existing client of the same product and model type that is currently enabled will be disabled. Unless you are absolutely sure that the new client will work with all software in your environment, you should leave the check box unchecked. You will be able to enable it at a later time by editing the properties of the client entry within the database. Click Finish to import the files into the database.

Once the new client has been added to the database, you will see the entry in the main window. In Figure 10.14, the new client is enabled since we chose to enable it during the ICA Client Distribution Wizard. The original client is disabled since we can have only one instance of a product or model of a client enabled at a time.

**FIGURE 10.14** ICA Client Update Configuration displaying the new client



ICA Client Update Configuration: C:\W2KMF\ICA\ClientDB

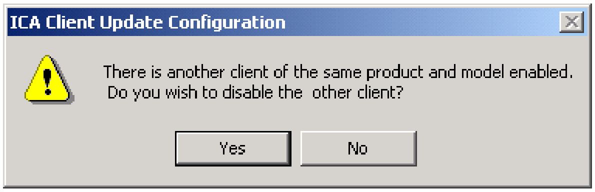
| Client | State | Version | Product | Model | Va... | Comment |
|---|---|---|---|---|---|---|
| Citrix ICA Win16 Client | Enabled | 6.01.961 | 1 | 2 | | Citrix ICA Client Version 6.01 |
| Citrix ICA Win32 Client | Disabled | 6.01.961 | 1 | 3 | | Citrix ICA Client Version 6.01 |
| Citrix ICA Win32 Client | Enabled | 6.20.985 | 1 | 3 | | Citrix ICA Client Version 6.20 |
| Citrix ICA 32 bit DOS Client | Enabled | 4.21.785 | E | 1 | | Citrix ICA Client Version 4.21 |
| Citrix ICA Client for Solaris | Enabled | 6.00.915 | 51 | 4 | | Citrix ICA Client Version 6.00 |
| Citrix ICA Client for Linux | Enabled | 6.00.908 | 51 | 7 | | Citrix ICA Client Version 6.00 |
| Citrix ICA Macintosh Client | Enabled | 6.00.066 | 52 | 1 | | Citrix ICA Client Version 6.0.66 |
| Citrix ICA x86 CE Client | Enabled | 6.00.911 | 1F09 | 6 | | Citrix ICA Client Version 6 |
| Citrix ICA SH3 CE Client | Enabled | 6.00.911 | 1F09 | 7 | | Citrix ICA Client Version 6 |
| Citrix ICA SH4 CE Client | Enabled | 6.00.911 | 1F09 | 8 | | Citrix ICA Client Version 6 |
| Citrix ICA MIPS CE Client | Enabled | 6.00.911 | 1F09 | 9 | | Citrix ICA Client Version 6 |
| Citrix ICA PPC CE Client | Enabled | 6.00.911 | 1F09 | A | | Citrix ICA Client Version 6 |
| Citrix ICA ARM CE Client | Enabled | 6.00.911 | 1F09 | B | | Citrix ICA Client Version 6 |

Ready

Default Database: C:\W2KMF\ICA\ClientDB

Any of the options that were available as you installed the new client to the database are available from the Properties sheet of the client image in the database. Right-click the client you wish to configure, and select Properties. You can enable or disable the client from the Description tab. If you attempt to enable a client when another version is already enabled, you will be presented with a warning dialog that asks you if you would like to disable the other version of the client, as shown in Figure 10.15.

**FIGURE 10.15** Warning shown when another version of the client is already enabled



ICA Client Update Configuration

There is another client of the same product and model enabled.
Do you wish to disable the  other client?

When you decide that you no longer need to support a client version within the database, you can remove the client by right-clicking it within the database and selecting Delete. You will be asked to confirm the removal before it will actually be deleted. If the client you are deleting is the enabled client for that product and model, you will have to enable another version; the system will not automatically enable another version of the client.

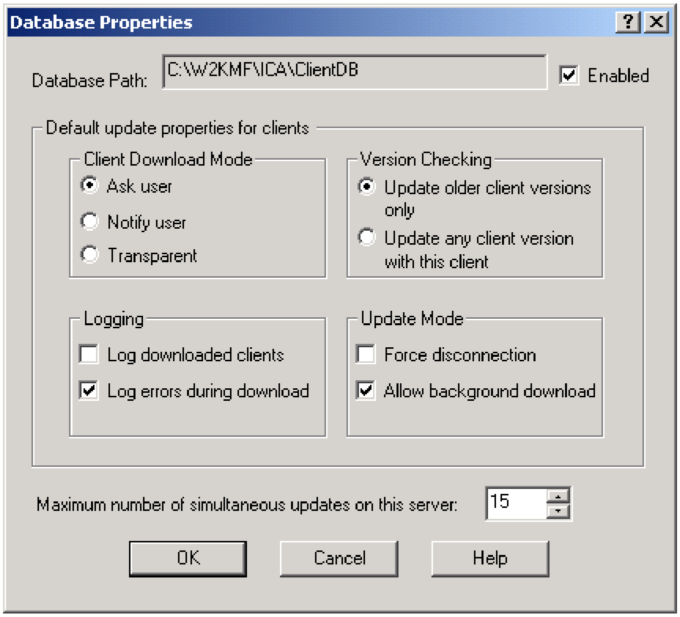
## Configuring the Database

The database itself can be configured to include default options that clients will adopt when they are added. You can also control which client database is used to determine which clients are available. While it is recommended that only one database be used, you can have separate databases for each server. To configure the options for the database, open the ICA Client Update Configuration utility, and from the Database menu, select Properties. Figure 10.16 shows the Database Properties screen.

To use the database, it must be enabled. Select the check box on the Properties page next to Enabled to make the database available. As long as the database is enabled, users will receive the updated clients according to the settings you configure. Another option available from the Properties page is the ability to control the number of simultaneous downloads that the server will grant. You should set this option to allow the maximum number of clients to download the update, yet not overload the server and prevent it from running user sessions.

The four configuration sections on this page contain the same options that we discussed earlier for controlling the download to the user's workstation. Any settings you make here become the default options whenever a new client is added to the database. These settings do not control the clients once they are installed, however. The settings in the Database Properties sheet will not override the settings you configure for the clients.

**FIGURE 10.16** Database Properties screen



Database Properties

Database Path: C:\W2KMF\ICA\ClientDB ☑ Enabled

Default update properties for clients

Client Download Mode

● Ask user

○ Notify user

○ Transparent

Version Checking

● Update older client versions only

○ Update any client version with this client

Logging

□ Log downloaded clients

☑ Log errors during download

Update Mode

□ Force disconnection

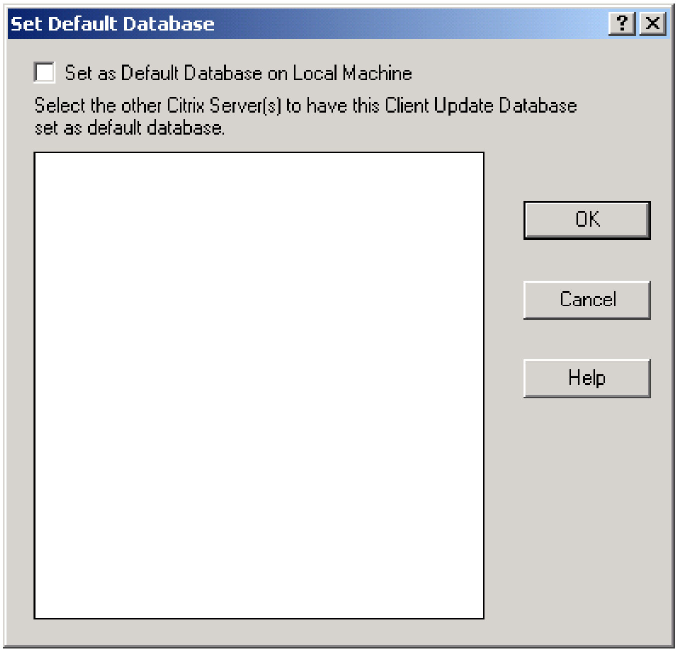
☑ Allow background download

Maximum number of simultaneous updates on this server: 15

To specify a default Client Update Database, choose Open from the Database menu. Specify the path to the default database and click Open. On the Database menu, click Set Default. When the Set Default Database dialog box appears, as shown in Figure 10.17, select the Set As Default Database On Local Machine check box. From this window, you can also select other Citrix servers and have them use the currently opened database as the default.

And so we close Chapter 10. Now that we have introduced you to the methods of installing the client software, we are ready to move on to configuring the client's Program Neighborhood. After performing the labs at the end of this chapter, you will have Program Neighborhood installed on your system and will be ready to start configuring it to access your MetaFrame XP servers.

**FIGURE 10.17** Setting the default database



Set Default Database

□ Set as Default Database on Local Machine

Select the other Citrix Server(s) to have this Client Update Database set as default database.

## Summary

To take advantage of using MetaFrame servers, you need to have client software that can connect to the server installed on your computer. MetaFrame uses the ICA Client to connect to the server and create sessions. These clients are available for nearly every type of business operating system currently in use.

To ease installation of the client software, Citrix offers several different types of deployment. You can use the ICA Client CD, make disks for the client by using the ICA Client Creator, access the client files from a network share, or use a web browser to access the files from a web server.

Another Citrix utility that can make administrators' lives easier is the ICA Client Update Configuration. With this utility, you can control the client version that is installed on the users' computers. As new clients are made available, you can add them to the database and automatically upgrade the client when the users log on.

Now that we have talked about installing the client, we need to move on to configuring and working with the client software. In the next chapter, we will be examining Program Neighborhood and configuring it for our users.

# Exam Essentials

**Know the minimum requirements for the platforms on which you are deploying clients.** Each client has its own requirements. Check the Administrator's Guide that ships with MetaFrame XP to determine the minimum requirements for the platforms you are using.

**Know how to add the client files to the server.** The Citrix ICA Client Distribution Wizard will assist you with installing the files from the CD or a network share.

**Know the different deployment methods available.** You can install the client from the ICA Client CD, installation disks, a network share, or a web server.

**Know how to create the ICA Client Update Database.** The Citrix ICA Client Distribution Wizard will guide you in creating the database and adding the initial clients.

**Know how to configure the default options for clients added to the database.** The Database Properties sheet contains settings that will be applied as the default properties when clients are added.

**Understand the client database settings.** These settings control whether or not the client is prompted when the new client is downloaded and the behavior of the client system after the files are downloaded.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Client Download Mode

Custom install

Event Logging

ICA Client Administrator's Guides

ICA Client CD

ICA Client Creator

ICA Client Update Configuration

ICA Client Update Database

ICA pass-through Client

`icaweb` directory

installation disks

network share

Typical install

Version Checking

`WebInst` directory

# Exercise

In the first part of this exercise, we'll install the Win32 ICA Client from a network share point. Then we'll add a new ICA Client to the ICA Client Update Configuration utility. Finally, we'll update the client on the server to the new version of the client.

## EXERCISE 10.1

### Installing the Client Software

First, let's install the Win32 ICA Client from a network share point:

1. Navigate to the `ICA32` directory on the network share.
2. Double-click to launch the Setup program.
3. At the Welcome screen, click Next.
4. At the Citrix License Agreement window, click Yes.
5. If the Choose Installation Type window appears, choose Upgrade The Existing Client.
6. Choose the path to install the client files from the Choose Destination Location screen, and click Next.
7. Select where the application icons will be created from the Select Program Folder screen, and click Next.
8. In the ICA Client Name window, keep the default, and click Next.
9. Choose No when asked if you would like to enable and automatically use your local username and password for Citrix sessions from this client, and click Next.

Be aware that the client installation starts immediately after you click Next.

### EXERCISE 10.1 *(continued)*

Next, we'll add a new ICA Client to the ICA Client Update Configuration utility:

1. Download the latest Windows 32-bit client from the Citrix website. Do not run this program; instead, close the download window when the download is complete.
2. Extract the files in the ICA Win32 Client executable (`ica32.exe`) with a program such as WinZip.
3. Start the ICA Client Update Configuration utility by clicking the appropriate icon in the MetaFrame XP toolbar or by selecting Start ➤ Programs ➤ Citrix ➤ MetaFrame XP ➤ ICA Client Update Configuration.
4. From the Client menu, select New to display the Description screen.
5. Enter the path or browse to the `update.ini` file so that it appears in the Client Installation File dialog box, and click Next.
6. Keep all defaults in the Update Options window, and click Next.
7. Keep all defaults in the Event Logging window, and click Next.
8. In the Enable Client window, make sure the Enabled check box is not checked, and click Finish.

Finally, we'll change the client on the server to the new version of the client:

1. Right-click the original Citrix ICA Win32 Client and select Properties.
2. In the Description tab, remove the check from the check box labeled Enabled.
3. Click OK.
4. Right-click the new Citrix ICA Win32 Client, and select Properties.
5. In the Description tab, place a check in the box labeled Enabled.
6. Click OK to close the Properties sheet.

# Review Questions

1. What are the different methods of ICA Client deployment? (Choose all that apply.)

   A. Web browser

   B. Download from a network share point

   C. Installation disks

   D. The Citrix ICA Client Update Configuration utility

2. A new Citrix ICA Client has been released, and you want to update all of your clients. Which installation option would be the best choice for a company that has many locations, with users employing a wide variety of operating system platforms?

   A. Web browser

   B. Download from a network share point

   C. Installation disks

   D. Citrix ICA Client Update Configuration utility

3. What is the name of the utility that allows you to install or upgrade the pass-through ICA Win32 Client on the server?

   A. Citrix Connection Configuration

   B. ICA Client Distribution Wizard

   C. ICA Client Update Configuration

   D. Citrix Management Console

4. If you want your NFuse website to have the ability to install ICA Client files from a web page, what directory from the ICA Clients CD should you copy to the MetaFrame server?

   A. `icaclients`

   B. `icaweb`

   C. `webclients`

   D. `nfuseweb`

**5.** You want your users to automatically download updated ICA Client files when they connect to your server via NFuse. What do you need to name the directory where you copy the files?

**A.** `icaweb`

**B.** `WebInst`

**C.** `nfuseweb`

**D.** `citrix`

**6.** If you want users to be able to update their ICA Client files from a web page, but you are not running NFuse, you can create an ICA Client download web page. In which directory are the installation web pages stored on the NFuse CD?

**A.** `icaweb`

**B.** `icainst`

**C.** `WebInst`

**D.** `nfuseweb`

**7.** Which utility creates installation disks for ICA Clients?

**A.** ICA Client Creator

**B.** Client Installation Creator

**C.** ICA Client Distribution Wizard

**D.** Client Disk Creator

**8.** Using the ICA Client Creator, for which operating system platforms can you create floppy disks? (Choose all that apply.)

**A.** DOS

**B.** Windows

**C.** OS/2

**D.** Macintosh

9. Which utility would you use to automatically update ICA Clients with newer versions of the ICA Client software?

   A. ICA Client Update Wizard

   B. ICA Client Configuration

   C. Client Update Configuration

   D. ICA Client Update Configuration

10. Which versions of the ICA Client will the ICA Client Update Configuration utility update? (Choose all that apply.)

    A. Older versions only

    B. Newer versions only

    C. Older or newer versions

    D. The version that is specified explicitly by number

11. Which options do you have in the Client Download Mode section of the Update Options tab when automatically updating your ICA Clients? (Choose all that apply.)

    A. Ask User

    B. Notify User

    C. Allow Background Download

    D. Transparent

12. You have a user on your network who is always installing the latest ICA Client from the Internet before you have a chance to test it and make it available to your users. How can you find out who is connecting to your server with unsupported clients?

    A. Place a check in the check box labeled Log Downloaded Clients in the Properties sheet of the client database.

    B. Place a check in the check box labeled Do Not Allow Nonstandard Clients in the Properties sheet of the client database.

    C. Place a check in the check box labeled Replace Newer ICA Clients in the Properties sheet of the client database.

    D. Click the radio button labeled Replace Newer ICA Clients in the Properties sheet of the client database.

**13.** If you want users to connect to the MetaFrame server with the new client immediately after downloading the new client, what should you do?

**A.** In the Client section of the Update Options tab of the Properties sheet, place a check in the box labeled Force Disconnection.

**B.** In the Download Options section of the Update Options tab of the Properties sheet, place a check in the box labeled Force Disconnection.

**C.** In the Update Options tab of the Properties sheet, select the radio button labeled Re-connect After Client Update.

**D.** In the Update Options tab of the Properties sheet, place a check in the box labeled Force Disconnection.

**14.** You are the administrator of a network that has over 1200 users who log in at 9:00 A.M. You update your ICA Client Database with a new client and set it to update any version of the ICA Client. Users start calling and report that the download is running extremely slowly. What can you do to prevent this the next time you update the client?

**A.** In the Database Properties sheet, reduce the number in the text box labeled Maximum Number Of Simultaneous Updates On This Server.

**B.** In the Database Properties sheet, place a check in the check box labeled Maximum Number Of Simultaneous Updates On This Server, and set the number to a lower number.

**C.** In the ICA Client Update Configuration utility, select the properties of the ICA Client and place a check in the check box labeled Maximum Number Of Simultaneous Updates On This Server, and set the number to a lower number.

**D.** In the ICA Client Update Configuration utility, select the properties of the ICA Client and reduce the number in the text box labeled Maximum Number Of Simultaneous Updates On This Server.

**15.** You want to add a new client to the Client Update Database. You need to add the client installation file. What is the filename that MetaFrame is looking for in this dialog box?

A. `client.ini`

B. `client.inf`

C. `update.ini`

D. `update.inf`

16. Where does the ICA Client Distribution Wizard place the `update.ini` file when it is run?

A. `%systemroot%\system32\ica`

B. `%systemroot%\system32\clients`

C. `%systemroot%\system32\citrix\clients`

D. `%systemroot%\system32\clients\ica`

17. Which of the following are features of the ICA Client Update Configuration? (Choose all that apply.)

A. Automatically detects the ICA Client software version

B. Can restore older ICA Clients when needed

C. Automatically checks the Citrix website for updates and installs them accordingly

D. Copies files over any ICA connection without user intervention

18. In the ICA Client Database, which client model number corresponds with the Win32 ICA Client?

A. 1/1

B. W/1

C. 1/2

D. 1/3

**19.** Which of the following clients can be automatically installed with the ICA Client Distribution Wizard? (Choose all that apply.)

**A.** Win32

**B.** Win16

**C.** Win CE

**D.** Linux

**20.** You want to install the new ICA Client for Win16. You decide to install it manually and not use the ICA Client Distribution Wizard. You download the new client from the Citrix website but find that it is a single executable file. What must you do first in order to add this client to the ICA Client Update Database?

**A.** Extract the file with a third-party unzip utility.

**B.** Execute the program; it will sense that it is installed on a server and will add itself to the database.

**C.** Open the ICA Client Update Database and add a new database; then point to the executable file.

**D.** Execute the program and install the ICA Client. Then add a new client in the database and point to the executable file.

# Answers to Review Questions

1. A, B, C. The ICA Client can be deployed by any of the following methods: using a web browser, downloading from a network share point, and using installation disks. You cannot install the client using the ICA Client Update Configuration utility, although it can be used to automatically update the client when a new version is available.

2. D. The Citrix ICA Client Update Configuration utility allows users to automatically receive ICA Client updates when they connect to a Citrix server.

3. B. You can use the ICA Client Distribution Wizard to install the pass-through ICA Win32 Client on the Citrix server.

4. B. To enable the NFuse website to include the ICA Client installation feature, copy the `icaweb` directory from the ICA Client CD to the MetaFrame server that is running NFuse.

5. D. Copy the `icaweb` directory from the ICA Client CD to a directory named `citrix` in the `NFuseClients` directory off the web server's web publishing root directory. You must copy the `icaweb` directory and all of its contents to this directory for web-based ICA Client installation to work with the NFuse website.

6. C. Installation web pages include hyperlinks to initiate the download of the ICA Client Setup files. The pages are distributed on the NFuse CD in the `WebInst` directory.

7. A. You can use the ICA Client Creator to create installation disks.

8. A, B. You can use the ICA Client Creator to create installation disks for DOS, for Win 95/98/Me/NT/2000, and for Win 3.*x*.

9. D. The Client Auto Update feature of the ICA Client Update Configuration updates ICA Clients with a standard version of the ICA Client software.

10. A, B, C. When a user logs onto a Citrix server, the server queries the ICA Client to determine the version number. If the version matches the one in the Client Update Database, the logon continues. If the server detects a different version number, depending on the settings within the database, the client software will be updated. The options that you can set include updating older versions of the client only or updating any version of the client.

**11.** A, B, D. The Client Download Mode section of the Update Options tab allows you to specify whether the client files will be updated automatically or user intervention will be involved. When a user connects to a Citrix server that has a different ICA Client version than the user is running, one of three things can happen. You can define whether the automatic update will ask the user, notify the user, or download transparently.

**12.** A. In the Event Logging tab of the Properties sheet, choose Log Downloaded Clients to log an event when a client runs the update.

**13.** D. In the Update Options tab, you can place a check in the box labeled Force Disconnection to require users to disconnect and complete the update process before continuing with their ICA session.

**14.** A. You can limit the bandwidth on the network that the ICA Client update process consumes. If you have a busy network, with a lot of clients connecting at one time to the network (say, 9:00 A.M.), you can limit the number of simultaneous downloads that take place on a given server by opening the Database Properties sheet and reducing the number in the text box labeled Maximum Number Of Simultaneous Updates On This Server.

**15.** C. In the Client Installation File dialog box, browse to or enter the path to the client installation file `update.ini`.

**16.** D. When you run the ICA Client Distribution Wizard, you can find the `update.ini` file in `%systemroot%\system32\clients\ica`.

**17.** A, B, D. ICA Client Update Configuration supports the following features: automatically detects the ICA Client software version; copies files over any ICA connection without user intervention; provides administrative control of update options for each ICA Client; updates ICA Clients from a single database on a network share point; safely restores older ICA Clients when needed.

**18.** D. Each ICA Client has a unique model number. The model number for the Win32 ICA Client is 1/3.

**19.** A, B, C, D. All of the clients listed above are automatically created when you run the ICA Client Distribution Wizard.

**20.** A. The program must be unzipped with a third-party utility so that you can extract the `update.ini` file. In the ICA Client Update Database, you will point to this `update.ini` file when adding a new client.

# Program Neighborhood

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **9. Citrix Program Neighborhood**

- 9a. Customizing Program Neighborhood interface and recognizing the ICA Toolbar Icons

In the previous chapter, we examined the various ways that client software can be loaded onto a user's computer. No matter which of the deployment methods you take advantage of, the end result is the same: *Program Neighborhood* is installed on the user's computer. Once it is installed, users are able to access published applications on your MetaFrame servers. Within this chapter, you will find the information to configure Program Neighborhood.

Although client software is available for nearly any operating system, we are going to concentrate on using Program Neighborhood in a Windows environment. Program Neighborhood is available only for Win32 clients. All other clients have a version of Remote Application Manager that they use to gain access to server desktops and published applications.

To start with, we will take a look at Program Neighborhood and the different views available in the tool. From there, we will discuss how to configure and manage this utility. When we have completed this chapter, you should be well on your way to configuring your clients with the information they need to access the applications they require.

TIP

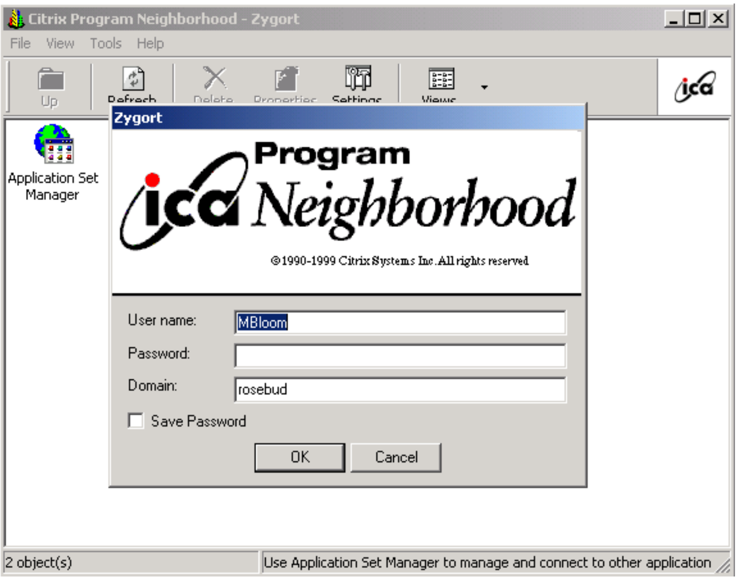
To make your life easier, you should not give users access to Program Neighborhood. If they cannot access the settings within this utility, they will not be able to make changes that could affect their sessions. As a rule, you should push the application icons to the user's Start menu and desktop. This will also reduce the amount of training necessary.

# Taking a Look at Program Neighborhood

Let's start off by opening Program Neighborhood and looking at the interface that is presented to users. Navigate to Start ➢ Programs ➢ Citrix ICA Client ➢ Citrix Program Neighborhood. Figure 11.1 shows Program

Neighborhood as it looks when it is first opened. Note that if the option to use the user's current logon information was not selected during the installation of the client software, you will be prompted to enter a username, password, and domain. Once you've entered this information and the application opens, you will see the published applications that are available to the user within the main window, as shown in Figure 11.2.

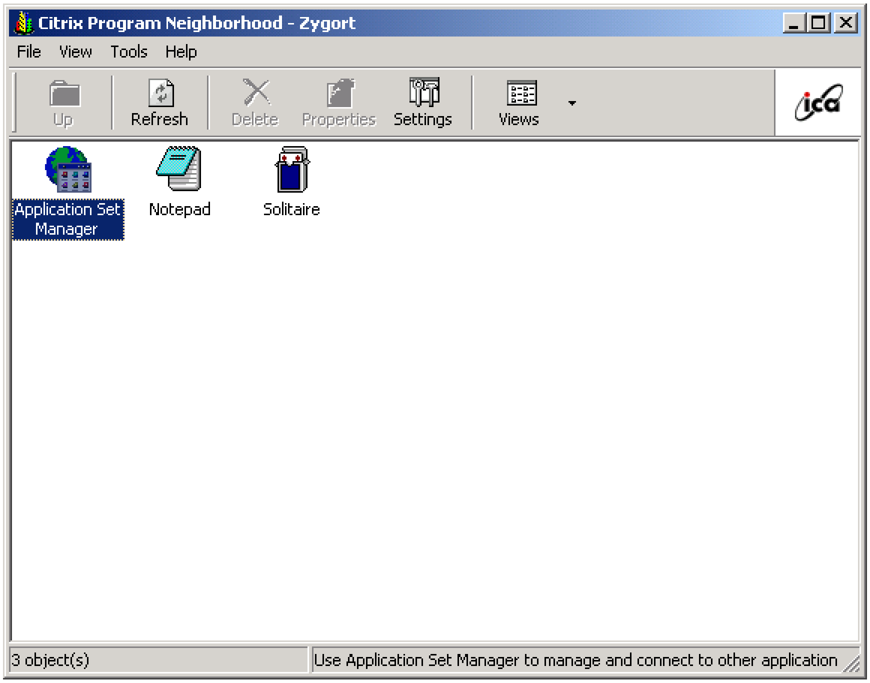
FIGURE 11.1 Opening Program Neighborhood


Citrix Program Neighborhood - Zygort
File View Tools Help
Up
Refresh
Delete
Properties
Settings
Views
Application Set Manager
Zygort
Program Neighborhood
©1990-1999 Citrix Systems Inc. All rights reserved
Save Password
OK
Cancel
2 object(s)
Use Application Set Manager to manage and connect to other application

User name: MBloom
Password:
Domain: rosebud
□ Save Password

Now that we have Program Neighborhood open and we can look at the options available to configure, let's take a moment and discuss what this utility can actually do. First, Program Neighborhood is a client-side utility that has been developed so that an administrator should not have to perform any tasks at the client computer in order for the user to connect to their applications. You can perform the entire configuration at the server level, so once Program Neighborhood is installed, the only thing the user has to do is log in. If you look at Figure 11.2, you will notice that immediately after logging in to the server farm, you can see the applications. Any applications you had published and given the user permission to use will show up automatically once they log on.

**FIGURE 11.2** Program Neighborhood's main screen



Second, Program Neighborhood provides a single logon when you access applications within the application set. If a user does not have permission to use a published application, the application will not appear within the list of applications for the application set. Once logged in, the user will not have to worry about authenticating again when they access an application from a different server unless RC5 encryption is used, which disables automatic logon to the Citrix servers.

## The Three Levels

Program Neighborhood is made up of three separate levels that allow you to control what is presented to the user. When a user first starts Program Neighborhood and logs in, that user is presented with the default *Application Set* level. This screen displays all of the published applications that the user has permission to use. From here, a user can access the *Application Set Manager* level, which lists all of the application sets the user has access to.

From within the Application Set Manager, the user can access the *Custom ICA Connections* level, where they can create published applications, server applications, and desktops of servers in your server farm. Let's take a look at each of these levels so that we are familiar with them when we start looking at how to configure Program Neighborhood.

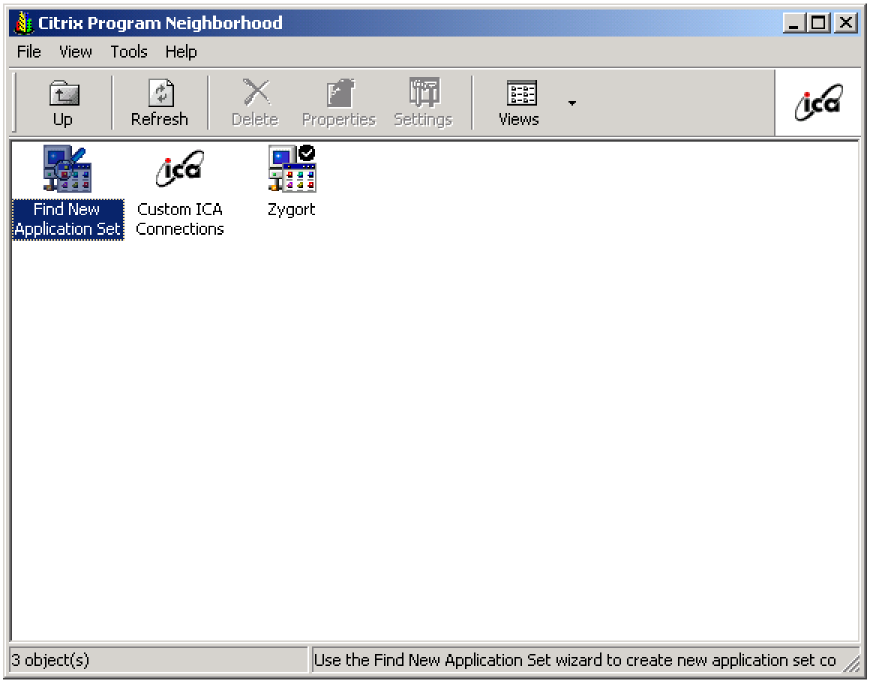
## Application Set

We have started Program Neighborhood and logged on. What we see before us is the Application Set screen. "What is an application set?" you ask. Remember back when we were working with Citrix Management Console and we were publishing applications? Those applications that we published became the applications that appear within Program Neighborhood as members of the application set. Only the applications that the user has been granted permission to use will show up in the application set. Two users may have completely different applications within their application sets. The information that appears on this screen is dependent upon which application set is selected as the default from within the Application Set Manager level. To get to this level, double-click the Application Set Manager icon. From here, you can right-click an application and choose Set As Default. Remember that access to each application set requires a valid logon.

## Application Set Manager

Even though there could be numerous application icons, two icons always appear on this screen, as shown in Figure 11.3: *Find New Application Set* and Custom ICA Connections. If you want to create a new application set, you can double-click this first icon. You will be prompted through a wizard that will assist you in locating and identifying the application set. You will have only one application set per server farm. While in theory you could create more than one application set per server farm, all of the applications within the two sets would be the same. If you do have more than one server farm available in your environment, you could create more than one application set so that the user will be able to access applications from all of the server farms. The applications from the application set that you designate as the default will appear on the Application Set screen.

**FIGURE 11.3** The Application Set Manager level



3 object(s)

Use the Find New Application Set wizard to create new application set co

## Custom ICA Connections

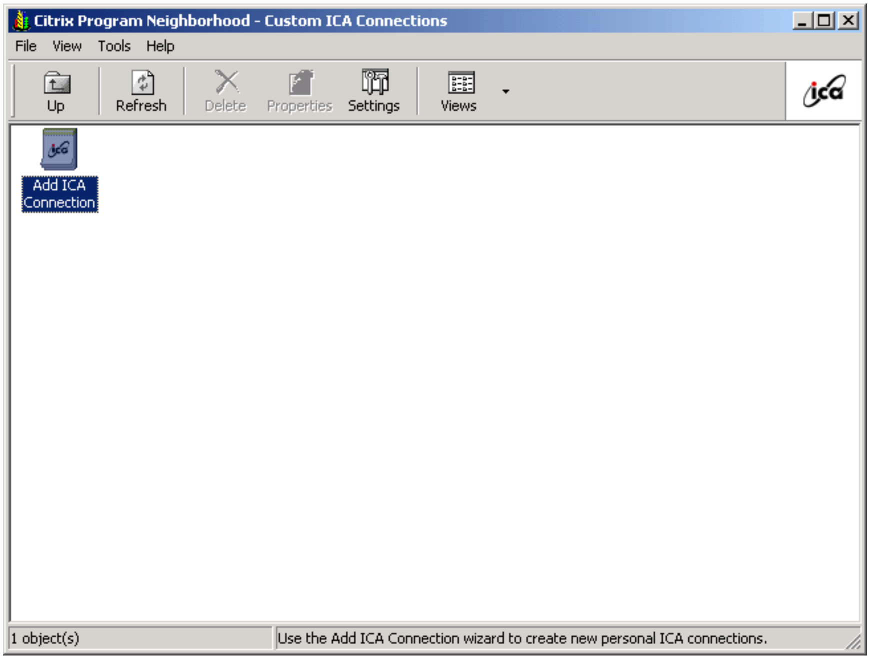
Double-clicking the second icon, Custom ICA Connections, takes you to the lowest level of Program Neighborhood, as shown in Figure 11.4. It is here that you may configure customized access to server desktops, server applications, and published applications. You should use this level only when you want to modify the properties of an individual published application, since modifying the application set affects all applications in that set.

NOTE

Although Program Neighborhood is not usually configured in this manner, you can elect to have the custom ICA connections as the default application set. If you do set the default this way, the custom applications that are configured within Program Neighborhood become the applications that appear on the Application Set screen when you log on.

Now that we have examined the Program Neighborhood interface, let's move on to configuring this utility so that our users see only what we want them to see.

**FIGURE 11.4** The Custom ICA Connections level



Use the Add ICA Connection wizard to create new personal ICA connections.

WARNING

If you let the users see exactly what you have configured, they can change those settings.

# Configuring Program Neighborhood

While there are configuration options available to control how the user accesses the MetaFrame server, you will most likely not have to make any changes to these settings. In most environments, the default settings will more than likely be sufficient. However, you should be familiar with the options available. Let's take a look at the menus we have to work with and how they control the user's environment, starting with the Application Set level.

## Application Set

We will start with the File menu. If you have not selected any of the icons within the main window, when you pull down the File menu you will see the options shown in Figure 11.5. There's not much here. You may have other choices depending on which icons you select at this level. Selecting the Application Set Settings menu item brings up the application set configuration options, as shown in Figure 11.6. And of course, selecting Close exits Program Neighborhood.

**FIGURE 11.5** File menu options

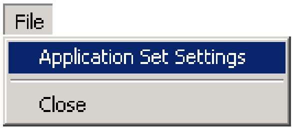
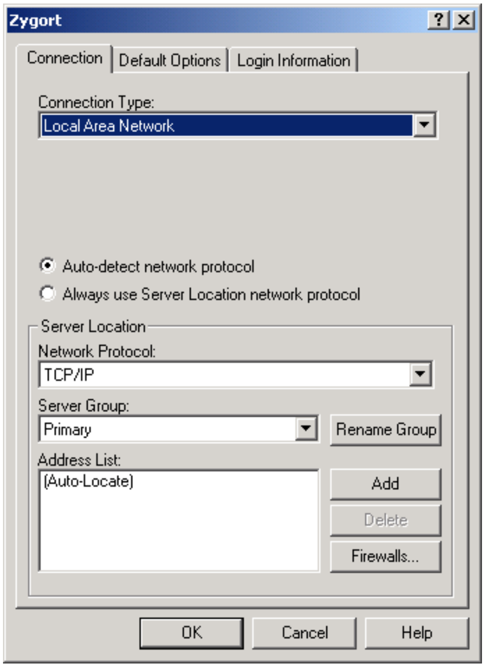


**FIGURE 11.6** Application set settings



Zygort

Connection | Default Options | Login Information

Connection Type: Local Area Network

● Auto-detect network protocol

○ Always use Server Location network protocol

Server Location

Network Protocol: TCP/IP

Server Group: Primary

Address List: (Auto-Locate)

More information about the application set settings is available later in this chapter.

If you select the Application Set Manager icon from Program Neighborhood's main screen and pull down the File menu, you will see an additional option, Open, as shown in Figure 11.7. Choosing this menu item has the same effect as double-clicking the icon itself. And finally, if you select any of the published application icons from the main screen, you will see three more menu items, *Create Desktop Shortcut*, *Copy to Custom Connections*, and Properties, as shown in Figure 11.8. Of these three, let's start with Properties. Choosing this menu item opens a Properties sheet for the selected application, as shown in Figure 11.9. Note that none of the properties are editable. You can only view the settings for the application, but you might be able to tell if the application is configured incorrectly for the user.

**FIGURE 11.7** File menu options available from clicking the Application Set Manager icon

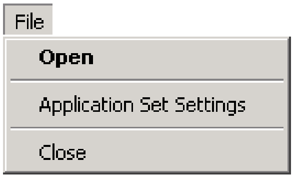
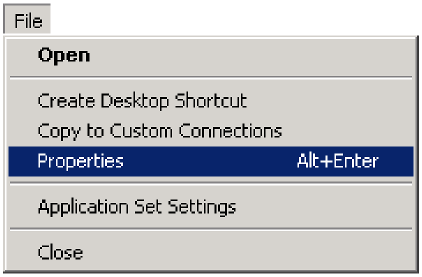
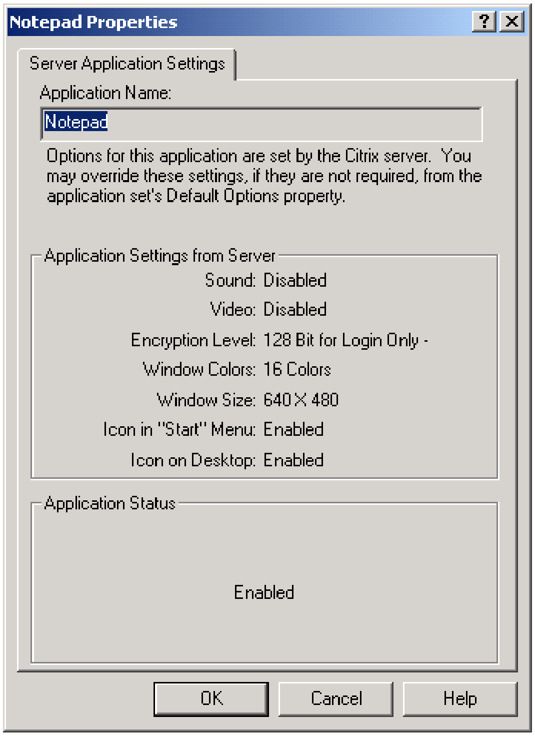


**FIGURE 11.8** File menu options available when an application is selected



The other two options allow the user or administrator to control the application icons so that they can place them to suit their needs. If you have an application selected and you choose the Create Desktop Shortcut option, the application's icon will be placed on the user's desktop, where they can activate the application without having to open Program Neighborhood.

**FIGURE 11.9** Properties sheet for an application



Notepad Properties

Server Application Settings

Application Name: Notepad

Options for this application are set by the Citrix server. You may override these settings, if they are not required, from the application set's Default Options property.

Application Settings from Server

Sound: Disabled

Video: Disabled

Encryption Level: 128 Bit for Login Only -

Window Colors: 16 Colors

Window Size: 640 X 480

Icon in "Start" Menu: Enabled

Icon on Desktop: Enabled

Application Status

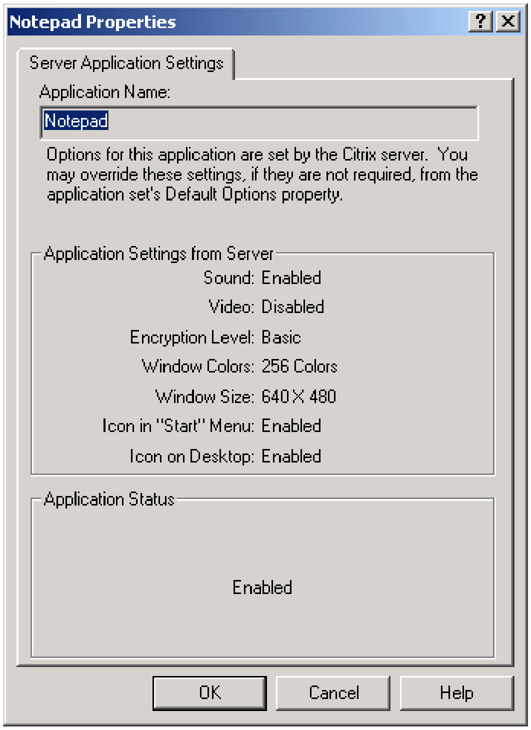
Enabled

NOTE

If you selected the Add Shortcut To The Client's Desktop option when you published the application, an icon will already exist on the user's desktop if the user is accessing their session from a Win32 client device or from Program Neighborhood. Choosing the menu item Create Desktop Shortcut creates another icon on the desktop for the same published application. An additional icon will appear on the desktop every time you select this option, so use it sparingly. The preferred method of placing an icon on the desktop is to push it down when publishing the application.

The last option from the File menu that we will discuss is Copy To Custom Connections. In the previous section, we looked at the three levels available to the user from within Program Neighborhood. The lowest level, Custom ICA Connections, contains custom-made connections to published applications, server applications, and desktops that are different from the settings configured at the server. Choosing this last option from the File menu copies the icon and its settings to the Custom ICA Connections area, where the application's properties may be modified. Figure 11.10 shows the properties of the Notepad published application, while Figure 11.11 shows the properties of the same application after it has been copied to Custom ICA Connections. Note that only the copied version can be modified.

**FIGURE 11.10** Properties of a published application



Application Name: Notepad

Options for this application are set by the Citrix server. You may override these settings, if they are not required, from the application set's Default Options property.

Application Settings from Server

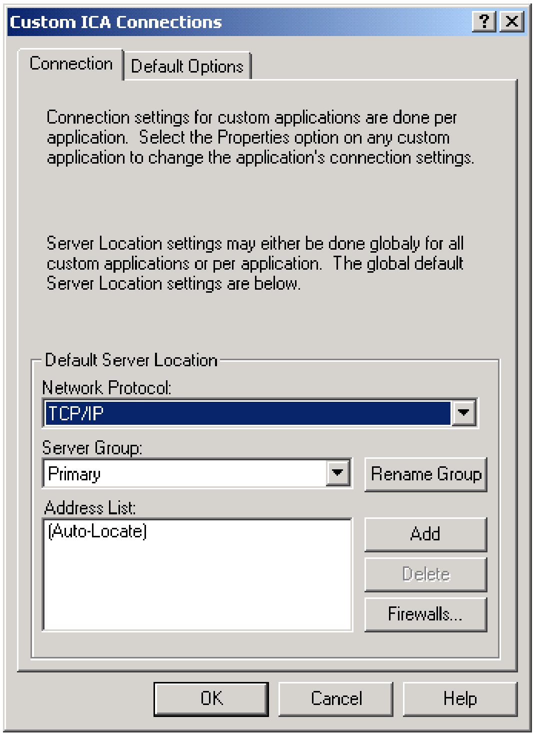
Sound: Enabled
Video: Disabled
Encryption Level: Basic
Window Colors: 256 Colors
Window Size: 640 X 480
Icon in "Start" Menu: Enabled
Icon on Desktop: Enabled

Application Status

Enabled

Of course, a rule of thumb is to not train users how to take advantage of these functions. If you publish the applications and push the icons to their desktop or Start menu and then not allow them access to Program Neighborhood, you can control their ability to make changes to the programs.

**FIGURE 11.11** Properties of an application copied to Custom ICA Connections



Connection settings for custom applications are done per application. Select the Properties option on any custom application to change the application's connection settings.

Server Location settings may either be done globaly for all custom applications or per application. The global default Server Location settings are below.

Default Server Location

Network Protocol: TCP/IP

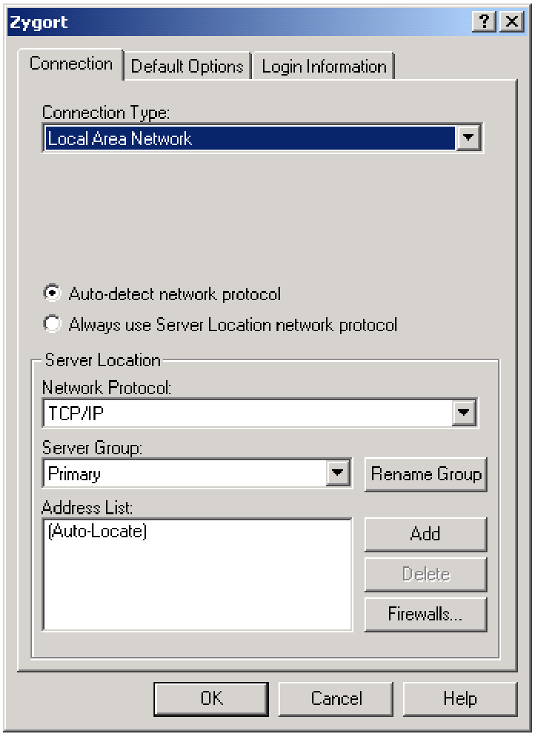
Server Group: Primary

Address List: (Auto-Locate)

If you choose Application Set Settings from the File menu, you will see the Properties sheet shown in Figure 11.12. From here, you can control how all of the applications within the application set behave. The Connection tab controls access to the application set. From the Connection Type pull-down menu, you can choose LAN, WAN, or dial-up connections. If you are connecting to the server farm using a dial-up connection, you are given the additional configuration option of choosing which dial-up networking connection to use. Figure 11.13 shows this same tab with the dial-up networking settings.

You can allow the client to automatically select the network protocol it will use when connecting to the server farm by clicking the Auto-detect Network Protocol radio button. If you want to control the protocol Program Neighborhood will use, select the other option, Always Use Server Location Network Protocol. Protocols available for use include TCP/IP, TCP/IP+HTTP, IPX, SPX, and NetBIOS.

**FIGURE 11.12** Connection settings



Connection Type: Local Area Network

● Auto-detect network protocol

○ Always use Server Location network protocol

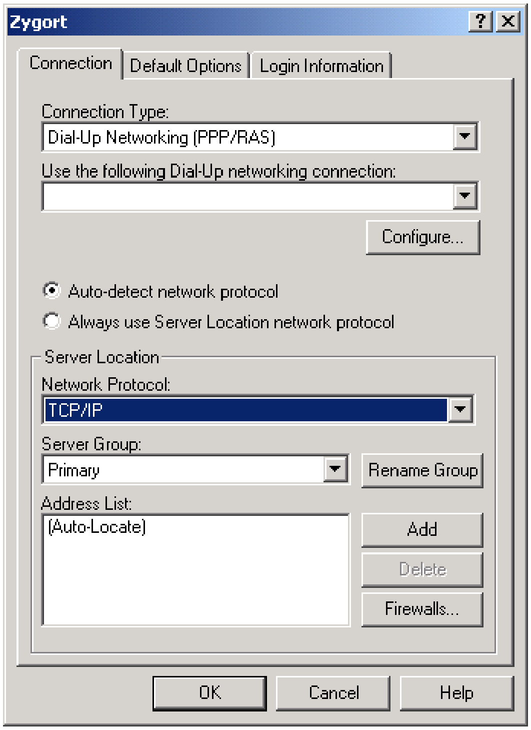
Network Protocol: TCP/IP

Server Group: Primary

Address List: (Auto-Locate)

From the Server Group pull-down menu, you can specify which groups of servers you will connect to: Primary, Backup1, or Backup2. If you do not like the names of these three options, you can select a group and click the Rename Group button to rename it. When you select a server group, the servers listed within the Address List will be used in attempting connections to the server farm, by contacting all servers that have been added to the first group (Primary). If there is no answer from any of the servers in the first group, the next group (Backup1), with all of its servers, will be contacted. If there is no answer from the second group, the final group (Backup2) will be contacted. Each group can contain five servers, giving a total of 15 servers available to contact. Within the Address List text box, you can add server names to which you want your clients to connect. The default entries for TCP/IP and TCP/IP+HTTP allow for automatic discovery of your servers. TCP/IP uses browser broadcasts to locate the master ICA browser for the server farm. Once it is found, the application set is populated for the user. You can use TCP/IP to access MetaFrame 1.*x* and MetaFrame XP server farms whether they are in mixed mode or native mode. You can use TCP/IP+HTTP to access a server from the Internet or through a router. When you make this selection, the client computer queries DNS for the existence of a host record with the name ica. To make this query successful, you must create a host record within the DNS server that points to the IP address of the data collector for the zone.

**FIGURE 11.13** Dial-up networking options



Zygort

Connection Type: Dial-Up Networking (PPP/RAS)

Use the following Dial-Up networking connection:

● Auto-detect network protocol

○ Always use Server Location network protocol

Server Location

Network Protocol: TCP/IP

Server Group: Primary

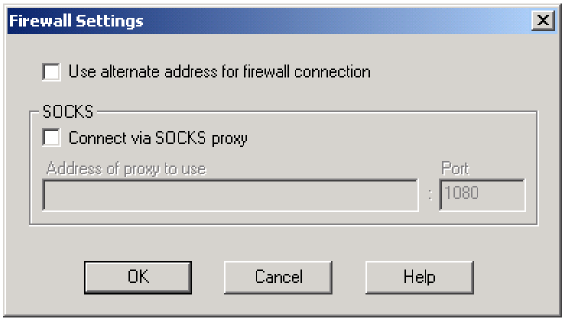
Address List: (Auto-Locate)

If you need to configure firewall support so that users can access the server, click the Firewalls button. Configurations made after clicking the Firewalls button apply as one setting to all servers in all groups. As shown in Figure 11.14, you can enable the alternate address and/or SOCKS proxy settings.

NOTE

For more information concerning the use of an alternate address and SOCKS proxy, see Chapter 8, "Security."

**FIGURE 11.14** Firewall Settings screen



Firewall Settings

☐ Use alternate address for firewall connection

SOCKS

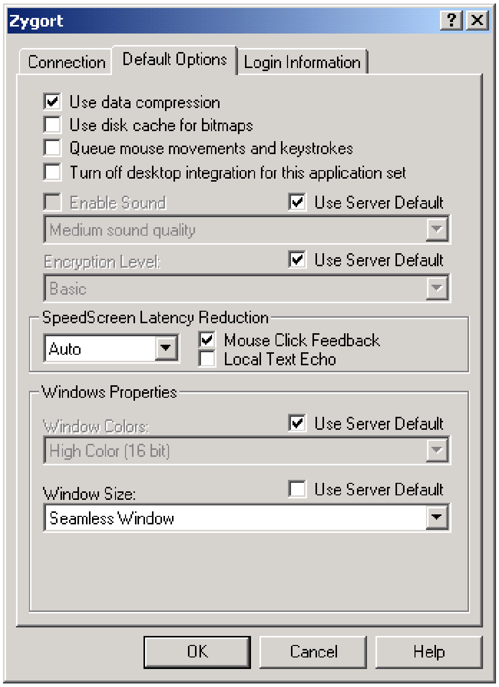
☐ Connect via SOCKS proxy

Address of proxy to use

Port: 1080

The Default Options tab of the Properties sheet contains the majority of the application set configuration settings. As shown in Figure 11.15, these are the available client-side options. You should recall configuring most of these options at the server level earlier in this book.

**FIGURE 11.15** Default Options settings



Zygort

☑ Use data compression
☐ Use disk cache for bitmaps
☐ Queue mouse movements and keystrokes
☐ Turn off desktop integration for this application set

☐ Enable Sound ☑ Use Server Default
Medium sound quality

Encryption Level: ☑ Use Server Default
Basic

SpeedScreen Latency Reduction
Auto ☑ Mouse Click Feedback
☐ Local Text Echo

Windows Properties
Window Colors: ☑ Use Server Default
High Color (16 bit)

Window Size: ☐ Use Server Default
Seamless Window

Starting at the top of the screen, the following options are available:

**Use Data Compression** This option enables compression of the data sent to the client.

**Use Disk Cache For Bitmaps** When this option is enabled, the bitmaps that are sent to the client will be cached on the hard drive. This will enhance the performance of remote clients since the bitmaps will not have to be resent from the server.

**Queue Mouse Movements And Keystrokes** In a slow environment, queuing these items allows the server to respond to commands more efficiently, but the user's interface is not as responsive. You should use this option only when a slow connection is utilized.

**Turn Off Desktop Integration For This Application Set** If you do not want application icons pushed to the desktop or the Start menu, select this option.

**Enable Sound** If you deselect Use Server Default, you can configure the sound options for the application set. You can choose a higher setting than what is configured for the connection, but the lowest setting between the two will be applied.

**Encryption Level** You can specify the encryption strength the client will use when running a session. If Use Server Default is selected, the client will negotiate the encryption level with the server on a per-application basis if RC5 encryption is used.

**SpeedScreen Latency Reduction** The settings applied here control whether the client takes advantage of SpeedScreen functions. Three choices are available: Auto, On, and Off. On takes advantage of the SpeedScreen options that are selected. Off turns the functionality off. Auto makes a determination based on the latency configured for the connection. You can enable two options:

> **Mouse Click Feedback** This option mimics the hourglass when the user double-clicks an application so that the user receives immediate feedback that work is being done.
>
> **Local Text Echo** This option places text into text boxes until the server refreshes the screen.

NOTE For more information on SpeedScreen Latency Reduction, see Chapter 6, "Other Administrative Tools."

**Window Colors** This setting allows you to configure the color depth for the application.

**Window Size** This setting allows you to configure the size of the window. The following options are available:

**Percent Of Screen Size** This option allows you to choose a percentage of the current desktop size.

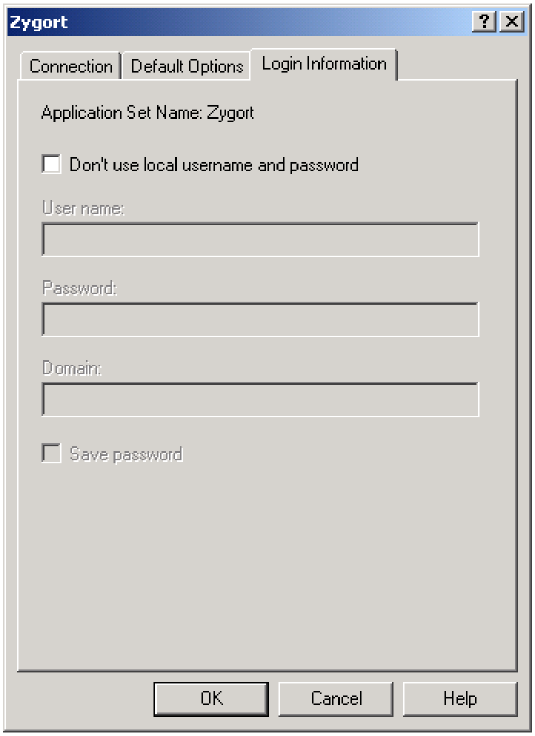
**Full Screen** Selecting this option consumes the entire desktop display area.

**Seamless Window** The application appears on the desktop as an application window, and the remote desktop will not appear.

NOTE Other settings allow a user to configure a specific screen size using the options available from the pull-down menu or customize the screen settings to a desired size.

The Login Information tab of the Properties sheet controls how the user is authenticated to the server farm when trying to access information to populate the application set. Figure 11.16 shows the options available from this tab. Besides the information you must complete to authenticate, there is one check box at the top of the screen, Don't Use Local Username And Password. This option appears if the Use Local Username And Password For Logon option is selected in the ICA Settings configuration screen and was chosen during the installation of the client. For more information on ICA Settings, see the "Program Neighborhood Tools" section later in this chapter.

**FIGURE 11.16** Login Information settings



Zygort

Connection | Default Options | Login Information

Application Set Name: Zygort

□ Don't use local username and password

User name:

Password:

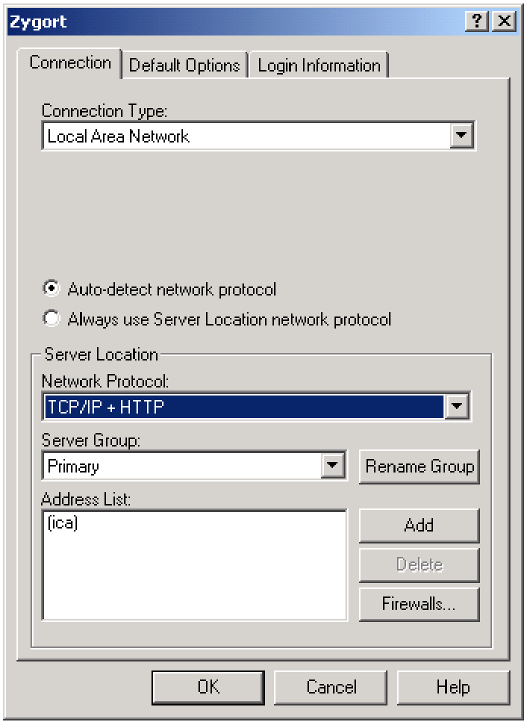
Domain:

□ Save password

## Application Set Manager Level

Once you log on, you have access to all of the server farms within your domain. Depending on how you have Program Neighborhood configured, various application sets are available. If you have chosen to use TCP/IP+HTTP as your protocol, as in Figure 11.17, you will notice that the (ica) entry is the default in the Address List section. If you have configured a Host record in your DNS server that identifies the IP address for ica, the client will be directed to that server, where it will obtain the application set information.

**FIGURE 11.17** The Connection tab configured to autolocate a MetaFrame XP server using TCP/IP+HTTP



Zygort

Connection Type: Local Area Network

● Auto-detect network protocol

○ Always use Server Location network protocol

Server Location

Network Protocol: TCP/IP + HTTP

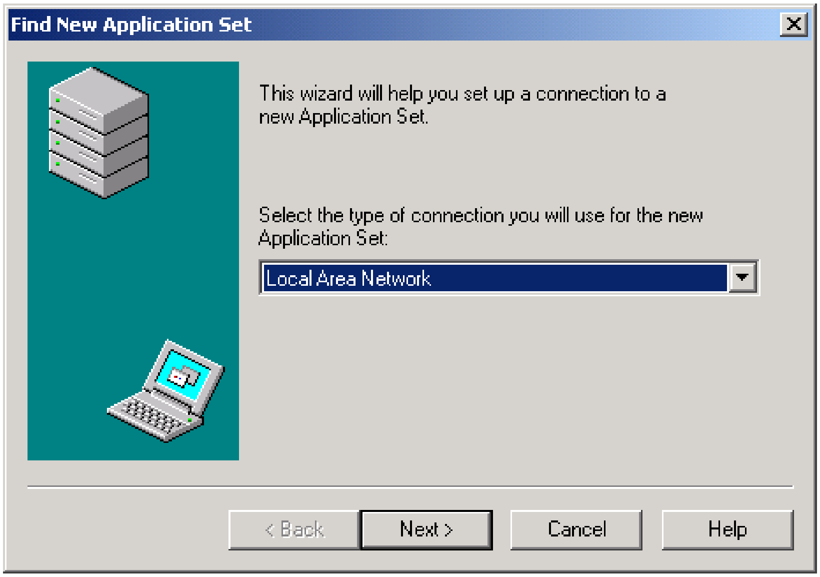
Server Group: Primary

Address List: (ica)

Once the application set loads, the user will see all of the applications within the server farm that they have been granted permission to see. If your organization has more than one server farm, you can double-click the Application Set Manager icon and add application sets at this level. Once these sets are added, users can open each of the application sets and access the applications within them. To add a new application set, double-click the Find New Application Set icon and follow the steps in the wizard. Figure 11.18 shows the first screen that appears, which asks for the connection type to be used to access the application set. Select the appropriate connection type and click Next.

You can specify a description of the application set on the next screen and then choose the application set from the pull-down list, as shown in Figure 11.19. If you click the *Server Location* button on this screen, you can choose the server or servers from which the application set information can be retrieved and loaded, as shown in Figure 11.20. Notice that the same options appear here as on the Connection tab we looked at in Figure 11.17.

**FIGURE 11.18** Choosing a connection type



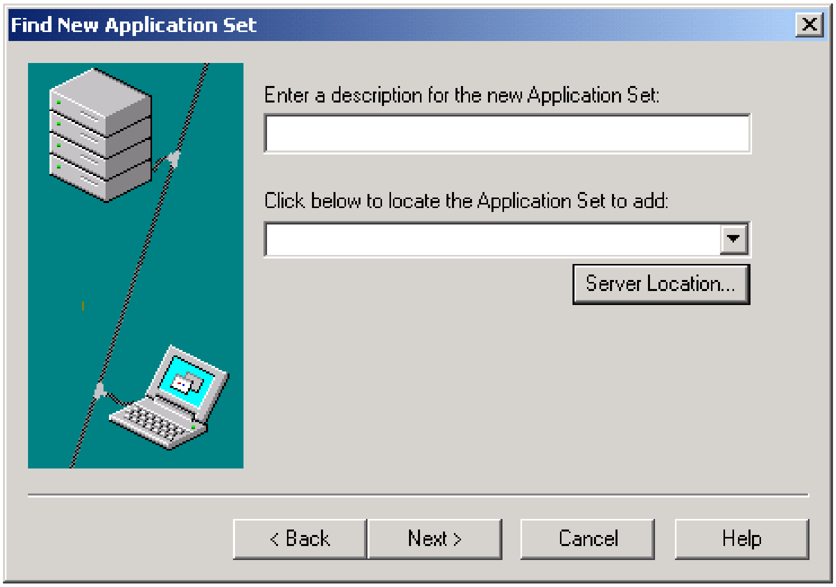
Find New Application Set

This wizard will help you set up a connection to a new Application Set.

Select the type of connection you will use for the new Application Set:

Local Area Network

**FIGURE 11.19** Choosing the application set

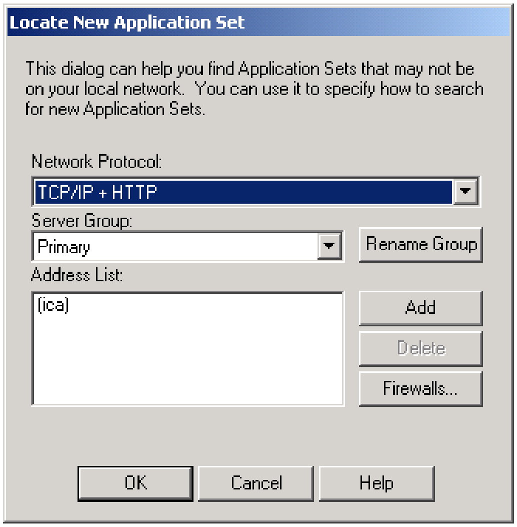


Find New Application Set

Enter a description for the new Application Set:

Click below to locate the Application Set to add:

**FIGURE 11.20** Selecting a server location



Locate New Application Set

This dialog can help you find Application Sets that may not be on your local network. You can use it to specify how to search for new Application Sets.

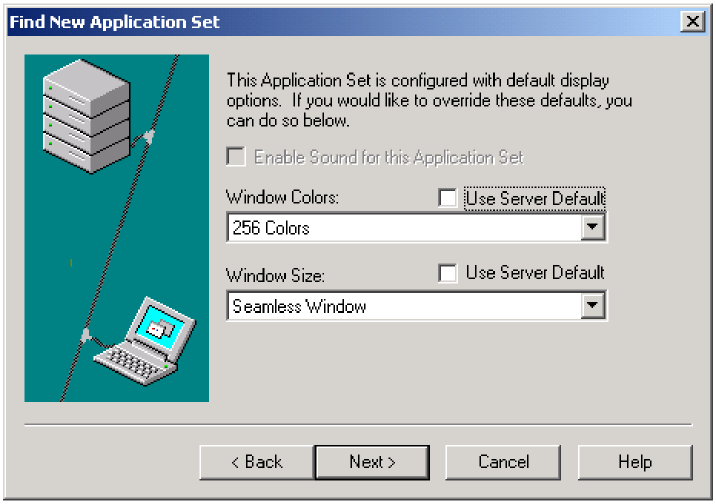
Network Protocol: TCP/IP + HTTP

Server Group: Primary

Address List: (ica)

The default application set options appear when you click the Next button. From the screen shown in Figure 11.21, you can specify the color depth and window size that will be used for the applications within this application set. When you click Next to continue, you are presented the final screen, which gives you one last chance to go back and make some changes or create the application set.

**FIGURE 11.21** Application set options



Find New Application Set

This Application Set is configured with default display options. If you would like to override these defaults, you can do so below.

□ Enable Sound for this Application Set

Window Colors: □ Use Server Default

256 Colors

Window Size: □ Use Server Default

Seamless Window

Once the application set is created, you can double-click its icon to view the applications that exist within the set. You can also right-click the application set icon to change any of the properties you set when creating it. One other option that is available from the context menu when you right-click the application set icon is *Set As Default*. If you select this option, the currently chosen application set becomes the application set whose published applications appear in the Application Set level of Program Neighborhood. Make sure that the applications the user needs to access are a part of the default application set.

Another icon appears at this level, Custom ICA Connections. Double-clicking this icon takes you down to the next level in Program Neighborhood, where you can control applications on an individual basis.

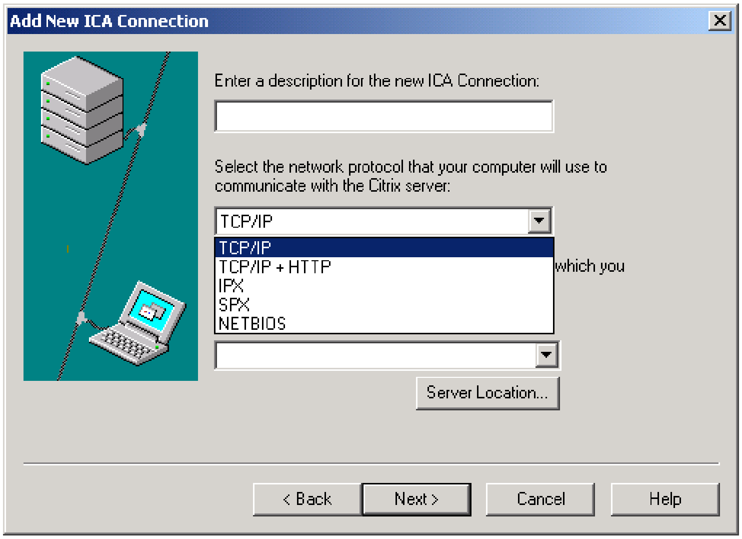
## Custom ICA Connections Level

This level is where you configure access to desktops, server applications, and published applications that are either not configured within the application sets or configured differently than the application set settings. From within this level, you can double-click the Add ICA Connection icon and configure the settings that control access. You can also right-click any application within the application sets at the other two levels and copy the application or desktop to this level. Once it is copied, you can modify the settings for the application, something that cannot be done at the other two levels.

First off, let's see how we can add a new custom ICA connection. Navigate to the Custom ICA Connection level and double-click the Add ICA Connection icon. A wizard should appear, allowing you to choose what type of connection to use. Most of the options within this wizard should look familiar since they are the same options that are presented when you attempt to connect to a server.

After choosing the connection type and clicking Next, you are prompted to provide a description for the connection, along with the protocol you wish to use to communicate with the server. Figure 11.22 shows the protocol options. Notice that TCP/IP and TCP/IP+HTTP are available. Once you select the protocol, you can specify which server desktop will be used or which published application this connection will access.

**FIGURE 11.22** Selecting the protocol for the new connection


Add New ICA Connection

Enter a description for the new ICA Connection:

Select the network protocol that your computer will use to communicate with the Citrix server:

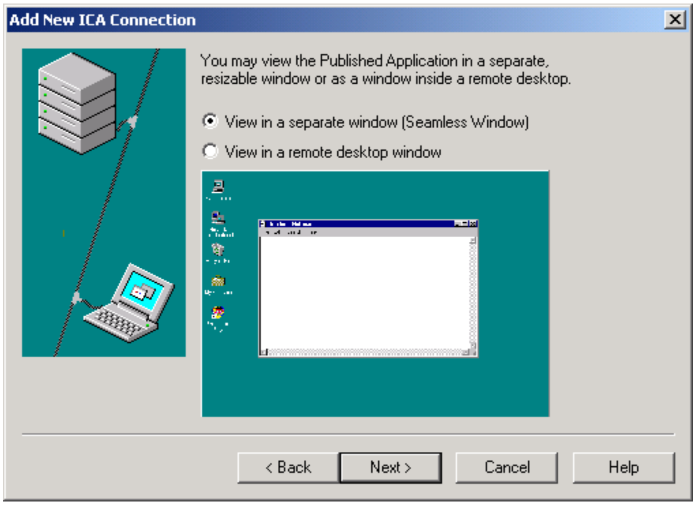
TCP/IP

From here, there are two differences between creating a connection to a server and creating a published application. Published applications need to know how the application will run on the user's desktop—either in a seamless window or within a remote desktop. Server desktops give you the option to run an application when the connection is made. As we step through the rest of the wizard, we will identify the two differences. The first one occurs as soon as you select a published application from the pull-down list and then click the Next button.

Figure 11.23 shows the screen you will see when you are creating a connection to a published application. After you decide which option to use and click Next, you are asked to select the desired *Encryption Level*, as shown in Figure 11.24. This is the same screen that appears immediately after clicking Next when you choose to connect to a server desktop.

The next screen allows you to specify the username, password, and domain that will be used when connecting to the server. You can leave this information blank if you want the user to supply credentials when connecting, or you can fill in the information so that the user is automatically authenticated when starting an application. Notice the Use Local User Name And Password check box, shown in Figure 11.25. If you select this option, the username and password from the current profile are used to authenticate the user.

**FIGURE 11.23** Choosing how the application appears



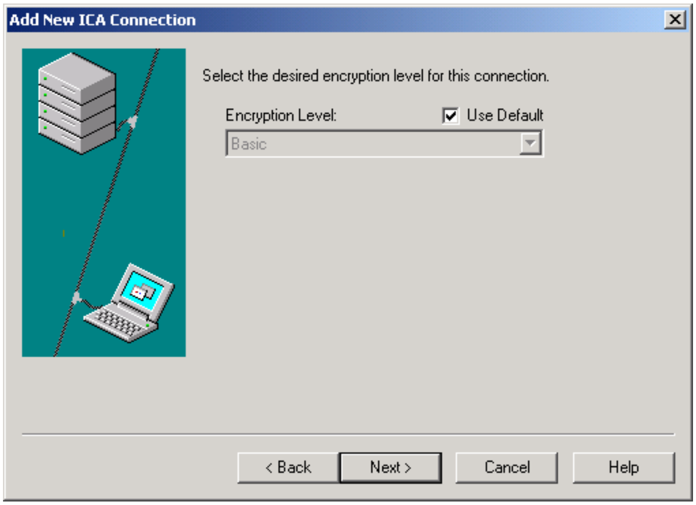
Add New ICA Connection

You may view the Published Application in a separate, resizable window or as a window inside a remote desktop.

● View in a separate window (Seamless Window)

○ View in a remote desktop window

**FIGURE 11.24** Choosing the encryption level

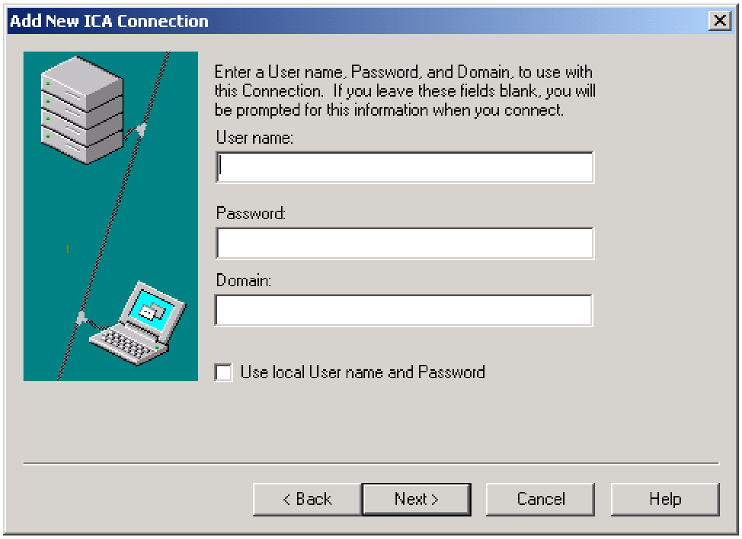


Add New ICA Connection

Select the desired encryption level for this connection.

Encryption Level: Basic ☑ Use Default

**FIGURE 11.25** Logon credentials



Add New ICA Connection

Enter a User name, Password, and Domain, to use with this Connection. If you leave these fields blank, you will be prompted for this information when you connect.

User name:

Password:

Domain:

□ Use local User name and Password

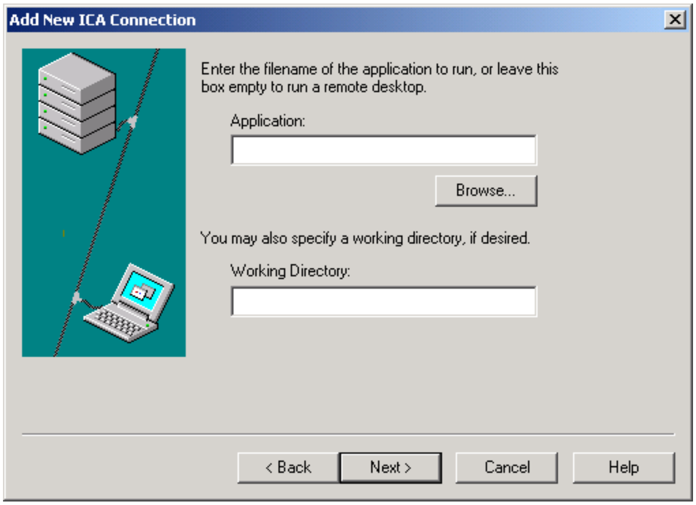
Click Next, and you can specify the color depth for the connection. Clicking Next again brings you to the next disparity between the two connection types. If you are connecting to a server desktop, you are given the option to run a specific application for this connection, as shown in Figure 11.26. From here, you could specify an application on the server whether it is published or not. However, using this option allows you to run only that application during the session. No other application can be run from the desktop. If you end the application, the session will end also.

NOTE

By not defining a specific application on this screen, you will be connecting to a desktop, which will allow you to run multiple applications on that server.

Of course, there is a final summary screen to the wizard that allows you to decide whether or not you really want to create the connection. If you click Finish, the new icon appears for the connection and you will be able to use it to connect to the server or published application. One very nice feature that Citrix provided is the ability to add the connections to the desktop. Once the connections are available in Program Neighborhood, you can right-click the icon and choose the option Create Desktop Shortcut. Using this function alleviates the need to educate users about navigating the levels of Program Neighborhood to find the applications and desktops that they use.

**FIGURE 11.26** Choosing an application to run



Add New ICA Connection

Enter the filename of the application to run, or leave this box empty to run a remote desktop.

Application:

You may also specify a working directory, if desired.

Working Directory:

To further control how Program Neighborhood functions, we can use the Tools menu and configure its options. In the next section, we will discuss the items available.

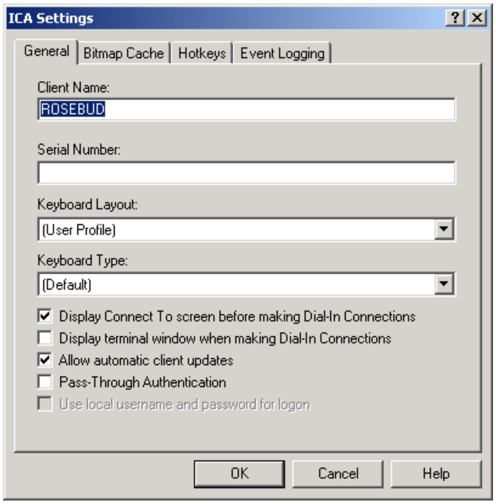
## Program Neighborhood Tools

The Tools menu has three options that allow you to control how Program Neighborhood connects and interacts with the MetaFrame servers and responds to client commands. This is where you control how modems call and connect to MetaFrame servers from remote clients, which key combinations act as hotkeys for sessions, and even how much hard drive space cached bitmaps consume.

### ICA Settings

When you select the first option, *ICA Settings*, you are presented with the configuration screen shown in Figure 11.27. The four tabs on this screen allow you to control Program Neighborhood and how it performs for the client.

**FIGURE 11.27** The ICA Settings General tab



ICA Settings

General | Bitmap Cache | Hotkeys | Event Logging

Client Name: ROSEBUD

Serial Number:

Keyboard Layout: (User Profile)

Keyboard Type: (Default)

☑ Display Connect To screen before making Dial-In Connections

☐ Display terminal window when making Dial-In Connections

☑ Allow automatic client updates

☐ Pass-Through Authentication

☐ Use local username and password for logon

The General tab offers the following information:

**Client Name** This is the name that is presented to the MetaFrame server when the client initiates a connection. This client name will appear in Citrix Management Console once a connection is made. It is then stored in the *wfcname.ini* file in the root of the system drive of the client computer.

**Serial Number** If you have purchased the Citrix PC Client Pack, you must enter the license number from the pack to allow the client to connect to the MetaFrame server.

**Keyboard Layout** This item specifies the layout of the keyboard so that the correct keystrokes are sent to the server. If you select User Profile, the setting within your user profile will determine which layout is used.

**Keyboard Type** This option determines the type of keyboard used by the client system so that the session will use the right identifiers when keyboard data is sent to the server.

**Display Connect To Screen Before Making Dial-In Connections** This item displays the Connect To screen when the user initiates a dial-in connection, allowing the correct connection to be selected. Selecting this option allows a client to choose among multiple connections. This comes in handy if the user connects to the Internet with one connection and the MetaFrame server with another.

**Display Terminal Window When Making Dial-In Connections** If you have any special requirements when you attempt to make a connection, you may have to select this option.

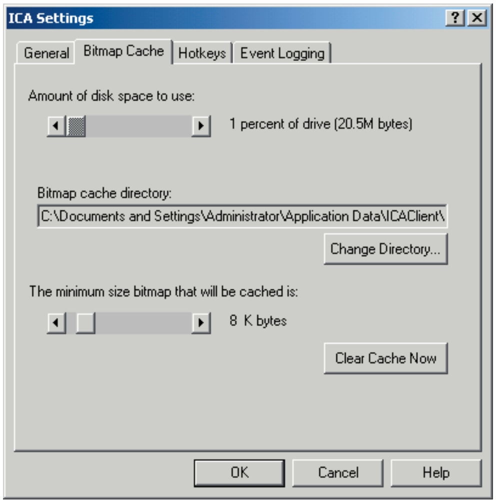
**Allow Automatic Client Updates** When this item is selected, if there are any updates for the client, the updated client software will download and update automatically.

**Pass-Through Authentication** When this option is selected, the user's current account information can be used to authenticate to the server farm. This selection must be checked in order for the Use Local Username And Password For Login selection to be available.

**Use Local Username And Password For Login** When this item is selected, the current username and password are used for the ICA session, negating the need for multiple authentications. This item will not be grayed out if you chose to use the local username and password during the installation of the client.

The next tab, shown in Figure 11.28, lets you control the bitmap cache on the client computer. The bitmap cache is one of the technologies that Citrix employs to enhance the performance of MetaFrame. Acting the same as the Temporary Internet Files do within Internet Explorer, the bitmap cache stores bitmaps locally on the client, and if they are needed again during the session, they can be retrieved from the hard drive instead of having to pass across the network.

**FIGURE 11.28** The Bitmap Cache tab



ICA Settings

Amount of disk space to use: 1 percent of drive (20.5M bytes)

Bitmap cache directory: C:\Documents and Settings\Administrator\Application Data\ICAClient\

The minimum size bitmap that will be cached is: 8 K bytes

Following are the options you can configure from this tab:

**Amount Of Disk Space To Use** This slider allows you to control the maximum amount of hard drive space that you will permit the client to consume before the oldest entries are deleted to make room for new entries. The default is 1 percent of the drive size.

**Bitmap Cache Directory** Clicking the Change Directory button allows you to browse the directory structure on the computer and select which directory you want to use to store the bitmaps.

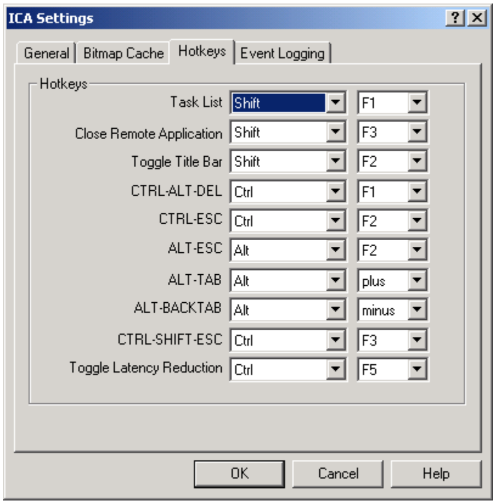
**The Minimum Size Bitmap That Will Be Cached Is** It may actually be more efficient to have very small files sent across the network than to access them from a slow hard drive. In this entry, specify the smallest size bitmap you want to cache. The default entry is 8KB.

**Clear Cache Now** Clicking this button flushes all of the bitmaps from the directory.

Next up is the *Hotkeys* tab. The entries specified here determine which key combinations act as the standard hotkeys within the session. If you are running Windows 2000 Professional or Windows NT Workstation 4.0 as your client and want to access the Security dialog box within the session, you cannot use the standard Ctrl+Alt+Delete key combination since the local desktop will react when you press those keys. These hotkeys take over those familiar functions. For instance, the default hotkey combination for accessing the Security dialog box in your session is Ctrl+F1. You will need to train your users so they know which key combinations to use. From this tab, you can modify the key combinations to suit your organization's needs. Figure 11.29 shows the default settings for each of the hotkey combinations.

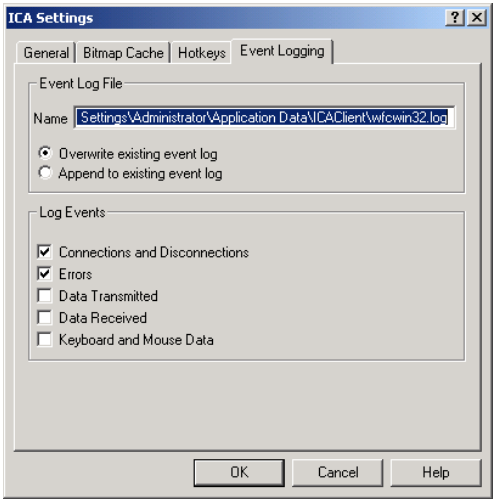
The final tab, Event Logging, is shown in Figure 11.30. You can control the location and amount of information that is logged from this tab.

**FIGURE 11.29** The Hotkeys tab



| | | |
|---|---|---|
| Task List | Shift | F1 |
| Close Remote Application | Shift | F3 |
| Toggle Title Bar | Shift | F2 |
| CTRL-ALT-DEL | Ctrl | F1 |
| CTRL-ESC | Ctrl | F2 |
| ALT-ESC | Alt | F2 |
| ALT-TAB | Alt | plus |
| ALT-BACKTAB | Alt | minus |
| CTRL-SHIFT-ESC | Ctrl | F3 |
| Toggle Latency Reduction | Ctrl | F5 |

**FIGURE 11.30** The Event Logging tab



Name: Settings\Administrator\Application Data\ICAClient\wfcwin32.log

● Overwrite existing event log
○ Append to existing event log

☑ Connections and Disconnections
☑ Errors
☐ Data Transmitted
☐ Data Received
☐ Keyboard and Mouse Data

The options available to configure are as follows:

**Name** This field shows the complete path and filename where the events are logged.

**Overwrite Existing Event Log** If you select this radio button, when a new session is initiated, the log file will be overwritten.

**Append To Existing Event Log** If you select this radio button, all entries are kept, and as a new session is started, the logged events are added to the end of the file.

**Log Events** The selections in this section control what types of events are logged. They include the following options:

**Connections And Disconnections** Checking this option logs an event whenever the client connects to or disconnects from the MetaFrame server.

**Errors** If this option is selected, whenever the client encounters an error, the error information is logged.

**Data Transmitted** Enabling this option logs an event for every packet sent from the client. It should not be enabled unless you are performing troubleshooting.

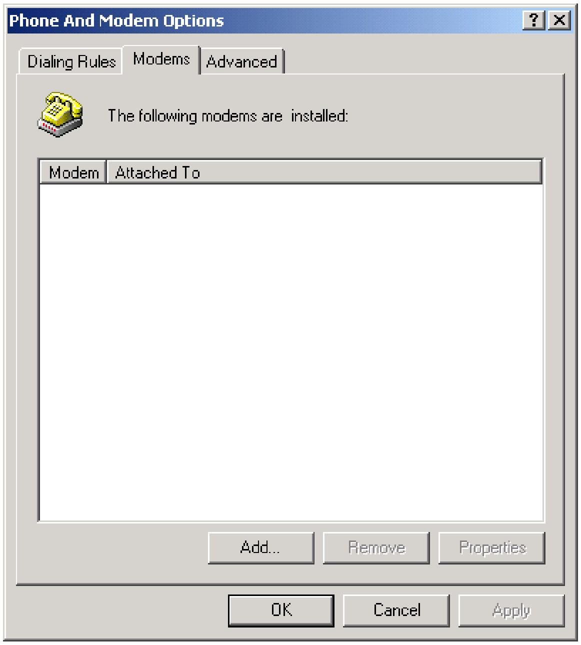
**Data Received** Enabling this option logs an event for every packet sent to the client. It should not be enabled unless you are performing troubleshooting.

**Keyboard And Mouse Data** If you enable this item, an event is logged for every keyboard or mouse entry. It should not be enabled unless you are performing troubleshooting.

## Modems

When you select the Modems option from the Tools menu, you will see the Phone And Modem Options screen shown in Figure 11.31. The options available on this screen depend on the operating system you are using, since the Modems option activates the dialing properties of the operating system. This is where you configure a user's computer to dial in to a MetaFrame server. If you have an async connection specified on the MetaFrame server, Program Neighborhood can dial in and run sessions across this connection.

**FIGURE 11.31** Phone And Modem Options screen

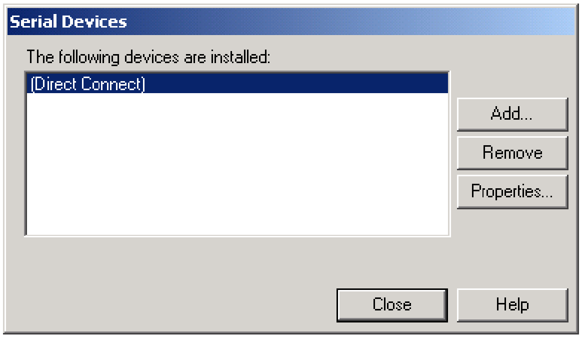


The following modems are installed:

## Serial Devices

The final selection from the Tools menu is Serial Devices, shown in Figure 11.32. From this screen, you can configure the serial ports that are used when connecting a modem or serial device to the computer.

**FIGURE 11.32** Serial Devices screen



The following devices are installed:

(Direct Connect)

Now that we have taken a good look at Program Neighborhood, you should be ready to go out and configure all the users' computers. Understanding how the client works when connecting with the server will save you lots of time in configuring Program Neighborhood. Since we've finished our discussion of the finer points of this client-side tool, we need to move on and talk about another such tool, NFuse. The next chapter is devoted to this up-and-coming web technology.

# Summary

Once you've configured the server to allow users to connect and start sessions that use published applications or server desktops, you must configure the client software on the users' computers to allow them access to the server. Program Neighborhood allows users to access applications and desktops in a server farm and presents it to them as an application set. This application set shows them every application in the server farm that they have been granted permission to use.

Each of the three levels of Program Neighborhood allows you to control what the user can access. The Application Set level displays the applications available in the default application set. The Application Set Manager level allows you to control which server farms are accessed and which application set is the default. The Custom ICA Connections level allows you to create custom connections to server desktops and published applications.

Using the Tools menu utilities, you can further customize how Program Neighborhood works in any environment. You can change how the user interacts with the interface by changing the hotkeys, and you can control modem connections to remote MetaFrame servers that have async connections available.

From here, we will move on to web technologies and will show how NFuse can make our lives easier in distributed and centralized environments. These web technologies are the wave of the future, and Citrix is planning on staying at the crest of the wave and riding it out.

# Exam Essentials

**Understand how to navigate the three levels of Program Neighborhood.** Program Neighborhood has three levels, the top of which is the Application Set. Next is the Application Set Manager level, which can be accessed through its icon on the Application Set level. From the Application Set Manager, you can double-click the Custom ICA Connections icon to gain access to that level.

**Know how to connect to a server farm.** Using the Application Set properties, you can specify the server to connect to or the data collector to connect to.

**Know how to configure the default application set.** From the Application Set Manager, you can right-click an application set and select Set As Default to configure it as the default application set.

**Know how to add application icons to the desktop.** You can right-click any application or desktop icon in Program Neighborhood and select Create Desktop Shortcut to add the icon to the desktop.

**Know how to modify application properties.** If you need different settings applied to an application session from the default settings provided for by the application set, you can right-click the application and select Copy To Custom Connections. From the Custom ICA Connections level, you can modify the properties of the new connection.

**Know how to add a new application set.** The Find New Application Set Wizard steps you through the process of locating a new application set.

**Know how to create a custom ICA connection.** The New ICA Connection Wizard steps you through the options to configure a new connection to a server desktop or published application.

**Know how to create a connection to an application on a server that is not published.** You can create a custom connection to a server and then specify the application path so that the application starts when the session is started.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Application Set
Application Set Manager
Copy To Custom Connections
Create Desktop Shortcut
Custom ICA Connections
Encryption Level
Find New Application Set
Hotkeys
ICA Settings
Program Neighborhood
Server Location
Set As Default
`wfcname.ini`

# Exercise

In this exercise, we'll modify the Program Neighborhood settings in several ways. First, we'll change the network protocol to TCP/IP+HTTP. Then we'll change the hotkey assignment for Ctrl+Alt+Delete. Finally, we'll add a server to the Address List of the Application Set Settings dialog box.

## EXERCISE 11.1

### Modifying Program Neighborhood Settings

First, let's change the network protocol to TCP/IP+HTTP:

1. Open Program Neighborhood.
2. Click File on the menu bar.
3. Select Custom Connection Settings from the File menu.
4. On the Connection tab, locate the Default Server Location area of the dialog box.

**EXERCISE 11.1 *(continued)***

5. Under Network Protocol, click the drop-down arrow and select TCP/IP+HTTP.
6. In the Address List area, click the Add button.
7. When the Add Server Location Address window appears, enter the hostname or IP address of the data collector on your network or subnet.
8. Enter the port number that the data collector uses to communicate with XML.
9. Click OK to close the Add Server Location Address window.
10. Click OK to close the Custom ICA Connections window.

Next, we'll change the hotkey for Ctrl+Alt+Delete. Let's say you have a software application that uses Ctrl+F1 as a special function, but when you run the application in an ICA session, every time you hit Ctrl+F1, the Windows Security screen pops up. To change the hotkey assignment, follow these steps:

1. Open Program Neighborhood.
2. In the Tools menu, select ICA Settings.
3. Click the Hotkeys tab.
4. In the option labeled CTRL-ALT-DEL, click the drop-down menu for Ctrl and change it to Alt.
5. Click OK.

Finally, we'll add a server to the Address List of the Application Set Settings dialog box:

1. Open Program Neighborhood.
2. From the File menu, select Application Set Settings.
3. Select the Connection tab.
4. Under Network Protocol, select TCP/IP+HTTP.

**EXERCISE 11.1 *(continued)***

5. In the Address List area, click Add.
6. When the Add Server Location Address window appears, enter the name or IP address of the data collector and the port number that XML uses to communicate.
7. Click OK to exit the Add Server Location Address window.
8. Click OK to exit the Application Set Settings window.

# Review Questions

1. Which ICA Clients can use Program Neighborhood?

   A. Win32

   B. Win16

   C. DOS 32

   D. Unix

2. What is the name of the user's view of published applications that the user has authority to access?

   A. Program group

   B. Program set

   C. Application group

   D. Application set

3. Published applications appear in the application set and contain information about which of the following? (Choose all that apply.)

   A. Session window size

   B. Audio compression

   C. Supported levels of encryption

   D. Server

4. How do you make settings that will take effect for all new ICA connections that are created?

   A. Navigate to the Custom ICA Connections level and open the Properties sheet from the File menu of Program Neighborhood.

   B. Navigate to the Custom ICA Connections level and open the Properties sheet from the Settings menu of Program Neighborhood.

**C.** Navigate to the Custom ICA Connections level and open the Custom Connection Settings dialog box from the File menu of Program Neighborhood.

**D.** Navigate to the Custom ICA Connections level and open the Custom Connection Settings dialog box from the Settings menu of Program Neighborhood.

**5.** Which type of connection is used when the MetaFrame XP server is running in mixed mode?

**A.** TCP/IP

**B.** TCP/IP+HTTP

**C.** HTTP

**D.** NetBIOS

**6.** Which type of connection is used when the MetaFrame XP server is running in native mode?

**A.** TCP/IP

**B.** TCP/IP+HTTP

**C.** HTTP

**D.** NetBIOS

**7.** Which network protocols are available in the Connection tab of the Properties sheet in Program Neighborhood? (Choose all that apply.)

**A.** TCP/IP

**B.** NetBIOS

**C.** AppleTalk

**D.** HTTP

8. Where do you change encryption settings for the connection to an individual server or published application?

   A. In the Options tab of the program's Properties sheet

   B. In the Settings tab of the Program Neighborhood's Custom Connections Settings sheet

   C. In the Default Options tab of the Custom Connection Settings tab in Program Neighborhood

   D. In the Settings tab of the Custom Connection Settings tab in Program Neighborhood

9. Where can you change the name of the client as it appears in the Citrix Management Console?

   A. In the Name field on the Client Settings tab of the ICA Settings dialog box

   B. In the Client Name field on the Settings tab of the ICA Settings dialog box

   C. In the Client Name field on the General tab of the ICA Settings dialog box

   D. In the Name field on the Connection Settings tab of the ICA Settings dialog box

10. What file contains the name of the client that appears in the Citrix Management Console?

    A. `wfcname.ini`

    B. `mfname.ini`

    C. `xpname.ini`

    D. `xpcname.ini`

11. You have just installed a new ICA Client on your workstation. Your ICA Client Distribution settings on your server farm say to replace any version of the client with the version that is in the database. How can you change this so your client will not be changed with the one that is in the database?

- **A.** Remove the check from the box labeled Allow Automatic Client Updates in the General tab of the ICA Settings dialog box.
- **B.** Remove the check from the box labeled Do Not Update This Client in the General tab of the ICA Settings dialog box.
- **C.** Remove the check from the box labeled Allow Automatic Client Updates in the Client tab of the ICA Settings dialog box.
- **D.** Remove the check from the box labeled Do Not Update This Client in the Settings tab of the ICA Settings dialog box.

**12.** By default, what is the minimum size bitmap that will be cached in the Bitmap Cache Directory?

- **A.** 4KB
- **B.** 8KB
- **C.** 16KB
- **D.** 24KB

**13.** By default, what is the hotkey combination for Ctrl+Alt+Delete?

- **A.** Ctrl+Tab
- **B.** Ctrl+Delete
- **C.** Alt+F1
- **D.** Ctrl+F1

**14.** Where can you change the default settings for hotkey combinations?

- **A.** The Hotkeys tab of the ICA Settings dialog box
- **B.** The General tab of the ICA Settings dialog box
- **C.** The Hotkeys tab of the Custom Connection Settings dialog box
- **D.** The Settings tab of the Custom Connection Settings dialog box

**15.** What are the path and filename that the ICA event log is stored to by default?

A. `%systemroot%\system32\wfcwin32.log`

B. `%systemroot%\system32\wfcevent.log`

C. `%userprofile%\Application Data\ICAClient\wfcwin32.log`

D. `%userprofile\Application Data\Citrix\wfcevent.log`

16. Which of the following events can you log in the Event Logging tab? (Choose all that apply.)

A. Errors

B. Data Received

C. The server name that is hosting the published application that you are running

D. Mouse Data

17. What is the default disk space used by MetaFrame for bitmap caching?

A. 5 percent

B. 1 percent

C. 100MB

D. 250MB

18. Where do you change settings for SpeedScreen Latency Reduction for ICA Clients in the server farm?

A. In the Options tab of the connection's Properties sheet

B. In the Connection tab of the connection's Properties sheet

C. In the Options tab of the Custom Connection Settings dialog box

D. In the Settings tab of the Custom Connection Settings dialog box

19. Which connection types are not available for network connections to the MetaFrame XP server farm when you create a custom ICA connection?

**A.** Local Area Network

**B.** ICA Dial-In

**C.** Direct cable connection

**D.** Dial-up networking

**20.** When using Program Neighborhood on a Windows 2000 Professional workstation, and the system drive is labeled as `C:` with the system files in the `C:\winnt` directory, where is the file that contains the name information for the client located on the client device?

**A.** `C:\`

**B.** `C:\winnt`

**C.** `C:\winnt\Citrix`

**D.** `C:\winnt\system32`

# Answers to Review Questions

1. A. Citrix ICA Win32 Clients use Program Neighborhood to connect to MetaFrame XP servers.

2. D. An application set is a user's view of the published applications that the user has authority to access.

3. A, B, C. Published applications appear as icons in the application set and are configured for such connection properties as session window size and colors, supported levels of encryption, audio compression, and video.

4. C. The Custom Connection Settings dialog box, which you access from the File menu of Program Neighborhood, contains settings that are defined as default for new connections. All new ICA connections inherit these settings unless specifically defined in the ICA connection itself.

5. A. TCP/IP is used for direct connections. It is also used when the MetaFrame XP server is set to mixed mode. This option will broadcast for an ICA browser to find the published application or server.

6. B. TCP/IP+HTTP is the recommended network protocol for ICA connections with MetaFrame XP running in native mode. The connection will look to the data store for connection information to a published application or server.

7. A, B. TCP/IP, TCP/IP+HTTP, IPX, SPX, and NetBIOS are the supported protocols that can be used for connections to MetaFrame XP servers.

8. A. Encryption settings can be defined and changed in the Options tab of the connection's Properties sheet.

9. C. The client name that appears in the Citrix Management Console is defined in the Client Name field on the General tab of the ICA Settings dialog box.

10. A. The client name that is defined in the ICA Settings dialog box is stored in the `wfcname.ini` file in the root of the system drive.

11. A. To prevent an individual workstation from being updated by the ICA Client Update Configuration utility, remove the check from the box labeled Allow Automatic Client Updates in the General tab of the ICA Settings dialog box.

12. B. This default setting for the minimum size of bitmap that will be cached is 8KB.

13. D. The default setting for the Ctrl+Alt+Delete hotkey is Ctrl+F1.

14. A. In the Hotkeys tab of the ICA Settings dialog box, you can view the current key combinations and what they are mapped to, and you can also change the combinations.

15. C. The ICA event log is stored by default in the `%userprofile%\Application Data\ICAClient\wfcwin32.log` for Win32 ICA Clients.

16. A, B, D. All of the following can be logged by selecting the appropriate choice in the Event Logging tab: Errors, Data Transmitted, Data Received, Connections And Disconnections, and Keyboard And Mouse Data.

17. B. Use the slider bar to determine how much local disk space to use for bitmap caching. The default is 1 percent.

18. A. SpeedScreen Latency Reduction settings are defined in the Options tab of the connection's Properties sheet and also in the Default Options tab of the Application Set Properties sheet.

19. C. When you run the Add ICA Connection Wizard, the Connection Type setting defines the type of network connection that will be used to connect to the MetaFrame XP server farm. Choices are Local Area Network, Wide Area Network, Dial Up Networking (PPP/RAS), and ICA Dial-In. The Application Set setting does not have ICA Dial-In as a choice.

20. A. The client name that is defined in the ICA Settings dialog box is stored in the `wfcname.ini` file in the root of the system drive.

# Chapter 12

# Web Connectivity and NFuse

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **10. Web Connectivity**

- 10a. Recognizing Citrix Web Components
- 10b. Identifying NFuse Features and Components

Welcome to the chapter that everyone wants to read about. *Web technologies* have become the most talked about technologies in the past few years. Everything from creating *dynamic pages* that are tailor-made for the user to accessing e-mail from a web page is a hot topic. *NFuse* is no exception. It has become such an integral part of the Citrix product offering that it is now packaged as part of every MetaFrame XP product. But NFuse is not the only piece of the web puzzle. In this chapter, we are going to introduce you to the finer aspects of MetaFrame XP web integration.

## How Does MetaFrame XP Work with the Web?

MetaFrame XP allows you to create web pages that include links to the published applications within your server farm. These links can be hard-coded into a web page, or you can use dynamic programming practices to present the links to users. You can provide every application that is published within your server farm to users from the web pages on your company's website. Presenting the applications in this manner allows you to give your users access to the applications they need. Instead of having them access your server farm through Program Neighborhood, they connect to a web page and all of the applications appear as hyperlinks on the page.

At the most basic level, you can design web pages to show the hyperlinks to applications. Static pages such as this can be written very quickly and are easy to implement within a web server. You can control which applications are accessible from the web page since only those that are presented on the web page are available to the user. There are drawbacks to using static pages, however. If you want to give users access to another application, you will have to edit the web page and add another hyperlink. Plus, if this is the only web page you are presenting to users, every user will see the same application hyperlinks, whether they have permission to actually use the applications or not.

Those administrators who have experience writing dynamic web pages, or have access to an experienced development staff, can take advantage of the newer web technologies that create web pages tailored to the individual user. You can control which applications are presented to the user through the dynamic content. Citrix has taken advantage of both *Active Server Pages (ASP)* and *Java* technologies and has provided web developers with the documentation that they need to build these pages.

And of course, Citrix has provided a very easy way to offer personalized pages that include only the applications the user has been given permissions to use. As long as you have a web server, MetaFrame server, and NFuse installed, you can build dynamic pages automatically for every user who connects to the default web page. Again, Citrix has provided all of the tools necessary to build and manage the pages. Later in this chapter, we will look at NFuse in more depth, but let's start off with a look at the pieces that make up the web puzzle.

# Web Components

MetaFrame is a very robust application that can take advantage of many of the newer technologies available today. Citrix has made sure that these technologies are not tied to a single platform for web accessibility. MetaFrame supports the most popular web servers. Within this section, we will take a look at the web servers, client software, and web browsers needed to access sessions through web technologies. Then we will examine published applications and the tools we need to take advantage of when configuring them for user access.

## Web Servers

All of the *web servers* shown in the following list have one thing in common—they all support active scripting, whether the scripting engine is Microsoft's Active Server Pages or Sun's *JavaServer Pages*. You can use any of these web servers in your MetaFrame environment, but we will concentrate on the Microsoft implementation of web services, Internet Information Server (IIS):

IIS 4.0 or later running on Windows NT Server 4.0

IIS 4.0 running on Windows NT Server 4.0, Terminal Server Edition

IIS 5.0 running on Windows 2000 Server

Netscape Enterprise Server version 3.6 on Solaris 7 or Solaris 8

iPlanet Web Server version 4.0 with Service Pack 4 on Solaris 7 or Solaris 8

iPlanet Web Server version 4.1 on Solaris 7 or Solaris 8

Apache Server 1.3.9 or later on Red Hat Linux 6.0 using Sun JDK 1.2.2, Apache JServ 1.1, and GNUJSP 1.0

Apache Server 1.3.9 or later on Solaris 7 or Solaris 8 using Sun JDK 1.2.2, Apache JServ 1.1, and GNUJSP 1.0

More platforms than this may be supported, but Citrix has not fully tested them. If the web server you are using does support JavaServer Pages, you may be able to use it as the web server in your MetaFrame environment. Test your server prior to deciding whether or not to change server platforms.

## Web Browser

*Web browsers* need to be able to take advantage of the scripting nature of NFuse. Most of the web browsers currently in use can take advantage of these features so you should not have any issues when trying to connect to the web server to access published applications. Microsoft's Internet Explorer and Netscape's Navigator have long supported the technologies that Citrix uses to implement NFuse. If you are unsure whether your web browser is supported, the only requirement is that your browser support Java.

## ICA Client Software

Any user who attempts to connect to a MetaFrame server to run a session needs ICA Client software installed on their computer. If Program Neighborhood is installed on the user's computer, the required software is already available to take advantage of any of the web technologies. Program Neighborhood is a large program. If the user's computer does not already have Program Neighborhood installed, and the user is accessing the website across a slow connection, downloading and installing Program Neighborhood could take an inordinate amount of time. To alleviate the problem of downloading such a large file, Citrix has provided a smaller program that does not include all of the functionality of Program Neighborhood, yet it does contain all of the required tools to connect to sessions that are started through a web interface.

This "Program Neighborhood Lite," `ica32t.exe`, can be found on the MetaFrame XP installation CD in the `icaweb\en\ica32` directory. Placing this file on your server and giving users access to it through a web page allow you to deploy the client software from a centralized location. Once this program is installed on your computer, the web browser will act as the user interface while the client software controls the access to the session.

NOTE

If you want to install Program Neighborhood instead of the "Lite" version on the client device, you can modify the entries within the `icaclientinfo.asp` file (or `icaclient.jsp` if you are using JavaServer Pages) to reference `ica32.exe` instead of `ica32t.exe`.

## Published Applications

Two options are available when you allow users to start a session using web technologies: They can connect to published applications or they can connect to desktops that are published on your server. As we discussed in Chapter 9, "Application Support," publishing applications and desktops is a relatively painless process once the application has been installed on the server.

After you open Citrix Management Console and navigate to the Applications node, all of the published applications for the server farm appear in the list. If you select one of the applications, you will notice that a new group of icons appears in the toolbar beneath the console menu items. Two of these icons open wizards that allow you to control how the application is accessed. The first of these two wizards creates an *ICA file* that is used to control the application session from the web. The second wizard builds an *HTML file* that you will use to present a hyperlink to the users when they connect to your website.

For the published applications themselves, no special settings are required when running through the Application Publishing Wizard. Once the application has been published, you will need to create the ICA file. If you are proficient at writing your own HTML code, you may not have to run the HTML Wizard. For more information on the special tags that are available to use when writing code for a published application's hyperlink or to see the entries that are available for the ICA file, check the Citrix website for the NFuse Administrator's Guide.

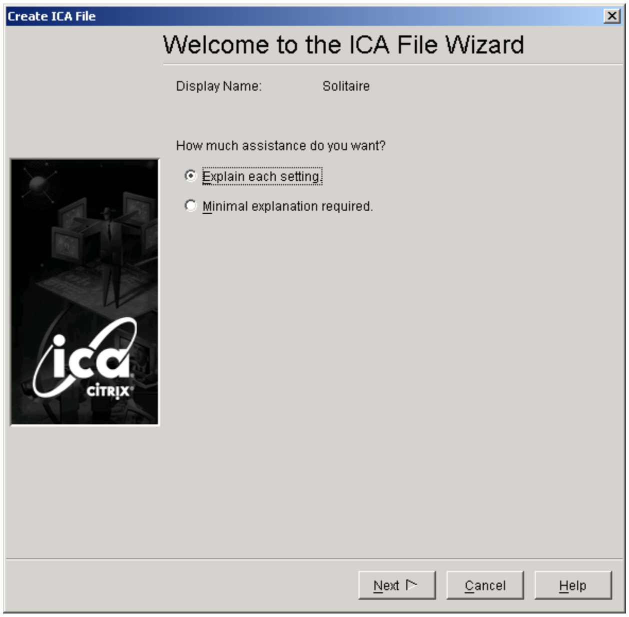
## ICA Files

Citrix has given us a very simple way to create an ICA file: a wizard. Now, as with nearly every other wizard available, the basic parameters are available to configure. If you want to include any special entries, you will need to edit the ICA file yourself. While we will take a good look at the wizard used to create the file and a brief look at the file itself, discussing the file in great detail is beyond the scope of this book. Citrix has a very well written Administrator's Guide available on their website if you would like to dig in deeper.

Once you have selected an application from the Applications node within Citrix Management Console, you can click the Create ICA File button to start the ICA File Wizard. Of course, there are many alternative methods of starting this wizard. You can right-click the application and select the Create ICA File menu item; you can navigate to Actions ➢ Application ➢ Create ICA File, or you can use the Ctrl+I key combination. Whichever method best suits you is fine.

Once the wizard starts, you are presented with a splash screen detailing what you are planning to do. Note on this page that the application name appears in the Display Name section, as shown in Figure 12.1. You will not be able to modify the display name at this point, but you can double-check to make sure you selected the right application when you started the wizard. Also on this screen you have the choice of a verbose wizard that explains every detail along the way or one that presents minimal information. Once you are familiar with the steps performed during the wizard, you may want to use the minimal option so that there is less information to look at on the screen. During this explanation, we will use the chatty wizard that explains everything.

**FIGURE 12.1** ICA File Wizard screen



Create ICA File

Welcome to the ICA File Wizard

Display Name: Solitaire

How much assistance do you want?

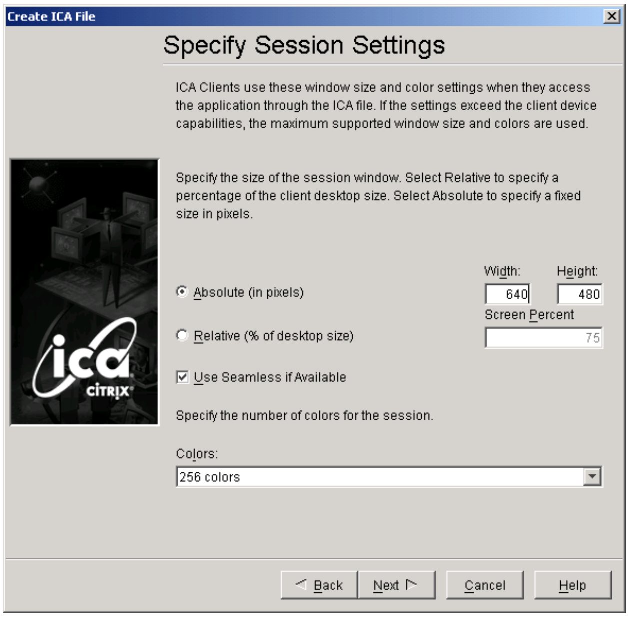
● Explain each setting.

○ Minimal explanation required.

Once you click Next, you will see the screen shown in Figure 12.2, which asks you to specify the settings you would like to use during the user's session. When the user starts a session, they will use these settings unless the client device cannot support them. If that is the case, the highest settings available on the client device will be used. If you need more information on any of the settings shown here, review the published application settings from Chapter 9.

Encryption and Specify ICA Compression are the next two screens that appear as you move through the wizard. When setting the encryption option, you need to select the lowest level of encryption that will be required when using the application, as shown in Figure 12.3. After choosing whether compression will be used, as shown in Figure 12.4, you will see the Select Audio Setting screen shown in Figure 12.5, where you can choose the audio setting to use for the ICA session.

**FIGURE 12.2** Specify Session Settings screen



Create ICA File

Specify Session Settings

ICA Clients use these window size and color settings when they access the application through the ICA file. If the settings exceed the client device capabilities, the maximum supported window size and colors are used.

Specify the size of the session window. Select Relative to specify a percentage of the client desktop size. Select Absolute to specify a fixed size in pixels.

● Absolute (in pixels) — Width: 640 Height: 480

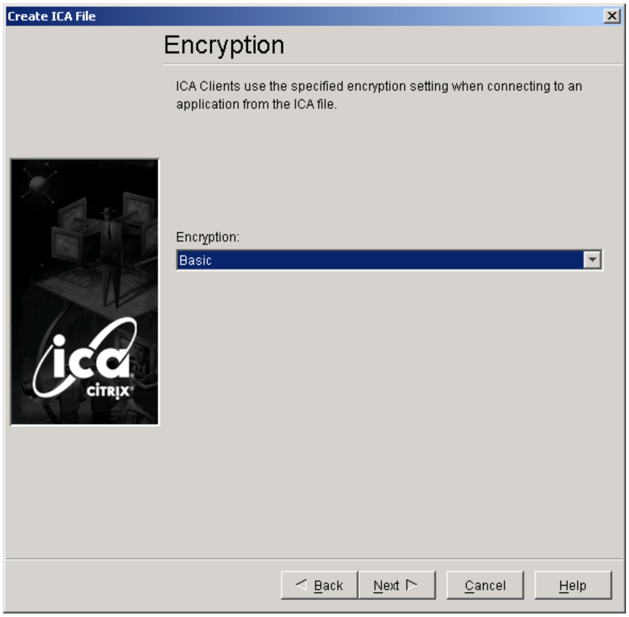
○ Relative (% of desktop size) — Screen Percent: 75

☑ Use Seamless if Available

Specify the number of colors for the session.

Colors: 256 colors

**FIGURE 12.3** Encryption setting



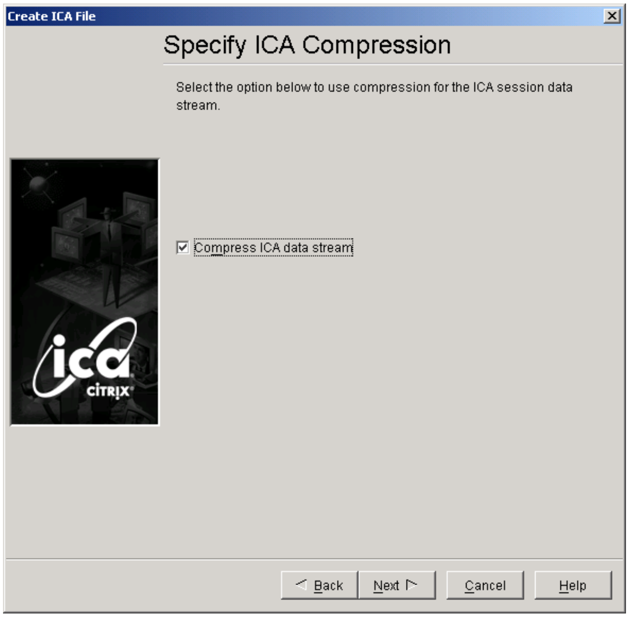
Create ICA File

Encryption

ICA Clients use the specified encryption setting when connecting to an application from the ICA file.

Encryption: Basic

**FIGURE 12.4** Compression setting



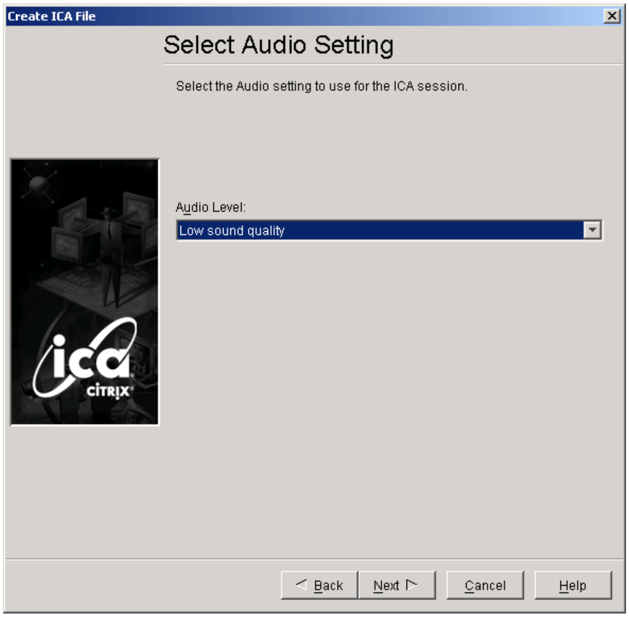
Create ICA File

Specify ICA Compression

Select the option below to use compression for the ICA session data stream.

☑ Compress ICA data stream

**FIGURE 12.5** Audio setting



Create ICA File

Select Audio Setting

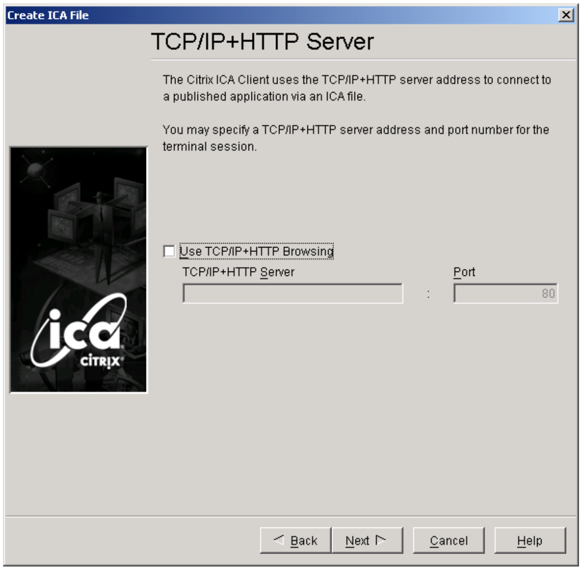
Select the Audio setting to use for the ICA session.

Audio Level:

Low sound quality

Once you've selected all of the settings for the connection, you will be prompted for the name of the server that will process the request, as shown in Figure 12.6. You should complete this option if you wish to connect directly to a server. If this option is not selected and configured, the client will attempt to discover the master browser using UDP. Entering the TCP/IP+HTTP server name and port through which to connect to the server allows you to send a directed packet that will pass through firewalls. You can specify only one connection during the wizard. If you have more than one server, you can edit the ICA file once it is created and add in that information.

**FIGURE 12.6** Specifying the server to connect to



Create ICA File

TCP/IP+HTTP Server

The Citrix ICA Client uses the TCP/IP+HTTP server address to connect to a published application via an ICA file.

You may specify a TCP/IP+HTTP server address and port number for the terminal session.

□ Use TCP/IP+HTTP Browsing

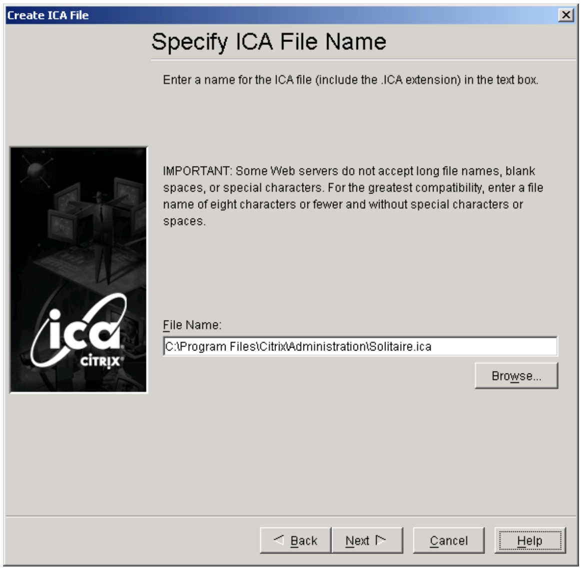
TCP/IP+HTTP Server

Port: 80

Once you have supplied the server name and port number, you are asked to provide the name of the ICA file and the path to where it will be saved. As shown in Figure 12.7, the default name of the file is the same as the name of the application. If you want to save the file elsewhere, click the Browse button and supply the path. Also read the Important notice on this screen about long filenames. Save the application with a short name and follow all of the requirements of your web server.

The final screen that requires your input simply asks whether you would like to start the HTML Wizard that will build the accompanying HTML file for the application, as shown in Figure 12.8. Select the appropriate option depending on whether you are planning to create the file, and then select Next. A summary of the options you selected during the wizard will be displayed. Review these options. If you see anything that is incorrect, you can go back and change the information. If everything is correct, click Finish, and the file will be created for you. Figure 12.9 shows the ICA file that we just created as we went through the wizard.

**FIGURE 12.7** Specify ICA File Name screen



Create ICA File

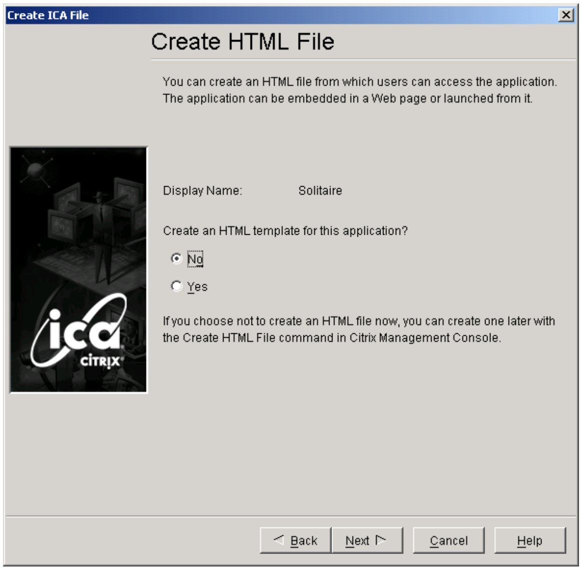
Specify ICA File Name

Enter a name for the ICA file (include the .ICA extension) in the text box.

IMPORTANT: Some Web servers do not accept long file names, blank spaces, or special characters. For the greatest compatibility, enter a file name of eight characters or fewer and without special characters or spaces.

File Name:
C:\Program Files\Citrix\Administration\Solitaire.ica

**FIGURE 12.8** Prompting to start the HTML Wizard



Create ICA File

Create HTML File

You can create an HTML file from which users can access the application. The application can be embedded in a Web page or launched from it.

Display Name: Solitaire

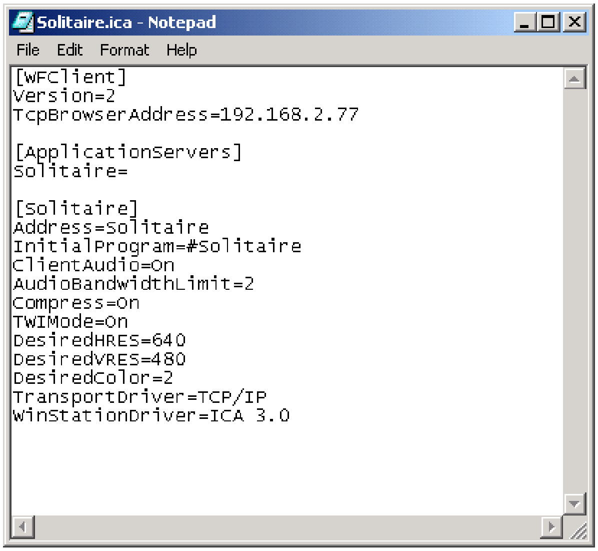
Create an HTML template for this application?

● No

○ Yes

If you choose not to create an HTML file now, you can create one later with the Create HTML File command in Citrix Management Console.

**FIGURE 12.9** The ICA file



```
[WFClient]
Version=2
TcpBrowserAddress=192.168.2.77

[ApplicationServers]
Solitaire=

[Solitaire]
Address=Solitaire
InitialProgram=#Solitaire
ClientAudio=On
AudioBandwidthLimit=2
Compress=On
TWIMode=On
DesiredHRES=640
DesiredVRES=480
DesiredColor=2
TransportDriver=TCP/IP
WinStationDriver=ICA 3.0
```

## HTML Files

HTML files contain all of the necessary code to display a web page to the user that includes the code that will start an application session when the user accesses it. These pages can be used as is and placed on a web server. Once the user opens the page, the application session will start. The code from the generated page can also be edited or copied into another web page.

Just as with the ICA file, a wizard will assist you in creating the HTML file. The last step of the ICA File Wizard allows you to select whether or not you want to create the HTML file. If you select Yes, the HTML File Wizard starts immediately after you click Finish in the ICA File Wizard. This wizard uses the same assistance level that you chose at the beginning of the ICA File Wizard.

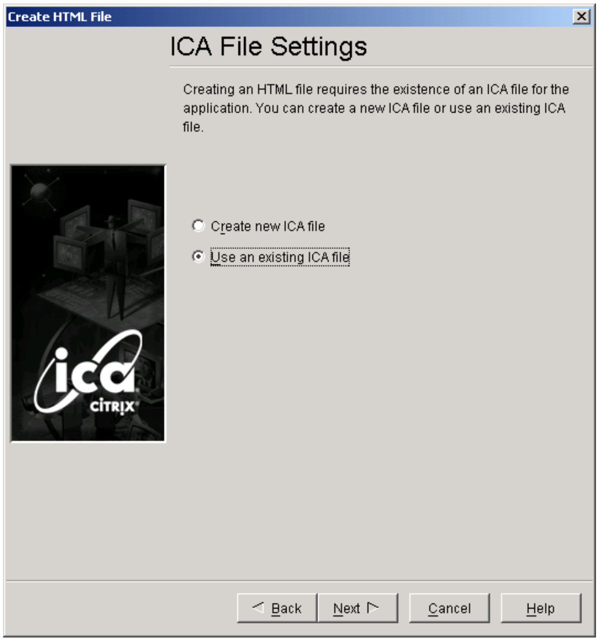
If you want to create the HTML file without first having to run the ICA File Wizard, you can start it by selecting the application and clicking the HTML File button, which sits right next to the ICA File button. Of course, there are additional methods of opening the wizard: navigating through Actions ➢ Application ➢ Create HTML File, right-clicking the application and selecting Create HTML File, or using the CTRL+H key combination.

Once the wizard starts, unless you have started it from the ICA File Wizard, you are prompted for the assistance level. Just like with the ICA

File Wizard, choosing Explain Each Setting will provide more information as you step through the wizard. Again, this is the setting we will use. Click Next to move to the ICA File Settings page.

Since you need to have an ICA file to associate the HTML file to, you are given the option of creating an ICA file before continuing or using an existing ICA file, as shown in Figure 12.10. If you choose to create an ICA file at this point, the ICA File Wizard will launch, prompting you through the creation of the file. Once the ICA File Wizard is complete, the HTML File Wizard resumes.

**FIGURE 12.10** Choosing to use an existing ICA file



Create HTML File

ICA File Settings

Creating an HTML file requires the existence of an ICA file for the application. You can create a new ICA file or use an existing ICA file.

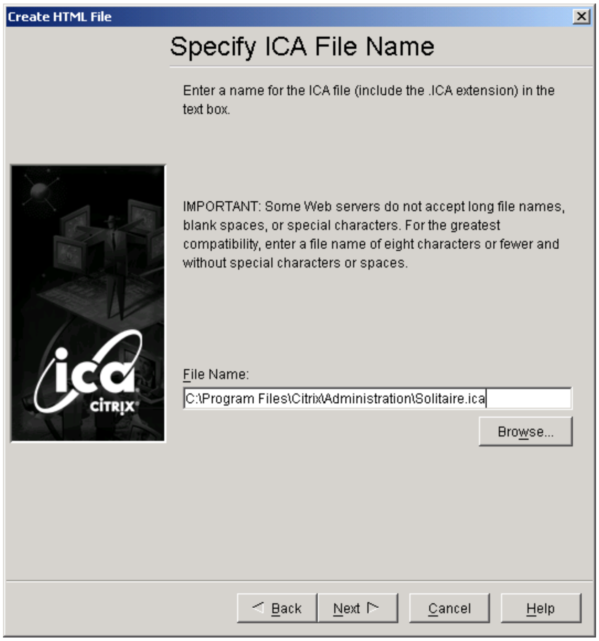
○ Create new ICA file

● Use an existing ICA file

After choosing to use an existing ICA file and clicking Next, you are prompted to provide the path to where the ICA file is located, as shown in Figure 12.11. Browse to the location where you wish to save it and then click Next.

The next screen to appear allows you to control how the application interacts with the user. The two options shown in Figure 12.12 are *Embedded* and *Launched*. Embedding an application allows you to run the application from within the web page. When using this option, the application requires that the appropriate web client be loaded on the user's computer and relies upon the web page remaining open. If the user closes the web page, the application is ended.

**FIGURE 12.11** Providing the path to the ICA file



Create HTML File

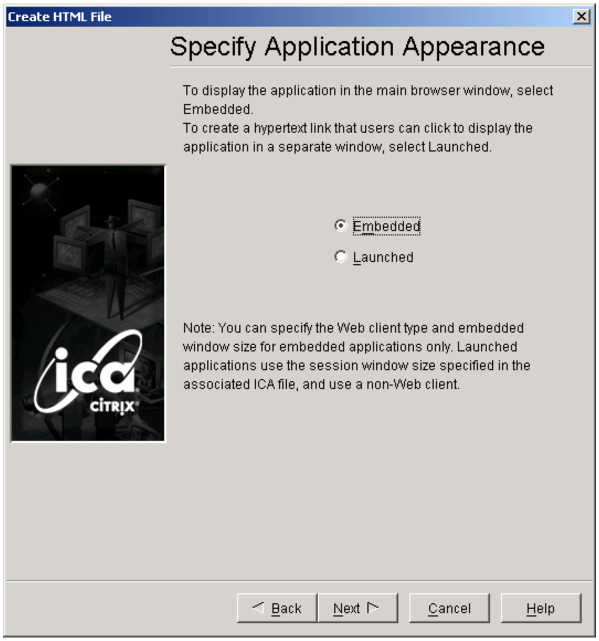
Specify ICA File Name

Enter a name for the ICA file (include the .ICA extension) in the text box.

IMPORTANT: Some Web servers do not accept long file names, blank spaces, or special characters. For the greatest compatibility, enter a file name of eight characters or fewer and without special characters or spaces.

File Name: C:\Program Files\Citrix\Administration\Solitaire.ica

**FIGURE 12.12** Specify Application Appearance screen



Create HTML File

Specify Application Appearance

To display the application in the main browser window, select Embedded.
To create a hypertext link that users can click to display the application in a separate window, select Launched.

● Embedded

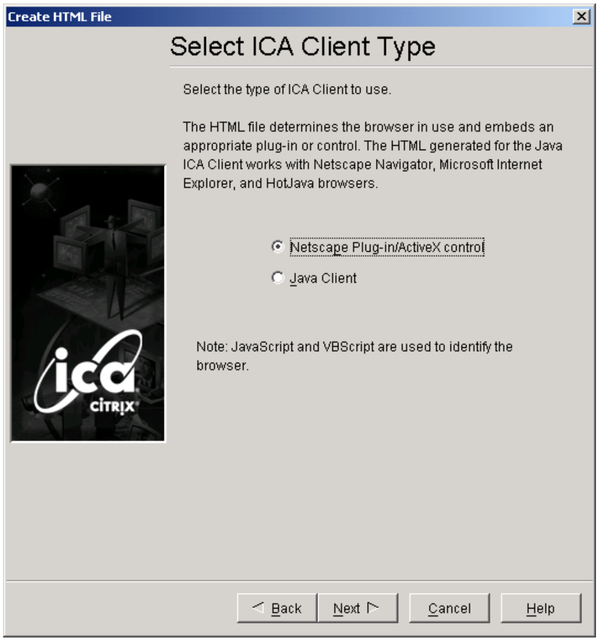
○ Launched

Note: You can specify the Web client type and embedded window size for embedded applications only. Launched applications use the session window size specified in the associated ICA file, and use a non-Web client.

Launching the application, on the other hand, opens the application in its own window and no longer relies on the web browser. The application runs whether or not the web page remains open. Non-web client software is used to allow the application to execute from its own session. Once you have selected the option you wish to use, click Next.

If you selected the option to embed the application, you will be presented with two additional configuration screens. The first of these, shown in Figure 12.13, prompts you to supply the ICA Client type that you wish to use for the web page. Selecting the *Netscape Plug-in/ActiveX Control* option downloads and registers the appropriate controls for those browsers. Once the controls are installed, these clients can host the session from within the web browser. If you choose Java Client, any Java-capable web browser can take advantage of hosting the session from within the web page.

**FIGURE 12.13** Select ICA Client Type screen



Create HTML File

Select ICA Client Type

Select the type of ICA Client to use.

The HTML file determines the browser in use and embeds an appropriate plug-in or control. The HTML generated for the Java ICA Client works with Netscape Navigator, Microsoft Internet Explorer, and HotJava browsers.

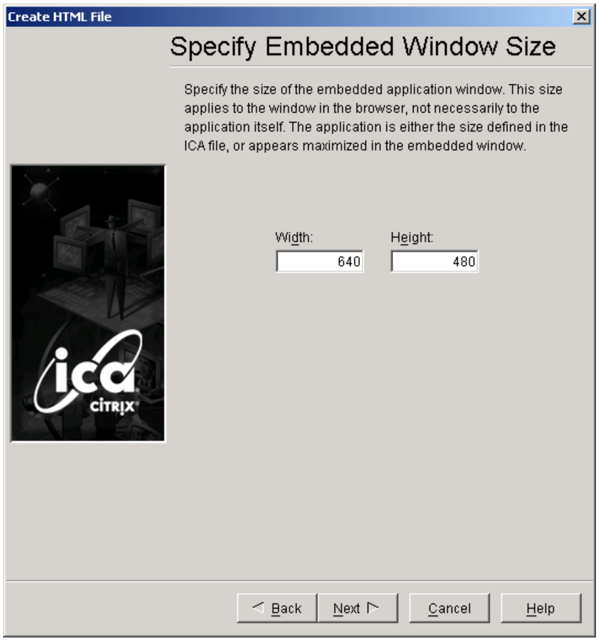
● Netscape Plug-in/ActiveX control

○ Java Client

Note: JavaScript and VBScript are used to identify the browser.

The second screen that is specific to an embedded application is the Specify Embedded Window Size screen, shown in Figure 12.14. From here, you can specify the maximum size of the application window as it is displayed in the web page. The size is represented in pixels and reflects the size consumed from the web page and not the application itself.

**FIGURE 12.14** Specify Embedded Window Size screen



Create HTML File

Specify Embedded Window Size

Specify the size of the embedded application window. This size applies to the window in the browser, not necessarily to the application itself. The application is either the size defined in the ICA file, or appears maximized in the embedded window.

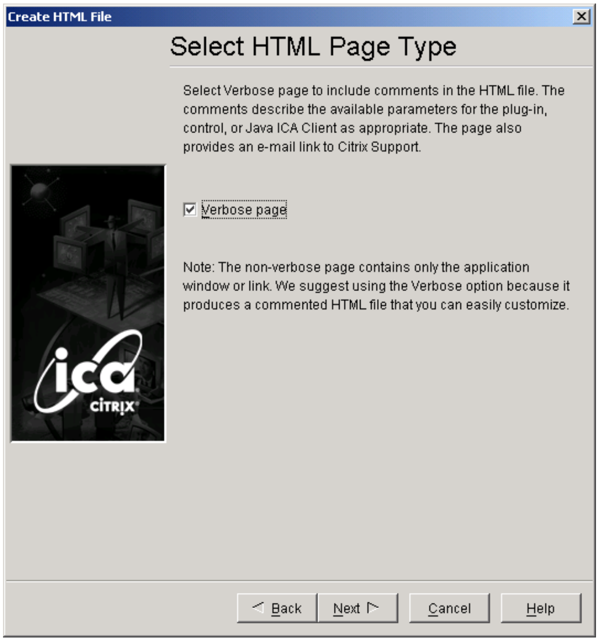
Width: 640

Height: 480

When you click Next on the Specify Embedded Window Size screen when creating an embedded HTML file or on the Application Appearance screen when creating a launched HTML file, you have the option to create a web page with detailed information. Figure 12.15 shows the Select HTML Page Type screen. If you select the Verbose Page check box, the page will contain additional information that explains how to use the web page and what happens as the application is accessed. You may want to provide this extra level of detail for users who are unfamiliar with accessing their applications from a web page or who are unfamiliar with MetaFrame technologies. If you want to conserve space on the web page and provide only summary information for your users, you can deselect this option.

Once you've selected all of the options through the wizard, you are prompted to provide the path to where you wish to save the file, as shown in Figure 12.16. This should be the same directory as the ICA file that you are using to access the application. Browse to the location where you wish to save the file and then click Next. The final screen to appear is a summary of the options you selected. Review it to make sure that the correct options are specified before clicking Finish.

**FIGURE 12.15** Choosing the level of detail for the web page



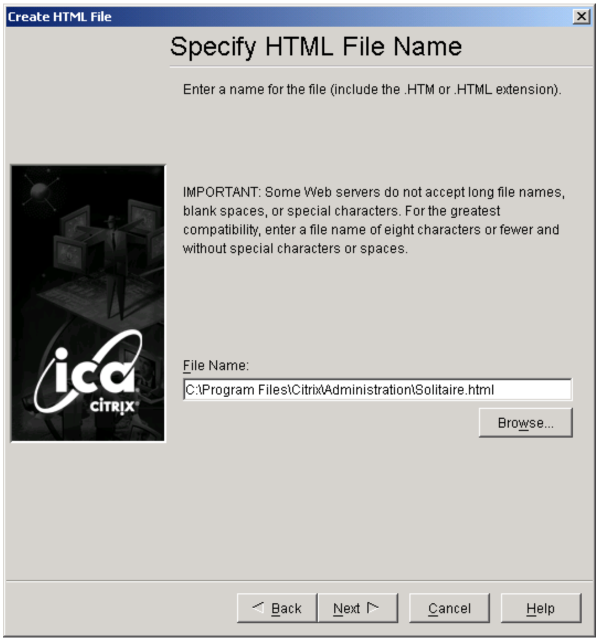
Select HTML Page Type

Select Verbose page to include comments in the HTML file. The comments describe the available parameters for the plug-in, control, or Java ICA Client as appropriate. The page also provides an e-mail link to Citrix Support.

☑ Verbose page

Note: The non-verbose page contains only the application window or link. We suggest using the Verbose option because it produces a commented HTML file that you can easily customize.

**FIGURE 12.16** Choosing the path where to save the file



Specify HTML File Name

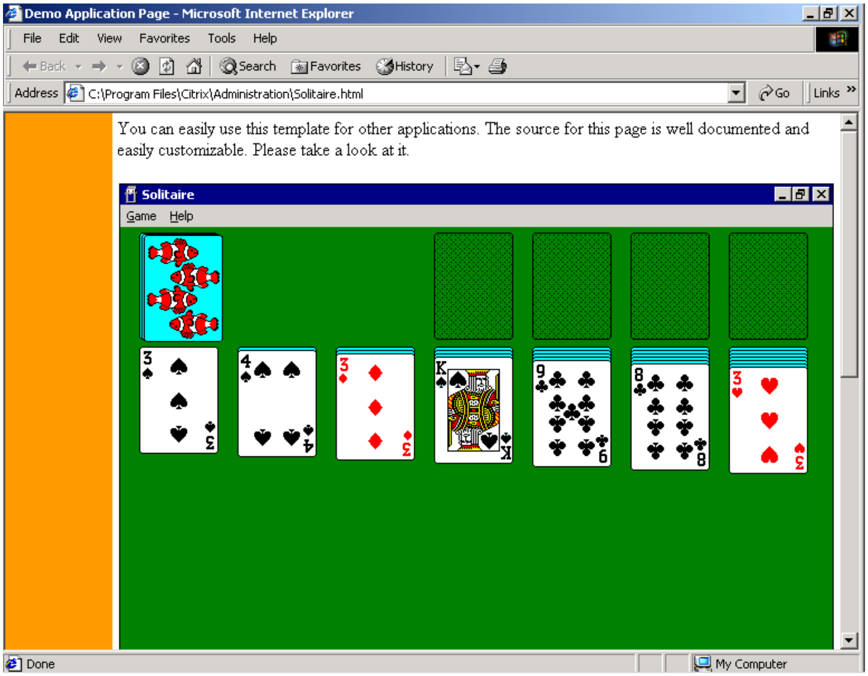
Enter a name for the file (include the .HTM or .HTML extension).

IMPORTANT: Some Web servers do not accept long file names, blank spaces, or special characters. For the greatest compatibility, enter a file name of eight characters or fewer and without special characters or spaces.

File Name: C:\Program Files\Citrix\Administration\Solitaire.html

Once both of the files have been created, you can place them in the web server's directory, create links to the pages, and allow users to gain access to them. As the users open the web page, they will be prompted to authenticate to the MetaFrame server. Once they are authenticated, the web page will open and they will see the application that has been configured for the page. Figure 12.17 shows our web page with the embedded Solitaire game running within it.

FIGURE 12.17 Embedded Solitaire game


Demo Application Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\Program Files\Citrix\Administration\Solitaire.html
Go Links
Solitaire
Game Help
Done
My Computer

You can easily use this template for other applications. The source for this page is well documented and easily customizable. Please take a look at it.

While creating web pages and allowing users access to their applications through a web interface is easy, Citrix has extended the functionality of web technologies to a product called NFuse. In the next section, we'll introduce and discuss NFuse. Note that the files we have configured in this section are also used within NFuse, so you already have a head start on how the web technologies work.

# What Is NFuse?

NFuse is described as Citrix's application management and deployment system. Utilizing the latest in web technologies, NFuse dynamically creates web pages that represent Program Neighborhood. All of the published applications that the user has been granted permission to use will be displayed on this page. The user will have access to their applications when they connect to a web page. For an administrator, no configuration of the client workstation is necessary, only the publishing of applications for the user. NFuse takes care of the rest by maintaining the client software on the user's computer and building the pages as the user connects. As a matter of fact, most of the work that was once necessary to put together your own web pages, load the client on the user's workstation, and configure access to the applications is now performed automatically by the NFuse service.

Of course, not all of this comes without a little work on the administrator's behalf. You must do some planning when deciding how you are going to implement your web servers, which users you will give access, and which applications will be available. The following list details the requirements for NFuse.

**Server farm** Servers in your server farm communicate with web servers via the XML service and provide information about the published applications, which are delivered to ICA Clients through TCP/IP.

**Client device** The client device must be able to execute ICA Client software and have a web browser installed.

**Web server** The web server is responsible for using server-side scripts that take advantage of the NFuse Java objects that allow it to connect to the server farm and present application information to the client devices.

In the next section, we will take a more in-depth look at each of these requirements and see how they fit together to bring the user a web-based view of their applications. For right now, let's take a look at the features and advantages of using NFuse.

## Advantages

NFuse provides a portal to all of the applications that the user has access to within the server farm. Whatever applications the user has permission to use will show up in the web page. The administrator does not have to manually create any web pages for the user to access. In addition, no user-level configuration is required. The NFuse-created web pages can determine whether or not the client device has the appropriate ICA Client files installed. If not, they are automatically provided to the client device before any session is started. If you no longer want a user to have access to an application, you simply modify the permissions on the published application and the user will no longer see that application in the web page. Conversely, if you add a new program and publish it for the user to access, the application will appear in the web page the next time the user accesses it. In the following section, we list the features of NFuse. The feature list includes the technologies that help bring forth the advantages discussed here.

## Features

Talk to anyone about their MetaFrame installation and you will undoubtedly hear many more positive statements than negative. This is due in part to the research and development that has gone into the product, but it is also due to the features that Citrix has plugged into MetaFrame. NFuse is no different than any other part of the MetaFrame product, and it is the features of NFuse that really let it shine. The main features of NFuse are shown here:

**Web-based user interface** Think of the web page that is generated for the user as another version of Program Neighborhood. In fact, the web client that is used to access the published application is a stripped-down version of Program Neighborhood. Instead of presenting the user interface containing the application set for the user, the web page becomes the user interface. After the application is accessed, the ICA Client software takes over and works with the session running on the MetaFrame server.

**Web Site Wizard** The *Web Site Wizard* assists the administrator in building the website that will host the NFuse pages. Using this wizard, the administrator can easily create pages that will check the user's system for the existence of ICA Client software and present the user's application set to them.

**Dynamically created web pages** When a user opens the NFuse web page, they are presented with a logon prompt. After the user supplies their credentials, the web server contacts a MetaFrame server within the server farm and retrieves the application set for the user. This information is used to create the web page containing all of the hyperlinks to the user's published applications.

**Web server–side scripting** Since all of the scripts that are used to generate the user's web page and start sessions are executed at the server, the client does not take on the additional processing and does not need to have additional code downloaded to it when starting sessions. This also centralizes the administration of scripts since they are written for and executed on the server only.

**SSL support** Using SSL Relay, NFuse redirects requests sent to the web server to the MetaFrame server farm. All data sent between the web server and the server farm is encrypted using SSL on port 443, keeping your data secure as it passes across every part of your network.

**User authentication tickets** When the administrator configures the servers to take advantage of *ticketing*, NFuse does not include the user's password in the ICA file that is sent to the user's ICA Client. Instead, it generates a "ticket" that identifies the user's password. The ticket is compared to the ticket value that is stored within the MetaFrame server and is used to identify the client as the application is started. These tickets have a predetermined time to live so that they cannot be taken advantage of if intercepted.

**Encrypted cookies** To keep the data that is contained in client-side cookies secure, the cookies are encrypted so that only the user to whom the cookie is issued can use the cookie.

**Application caching and filtering** By caching the information of a published application, which includes the permitted users, the NFuse web server does not have to contact the server farm every time a user requests the application.

**Backup servers** In case of server failure, you can use backup servers to access the server farm in its place. This redundancy allows you have the published applications available at all times.

**ICA Client deployment** If a client device does not have the ICA Client software installed, the web server can prompt the user to initiate the installation of the client files.

**Multiple farm access** You can configure the NFuse web pages to access multiple server farms, including server farms based on MetaFrame for Windows and MetaFrame for Unix.

# NFuse Components

Three main components make up NFuse: the server farm, the web server, and the ICA Client device. Each piece plays an important role in allowing the user to connect to a session through the web. The following sections detail each of these components and what they provide when used within an NFuse environment.

## Server Farm

The web pages that are generated take advantage of the server farm information that is gathered by the data collector for the zone. When applications are published within the server farm, the data collectors receive information about the published applications and who has permission to use them. When the user accesses an NFuse-based web page, the web server requests a list of the applications the user has access to. Just like in Program Neighborhood, the list of applications is presented to the user, except in this case they appear in a web page instead of in the Program Neighborhood interface.

For this technology to work, the web server needs to be able to communicate with the XML service running on the data collectors. If the port is not the standard port 80, all of the servers must be configured with the correct port numbers.

## Web Server

The web server itself needs to be configured to communicate with the data collectors in the server farm. Citrix has provided software that you can use to add *NFuse Java objects* to the web server. These objects perform functions of behalf of the client, including authenticating the user to the server farm, modifying the properties of an application before presenting the application to the user, retrieving the application set for the user to see, and creating and sending ICA files that are necessary to start an ICA session.

The web server need not reside on the MetaFrame server. As a matter of fact, Citrix discourages this configuration since the web server would steal vital resources from the MetaFrame server and limit the number of sessions available. The software that adds the NFuse Java objects prompts you for the location of the MetaFrame server and will add in the appropriate configuration settings to allow the web server to access the MetaFrame server locally or remotely.

## ICA Client Device

The last piece of our component puzzle is the ICA Client device. As long as the client device has a web browser that supports Java, the device can be used to start a session. One advantage to using NFuse is the client detection that occurs. As the NFuse login page appears, client detection occurs. If the client device does not have a client installed, the user is prompted to install the client files. As stated earlier, the default client that is downloaded to the client device is a version of Program Neighborhood that does not include the Program Neighborhood user interface. This makes the client file smaller and faster to download, especially over slow links. If the client device already has an ICA Client loaded that can take advantage of the web technologies, the client-detection phase will recognize this and will not present the option to install the client software.

All three of these components work together to allow users to create sessions and use the published applications to which they have been given access. The following steps show what occurs as a client attempts to start a session:

1. The ICA Client enters the URL in the web browser.
2. The MetaFrame server sends an authentication challenge to the user.
3. The client enters the appropriate authentication information.
4. The web browser on the client delivers the user's credential to the web server via an HTTP request.
5. The web server uses the NFuse Java objects to forward the user's information to the Citrix XML service in the server farm.

NOTE

If user authentication tickets are to be used, the XML service must be installed on every server in the farm. If user authentication tickets are not going to be used, the XML service needs to be installed on only one server in the farm.

6. The XML service contacts the other servers in the server farm using the Program Neighborhood service.
7. The Program Neighborhood service evaluates which applications the user can access based on the credentials the user provided.

8. The Program Neighborhood service uses the XML service to forward the user's application set to the NFuse Java objects running on the web server.

9. The NFuse Java objects on the web server build an HTML page that contains links to the applications in the user's application set.

10. The web server delivers the HTML page to the client, where it is displayed in the web browser.

11. When the user at the client device clicks a hyperlink for a published application on the auto-created web page, the web browser on the client device sends the request to the web server.

12. The web server retrieves the ICA file that is associated with the selected application.

13. The web server passes the ICA file to the XML service, which renders a dynamic ICA file for the current application. The NFuse Java objects replace all substitution tags in the ICA file. Information specific to the user and the requested published application replaces these substitution tags.

14. The NFuse Java object delivers the customized ICA file to the web browser on the client device.

15. The web browser on the client device passes the ICA file to the ICA Client on the client device.

16. The ICA Client on the client device initiates an ICA session with a MetaFrame XP server using the information found in the ICA file.

Once the ICA session starts, the user has full access to the application. Since Program Neighborhood takes over the processing of the session, the user will have all of the functionality of the application, just as though they had started it from Program Neighborhood.

# Using NFuse to Ease Client Connectivity

Now comes the fun stuff. We are going to walk through the steps involved in creating the NFuse environment. Starting with configuring the web server, we will go through the steps to install the NFuse extensions on the server so that it can communicate with the server farm. Then we will create the website that our users will access when they connect to the web server. Finally, we will configure the client devices and web browsers so that they will have access to the NFuse environment.

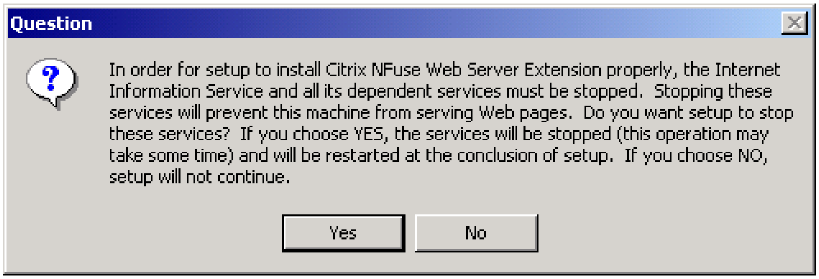
## Configuring the Web Server

To install the NFuse extensions and NFuse Java objects on the web server, you will need to have the NFuse CD available. This CD ships with all versions of MetaFrame XP. You will also need to know which MetaFrame XP server you are going to use as the intermediary between the web server and the server farm as well as the port that the XML service is operating on. By default, this port (80) is shared by the IIS service and XML service. If you are unsure of the port number that is used, open the properties of the server from within Citrix Management Console and select the MetaFrame Settings tab. If the port number displays Sharing With IIS, you will have to look within the IIS configuration to determine which port is in use; the default is port 80.

You will also need to supply the path to the web directory for the website. The default path for a website created on an IIS is `c:\inetpub\wwwroot`. A directory named `Citrix` will be created beneath the root web server directory. After you have noted the required information, you can start the installation of the web extensions by placing the CD in the CD drive or accessing the downloaded files and starting the `NfuseWebExt-IIS.exe` program. When the Setup Wizard starts, it will guide you through the following steps:

1. A splash screen will appear, detailing the steps you are about to perform. When you click Next, a warning dialog will appear, stating that the IIS services will be stopped during the installation of the extensions, as shown in Figure 12.18.

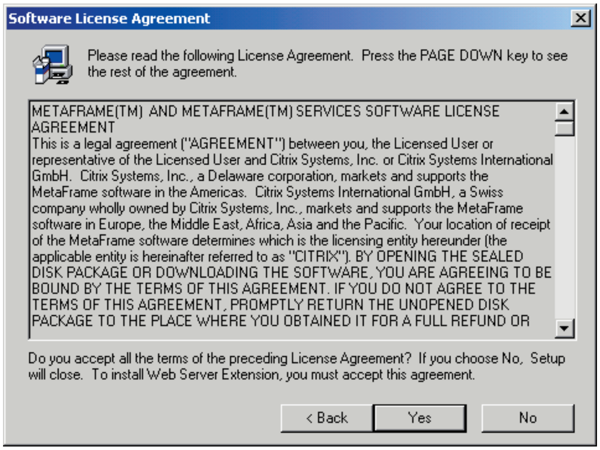
**FIGURE 12.18** Stopping the services warning



In order for setup to install Citrix NFuse Web Server Extension properly, the Internet Information Service and all its dependent services must be stopped. Stopping these services will prevent this machine from serving Web pages. Do you want setup to stop these services? If you choose YES, the services will be stopped (this operation may take some time) and will be restarted at the conclusion of setup. If you choose NO, setup will not continue.

2. If you click the Yes button, the services will be stopped. After the services stop, you are presented with a Software License Agreement, shown in Figure 12.19, that you need to agree to if you wish to install the extensions. Click the Yes button to continue.

**FIGURE 12.19** Software License Agreement screen



Software License Agreement

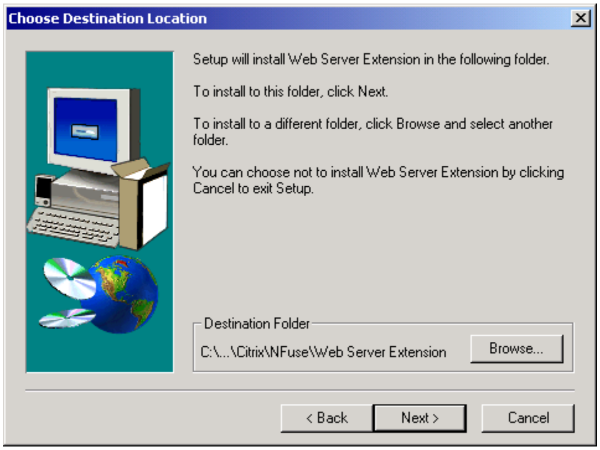
Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

METAFRAME(TM) AND METAFRAME(TM) SERVICES SOFTWARE LICENSE AGREEMENT
This is a legal agreement ("AGREEMENT") between you, the Licensed User or representative of the Licensed User and Citrix Systems, Inc. or Citrix Systems International GmbH. Citrix Systems, Inc., a Delaware corporation, markets and supports the MetaFrame software in the Americas. Citrix Systems International GmbH, a Swiss company wholly owned by Citrix Systems, Inc., markets and supports the MetaFrame software in Europe, the Middle East, Africa, Asia and the Pacific. Your location of receipt of the MetaFrame software determines which is the licensing entity hereunder (the applicable entity is hereinafter referred to as "CITRIX"). BY OPENING THE SEALED DISK PACKAGE OR DOWNLOADING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNOPENED DISK PACKAGE TO THE PLACE WHERE YOU OBTAINED IT FOR A FULL REFUND OR

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install Web Server Extension, you must accept this agreement.

3. When the Choose Destination Location screen appears, shown in Figure 12.20, browse to the location where you would like to store the files, and click Next.

**FIGURE 12.20** Choosing the destination folder



Choose Destination Location

Setup will install Web Server Extension in the following folder.

To install to this folder, click Next.

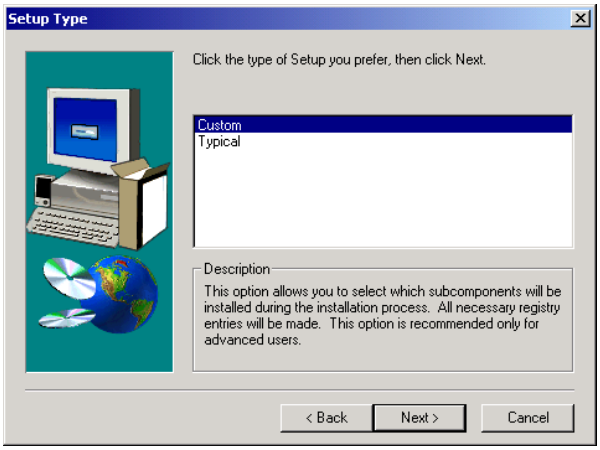
To install to a different folder, click Browse and select another folder.

You can choose not to install Web Server Extension by clicking Cancel to exit Setup.

Destination Folder
C:\...\Citrix\NFuse\Web Server Extension

4. Next up are the installation choices, shown in Figure 12.21. Choosing to use the Typical install loads all of the NFuse files on the web server, including the sample web pages. If you do not want to consume the additional space, you can choose the Custom option and modify what is installed.

**FIGURE 12.21** Setup Type screen



Setup Type

Click the type of Setup you prefer, then click Next.

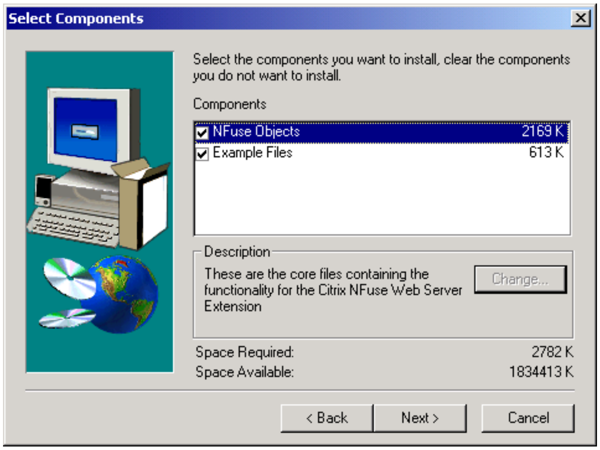
Custom
Typical

Description

This option allows you to select which subcomponents will be installed during the installation process. All necessary registry entries will be made. This option is recommended only for advanced users.

5. If you selected the Custom option, you will see the screen shown in Figure 12.22. From here, you can select the components you wish to install. If you do not want the sample web pages, you can deselect the check box next to Example Files. Click Next to continue.

**FIGURE 12.22** Select Components screen



Select Components

Select the components you want to install, clear the components you do not want to install.

Components

☑ NFuse Objects 2169 K
☑ Example Files 613 K

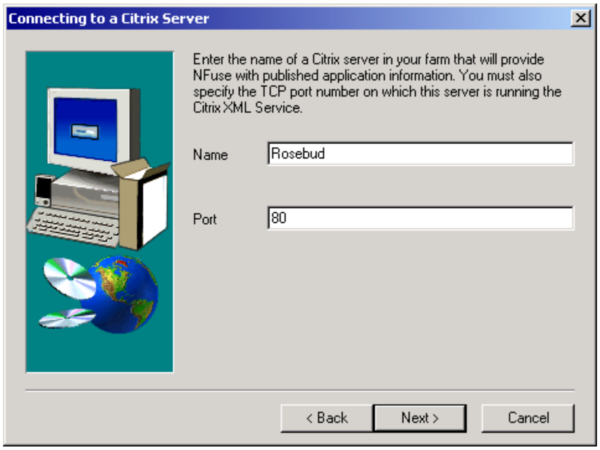
Description

These are the core files containing the functionality for the Citrix NFuse Web Server Extension

Space Required: 2782 K
Space Available: 1834413 K

6. Using the information you recorded when you were determining which MetaFrame server the web server would connect to, enter the MetaFrame server name and the port used by the XML service, as shown in Figure 12.23. This will become the default server for the websites that you create.

**FIGURE 12.23** Selecting the MetaFrame server



Connecting to a Citrix Server

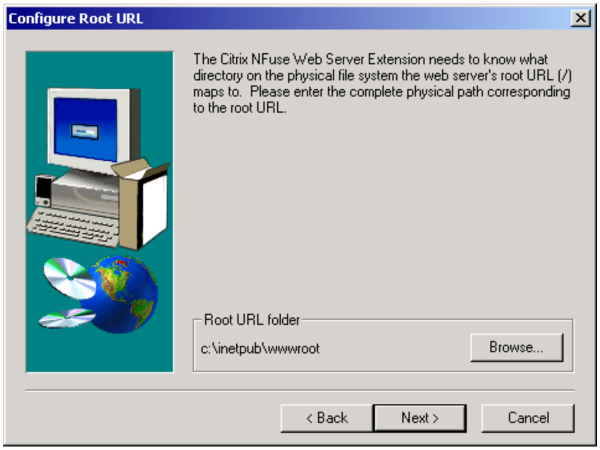
Enter the name of a Citrix server in your farm that will provide NFuse with published application information. You must also specify the TCP port number on which this server is running the Citrix XML Service.

Name: Rosebud

Port: 80

7. After clicking Next, you will need to provide that path to the website's root folder. The default path appears when you reach the Configure Root URL screen shown in Figure 12.24. If you have another path you wish to use, you can browse to it.

**FIGURE 12.24** Configuring the website's root directory



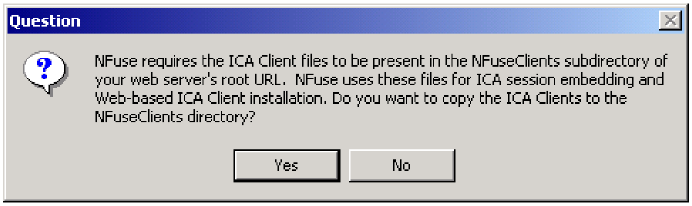
Configure Root URL

The Citrix NFuse Web Server Extension needs to know what directory on the physical file system the web server's root URL (/) maps to. Please enter the complete physical path corresponding to the root URL.

Root URL folder: c:\inetpub\wwwroot

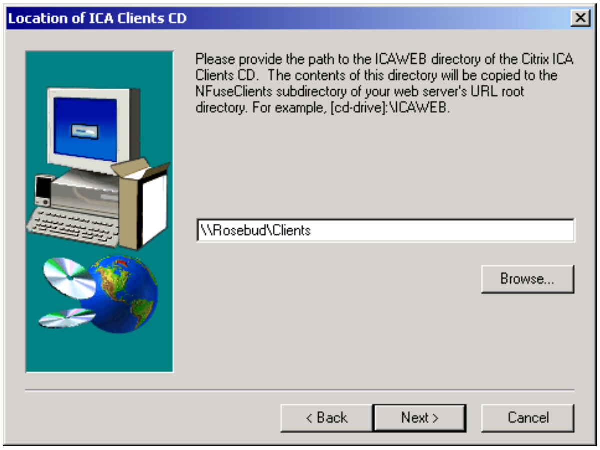
8. After you enter the path to the root directory and click Next, the Setup program informs you that the web clients need to be installed so that the server can download the client files to the user's client device. Figure 12.25 shows the warning dialog. Clicking Yes causes the Setup program to ask for the path to the ICA web client files. As shown in Figure 12.26, you need to provide the path to the `icaweb` directory, either on the ICA Client CD or a network share point that hosts the files. Once you click Next, the ICA web client files will be copied to the `NFuseClients` directory beneath the web server's root directory.

**FIGURE 12.25** ICA web client warning


Question

NFuse requires the ICA Client files to be present in the NFuseClients subdirectory of your web server's root URL. NFuse uses these files for ICA session embedding and Web-based ICA Client installation. Do you want to copy the ICA Clients to the NFuseClients directory?

**FIGURE 12.26** Providing the path to the ICA web client files


Location of ICA Clients CD

Please provide the path to the ICAWEB directory of the Citrix ICA Clients CD. The contents of this directory will be copied to the NFuseClients subdirectory of your web server's URL root directory. For example, [cd-drive]:\ICAWEB.

\\Rosebud\Clients

9. After the client files are installed, a summary screen appears, detailing the options that you selected. Once you click Next, the installation runs and the services are restarted. When everything completes, a final screen appears, informing you that the installation is complete. Click

the Finish button, and you are ready to start building your web pages and using NFuse.

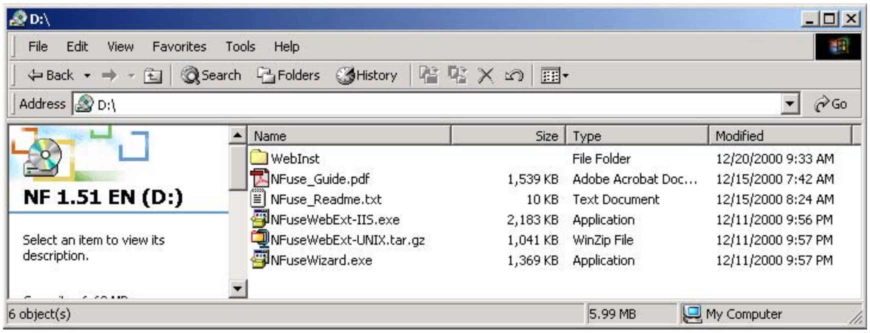
## Creating the Website

Once you've added the additional extensions for the NFuse Java objects to the web server, you are ready to create your website. You have the option of writing your own web pages, which you may want to do if you have a web development staff or you are well versed in web page creation. If this is the route you want to take, Citrix has provided the NFuse Administrator's Guide, which includes the NFuse Java object tags. Writing your own web pages goes beyond the scope of this book, so we will concentrate on the easier of the two methods of creating web pages.

Included on the NFuse CD is the installation program for the Citrix NFuse Web Site Wizard. Using this wizard greatly reduces the amount of work an administrator needs to perform when trying to develop a web page for users to take advantage of. It also saves the administrator from having to learn how to write web pages.

To install the NFuse Web Site Wizard, log on to your web server with an account that has administrative privileges. Place the NFuse CD in the CD drive, and view the root of the drive in Windows Explorer, as shown in Figure 12.27. The `NFuseWizard.exe` file is the installation program. This executable file is also available in the downloaded version of NFuse. Double-click this program to start the installation.

**FIGURE 12.27** The contents of the NFuse CD

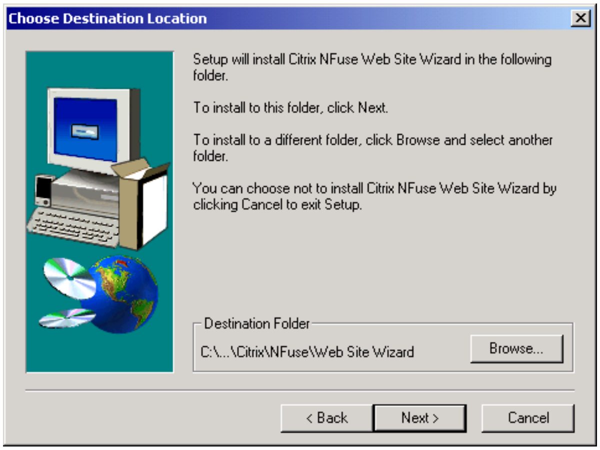


| Name | Size | Type | Modified |
|---|---|---|---|
| WebInst | | File Folder | 12/20/2000 9:33 AM |
| NFuse_Guide.pdf | 1,539 KB | Adobe Acrobat Doc... | 12/15/2000 7:42 AM |
| NFuse_Readme.txt | 10 KB | Text Document | 12/15/2000 8:24 AM |
| NFuseWebExt-IIS.exe | 2,183 KB | Application | 12/11/2000 9:56 PM |
| NFuseWebExt-UNIX.tar.gz | 1,041 KB | WinZip File | 12/11/2000 9:57 PM |
| NFuseWizard.exe | 1,369 KB | Application | 12/11/2000 9:57 PM |

6 object(s) 5.99 MB My Computer

Once the installation program starts, you will see a typical splash screen. Click Next on this screen to read the Software License Agreement. Here you will need to click the Yes button to continue with the installation. Once you click Yes, the Setup program prompts you for the path where the program files should be created, as shown in Figure 12.28.

**FIGURE 12.28** Providing the path for the files



Choose Destination Location

Setup will install Citrix NFuse Web Site Wizard in the following folder.

To install to this folder, click Next.

To install to a different folder, click Browse and select another folder.

You can choose not to install Citrix NFuse Web Site Wizard by clicking Cancel to exit Setup.

Destination Folder

C:\...\Citrix\NFuse\Web Site Wizard

After providing the path and clicking Next, you can provide the program group in which the icons will be created. The default entry is the Citrix folder. Enter the folder name and click Next to see the summary information. Double-check this information before moving on. Once you click the Next button, the files will be installed on the computer.

Navigate to the program group you selected during the setup, and you will see the NFuse folder containing the Web Site Wizard icon. In Figure 12.29, we are accessing the program through the default location and choosing Start ➢ Programs ➢ Citrix ➢ NFuse ➢ Web Site Wizard. When the wizard starts, you are shown the first of eight pages that assist you in creating the web pages for your users to access. Since this is simply a splash screen, you can click the Next button to move on to the meat of the wizard.

The second page contains options that you can use to specify the server connection for the web server. By default, the web server will contact the MetaFrame server that was specified during the installation of the NFuse web extensions. If you wish to override this setting, select the first check box shown in Figure 12.30, Override Default Citrix Server. Once this option has been selected, you can enter the server name and XML port. Additional code is added to the web pages that are created from this wizard to control the connections to the MetaFrame server.

**FIGURE 12.29** Accessing the Web Site Wizard

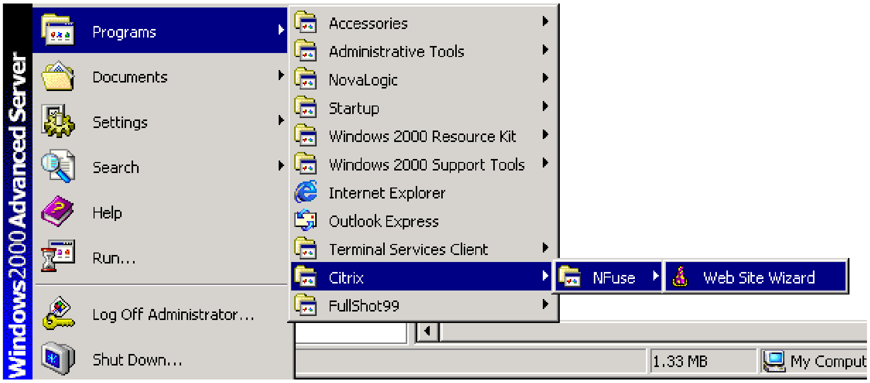
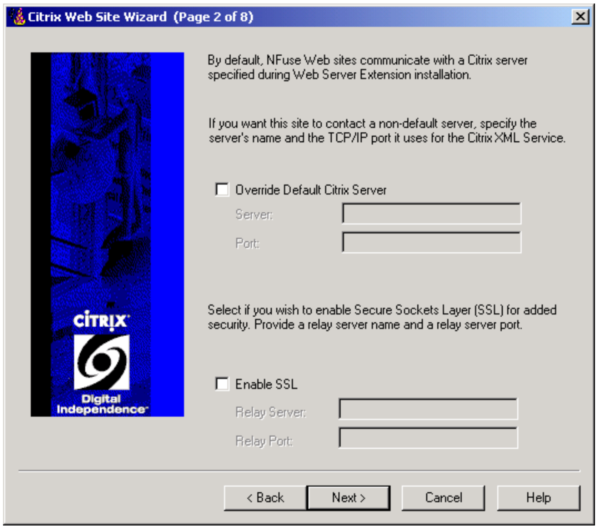


**FIGURE 12.30** Selecting server options



By default, NFuse Web sites communicate with a Citrix server specified during Web Server Extension installation.

If you want this site to contact a non-default server, specify the server's name and the TCP/IP port it uses for the Citrix XML Service.

☐ Override Default Citrix Server

Server:

Port:

Select if you wish to enable Secure Sockets Layer (SSL) for added security. Provide a relay server name and a relay server port.

☐ Enable SSL

Relay Server:

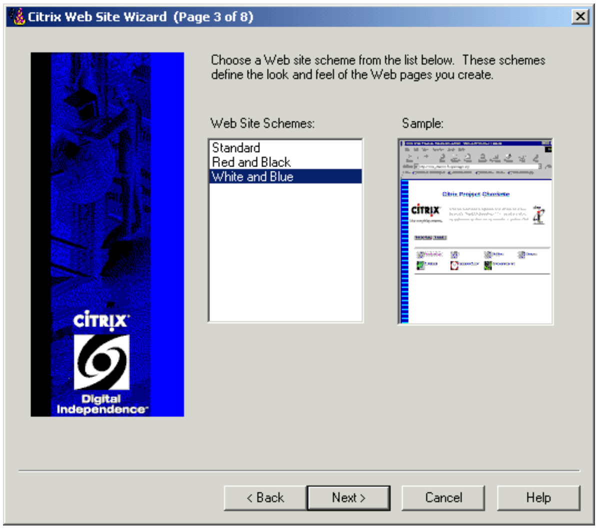
Relay Port:

The second option on the second page of the wizard allows you to configure the SSL Relay server. If you are going to secure the connections from the clients with SSL, you may need to configure an SSL Relay server. Once you've configured these settings (if necessary), click Next to move to page 3 of the wizard.

For more information on the SSL Relay server, see Chapter 8, "Security."

You have the option of selecting one of three website schemes. The choice is solely up to your tastes. Figure 12.31 shows the White And Blue option. If you like one of the other options better, or if it conforms to your organization better, you can select it. Your selection will not affect anything except how the user sees the applications that are displayed.

**FIGURE 12.31** Choosing a scheme


Citrix Web Site Wizard (Page 3 of 8)

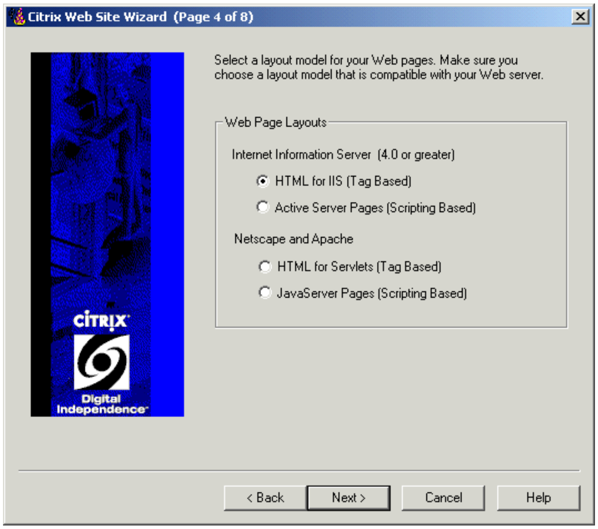
Choose a Web site scheme from the list below. These schemes define the look and feel of the Web pages you create.

Web Site Schemes:
- Standard
- Red and Black
- White and Blue

After you select the scheme for your web pages, the wizard presents the layout model selection options. From this screen, you can select which type of dynamic page creation you want to use. Two server choices appear: Internet Information Server and Netscape and Apache servers, as shown in Figure 12.32. Within each of these choices, you have the option to use a substitution-tag-based layout, which takes advantage of HTML, or a scripting-based layout, which takes advantage of Active Server Pages or JavaServer Pages.

Pages that are created using the substitution-tag-based layout are, by their nature, very basic pages. The main advantage for the administrator of the site is that the pages do not contain any scripting language tags that may be difficult to modify. Both the *HTML For IIS* settings and *HTML For Servlets* options substitute the tagged data within the HTML file with the entries from the ICA file. The newly constructed HTML file is sent for processing by the client. If you have any other web server besides Microsoft's IIS, you should choose the HTML For Servlets option.

**FIGURE 12.32** Selecting a layout model



Select a layout model for your Web pages. Make sure you choose a layout model that is compatible with your Web server.

Web Page Layouts

Internet Information Server (4.0 or greater)

● HTML for IIS (Tag Based)

○ Active Server Pages (Scripting Based)

Netscape and Apache

○ HTML for Servlets (Tag Based)

○ JavaServer Pages (Scripting Based)

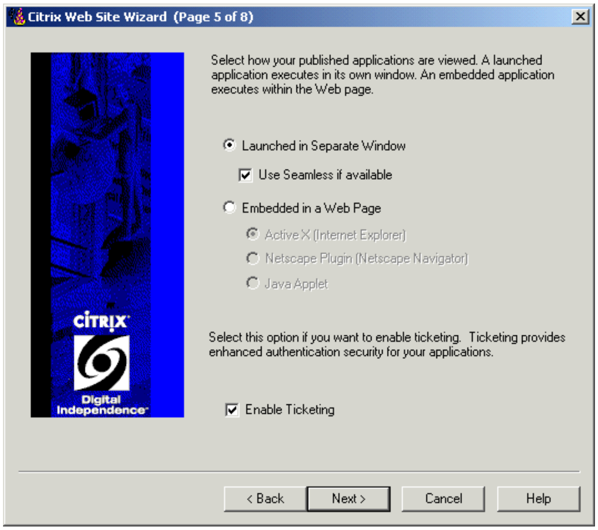
If you want the flexibility of scripted pages that can supply more detailed information on the page, the two scripting options are for you. While they are more complex, and the administrator must have a thorough understanding of the scripting language, the pages will be more robust and more efficient. If you have any server besides Microsoft's IIS, you need to specify JavaServer Pages.

After choosing your layout model and clicking Next, you will find the options for launching or embedding the application, as shown in Figure 12.33. As we discussed earlier in the chapter, if you wish to keep the application tied to the web page, you need to embed it. If you choose this option, you then need to specify the client type that you want the client device to use. Selecting the options here will embed code into the web page that specifies where to locate the ICA Client.

NOTE

For more information about ActiveX controls, the Netscape plug-in, or the Java applet, see the Citrix ICA Client Administrator's Guide.

**FIGURE 12.33** Launching or embedding the application



Citrix Web Site Wizard (Page 5 of 8)

Select how your published applications are viewed. A launched application executes in its own window. An embedded application executes within the Web page.

● Launched in Separate Window

☑ Use Seamless if available

○ Embedded in a Web Page

● ActiveX (Internet Explorer)

○ Netscape Plugin (Netscape Navigator)

○ Java Applet

Select this option if you want to enable ticketing. Ticketing provides enhanced authentication security for your applications.

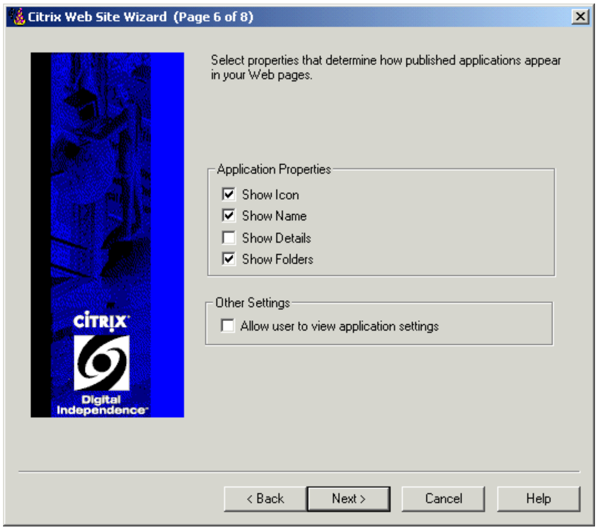
☑ Enable Ticketing

If you want to launch your applications so they become independent of the browser window, you should select the option to launch the application in a separate window. When you do, the Use Seamless If Available check box becomes available. Selecting this check box allows any client that can take advantage of seamless windows to run the application in its own window instead of being tied to a desktop session.

The final option on this screen is ticketing support. If you do not want the user's credentials to be included in the files that are sent to the client device, you can enable ticketing, which creates a ticket for the user account. Every application that is accessed uses the ticket value in place of the user's credentials. Since each ticket has an expiration time, the ticket is valid for only a short period. Once the ticket expires, it is no longer valid for starting an application session.

Figure 12.34 shows the sixth page of the wizard. From here, you can choose the application properties that are displayed within the web page. The first three options allow you to control how much information is displayed about the published application. Show Icon displays the application's default icon, Show Name displays the name under which the application was published, and Show Details displays the description that was supplied when the application was published.

**FIGURE 12.34** Selecting the application properties



Citrix Web Site Wizard (Page 6 of 8)

Select properties that determine how published applications appear in your Web pages.

Application Properties

☑ Show Icon
☑ Show Name
☐ Show Details
☑ Show Folders

Other Settings

☐ Allow user to view application settings

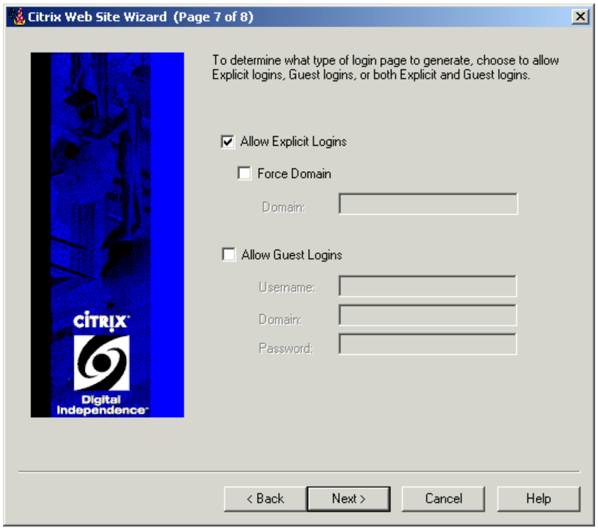
If you have configured folders in which to organize your applications within the server farm, you can allow users to see that same folder hierarchy by selecting the Show Folders option. If you leave this option deselected, all of the applications will appear together on the same web page.

If you are using one of the script-based layout models, you will also have the Allow User To View Application Settings option. If you select this option, a View Settings button will appear on the web page. Users will be able to click this button to gain access to additional information about the application.

Page 7 of the wizard, shown in Figure 12.35, is used to control the user authentication method. The default option, *Allow Explicit Logins*, is to force the users to authenticate. When you select this option, the default web page is generated with fields where a user can supply their username, password, and domain. If you want to control the domain used, select the Force Domain option. When you select this option, only the username and password fields will appear on the web page since the domain will be provided by the web server.

If you select the Allow Guest Logins option along with the Allow Explicit Logins option, the login screen will appear with the same information as the Allow Explicit Logins–generated screen, but it will also include a Guest button. If the user does not want to authenticate, the guest account and password supplied from the web server are used to authenticate the user, but the user will have access only to those applications for which the guest account has been given access. If the Guest option is the only option selected, no login page is generated, and the application set is the first thing the user sees.

**FIGURE 12.35** Choosing authentication methods



Citrix Web Site Wizard (Page 7 of 8)

To determine what type of login page to generate, choose to allow Explicit logins, Guest logins, or both Explicit and Guest logins.

☑ Allow Explicit Logins

□ Force Domain

Domain:

□ Allow Guest Logins

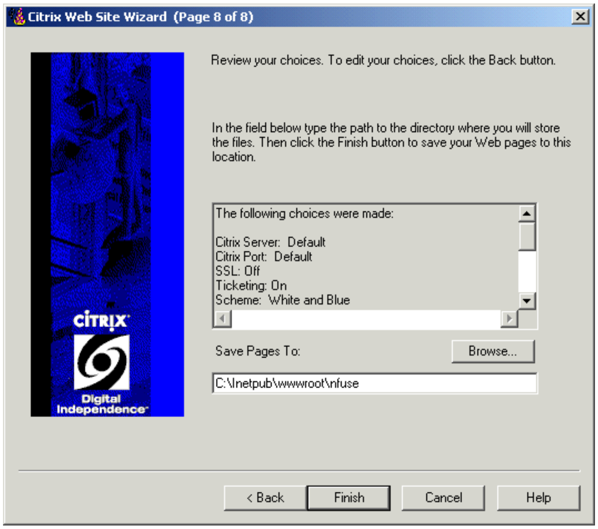
Username:

Domain:

Password:

The final page of the wizard, shown in Figure 12.36, is a summary screen that displays the options selected. Review these settings and then select a location where the files are to be generated. You should choose a subdirectory beneath your web server root directory in which to save the files.

**FIGURE 12.36** Finishing the wizard



Citrix Web Site Wizard (Page 8 of 8)

Review your choices. To edit your choices, click the Back button.

In the field below type the path to the directory where you will store the files. Then click the Finish button to save your Web pages to this location.

The following choices were made:

Citrix Server: Default
Citrix Port: Default
SSL: Off
Ticketing: On
Scheme: White and Blue

Save Pages To:

C:\Inetpub\wwwroot\nfuse

Once you have completed the wizard and clicked the Finish button, the `NFuseMedia` directory is created beneath the web root, and the supporting files for the web pages are stored in the directory that you supplied in the last page of the wizard. All the pages that were generated are complete and ready to be put into production. You may modify them to your satisfaction, but it is not necessary to do so.

## Configuring Client Devices

Before the client device can automatically install the ICA Client, the ICA Client files must be present on the web server. If you installed the ICA Client files while adding the NFuse Java Objects extensions, you will not have to worry about locating these files. If you did not copy these files at that time, you will need to locate the ICA Client files and copy them to the `NFuseClients` directory on the web server. These files can be found on the ICA Clients CD under the `icaweb` directory. Copy the contents of this directory and not the `icaweb` directory itself.

Once you've copied the files, when the user connects to the web page, NFuse checks the client device for the existence of an ICA Client. The following steps map out what occurs as the client device is checked:

1. The `default.htm` file tries to find a cookie placed on the client device that specifies that client detection should not be attempted. If it finds this entry in a cookie, it redirects the user to the login web page.

NOTE The `noClientDetect` entry appears in a cookie only if the client has selected the Do Not Show This Window At Login option from the client install window.

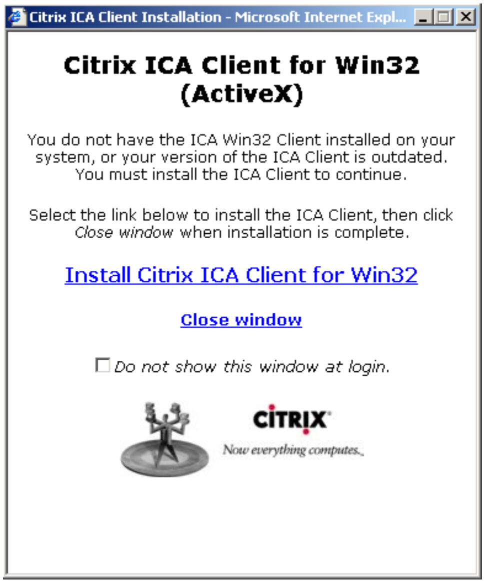
2. If the cookie does not include the option to ignore client detection, NFuse executes a script to determine which operating system and web browser are in use on the client device. It determines the ICA Client type from the information gathered from this script and places an entry in a cookie detailing the client type. If the client device is one of the following, the script should successfully detect it:
   - 32-bit Windows
   - 16-bit Windows
   - Macintosh
   - Solaris/SPARC, Solaris/*x*86

- SunOS
- SGI
- HP/UX
- IBM/AIX
- SCO
- DEC/Tru64
- Linux

For all other platforms, the script will try to write an entry in a cookie suggesting the ICA Java Client.

3. The client is redirected to the `icaclient.asp` file. If a 32- or 16-bit Windows client device is detected and the script contained on this page detects that the client device already has an ICA Client installed, the login page is presented to the user. If the script does not detect the existence of an ICA Client or the client is not a 32- or 16-bit Windows client, the `icaclient.asp` script displays a pop-up screen, shown in Figure 12.37, where the user can click a link to install the ICA Client. If the option to block showing the screen is selected, the `icaclient.asp` file will not run and client detection will not occur.

**FIGURE 12.37** The install client pop-up window



Citrix ICA Client Installation - Microsoft Internet Expl...

Citrix ICA Client for Win32 (ActiveX)

You do not have the ICA Win32 Client installed on your system, or your version of the ICA Client is outdated. You must install the ICA Client to continue.

Select the link below to install the ICA Client, then click *Close window* when installation is complete.

Install Citrix ICA Client for Win32

Close window

□ *Do not show this window at login.*

4. After clicking the Install Citrix ICA Client hyperlink, the user is presented with the installation options based on the detected client device type. For 32-bit Windows clients, the `icaclient.asp` script will determine the file to use by checking the information contained in the `icaclientinfo.asp` script. Depending on the operating system in use, the ICA Client will either automatically install, as is the case with Windows 2000, or the user will be prompted to save or run the file.

### Configuring Web Browsers

Most of the supported web browsers need no further configuration. Citrix has provided all of the necessary files to allow the browser to interact with the NFuse-generated web pages and support the launching and embedding of applications. If you have Internet Explorer or Netscape, you should not have any problems when attempting to use the browsers. The ICA Java Client and the ICA Macintosh Client require additional configuration on the client device. For more information concerning the special configuration needed, see the NFuse Administrator's Guide.

Contained in this chapter is all the information you need to start building your own websites using the web technologies provided by Citrix. Using NFuse, which is included in every version of MetaFrame XP, you can configure web-based access to your server farm quickly and easily. From here, we move on to what used to be one of the most dreaded parts of the MetaFrame world, printing. You will find many enhancements to printing in the XP version of MetaFrame, something many administrators will be glad to see.

## Summary

NFuse and the web technologies that Citrix has taken advantage of are becoming one of the easiest ways to allow your users to connect to MetaFrame servers to access their published applications. While you can build your own web pages using the information provided by Citrix, you will need a good understanding of HTML and scripting languages. NFuse provides an easier method of creating the web pages and controlling the web environment. Included in the NFuse product are the extensions that are required on the web server to allow it to communicate with the XML service on a MetaFrame server within the server farm. Also included is the Web Site

Wizard, which will assist you in creating a web page that dynamically generates a web page for every user who authenticates. Using these tools, an administrator can quickly and easily create an entire website that will allow the users access to all of the published applications they have been given permission to use.

# Exam Essentials

**Know the components that make up Citrix's web technologies.** Citrix's web technologies take full advantage of the features of the server farm, web servers, and web browsers.

**Understand what an ICA file is.** An ICA file includes entries that are used to control the published application session when accessed through a web interface.

**Understand what an HTML file is.** An HTML file includes the code to generate a web page that allows a user to access published applications through a web browser.

**Understand what NFuse is.** NFuse is Citrix's web-based application management and deployment tool.

**Know the default port used by the XML service.** By default, the XML service shares port 80 with the web server.

**Understand what ticketing is.** When using ticketing, a user's authentication credentials are not included in the files delivered to the web browser when the user attempts to start a published application. Instead, the value of the ticket that is associated with the user account is substituted for the credentials.

**Know how to install the NFuse web extensions.** From the NFuse CD or from the NFuse files downloaded from the Citrix website, run the `NfuseWebExt-IIS.exe` file to add the NFuse Java objects to the server.

**Know how to install the NFuse Web Site Wizard.** From the NFuse CD or from the NFuse files downloaded from the Citrix website, run the `NFuseWizard.exe` file to install the NFuse Web Site Wizard.

**Know how to create a website with the NFuse Web Site Wizard.** The wizard contains eight pages that will step you through creating a web page.

**Understand how the ICA Client software is detected from a web page.** The NFuse-generated `default.htm` file contains a script that will check a cookie for the existence of the `noClientDetect` entry once the NFuse web page is started. If this entry does not exist, the `icaclient.asp` file is called, and the script contained within this file will detect the client device and web browser type.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Active Server Pages (ASP)<br>
ActiveX control<br>
Allow Explicit Logins<br>
dynamic pages<br>
embedded<br>
HTML file<br>
HTML For IIS<br>
HTML For Servlets<br>
ICA file<br>
Java<br>
JavaServer Pages<br>
launched<br>
Netscape plug-in<br>
NFuse<br>
NFuse Java objects<br>
ticketing<br>
web browsers<br>
web servers<br>
Web Site Wizard<br>
web technologies

# Exercise

This exercise steps through the installation of the extensions on an Internet Information Server and then creates a website using the Web Site Wizard.

**EXERCISE 12.1**

### Installing and Configuring NFuse

Perform the following steps on the web server:

1. Run `NFuseWebExt-IIS.exe` from the root of the NFuse CD-ROM.
2. On the Welcome screen, click Next.
3. A question window pops up, asking if you want to stop the IIS web services. Click Yes.
4. On the Software License Agreement page, click Yes.
5. In the Choose Destination Location window, enter the path to the directory where you would like to save the files, and click Next.
6. In the Setup Type window, select Typical and click Next.
7. In the Connecting To A Citrix Server window, enter the name of a Citrix server on your network that is running the XML service. Also enter the port number that the server is using for XML communication in the box labeled Port. If you use another port besides the default port 80 for XML communication on your MetaFrame farm, a warning window will appear. If the warning window appears, verify that you have the correct XML port and click OK in the warning window.
8. In the configure Root URL field, verify that the entry is what you have used as your server's root folder and click Next.
9. A question window appears, asking if you want to copy the ICA Clients to the web server. Click Yes.
10. In the Start Copying Files window, click Next.
11. In the Setup Complete window, click Finish.

You should perform these steps on the web server:

1. Run `NFuseWizard.exe` from the root of the NFuse CD-ROM.
2. On the Welcome screen, click Next.
3. On the Software License Agreement page, click Yes.

**EXERCISE 12.1** ***(continued)***

4. On the Choose Destination Location window, enter the path to the directory where you would like to save the files and click Next.

5. In the Select Program Folder window, click Next.

6. In the Start Copying Files window, click Next.

7. In the Setup Complete window, click Finish.

You should perform these final steps on the web server:

1. Open the Web Site Wizard by choosing Start ➢ Programs ➢ Citrix ➢ NFuse ➢ Web Site Wizard.

2. On page 1 of the Web Site Wizard, click Next.

3. On page 2 of the Web Site Wizard, click Next.

4. On page 3 of the Web Site Wizard, choose a website scheme from the list and click Next.

5. On page 4 of the Web Site Wizard, select the layout model for your website depending on the type of web server you have installed, and click Next.

6. On page 5 of the Web Site Wizard, select the settings you would like to use for viewing the published applications. If you choose Embedded In A Web Page, make sure you choose the appropriate setting for your web browser. Click Next after you have made your changes.

7. On page 6 of the Web Site Wizard, click Next.

8. On page 7 of the Web Site Wizard, click Next.

9. On page 8 of the Web Site Wizard, enter the following path in the Save Pages To area of the window: **`%webroot%\nfusetest\`**. (By default, IIS places its `%webroot%` in `c:\inetpub\wwwroot`. This path may be different on your computer if you chose a different location or if you are running a different web server. Replace **`%webroot%`** with the path to your web server's root directory.)

10. You should now be able to view the pages by opening a web browser and navigating to `http://`*`servername`*`/nfusetest`.

# Review Questions

1. NFuse is a web interface to which Citrix MetaFrame XP utility?

   A. Published Application Manager

   B. Citrix Management Console

   C. Program Neighborhood

   D. Application Publication Manager

2. Which license level must you have in your farm to install and run NFuse?

   A. MetaFrame XPa

   B. MetaFrame XPe

   C. NFuse can be installed in any Citrix MetaFrame farm.

   D. The NFuse license is included with each version of Citrix MetaFrame, but it must be activated.

3. If IIS and NFuse are installed on the same computer, which technology that dynamically creates HTML-based web pages is installed automatically?

   A. Active Server Pages (ASP)

   B. Tag-based technology

   C. Java Virtual Machine (JVM)

   D. Application Programming Interface (API)

4. What technology eliminates the need to include user credentials with ICA files being sent from the web server to client devices?

   A. XML

   B. Ticketing

   C. Certificates

   D. ASP

5. If you use ticketing in your Citrix MetaFrame XP server farm, on which servers in your farm must you run the XML service?

   **A.** Every server in the farm that hosts published applications

   **B.** Every server in the farm

   **C.** The web server and one Citrix server

   **D.** The web server and the data collector

6. If ticketing is not used in your Citrix MetaFrame XP server farm, on which servers must you run the XML service?

   **A.** Every server in the farm that hosts published applications

   **B.** Every server in the farm

   **C.** One Citrix server in the farm

   **D.** The web server and the data collector

7. Which of the following platforms is not supported by NFuse?

   **A.** Internet Information Server 4.0 or later running on Windows NT Server 4.0

   **B.** iPlanet Web Server version 4.1 running on Solaris 7 or Solaris 8

   **C.** Internet Information Server 4.0 or later running on Windows NT Server 4.0, Terminal Server Edition

   **D.** Internet Information Server 3.0 running on Windows NT Server 4.0 or later

8. Active Server Pages can be used when which of the following conditions are met? (Choose all that apply.)

   **A.** Microsoft Internet Information Server is used as the web server.

   **B.** A scripting language such as VBScript is used to create the script.

   **C.** The ASP engine is installed on the web server.

   **D.** The XML engine is installed on the web server.

9. What utility can create an entire website based upon your Citrix environment?

   A. Web Site Wizard

   B. Web Site Manager

   C. Web Site Creation Wizard

   D. Web Management Wizard

10. On which port does SSL Relay listen by default?

    A. 1239

    B. 1494

    C. 8080

    D. 443

11. Which two ways can you configure published applications to run when executed from an NFuse web page? (Choose all that apply.)

    A. Launched

    B. Encoded

    C. Embedded

    D. Independent

12. Which of the following is not an option when choosing to embed the application on a web page?

    A. Java applet

    B. ActiveX

    C. Linux plug-in

    D. Netscape plug-in

13. If you are running Internet Information Server 4.0 or higher and want to use tag-based web pages, which setting would you choose during the Web Site Wizard for your site?

A. HTML For IIS

B. Active Server Pages

C. HTML For Servlets

D. JavaServer Pages

14. If you are running Netscape Web Server and want to use scripting-based web pages, which setting would you choose during the Web Site Wizard for your site?

A. HTML For IIS

B. Active Server Pages

C. HTML For Servlets

D. JavaServer Pages

15. If you are running Apache Web Server and want to use tag-based web pages, which setting would you choose during the Web Site Wizard for your site?

A. HTML For IIS

B. Active Server Pages

C. HTML For Servlets

D. JavaServer Pages

16. If you are running Internet Information Server and want to use scripting-based web pages, which setting would you choose during the Web Site Wizard for your site?

A. HTML For IIS

B. Active Server Pages

C. HTML For Servlets

D. JavaServer Pages

**17.** NFuse Java objects are responsible for which of the following? (Choose all that apply.)

**A.** Authentication to a server farm

**B.** Allowing the user to customize the web page that is presented

**C.** Querying Program Neighborhood randomly for new published applications

**D.** Creating and sending ICA files that users can use to start ICA sessions

**18.** ICA Clients can be installed from an NFuse web page, but you must copy them from the ICA Clients CD-ROM to the NFuse server. In which directory are these clients located on the CD-ROM?

**A.** `Webroot`

**B.** `ICAWeb`

**C.** `ICANfuse`

**D.** `NFuseClients`

**19.** ICA Clients can be installed from an NFuse web page, but you must copy them from the ICA Clients CD-ROM to the NFuse server. Which directory are these client files copied to on the NFuse server?

**A.** `Webroot`

**B.** `ICAWeb`

**C.** `ICANfuse`

**D.** `NFuseClients`

**20.** The Citrix XML service communicates with which service on all servers in the farm?

**A.** NFuse

**B.** World Wide Web Publishing

**C.** Citrix XML

**D.** Program Neighborhood

# Answers to Review Questions

1. C. NFuse is a web interface for Program Neighborhood.

2. C. NFuse comes with Citrix and can be installed in any Citrix MetaFrame farm. You do not need to purchase any more licenses or activate any licenses.

3. C. If IIS is installed on the same computer as NFuse, the Microsoft Java Virtual Machine (JVM) is installed automatically. Java object technology dynamically creates HTML-based web pages based on the applications that are available in the server farm for that user.

4. B. A user authentication ticket authenticates the user to applications on MetaFrame XP servers. Tickets have a configurable expiration period and are valid for a single logon. Tickets eliminate the need to include user credentials with ICA files being sent from the web server to client devices.

5. A. When tickets are used, the XML service must be installed on every server in the farm that hosts published applications.

6. C. If tickets are not used, the XML service needs to be installed on only one server in the server farm.

7. D. NFuse will not run on Internet Information Server 3.0. The supported versions of Internet Information Server are 4.0 and higher.

8. A, B. Active Server Pages may be used when Microsoft Internet Information Server is used on the web server and a scripting language such as VBScript is used to create the script. In addition, the web page must be capable of performing complex tasks.

9. A. The NFuse Web Site Wizard creates a complete site that includes a logon page, a main application list, back end support files, and ICA Client installation and graphic images used for navigation.

10. D. The Citrix SSL Relay service listens on port 443 by default. This is the standard port for the SSL protocol.

11. A, C. A launched application will launch a new window, and a published application will run in its own window. An embedded application will execute within the web page.

**12.** C. If you choose to embed the application on the web page, you must choose between ActiveX (IE), Netscape plug-in (Netscape Navigator), or a Java applet.

**13.** A. You would select HTML For IIS if you would like to use tag-based web pages in your NFuse environment with IIS.

**14.** D. If you are using Netscape and want to use scripting-based web pages, you must choose JavaServer Pages (Scripting Based) during the Web Site Wizard.

**15.** C. If you are using Apache Web Server and want to use tag-based web pages, you must choose HTML For Servlets (Tag Based) during the Web Site Wizard.

**16.** B. You would select Active Server Pages (Scripting Based) if you would like to use scripting-based web pages in your NFuse environment.

**17.** A, D. The NFuse Java objects do all of the following: authenticate users to a server farm, retrieve application sets available to a user, modify the properties of individual applications before presenting them to users, and create and send ICA files that users can use to start ICA sessions.

**18.** B. The ICA Client files that can be installed from the NFuse website are located in the `ICAWeb` directory on the ICA Clients CD and must be copied to the NFuse server.

**19.** D. The ICA Client files that can be installed from the NFuse website are located in the `ICAWeb` directory on the ICA Clients CD and must be copied to the NFuse server and placed in the `NFuseClients` directory.

**20.** D. The XML service communicates with the other servers in the server farm using the native Program Neighborhood service that is running on all servers in the farm.

# Chapter 13 Printing

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **11. Printing**

- 11a. Creating Client, Network and Local Printers
- 11b. Replicating Print Drivers and Importing Print Servers

# Printing Primer

Once the bane of the Citrix Administrator's job, printing has come into its own with MetaFrame XP. As many administrators can testify, most of the issues they faced when working in a MetaFrame environment stemmed from problems with *client printing* and *printer drivers* that would not work with MetaFrame. Citrix has taken steps to rectify most of the problems that arose from driver-compatibility issues. Most of the new functionality of the printing subsystem stems from Microsoft's attempt to certify the print drivers for the Windows 2000 family of operating systems and the ability to control the drivers used at the server and the client operating system.

One thing we need to clarify before we get too deep into the discussion of the MetaFrame XP printing subsystem is the terminology. As we progress through this chapter, we will use the following terms when discussing the various objects:

**Print device** The *print device* is the actual hardware that accepts the print jobs and performs the task of printing the physical document.

**Printer** A *printer* is the software representation of the print device. The printer consists of the configuration settings that control the print job and the driver that is used to structure the print job into a format the print device can understand.

**Client printer** The *client printer* is a printer that is created for a user's session that redirects the print job to the printer on the client's workstation.

Printers fall into three classifications within a MetaFrame XP environment: local, network, and client printers. Each of these types of printers has its own configuration requirements and is accessed differently by clients. Let's take a brief look at each of these configurations:

**Local printers** *Local printers* are created for use within the server farm. Whenever a printer is added to a MetaFrame XP server in the server farm, all of the servers within the server farm can use it as a local printer, allowing client devices to print to it. Printer drivers for the local printers can be replicated to all of the MetaFrame XP servers in the server farm to ease administration.

**Network printers** *Network printers* are print devices that have been shared on the network for multiple users to access. These include print devices that are attached to, and shared by, the client device. If a client has added a printer to their local Windows computer, that printer will become a client device within their session.

**Client printers** *Client printers* come in two flavors: 32-bit Windows printers and DOS-, Windows CE-, and Macintosh-based printers. Whenever a client running a 32-bit Windows operating system (Windows 2000, Windows NT, or Windows 9*x*) starts a session, the printers that are configured on their local system are configured as printers within their session. The non-Win32 operating systems can access their printers when running a session as long as the printer is defined for them within their session.

From within a session, users may have access to any of these printer types. Once printers are configured on your network, your clients have access to printers that are connected directly to MetaFrame XP servers, printers connected directly to other client devices, virtual printers configured to print to a file, and printers connected to print servers on the network. This functionality is so robust, in fact, that you can reach nearly any printer available in your network environment from your MetaFrame session.

The Citrix Management Console is used to manage the print subsystem. Since the entire print driver information is stored in the IMA database, any changes made to the configuration of our printing subsystem are made available to the clients. As changes are made to the configuration of your printing subsystem, the settings are stored within the file *wtsprnt.inf*. This file is populated with the mappings that exist within the IMA database as the system is started.

WARNING

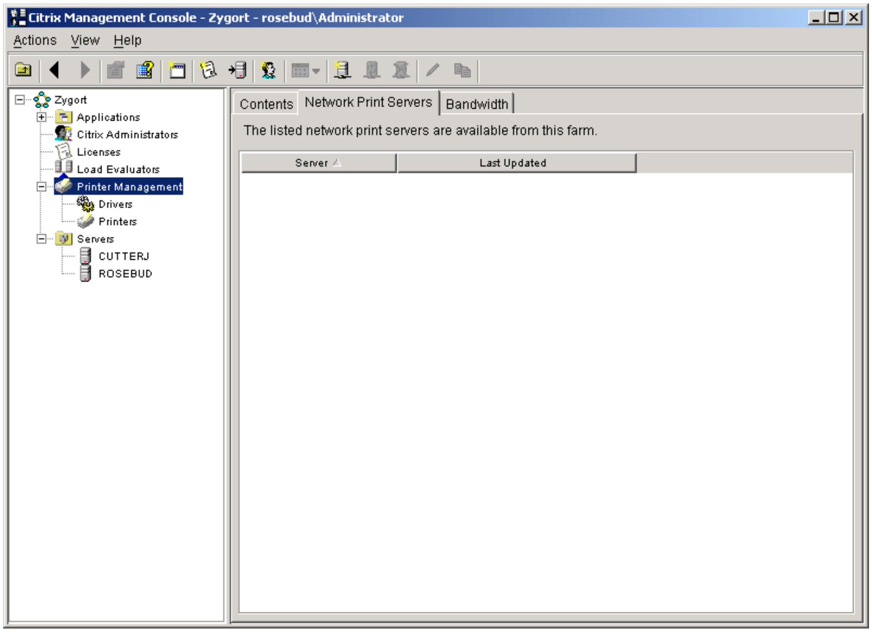
Do not edit the `wtsprnt.inf` file directly. The edits will not be imported into the database; instead, they will be overwritten as changes are made to the printing subsystem or when the server is rebooted.

Since the IMA database contains entries for all of the print drivers in the server farm, the length of time it takes to initiate the database relies in part on the amount of driver information that needs to be read. You should load the drivers only for those printers used within the farm. If clients do not use the drivers, the additional information only adds to the processing that is required by the server. If possible, try to use generic drivers that work for multiple printers.

When configuring the printing subsystem, you have the following nodes and options available:

**Printer Management node** This node is used to control nearly every function within the printing subsystem. As you can see in Figure 13.1, it is here that all of the printers, print drivers, and configuration options are controlled. The tabs found at this level are Contents, Network Print Servers, and Bandwidth.

**FIGURE 13.1** Printer Management node



The listed network print servers are available from this farm.

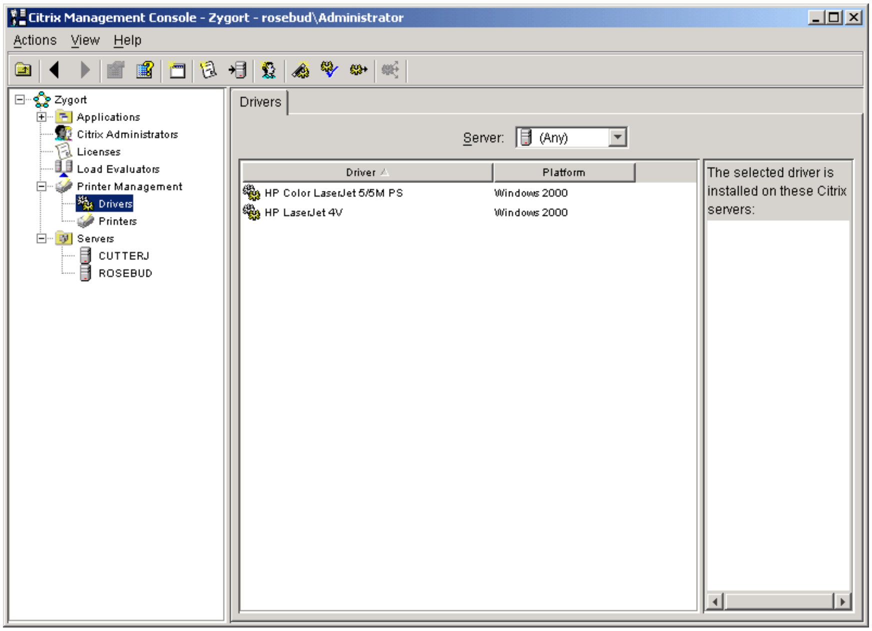
**Contents** This tab displays the containers found within the Printer Management node. The two containers, Drivers and Printers, are described below after we take a quick look at the other two tabs next to Contents.

**Network Print Servers** This tab contains information about the *print servers* that have been imported. Users can access the printers that have been configured on the print servers once they have been imported. Along with importing print servers from this tab, you can also remove those print servers that are no longer needed.

**Bandwidth** This tab allows an administrator to control the amount of network bandwidth that a server can use for printing purposes.

**Drivers container** This level contains information about the drivers installed on the MetaFrame servers in your farm for the printers used by clients. There is only one tab within this container, Drivers, shown in Figure 13.2, and it shows the drivers that are installed and the corresponding servers on which the driver is loaded.

**FIGURE 13.2** Drivers container



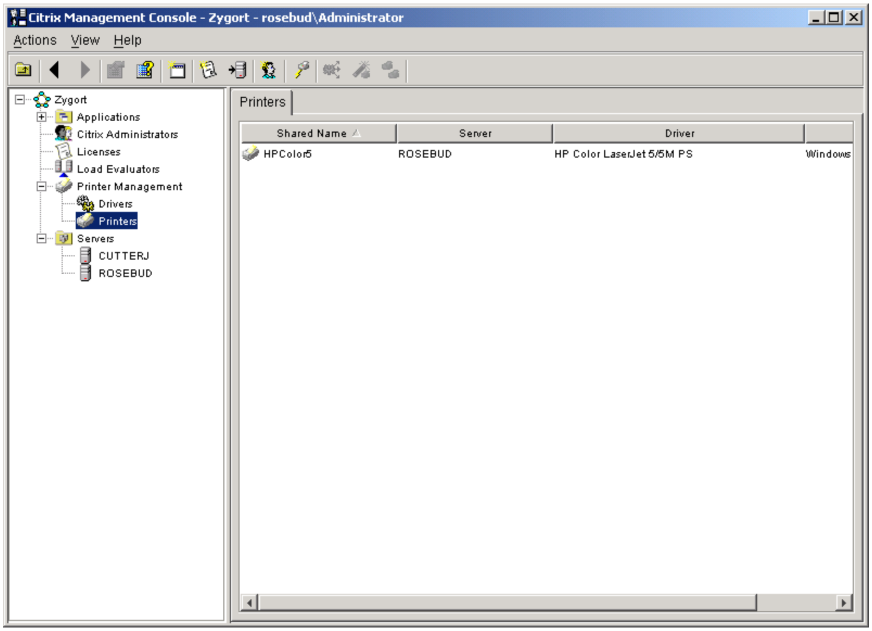
Server: (Any)

| Driver | Platform |
|---|---|
| HP Color LaserJet 5/5M PS | Windows 2000 |
| HP LaserJet 4V | Windows 2000 |

The selected driver is installed on these Citrix servers:

**Printers container** This container displays the network and local printers that are loaded or imported into the server farm. The only tab in this container, shown in Figure 13.3, is the Printers tab, and it displays the printer and the platform on which the printer is loaded. This tab does not list any client printers.

**FIGURE 13.3** Printers container



| Shared Name | Server | Driver | |
|---|---|---|---|
| HPColor5 | ROSEBUD | HP Color LaserJet 5/5M PS | Windows |

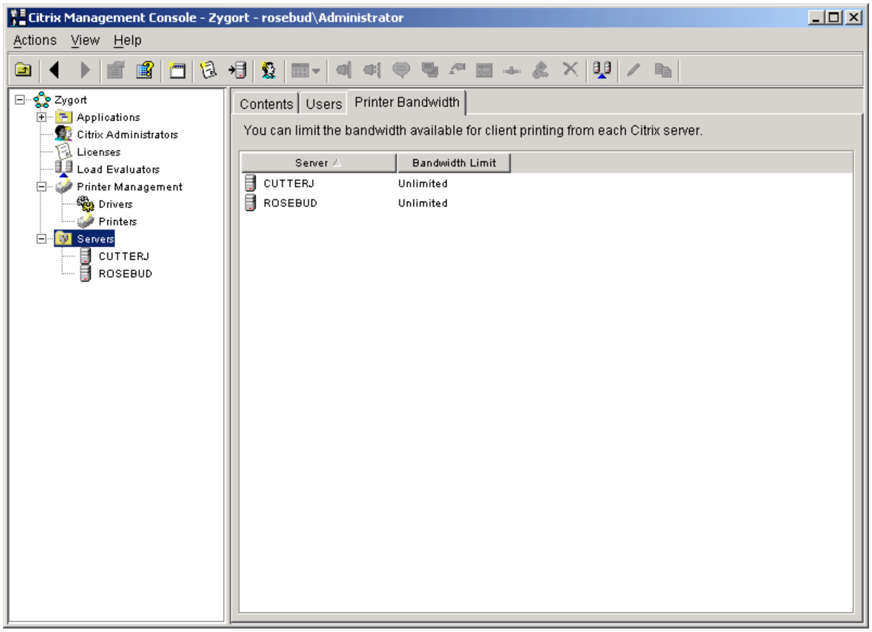
**Servers node** The Servers node contains many configuration options other than printing, but we will only look at the printing options at this point. The *Printer Bandwidth* tab, shown in Figure 13.4, displays the same information found in the Bandwidth tab in the Printer Management node.

**Server level** Again, the Server level, shown in Figure 13.5, has many more configuration options than just printing, but we will concern ourselves with only those printing options. Two tabs are dedicated to printing functions here:

**Printers** This tab shows the printers that are installed on the selected server.

**Printer Drivers** This tab shows the printer drivers that are installed on the selected server.

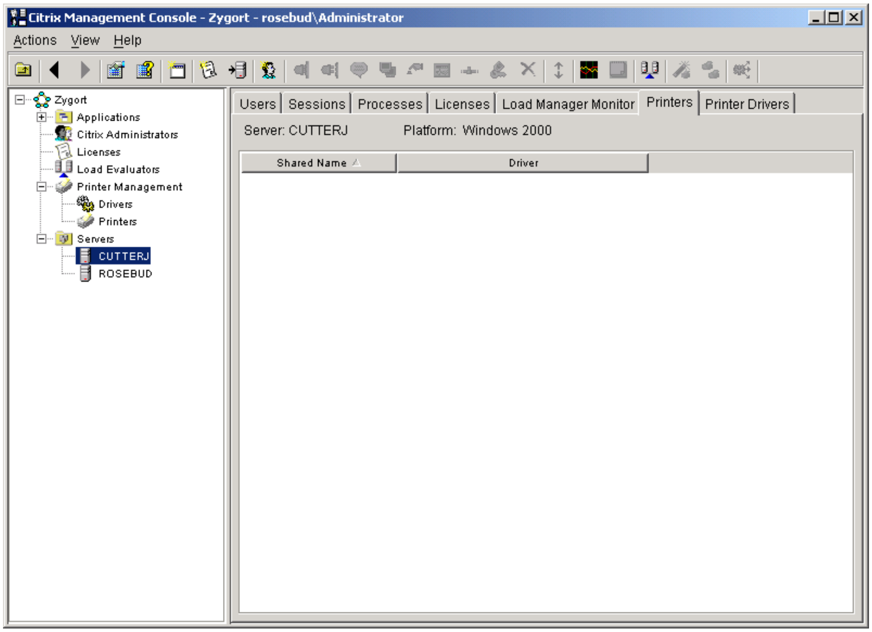
**FIGURE 13.4** The Servers node



You can limit the bandwidth available for client printing from each Citrix server.

| Server | Bandwidth Limit |
|---|---|
| CUTTERJ | Unlimited |
| ROSEBUD | Unlimited |

**FIGURE 13.5** Server level tabs



Server: CUTTERJ Platform: Windows 2000

| Shared Name | Driver |
|---|---|

WARNING

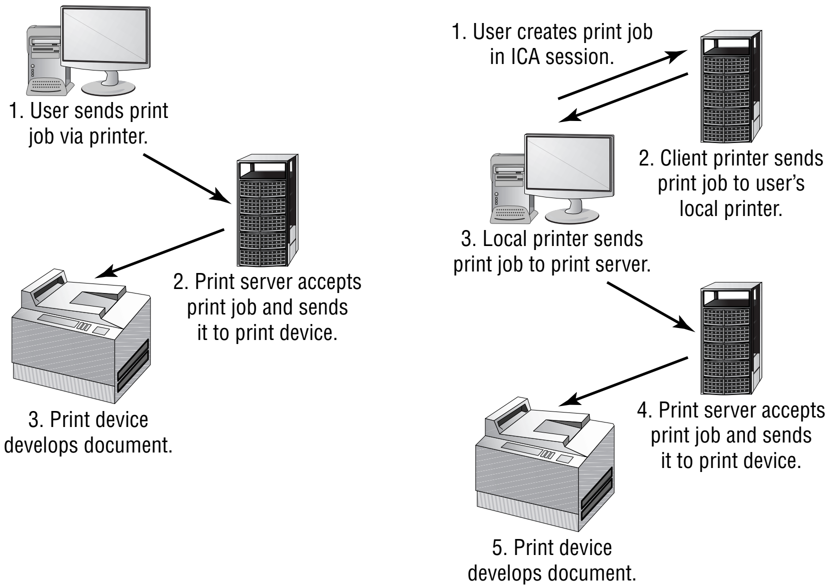
If you delete a printer driver, the Registry entry will still exist for future reference. If you delete the Registry information, you will need to reboot the server.

As an administrator, you can exert control over nearly every aspect of printing. You can control which printers are available to each user. You can import print servers, create printers on the MetaFrame servers, and even configure the connection parameters that control which client printers are mapped within the session. In the following sections, we will delve into the glory that is printer management and administration.

## Creating and Managing Printers

Any time a user needs access to a print device, a printer must be created on their computer. This software representation is actually an icon of the print driver that allows a document to be formatted appropriately for the print device. Whenever a user wants to print out a document, the printer is selected and the document is formatted for the print device and delivered to the print device to be printed.

MetaFrame sessions add another level of complexity to this scenario. The user's session is not usually running on the same device where the print device is connected. In the case of a network printer, the print device is connected to another computer on the network, but the user's printer object is local to the computer. When the user starts a session, the session creates a client printer that redirects print requests to the user's local computer. The local computer redirects the print request to the print server, which then passes the print job to the print device. The following graphic shows two scenarios, comparing the print job path from a user's computer to the print job path from a user's session.

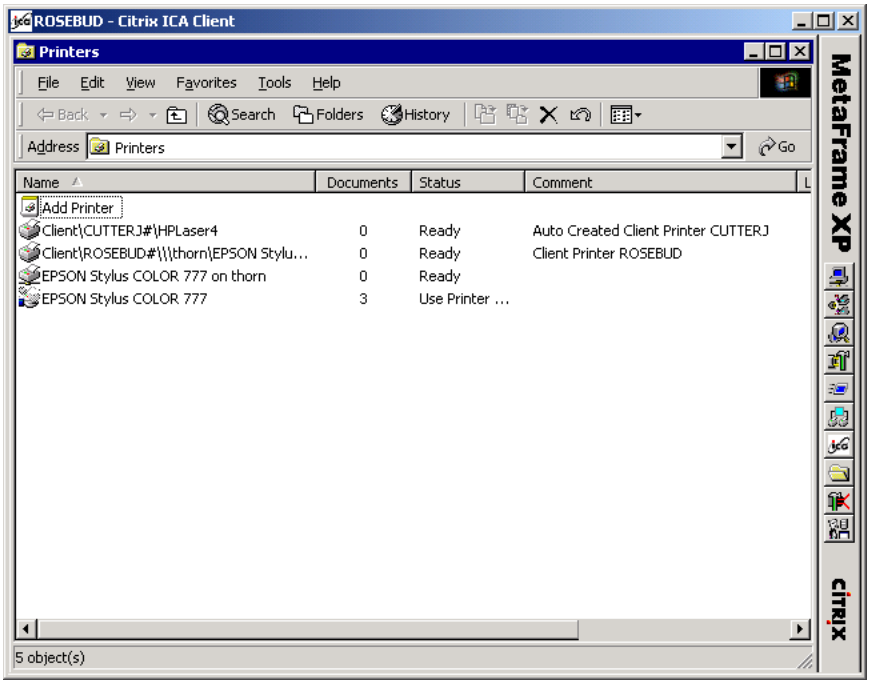

1. User sends print job via printer.
2. Print server accepts print job and sends it to print device.
3. Print device develops document.
1. User creates print job in ICA session.
2. Client printer sends print job to user's local printer.
3. Local printer sends print job to print server.
4. Print server accepts print job and sends it to print device.
5. Print device develops document.

Any printer that is configured on a user's computer can be a client printer within the user's session. As long as the user has the appropriate rights, they can create a printer, but we usually reserve this right for our technical staff. Using the standard Add Printer Wizard, we can create the printer, and the user will have access to it when the session is started. Client printers are represented within the user's printer control panel as *clientname#\printername*. If you have created a printer named HPLaser4 on a client device named CutterJ, the client printer will be represented as CutterJ#\HPLaser4, as shown in Figure 13.6.

WARNING

Throughout this text, you will see the client printer names referenced as *clientname#\printername*. You will also note that Citrix's documentation refers to the client printer names as *#clientname\printername*. This could prove to be an issue on the exam. We do not profess to know how you should answer an exam question since we do not know whether the exam questions were written from the documentation or from actually working with the product. Since we do not want to mislead anyone who may be using this book as a reference, we will use the real-world naming convention.

**FIGURE 13.6** Client printer shown in the printer control panel


ROSEBUD - Citrix ICA Client
Printers
File Edit View Favorites Tools Help
Back Search Folders History
Address Printers
Go
MetaFrame XP
CITRIX

| Name | Documents | Status | Comment |
|---|---|---|---|
| Add Printer | | | |
| Client\CUTTERJ#\HPLaser4 | 0 | Ready | Auto Created Client Printer CUTTERJ |
| Client\ROSEBUD#\\\thorn\EPSON Stylu... | 0 | Ready | Client Printer ROSEBUD |
| EPSON Stylus COLOR 777 on thorn | 0 | Ready | |
| EPSON Stylus COLOR 777 | 3 | Use Printer ... | |

5 object(s)

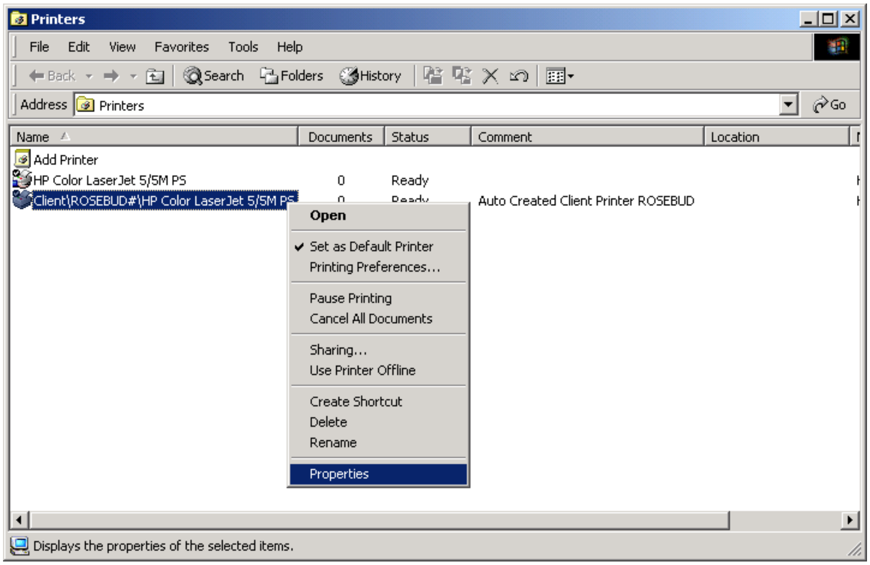
Since these mappings are created automatically, the user does not have to rebuild any connections to printers when they are using a MetaFrame session. You will have to educate users on the naming convention used for their printer since the client printer will not have as friendly a name as they are used to. Once you explain it to them, most users should be able to understand how to access their printers while in a session.

Printers that are created on the MetaFrame server are also available to the user when they are running a session. They appear in the printer control panel as though they are a printer connected to the user's device. This might cause some confusion for a user who is unaccustomed to working in a MetaFrame environment. Printers that are created on their local workstation are shown as networked, and printers that are created on a MetaFrame server are shown as local within the session. Unfortunately, this scenario is not configurable, so training is the best solution.

As mentioned earlier in this section, each of the client printers is created as the user starts a session. The overhead generated as these sessions are created is usually minimal. However, as many users start logging on to their sessions, the server may become bogged down with requests to create client printers. If you have printers that you want to be accessible to the client every time they connect to the MetaFrame server, you can store the mapping within the user's profile. All that is necessary is to change the description of the client printer. If you look at the list of printers that appear when a client is connected, you will see that the client printers appear with a description that starts with the words *Auto Created Client Printer*. Once you change the description from this default wording, the MetaFrame server will not delete the mapping.

To change the description of the client printer, make sure you have a session running and navigate to Start ➢ Settings ➢ Printers in the MetaFrame session. Right-click the printer and select the Properties menu item, as shown in Figure 13.7. You can change the description that appears in the Comment field on the General tab of the Properties sheet, shown in Figure 13.8. Once you change it, the printer mapping will not be deleted when the user's session ends. You can force the deletion by changing the description back to the original description, or you can delete the printer just as you would any other printer. Right-click the printer and select Delete from the context menu. The printer and its icon on the local desktop will be deleted from the client's session.

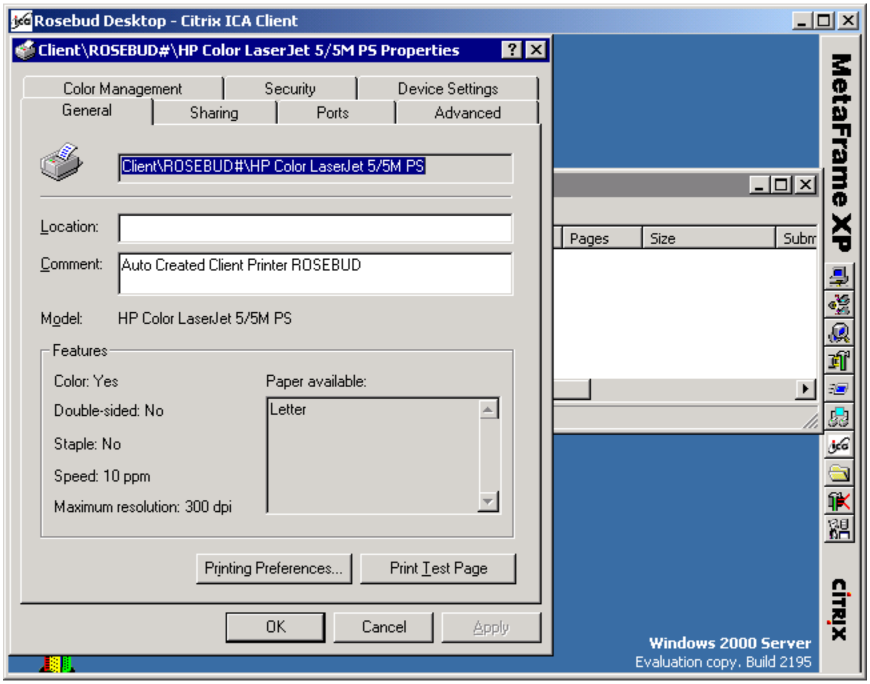
**FIGURE 13.7** Choosing the printer's properties



| Name | Documents | Status | Comment | Location |
|---|---|---|---|---|
| Add Printer | | | | |
| HP Color LaserJet 5/5M PS | 0 | Ready | | |
| Client\ROSEBUD#\HP Color LaserJet 5/5M PS | 0 | Ready | Auto Created Client Printer ROSEBUD | |

Displays the properties of the selected items.

**FIGURE 13.8** Printer Properties sheet



Rosebud Desktop - Citrix ICA Client

Client\ROSEBUD#\HP Color LaserJet 5/5M PS Properties

Client\ROSEBUD#\HP Color LaserJet 5/5M PS

Location:

Comment: Auto Created Client Printer ROSEBUD

Model: HP Color LaserJet 5/5M PS

Features

Color: Yes

Double-sided: No

Staple: No

Speed: 10 ppm

Maximum resolution: 300 dpi

Paper available:

Letter

Windows 2000 Server
Evaluation copy. Build 2195

Of course, the amount of network bandwidth consumed during the creation of client printers does not compare to the bandwidth consumed when print jobs are sent across an ICA session. The next section deals with controlling the amount of bandwidth used when clients print.

## Controlling Bandwidth Consumption

Printing to networked printers creates additional traffic on the network. Instead of passing the print job to a print device on a local port, the printing subsystem sends the print job to another computer that has the print device connected to it. If you send a large number of print jobs in this manner, the additional traffic on the network could cause congestion when you're trying to perform other tasks.

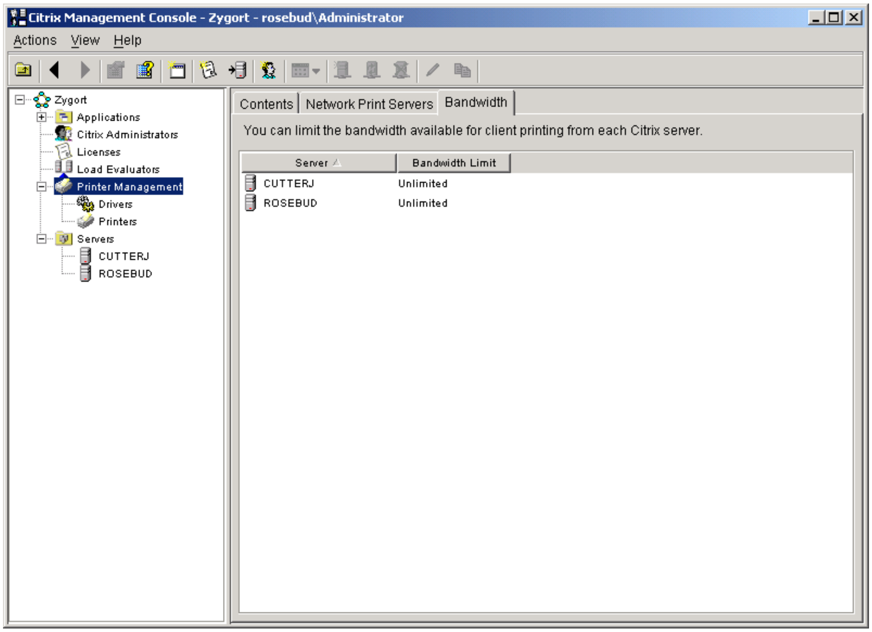
In the case of MetaFrame, another level of network traffic is generated since the print jobs a user sends to their local printer actually have to be sent across the network from the MetaFrame server. To control this additional network traffic, you can throttle the amount of bandwidth consumed by the

MetaFrame server when processing print jobs. Not only will this alleviate some of the network congestion, you will make more bandwidth available for user sessions.

You can control the bandwidth at two points within the Citrix Management Console. From the Printer Management node, once you select the Bandwidth tab, shown in Figure 13.9, you will see a list of all the servers in your server farm and their current setting. From the Servers node, once you select the Printer Bandwidth tab, shown in Figure 13.10, you will see the same list of servers. Both of these areas perform the same function.

The default setting for any of the servers is Unlimited. This allows a server to function normally by not throttling any of the print jobs sent to client printers. To change the bandwidth restrictions, right-click the server you want to throttle and select Edit from the menu shown in Figure 13.11. When the Edit Bandwidth Limit dialog box appears, shown in Figure 13.12, enter the total amount of bandwidth the server can use for printing.

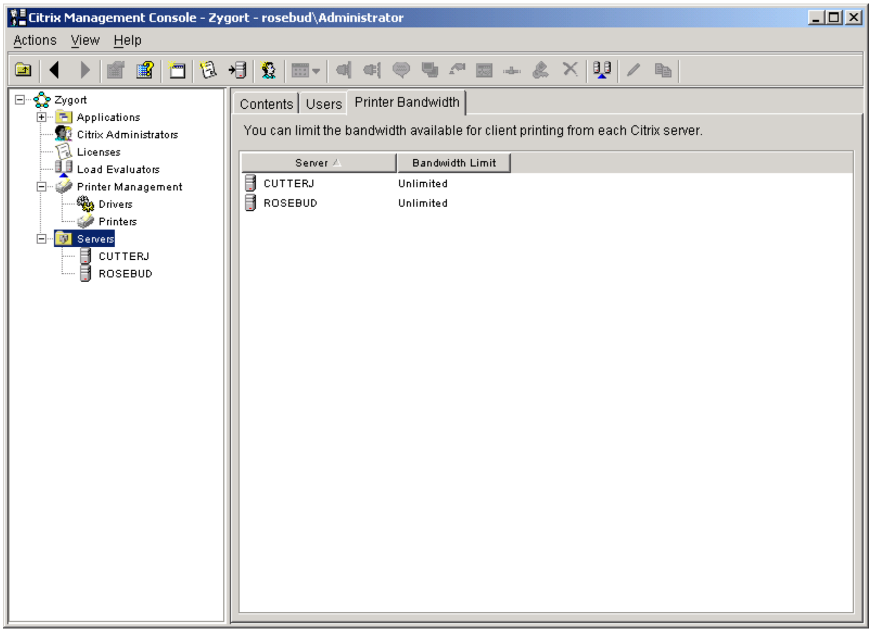
**FIGURE 13.9** The Bandwidth tab in Printer Management node



You can limit the bandwidth available for client printing from each Citrix server.

| Server | Bandwidth Limit |
|---|---|
| CUTTERJ | Unlimited |
| ROSEBUD | Unlimited |

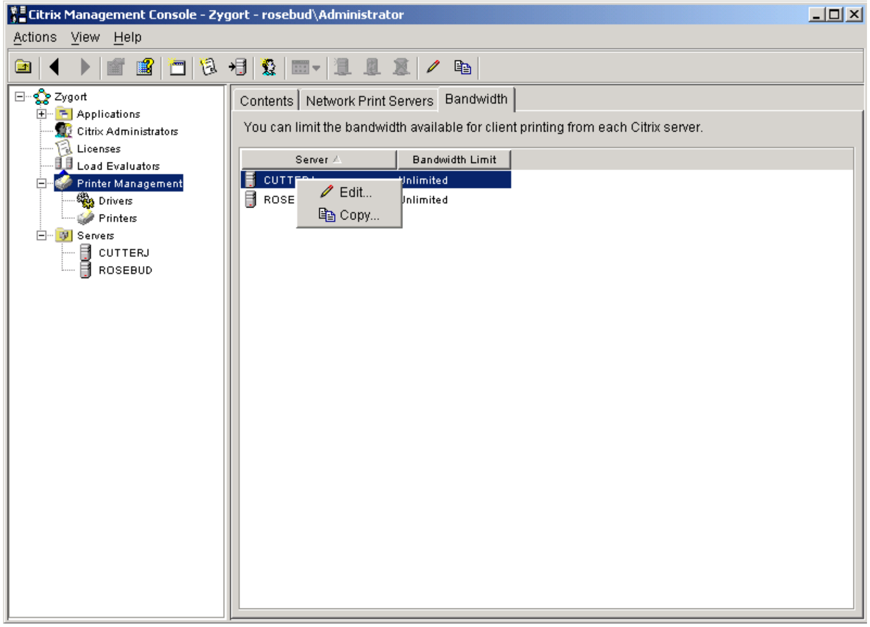
**FIGURE 13.10** The Printer Bandwidth tab in Servers node



You can limit the bandwidth available for client printing from each Citrix server.

| Server | Bandwidth Limit |
|---|---|
| CUTTERJ | Unlimited |
| ROSEBUD | Unlimited |

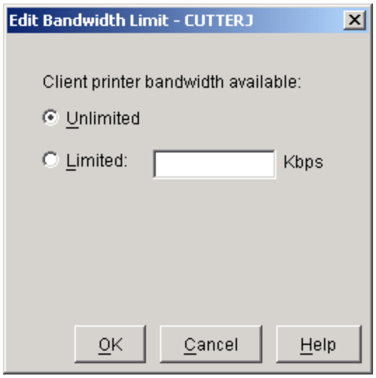
**FIGURE 13.11** Choosing to edit the bandwidth



You can limit the bandwidth available for client printing from each Citrix server.

| Server | Bandwidth Limit |
|---|---|
| CUTT | Unlimited |
| ROSE | Unlimited |

**FIGURE 13.12** The Edit Bandwidth Limit dialog box



Edit Bandwidth Limit - CUTTERJ

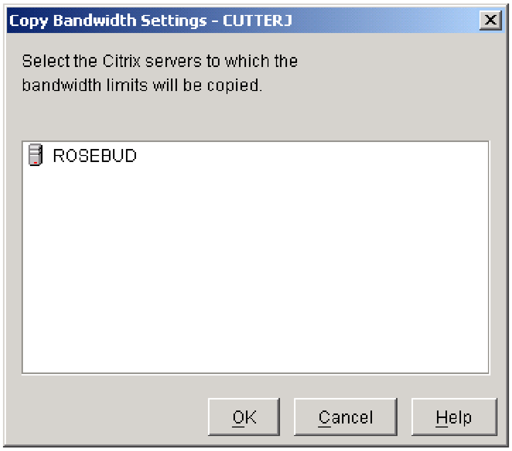
Client printer bandwidth available:

● Unlimited

○ Limited: Kbps

If you want to apply the same restrictions to other servers, you can duplicate the settings very easily. Once you have settings configured for one server, you can copy those settings to any other server by selecting the Copy option when you right-click the server. The Copy Bandwidth Settings screen shown in Figure 13.13 appears. Here you can select all of the servers on which you are going to set the restrictions. Once you click OK, the settings are applied to all of the selected servers.

**FIGURE 13.13** Duplicating the bandwidth restrictions



Copy Bandwidth Settings - CUTTERJ

Select the Citrix servers to which the bandwidth limits will be copied.

ROSEBUD

After you have made the changes to the server printing bandwidth, you will see those changes reflected in the two Bandwidth tabs. At this point, the network consumption of the throttled servers will not exceed the amount that you have specified. This is true even when there is a surplus of bandwidth available. Of course, you should monitor your servers to make sure that you have configured them for the optimum amount of bandwidth. Networks are usually in a constant state of flux, so you may have to change your configurations from time to time.

NOTE For more information on the tools used to monitor your MetaFrame XP environment, see Chapter 14, "Monitoring and Troubleshooting."

## Print Driver Replication

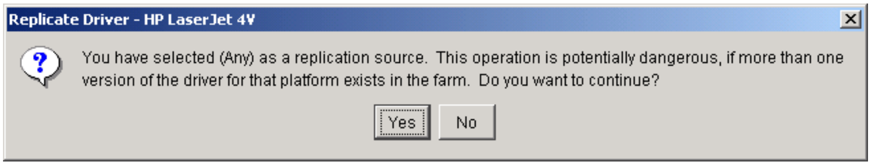
New to MetaFrame XP is the ability to replicate print drivers to other MetaFrame XP servers in the server farm. As you can imagine, this can be of great benefit to an administrator who has several MetaFrame XP servers. Not only can the print driver be installed on just one server and then replicated to all other servers where the driver is needed, but if the MetaFrame XP servers are spread out in different geographical areas, the administrator can distribute the driver to the servers without actually visiting them.

Another benefit is the ability to choose from which servers the driver is replicated. You can choose one server to be the master server that pushes the driver to the other servers, or you can specify that any server that has a copy of the driver can push the driver to any other server. Both of these options have their benefits and drawbacks. When you select only one server to push the driver, you are guaranteed that the driver you just installed is the copy that is pushed to all servers. The drawback is that the server acting as the master becomes your single point of failure. If it goes down, other servers may not receive the driver. Using multiple servers to push out the drivers alleviates this problem, but you run the risk of pushing out the wrong driver if one of the servers is configured incorrectly.

Using Citrix Management Console, you can configure the print driver replication. After opening Citrix Management Console, choose the Printer Management node. Two containers exist beneath this node: Drivers and Printers. The Drivers container lists all of the drivers available within the server farm and the servers on which they are loaded. When you select any of the drivers from this list, you can view the servers that have a copy of the driver loaded. These drivers appear in this list when a client has connected to the server farm and created a client printer using that driver or when the driver is replicated to the server.

*Printer replication* can occur either manually or automatically. If you want to replicate a driver immediately to servers in your farm, you can select a server from which to push the driver, right-click the driver to replicate, and select Replicate Drivers from the context menu. If you have selected the (Any) option from the server list, you will see the message shown in Figure 13.14. As mentioned earlier, choosing this server option can actually cause unpredictable results if different versions of the driver exist. This is the most reliable option, though, since the driver is available from multiple servers and there is no single point of failure.

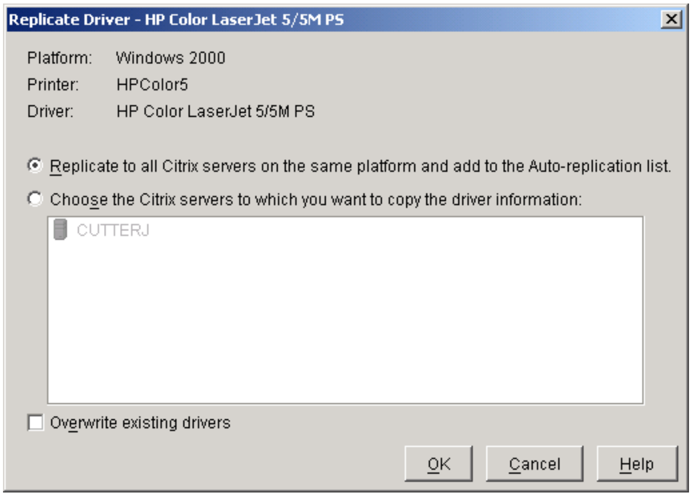
**FIGURE 13.14** Replicate Driver warning



You have selected (Any) as a replication source. This operation is potentially dangerous, if more than one version of the driver for that platform exists in the farm. Do you want to continue?

Figure 13.15 shows the replication options available. The default option is to replicate the driver to all servers in the farm that are running on the same platform. If the driver is loaded onto a Windows 2000 Server, the driver will automatically be pushed out to all of the Windows 2000 Servers. This option also adds the server and driver to the *Auto-replication* list, causing it to replicate again whenever a driver update is enacted on a server.

**FIGURE 13.15** Replication options



Platform: Windows 2000
Printer: HPColor5
Driver: HP Color LaserJet 5/5M PS

● Replicate to all Citrix servers on the same platform and add to the Auto-replication list.
○ Choose the Citrix servers to which you want to copy the driver information:

□ Overwrite existing drivers

The second option allows you to target the servers that will have the driver replicated to them. This option allows you to control the drivers loaded onto servers in the farm. Choosing this option does not add the driver to the Auto-replication list; you will have to configure those items yourself.

The final option on this screen is the Overwrite Existing Drivers check box. When it is checked, any existing drivers on the target servers are overwritten with the driver that you have chosen to replicate. This may not be a valid option if you have chosen to replicate the driver from any server in the farm. If you have updated a driver and are planning on pushing it out to other servers in the farm, this option could cause an older version of the driver to be put into place on some servers. If you're pushing out a new driver, select a single server to replicate the driver.

WARNING

Replicating the drivers to servers without using the Auto-replication feature will not automatically push new versions of the driver to other servers. As drivers are updated, the new information must be manually replicated.

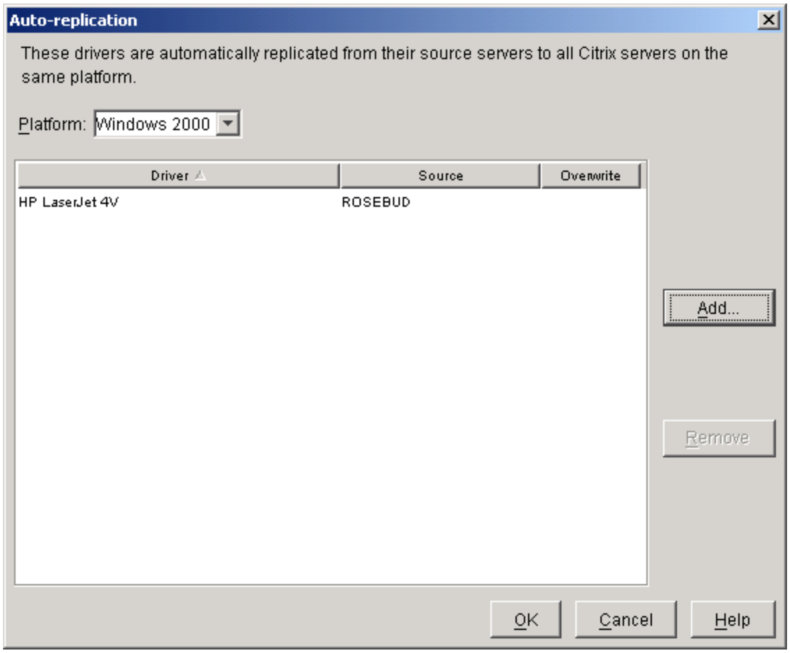
To configure the Auto-replication settings for a driver, select the Auto-replication option from the menu that appears when you right-click a driver. You will be presented with the Auto-replication screen shown in Figure 13.16. From here, you have the ever-popular choice of selecting from which platform you want to replicate the driver. Selecting Windows 2000 displays the drivers for that platform, while choosing Windows NT shows the drivers for those servers.

Clicking the Add button allows you to identify a driver that you want to replicate to the other servers in the farm, as shown in Figure 13.17. From here, you can specify which server will be used to push the driver information to the other servers. Also notice that the option for overwriting existing drivers is shown on this page. The same warnings discussed in the previous paragraphs concerning the selection of the (Any) server option apply here as well.

WARNING

Using the Auto-replication feature only allows you to replicate the drivers out to all of the servers in the server farm. You do not have control over which servers will have the drivers pushed to them. If you do not want to replicate the driver to all servers, do not use this feature.

**FIGURE 13.16** Auto-replication screen



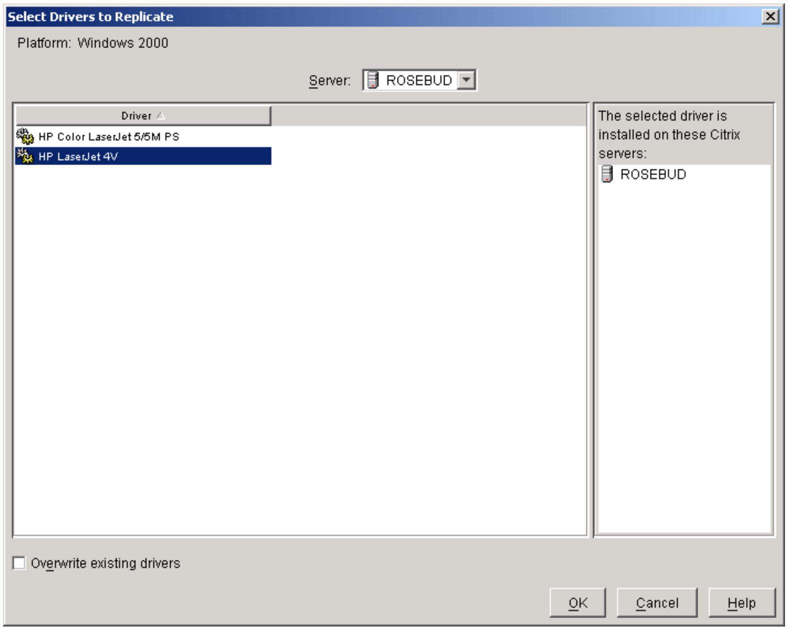
Auto-replication

These drivers are automatically replicated from their source servers to all Citrix servers on the same platform.

Platform: Windows 2000

| Driver | Source | Overwrite |
|---|---|---|
| HP LaserJet 4V | ROSEBUD | |

**FIGURE 13.17** Selecting the drivers to replicate



Select Drivers to Replicate

Platform: Windows 2000

Server: ROSEBUD

| Driver |
|---|
| HP Color LaserJet 5/5M PS |
| HP LaserJet 4V |

The selected driver is installed on these Citrix servers:

ROSEBUD

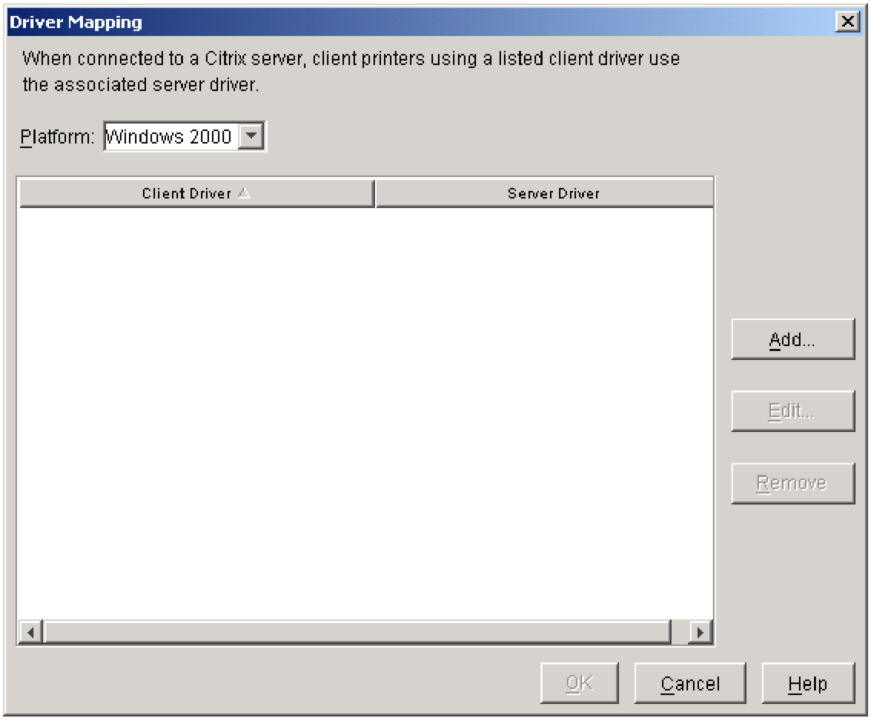
□ Overwrite existing drivers

## Driver Mapping

When you use Windows 2000 Professional or Window NT Workstation 4.0 as your client operating system, as you add printers, the print driver is automatically added to the Drivers container. Since the print drivers use the same names, the administrator has very little work to perform. Mappings are made automatically between the driver on the MetaFrame server and the client device.

When you use another operating system, the mapping is not as easy. The administrator must map the appropriate client print driver to the Windows 2000 or Windows NT driver, depending upon which operating system you are using to host MetaFrame XP. If you right-click within the Drivers container, the last option on the menu that appears is Mapping. When you select this option, you will see the screen shown in Figure 13.18. All of the client-to-server mappings you have made appear in the main list. If your server farm contains both Windows 2000 and Windows NT 4.0 servers hosting the MetaFrame XP sessions, the Platform pull-down list will reflect that information. When you choose Windows 2000 from this pull-down list, the mappings for all of the Windows 2000-based MetaFrame XP servers appear. The same holds true if you select Windows NT.

**FIGURE 13.18** Driver Mapping screen



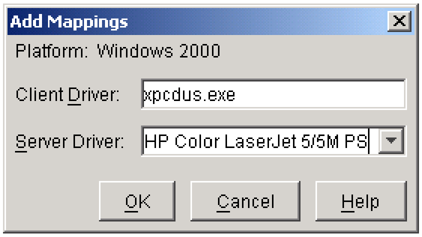
Driver Mapping

When connected to a Citrix server, client printers using a listed client driver use the associated server driver.

Platform: Windows 2000

If you have a printer whose driver name is different for the client than it is for the server, you will need to add a mapping to this list so that MetaFrame can use the correct driver when formatting the print job. Install a printer on the server so that the driver is available. Then right-click the Drivers container, open the Driver Mapping screen, and click the Add button to enter a client-to-server driver mapping. Figure 13.19 shows the dialog box that appears. You will need to know the exact name used on the client device. If you do not enter the name perfectly, the mapping will not work. Once you have entered the client driver name, you can use the pull-down list for the server driver name. All of the drivers that are currently installed on the selected server will appear.

**FIGURE 13.19** Add Mappings dialog box



Add Mappings

Platform: Windows 2000

Client Driver: xpcdus.exe

Server Driver: HP Color LaserJet 5/5M PS

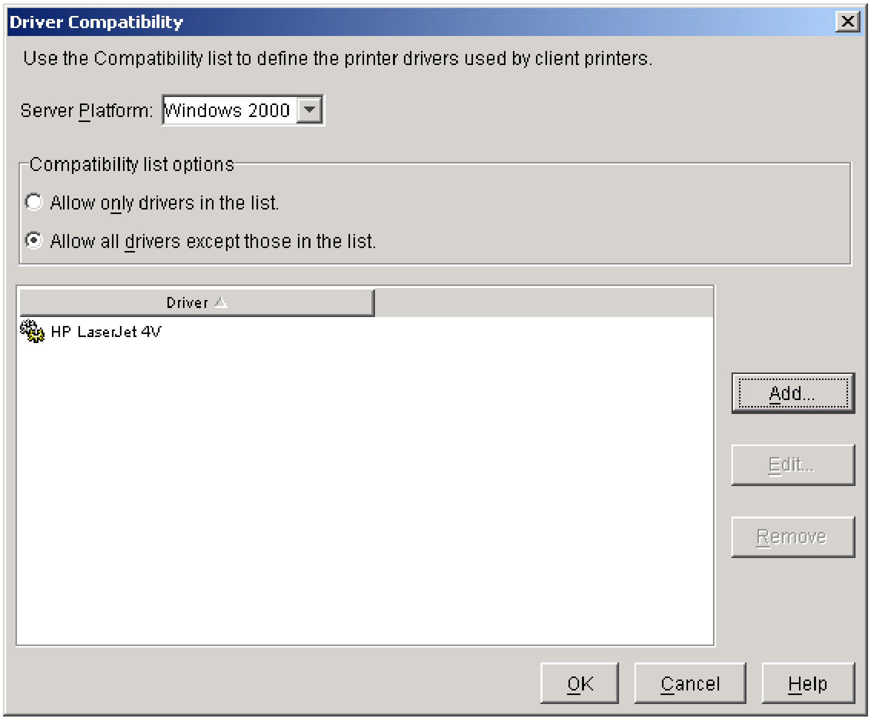
Once you've added the mapping, as the client attempts to print to the client printer, the server will take advantage of the server print driver and direct the print job to the client printer. This alleviates many of the problems associated with using a client printer on operating systems other than Windows 2000 and Windows NT 4.0. Notice the two other buttons on the Driver Mapping screen, Edit and Remove, shown previously in Figure 13.18. If you wish to delete a mapping, you can select the appropriate mapping and click Remove. If you need to make any changes to a listed mapping, select the mapping and click Edit. You will then be able to change either the Client or Server entry.

## Driver Compatibility

Of course, there are print drivers that will not play nicely in a MetaFrame environment. These drivers can cause problems for the user and the administrator—everything from simply not passing the print job to the client device to causing the session to lock up completely, forcing the user to start a new session and possibly losing the data from the previous session.

If you have identified a print driver as incompatible within your MetaFrame sessions, you can designate it as incompatible within the Drivers container. Open the Drivers container and right-click within the Drivers contents pane. From the context menu, select the Compatibility option. Figure 13.20 shows the *Driver Compatibility* screen that appears.

**FIGURE 13.20** Driver Compatibility screen



Driver Compatibility

Use the Compatibility list to define the printer drivers used by client printers.

Server Platform: Windows 2000

Compatibility list options

○ Allow only drivers in the list.

● Allow all drivers except those in the list.

| Driver |
|---|
| HP LaserJet 4V |

Again, you can choose on which server platform to configure the compatibility issue. If you have a problem only with drivers not playing nicely with Windows NT 4.0, you can select that option from the Server Platform pull-down list. The same holds true for Windows 2000. There may be drivers that will not work with either of these platforms. When this is the case, you will have to configure the driver compatibility twice, once for each server platform.

In the section labeled Compatibility List Options, you need to choose the default behavior of the compatibility list. The first choice, Allow Only Drivers In The List, makes every driver incompatible unless you explicitly add it to the list. Selecting this option allows you to control exactly which print drivers are allowed within your environment. If your clients are primarily Windows 9*x*–generation clients, this may be your best choice. You will have complete control over the print drivers used by your clients. The drawback to this option is that you will have more administrative overhead when you need to map new drivers.

The second option, Allow All Drivers Except Those In The List, excludes only those drivers that you specify. This option is used most often if your client base consists of Windows 2000 and Windows NT 4.0 clients. Every server in the farm will attempt to use the local driver that is named the same as the client's driver. As clients connect, the driver is added to the farm's list of drivers. The only time a driver will not be used is when the administrator has added the driver to the list on the Driver Compatibility screen. The drawback to this setting is your loss of control. If a client connects to a server, and one of the client's drivers is incompatible, problems could arise with the user's session.

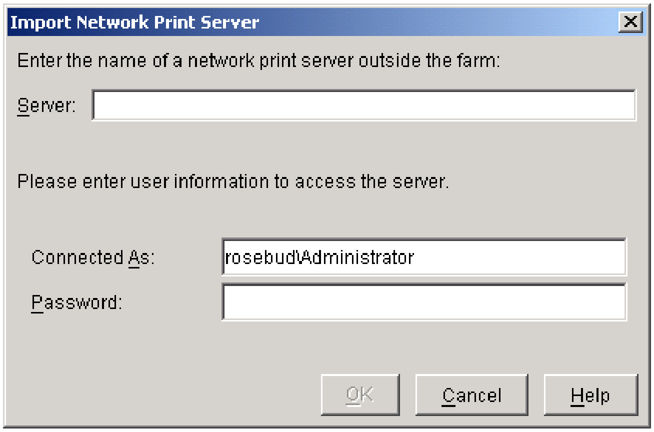
The three buttons on this screen allow you to add a driver to the list, edit existing driver information, and remove a driver from the list. Use caution with this screen since you must make sure which of the Compatibility List Options is enabled. If you add in a printer driver that you want to block, but the list is configured as Allow Only Drivers In The List, you will give the driver permission to run.

# Importing Print Servers

If you have print servers that host printers, or if you have printers available on MetaFrame servers that reside outside of your server farm, and you want to allow your users to access them, you can import those servers into your Printer Management node. Once the servers are added, these printers become available to your clients when they start a session.

Adding these printers is an easy task, but you will need to have the appropriate permissions to access the server that hosts the printers. Navigate to the Printer Management node within Citrix Management Console. Once you have selected the Network Print Servers tab, you can right-click anywhere in the contents window and select *Import Network Print Server*. This brings up the dialog box shown in Figure 13.21. Enter the name of the server that hosts the printers you want to import. The print server itself will appear within the Network Print Servers tab. All of the printers available on the newly added print server will appear within the Printers container of the Printer Management node. These printers will also appear within your client's sessions.

**FIGURE 13.21** Import Network Print Server dialog box



Import Network Print Server

Enter the name of a network print server outside the farm:

Server:

Please enter user information to access the server.

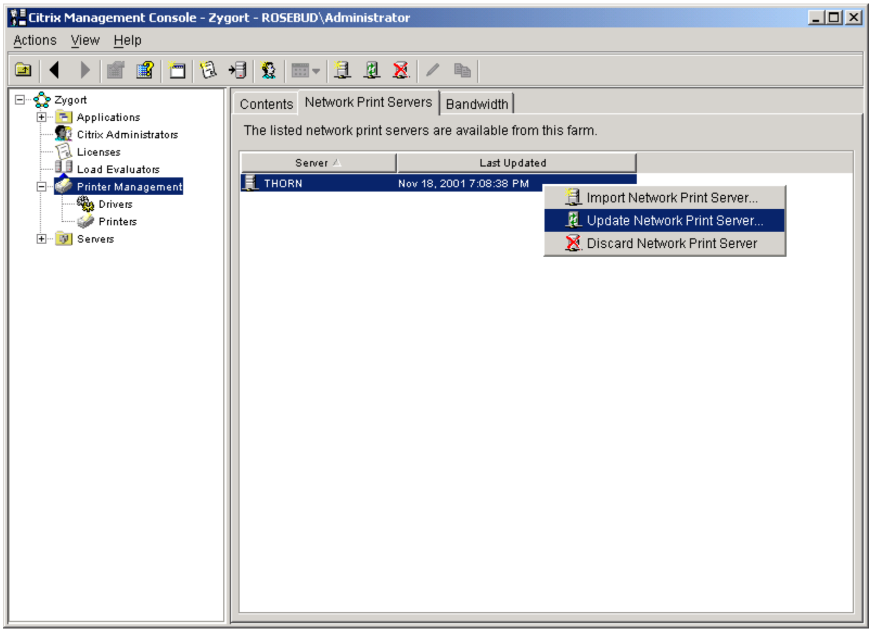
Connected As: rosebud\Administrator

Password:

One of the drawbacks to using network print servers is the inability to automatically update the printers. Whenever you add a new printer to the print server or remove an old one, you will have to update the print server information within the Network Print Servers tab. After adding the appropriate printer to the print server, right-click the server and click the Update Network Print Server option, as shown in Figure 13.22. You will be prompted to supply your credentials to access the printing subsystem on the remote server. Once you are authenticated, any printer changes that had been applied on the server will be updated within the server farm.

As your network changes, some systems become obsolete while other systems come online to take their place. Your MetaFrame environment needs to reflect when print servers are decommissioned. To remove a print server from the list, right-click the server and select Discard Network Print Server from the context menu. Not only will this remove the icon of the print server from the Network Print Servers tab, it will also remove the print drivers from the list of drivers available within the server farm.

**FIGURE 13.22** Updating the print server information



The listed network print servers are available from this farm.

| Server | Last Updated |
|---|---|
| THORN | Nov 18, 2001 7:08:38 PM |

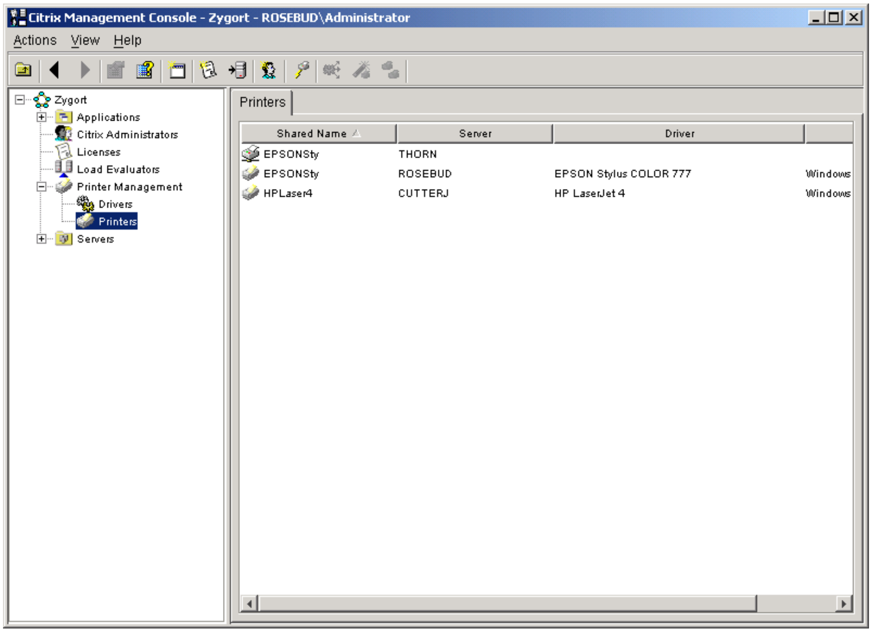
# Controlling Printer Access

So far, we have concentrated on the printer driver side of printer management. The other container within the Printer Management node is Printers. This container lists the printers that are available on MetaFrame servers within your server farm as well as print servers that have been imported into your farm. Those print servers that are imported into your farm do not list the driver and platform information; only the MetaFrame XP servers display this information, as shown in Figure 13.23.

You can configure the printers that are listed within this container so that a client is automatically mapped to the printer when it starts a session. This alleviates having to install the printer on the client's workstation. Right-clicking the printer brings up a menu that contains the Auto-Creation option. Once you select this option, the screen shown in Figure 13.24 appears. This screen should look familiar since it offers the same options that appear when you are configuring a published application for use.

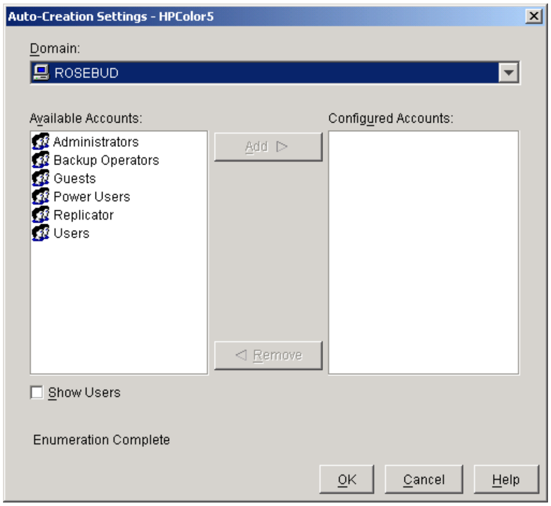
In essence, you are applying permissions to the users who need to have access to the printer, but the additional level of auto-creating the printer for the users comes into play.

**FIGURE 13.23** Printers container showing printers in the farm



| Shared Name | Server | Driver | |
|---|---|---|---|
| EPSONSty | THORN | | |
| EPSONSty | ROSEBUD | EPSON Stylus COLOR 777 | Windows |
| HPLaser4 | CUTTERJ | HP LaserJet 4 | Windows |

**FIGURE 13.24** Printer Auto-Creation Settings screen



Domain: ROSEBUD

Available Accounts:

- Administrators
- Backup Operators
- Guests
- Power Users
- Replicator
- Users

Configured Accounts:

□ Show Users

Enumeration Complete

Once you select the domain where the accounts reside, you can specify which groups will have their members' printers auto-created when they connect to the server. If you select the Show Users check box, user accounts will appear in the Available Accounts list, allowing you to add them so that you can control the printer creation on a user-by-user basis. After the printer is configured for auto-creation, you can copy the settings to other printers by simply right-clicking the printer in the Printers container and selecting Copy Auto-Creation Settings from the context menu.

TIP

Always use groups when assigning rights and permissions to user accounts. Even though you may have only one person to assign these to, you will undoubtedly have another user in the future who will need the same rights and permissions. Adding the user to a group is easier than adding another user with the same permissions.

You will need to replicate the print driver to all of the servers where the users are starting their sessions. Failure to do so could cause the user to have the wrong print driver while printing from their session, or the printer will not be created for them, depending on the settings you have applied to the server farm. When the user logs on after you have applied auto-creation settings, the printers you configured will be available within their session without you visiting their workstation to configure their printers.

## DOS and Windows CE

DOS and Windows CE clients do not have the same print driver structure that Windows 2000 and Windows NT 4.0 use. For these clients, mappings must exist, or the printer must exist on all the servers on all platforms within the server farm. Figure 13.25 shows the Client Printers screen that appears when you select the Client Printers option from the context menu after right-clicking in the Printers container.

The four buttons available on this screen allow you to perform the following tasks:

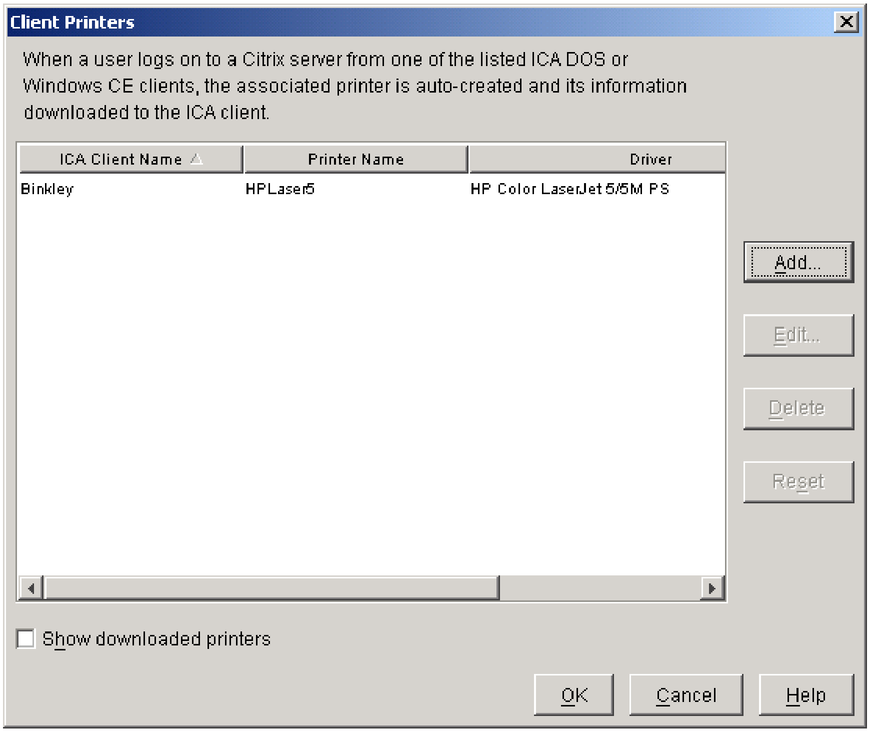
**Add** Clicking the Add button generates a dialog box that specifies the properties of the client printer to be created for a DOS or Windows CE client.

**Edit** From the Edit button, you can modify the properties of the client printer.

**Delete** You can remove any client printers that are no longer needed by clicking this button.

**Reset** Clicking this button changes the status of the client printer driver download to Pending. Upon the next connection by the client, the printer driver is downloaded again.

**FIGURE 13.25** Client Printers screen



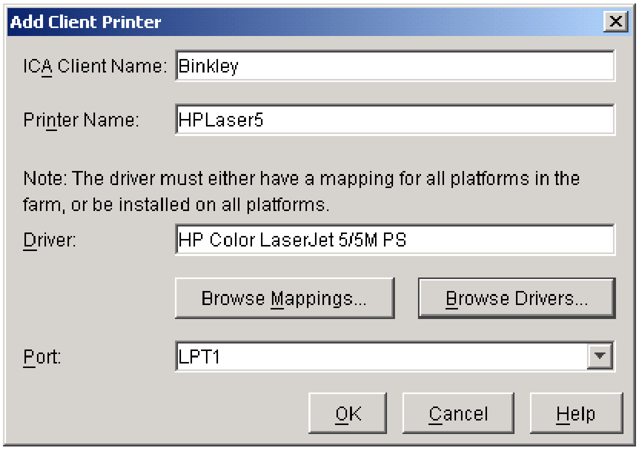
When a user logs on to a Citrix server from one of the listed ICA DOS or Windows CE clients, the associated printer is auto-created and its information downloaded to the ICA client.

| ICA Client Name | Printer Name | Driver |
|---|---|---|
| Binkley | HPLaser5 | HP Color LaserJet 5/5M PS |

□ Show downloaded printers

Clicking the Add button brings up the Add Client Printer dialog box shown in Figure 13.26. From here, you need to identify the client device on which the printer is configured. You also need to know the name of the printer on the client device. As mentioned earlier in the discussion of printer mappings, you must enter this information exactly as it appears on the client device.

**FIGURE 13.26** The Add Client Printer dialog box



ICA Client Name: Binkley

Printer Name: HPLaser5

Note: The driver must either have a mapping for all platforms in the farm, or be installed on all platforms.

Driver: HP Color LaserJet 5/5M PS

Port: LPT1

The Driver option of the Add Client Printer dialog box allows you to choose the driver that is used by the server from within the client's session. The two Browse buttons let you choose either a driver mapping or a driver loaded in the server farm. If the client printer driver has a different name than the server driver, you will need to choose a mapping from the list. Otherwise, if the driver name is the same as the driver used on the MetaFrame servers, you can click the Browse Drivers button and select the appropriate driver.

The final choice within the dialog is the Port option. Select the port on which the client printer is connected to the client device. This information is used when the client printer is created as the user starts a session. These client printers are represented as *clientname*#LPT*x*, where *clientname* is the name of the client device and LPT*x* is the port used (*x* is replaced with the actual port number).

Once configured, the client printer appears on the screen with the status of Pending. After the client connects for the first time, the status changes to Downloaded. The printer will remain in this state until the administrator clicks the Reset button when selecting the printer from the screen. The printer will revert to a Pending state and will be downloaded to the client the next time they connect.

## Client Connections

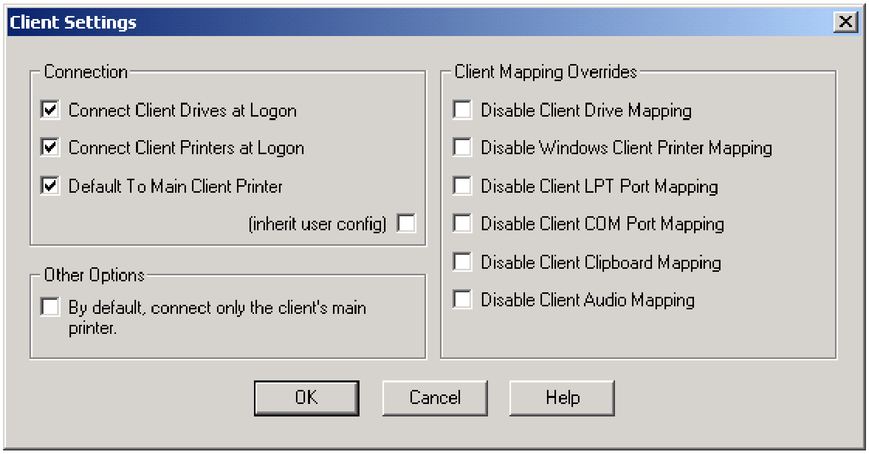
The final topic we will approach in this section is controlling the printer connections from the initial client connection parameters. If you remember back in Chapter 6, “Other Administrative Tools,” we introduced the Citrix Connection Configuration utility. This utility is used to control connections to MetaFrame servers. Usually, the default options are sufficient, and the user’s profile information controls how the session is created and what it has access to.

After opening the Citrix Connection Configuration utility and choosing to edit the properties of the connection you wish to control, you can click the Client Settings button to view the dialog box shown in Figure 13.27. Several printing options exist here. By default, two options appear in the Connection section:

**Connect Client Printers At Logon** When this option is selected, client printers will be created for the printers installed on the client device. If it is deselected, the client printers will not be automatically mapped at logon.

**Default To Main Client Printer** When this option is selected, the default printer defined in the user’s profile becomes the default client printer when the user logs on. If it is deselected, the default printer configured on the MetaFrame server is used as the default client printer within the user’s session.

**FIGURE 13.27** Client Settings dialog box



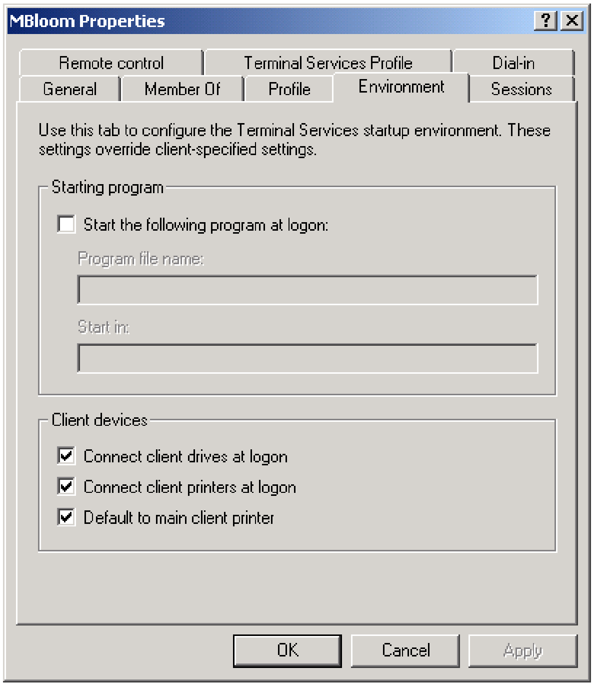
Connection
- ☑ Connect Client Drives at Logon
- ☑ Connect Client Printers at Logon
- ☑ Default To Main Client Printer
- (inherit user config) □

Other Options
- □ By default, connect only the client's main printer.

Client Mapping Overrides
- □ Disable Client Drive Mapping
- □ Disable Windows Client Printer Mapping
- □ Disable Client LPT Port Mapping
- □ Disable Client COM Port Mapping
- □ Disable Client Clipboard Mapping
- □ Disable Client Audio Mapping

If the (Inherit User Config) check box is checked, the options chosen within the Environment tab of the user’s profile take precedence, as shown in Figure 13.28.

**FIGURE 13.28** User properties controlling printer mappings



Use this tab to configure the Terminal Services startup environment. These settings override client-specified settings.

Starting program

□ Start the following program at logon:

Program file name:

Start in:

Client devices

☑ Connect client drives at logon

☑ Connect client printers at logon

☑ Default to main client printer

Under the Client Mapping Overrides section of the Client Settings dialog box, the following options are available to configure printing:

**Disable Windows Client Printer Mapping** When you select this option, the client's printers are not available through client mappings. If the client system has the printers shared for network access, the printer may still be used through standard printer mappings.

**Disable Client LPT Port Mapping** When you select this option, the client's LPT ports are not available for mapping from within a session.

The last option on this screen, By Default, Connect Only The Client's Main Printer, maps only the printer that is configured as the default printer in the user's profile. You can map other client printers after the session has started, but they will not be mapped initially.

Thus we end our discussion on printers and client printers. Although Citrix has made printing easier and more reliable, an administrator still has plenty of configuration to perform. From here we move to our final topic: maintenance and troubleshooting.

# Summary

The MetaFrame XP printing subsystem has gone through a major overhaul and performs far more efficiently than its MetaFrame 1.*x* counterpart. Additional functionality and easier administrative support are the hallmarks of the new printing subsystem. If a user is running Windows 2000 or Windows NT 4.0 as the operating system on the client device, the print drivers usually have the same name and are automatically configured for the session. If another operating system is employed, you may need to map the client device's printers to allow proper use of the printer.

Printer drivers may be replicated to all of the servers within the server farm. Since all of the MetaFrame XP servers share information within the farm, any of the servers can take advantage of the driver information from one centralized location. You can configure DOS and Windows CE drivers so that a user's printers are configured as the user starts a session.

You can also import print server information into the farm so that users can take advantage of the printers loaded on the print server. Once you import this information, the server information will have to be updated automatically, but the printers will be available for all users to access if they have the appropriate permissions to use them.

# Exam Essentials

**Understand how client printers are created for Windows clients.** Client printers are automatically created for every printer that is added to a client device if the operating system is a Win32-based client.

**Understand how to map drivers for Windows 9*x* clients.** Print drivers for Windows 9*x* clients do not always have the same name as those for Windows 2000 and Windows NT 4.0 operating systems. You will need to create driver mappings so that the server uses the correct driver for the client print device.

**Know the three types of printers within a MetaFrame XP environment.** The three types are client printer, local printer, and network printer.

**Know how to control the amount of network consumption printing uses.** The Bandwidth options allow you to configure exactly how much network bandwidth the server can use when sending print jobs.

**Understand print driver replication.** Print drivers can be installed on one server and then replicated to any other or all of the servers within the server farm.

**Know how to import a print server.** When you use the Network Print Servers tab in the Printer Management node of Citrix Management Console, you can import a print server. After you choose the print server to import, the printers installed on that server become available to clients.

**Know how to configure DOS and Windows CE client printers.** You can add printers that will be automatically loaded onto these clients by using the Client Printer options within the Printers container of the Printer Management node of Citrix Management Console.

# Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Auto Created Client Printer
Auto-replication
client printers
client printing
*clientname#\printername*
Driver Compatibility
Import Network Print Server
local printers
network printers
print device
print servers
printer
Printer Bandwidth
printer drivers
printer replication
`wtsprnt.inf`

# Exercise

This exercise is meant to reinforce your understanding of importing network print servers, auto-creating client printers, controlling the bandwidth used, and configuring driver replication. For these techniques to work, you will need to have three servers: two running MetaFrame XP and installed in the same server farm and the other configured as a stand-alone server that is not part of your server farm.

## EXERCISE 13.1

### Printing

The first part of this exercise deals with importing a network print server:

1. Open Citrix Management Console.
2. Click the Printer Management node.
3. Click the Network Print Servers tab.
4. Right-click in the details pane and select Import Network Print Server from the context menu.
5. In the Server field enter ***printserver***, where ***printserver*** is the name of the network print server you are importing.
6. Enter the username and password of an administrative account in the Connect As and Password fields.
7. Verify that the printers that are installed on the network print server are listed in the Printers container.

The next part of this exercise replicates the print drivers of the printer added when you imported the network print server to the MetaFrame servers in your farm:

1. Open the Drivers container beneath the Printer Management node.
2. Right-click the driver for the printer you wish to replicate, and select Replicate Drivers from the context menu.
3. Answer **Yes** to the message that appears.

**EXERCISE 13.1** ***(continued)***

4. Make sure the option Replicate To All Citrix Servers On The Same Platform And Add To The Auto-replication List is selected, and select the Overwrite Existing Drivers option. Click OK.
5. Right-click the driver again, and select Auto-replication from the menu.
6. Click Add and select your driver.
7. Select Overwrite Existing Drivers and click OK.

The next section configures the bandwidth allowance for the server:

1. Click the Printer Management node and click the Bandwidth tab.
2. Right-click one of your MetaFrame XP servers and choose the Edit option from the context menu.
3. Choose the Limited option and enter **96** in the Kbps field. Click OK.
4. Right-click the same server, and choose the Copy option from the context menu.
5. Select your other MetaFrame server from the list and click OK.
6. Verify that both servers have a bandwidth limit of 96Kbps.

Finally, we configure an auto-created client printer for a user:

1. Choose the Printers container beneath the Printer Management node.
2. Right-click the printer that was added when the Network Print Server was imported into the farm. Select Auto-Creation from the menu.
3. Choose one of your MetaFrame servers from the Domain list.
4. Select the Users group, and click the Add button. Click OK.

# Review Questions

1. ICA Clients have access to which of the following types of printers? (Choose all that apply.)

   A. Network printers defined on a network print server

   B. Local printers connected to a MetaFrame XP server

   C. Local printers connected to their client workstation

   D. A virtual printer that creates a file on the user's client workstation

2. Which of the following is not a type of printer connection?

   A. Client connection

   B. Network connection

   C. Virtual connection

   D. Local connection

3. What type of printer would a PostScript printer connected to a Macintosh computer by a serial cable be considered?

   A. Network printer

   B. Virtual printer

   C. Local printer

   D. Client printer

4. A user has a printer that is defined in Windows. She connects to an ICA session and has access to that printer. Which type of printer is this considered?

   A. Network printer

   B. Virtual printer

   C. Local printer

   D. Client printer

**5.** Which of the following statements best describes what MetaFrame considers a network printer?

**A.** A printer that is connected to a print server and shared on a Windows network

**B.** A printer that is defined on a MetaFrame server

**C.** A printer that is connected to the ICA Client and accessible through the session

**D.** A printer that is defined on a MetaFrame server and accessible through the session

**6.** Which of the following best describes a local printer in MetaFrame XP?

**A.** A printer that is connected directly to the ICA Client's workstation and available through the ICA session

**B.** A printer that is connected directly to a MetaFrame XP server

**C.** A printer that is connected directly to a print server and shared on a Windows network

**D.** A printer that is connected directly to the ICA Client's workstation and mapped to the ICA session

**7.** Your computer is running Windows 98 and you have a printer connected to your LPT1 port. When you connect to a MetaFrame server, you notice that your local printer is not available in your ICA session. You check the ICA Client settings within the Citrix Connection Configuration and find that you have the Connect Client Printers At Logon option enabled. What must you do next so the printer will automatically be created the next time you log on?

**A.** Configure printer drive mappings on the MetaFrame XP server and replicate the drivers to the other MetaFrame XP servers.

**B.** In the ICA session, use the Add Printer Wizard and install the printer as a network printer through the client network.

**C.** Share the printer in Windows 98. Log on to the ICA session and use the Add Printer Wizard to install the printer as a network printer through the Microsoft network.

**D.** Map the printer using the `<net use LPT1 \\computername \printername /persistent:yes>` command.

8. In which format will an auto-created client printer appear in the Printers folder on a MetaFrame server?

   A. *clientname#\printername*

   B. *clientname\printername*

   C. \\*clientname\printername*

   D. \\*clientname#\printername*

9. You have defined a network print server so that your clients will have access to all of that server's printers. You add a new printer to the print server, but your users cannot see the new printer. What could be the problem?

   A. You must update the print server information manually.

   B. The users must log off and log back on to view the new settings.

   C. The users must refresh the Printers folder to see the new printers.

   D. Any printers added after the print server is imported must be set up manually for the user.

10. What steps must you go through to remove a print server from a farm?

    A. In the Printer Management node of the Citrix Management Console, right-click the print server and choose Properties. In the Settings tab, place a check in the box labeled Disable From Farm View.

    B. On the MetaFrame XP server, remove the printers that are serviced by that print server, and then remove the print server by opening the Printer Management node of the Citrix Management Console, right-clicking the print server to remove, and choosing Discard Network Print Server from the context menu.

    C. In the Printer Management node of the Citrix Management Console, right-click the print server to remove and choose Remove Network Print Server from the context menu.

    D. In the Printer Management node of the Citrix Management Console, right-click the print server to remove and choose Discard Network Print Server from the context menu.

**11.** You configure printer bandwidth for a server on your network and want to make the same changes to all of the other servers in your farm. What is the best way to do this?

**A.** Make the changes on the data collector server and they will be replicated to all of the other Citrix servers in the farm.

**B.** Do nothing. The settings will automatically be copied to all other Citrix servers in the farm.

**C.** Select a server in the Server list in the Bandwidth tab and use the Copy command to copy the bandwidth settings to other servers in the farm.

**D.** Select a server in the Server list in the Bandwidth tab and place a check in the check box labeled Replicate Settings To All Other Servers In The Farm.

**12.** You want to copy a print driver to other servers in the farm. What are the best ways to do this? (Choose all that apply.)

**A.** Right-click a driver and choose Replicate Drivers from the Drivers container of the Printer Management node.

**B.** Select the driver from the Drivers tab of the Drivers container in the Printer Management node. From the Actions menu, select Printer Management and click Replicate Drivers.

**C.** Select the driver from the Replication tab. Right-click the driver and choose Replicate Now.

**D.** In the Replication tab of the Printer Management node of the Citrix Management Console, select the driver from the list and click Add to add it to the list of replicated drivers.

**13.** When you click the Printers node in the Citrix Management Console, which types of printers show up in the Printer list? (Choose all that apply.)

**A.** A laser printer that resides on a user's local workstation that has been automatically created

**B.** An HP DeskJet printer connected to a user's local workstation via the Com1 port

**C.** A laser printer connected to the MetaFrame server's LPT1 port and shared on the network

**D.** An inkjet printer connected to a print server that has been imported into the farm

**14.** Which of the following statements is true about automatic replication of printer drivers?

**A.** MetaFrame XP maintains one Auto-replication list that contains replication information about each print server, driver, and printer in the MetaFrame XP farm.

**B.** MetaFrame XP maintains one Auto-replication list that contains replication information about each print server and the platform for each driver and printer that are on each print server.

**C.** MetaFrame XP maintains one Auto-replication list for each platform in the server farm.

**D.** MetaFrame XP maintains one Auto-replication list for each print server in the farm.

**15.** Which of the following statements is true about driver replication?

**A.** Drivers from network printers cannot be replicated because MetaFrame XP does not have the driver installed locally on the server.

**B.** Drivers from local computers cannot be replicated.

**C.** Drivers from network printers cannot be replicated because MetaFrame XP does not have guaranteed access to the driver files.

**D.** Drivers from client-mapped printers cannot be replicated because they may be non-standard drivers.

**16.** When will you need to map print drivers in MetaFrame XP?

**A.** When the print drivers have different names for different Windows platforms

**B.** When the printers are not supported on the client's operating system

**C.** When the driver is a universal print driver

**D.** When connecting to a MetaFrame XP server from an ICA Client prior to version 6

**17.** What is the name of the file where the printer mappings are stored?

**A.** `xpprint.inf`

**B.** `ctxprnt.ini`

**C.** `wtsprnt.inf`

**D.** `ctxprint.inf`

**18.** You have just installed a new printer on your network and added the driver to the MetaFrame XP server. You suspect that this new printer is causing your server to crash. What MetaFrame XP feature allows you to prohibit the use of this driver?

**A.** Printer Driver Compatibility

**B.** Driver Mapping Compatibility

**C.** Printer Mapping Compatibility

**D.** Driver Compatibility Manager

**19.** How will an auto-created client printer on a Windows CE device appear in the Printers folder?

**A.** *clientname#\printername*

**B.** *clientname#/printername*

**C.** *#clientname\printername*

**D.** *clientname*#LPT*x*

20. You want an auto-created printer to remain on the server after the user logs off the network. By default, if there are no jobs in the print queue, the printer is deleted upon logoff. How can you change this so that the printer remains on the server?

   A. From the server, open the Printers folder, right-click the client printer, and select Properties. In the Properties sheet, modify or delete the text Auto Created Client Printer from the Comment field.

   B. From the workstation, open the Printers folder, right-click the client printer, and select Properties. In the Properties sheet, modify or delete the text Auto Created Client Printer from the Comment field.

   C. From the server, open the Printers folder, right-click the client printer, and select Properties. In the Properties sheet, click the Connection tab and remove the check from the box labeled Delete From Server Upon Logoff.

   D. From the server, open the Printers folder, right-click the client printer, and select Properties. In the Properties sheet, click the General tab and remove the check from the box labeled Delete From Server Upon Logoff.

# Answers to Review Questions

1. A, B, C, D. ICA Clients can print to the following types of printers: printers that are connected to ports on the user's client devices on Windows, Windows CE, DOS, and Mac OS platforms; virtual printers created for tasks such as printing from a PostScript driver to a file on a Windows client device; shared printers that are connected to print servers on a Windows network; and printers that are connected directly to MetaFrame XP servers.

2. C. There are three types of connections in a MetaFrame XP server farm: client connections, network connections, and local connections.

3. D. A PC or PostScript printer connected to a serial port on a Mac OS would be considered a client printer.

4. D. Win32 clients have client printers that are set up in Windows. They appear in the Printers folder on the client computer. Locally connected printers, printers that are connected on a network, and virtual printers are all client printers.

5. A. Network printers are printers that are connected to a print server and shared on a Windows network. On a Windows network, users can set up a network printer on their computers if they have permission to connect to the print server. MetaFrame servers that have shared printers and are not part of the same farm are also considered as network printers.

6. B. Printers that are connected directly to MetaFrame XP servers are local printers within a particular server farm. This includes printers that are connected to MetaFrame XP servers that host a user's ICA session, as well as printers that are connected to other MetaFrame XP servers in the same server farm.

7. A. If users have printers set up locally on their computer, whether they are local printers or network printers, you can install the print driver on the MetaFrame XP server and use the replication feature in CMC to distribute the drivers to all the servers in the farm.

8. A. Installed client printers appear in Windows in the following form: *clientname#\printername*, where *clientname* is the name of the client device and *printername* is the name for the installed client printer.

9. A. If you add or remove printers from a network print server, you must update the print server information to be sure that the console displays the available printers on the Printers tab. You can update server information by selecting a print server and choosing the Update Network Print Server command from the context menu, the toolbar, or the Actions menu. Updates of print server information are not automatic, so you must take this action manually.

10. D. To remove print servers, select the print server to remove and choose Discard Network Print Server from the context menu, the console toolbar, or the Actions menu. After you do this, the print server will no longer appear on the Network Print Server tab, and its printers will not appear on the Printers tab.

11. C. You can use the Bandwidth tab to configure or remove print stream bandwidth limits on MetaFrame XP servers and copy those settings from one server to other servers in the farm. When you select a server in the list on the Bandwidth tab, you can use the Edit command to change its bandwidth settings or use the Copy command to copy its bandwidth settings to other servers in the farm. You can use these commands from the context menu, the console toolbar, or the Actions menu.

12. A, B. To copy a print driver, select the driver from the Drivers tab in the Printer Management node. Or you can use the Replicate Drivers command from the console toolbar, the context menu, or the Actions menu.

13. C, D. When you select Printers in the CMC tree, the Printers tab in the right pane lists all of the printers that you can configure in the farm. The list contains the following printers: local shared printers that are connected directly to MetaFrame XP servers in the farm and network printers that are installed and connected to network print servers when you import the print servers into the farm.

14. C. MetaFrame XP maintains one Auto-replication list for each platform in the server farm. When you select a print driver for replication, MetaFrame XP adds the driver to the Auto-replication list.

15. C. MetaFrame XP cannot replicate drivers from network printers because MetaFrame XP does not have guaranteed access to the driver files. If driver replication fails because of communication errors, the console displays an error message and records the error in the event log for each server where the operation failed.

16. A. When print drivers have different names for different Windows platforms, you must map the print drivers to identify them.

17. C. Printer mappings are listed in the `wtsprnt.inf` file.

18. A. If you find that a driver that you have configured to auto-replicate throughout your farm is a bad driver, you can use the Driver Compatibility feature in the CMC to designate drivers that you want to allow or prohibit for use with client printers.

19. D. Auto-created client printers appear in the form *clientname*#LPT*x*. The machine name of the client computer replaces the *clientname* and the printer port number replaces the *x*.

20. A. Open the Printers folder within the ICA session. Right-click the client printer and select Properties. The Properties sheet displays a Comment field that contains the text Auto Created Client Printer for automatically created client printers. If you modify or delete this description, MetaFrame XP will not delete the printer when a user logs off from the server. Subsequent logons by the same user employ the printer already defined and do not modify it.

# Chapter 14

# Monitoring and Troubleshooting

## THE FOLLOWING CITRIX EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **12. Monitoring and Troubleshooting MetaFrame XP Servers**

- 12a. Using Event Viewer and System Information
- 12b. Managing Resource and Citrix Network Manager and Troubleshooting Network Monitor

Up until this point, we have concerned ourselves with the configuration and control of our MetaFrame XP servers and the client connections. In this, the final chapter, we are going to discuss the tools used to monitor our servers and clients as well as the tools used to troubleshoot problems that may crop up. Many of these tools are included with Windows 2000, while others are included with certain versions of MetaFrame XP. We will start by looking at the tools native to the operating system and then move on to working with the MetaFrame XP tools.

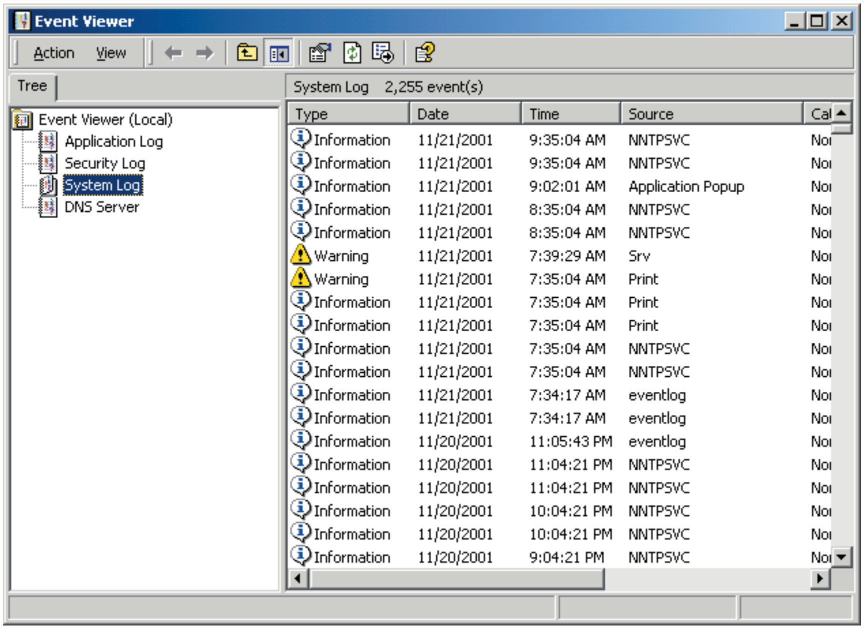
# Windows 2000 Tools

Included in Windows 2000 are tools that you can use to monitor and troubleshoot your network. Even though these tools were not created with MetaFrame XP in mind, MetaFrame XP can take advantage of them. You are probably familiar with most of these tools if you have worked within a Microsoft networked environment. The tools we will discuss in this section of the chapter are *Event Viewer*, *System Monitor*, *System Information*, and *Task Manager*.

## Event Viewer

The first, and possibly most useful, tool is Event Viewer, shown in Figure 14.1. It is a starting point for most troubleshooting processes. It is also a good tool for monitoring warnings and errors. Event Viewer reports errors that the system or applications encounter and provides warnings that can aid in the prevention of future problems. You should make a point of checking Event Viewer at least once a day. We check our logs first thing in the morning. As a matter of fact, along with checking our e-mail, it has become a morning ritual. By checking Event Viewer regularly, you may be able to spot and correct problems before your users can attack you when something goes wrong.

**FIGURE 14.1** Event Viewer tool



System Log 2,255 event(s)

| Type | Date | Time | Source | Cal |
|---|---|---|---|---|
| Information | 11/21/2001 | 9:35:04 AM | NNTPSVC | Noi |
| Information | 11/21/2001 | 9:35:04 AM | NNTPSVC | Noi |
| Information | 11/21/2001 | 9:02:01 AM | Application Popup | Noi |
| Information | 11/21/2001 | 8:35:04 AM | NNTPSVC | Noi |
| Information | 11/21/2001 | 8:35:04 AM | NNTPSVC | Noi |
| Warning | 11/21/2001 | 7:39:29 AM | Srv | Noi |
| Warning | 11/21/2001 | 7:35:04 AM | Print | Noi |
| Information | 11/21/2001 | 7:35:04 AM | Print | Noi |
| Information | 11/21/2001 | 7:35:04 AM | Print | Noi |
| Information | 11/21/2001 | 7:35:04 AM | NNTPSVC | Noi |
| Information | 11/21/2001 | 7:35:04 AM | NNTPSVC | Noi |
| Information | 11/21/2001 | 7:34:17 AM | eventlog | Noi |
| Information | 11/21/2001 | 7:34:17 AM | eventlog | Noi |
| Information | 11/20/2001 | 11:05:43 PM | eventlog | Noi |
| Information | 11/20/2001 | 11:04:21 PM | NNTPSVC | Noi |
| Information | 11/20/2001 | 11:04:21 PM | NNTPSVC | Noi |
| Information | 11/20/2001 | 10:04:21 PM | NNTPSVC | Noi |
| Information | 11/20/2001 | 10:04:21 PM | NNTPSVC | Noi |
| Information | 11/20/2001 | 9:04:21 PM | NNTPSVC | Noi |

MetaFrame sends information messages, warnings, and error messages to the Windows 2000 Event Viewer. Depending upon the message type, the messages are written to one of the three logs that make up the Event Viewer database: the *Application log*, the *Security log*, and the *System log*. Each of these logs tracks information that the administrator can use to view the processes and problems on the system.

**Application log** Events from programs or applications are logged in the Application log. Most applications that are written to meet the Microsoft certification requirements record errors in the Application log of Event Viewer.

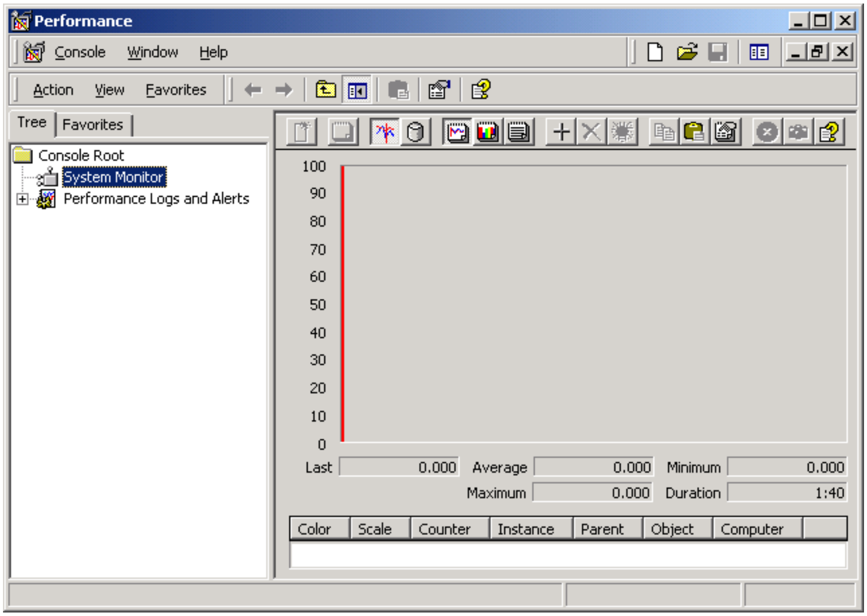
**Security log** Events defined in the *auditing policy* are recorded here. When auditing is enabled in Group Policy in Windows 2000, events such as valid and invalid logon attempts are recorded. For example, if you have defined your Group Policy to record events for failed logons, all unsuccessful logon attempts will be recorded in the event log under the Security log.

**System log** The System log contains events that are logged by system components. System components that fail during startup will record events in this log.

## System Monitor

Another useful tool in monitoring and troubleshooting problems is Microsoft's System Monitor. System Monitor is a utility that tracks processes on a Windows 2000 system. Used as a real-time monitoring system, it displays results in a graphical format. Figure 14.2 shows System Monitor when it is first opened. You can access this tool by navigating to Start ➢ Programs ➢ Administrative Tools ➢ Performance.

**FIGURE 14.2** System Monitor tool



Last 0.000 Average 0.000 Minimum 0.000
Maximum 0.000 Duration 1:40

### The System Monitor Control Dilemma

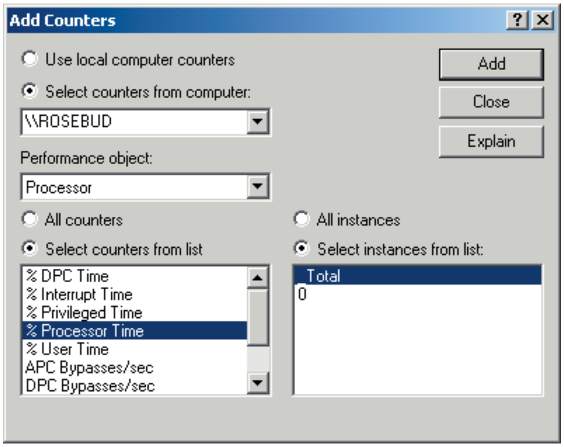
Most administrators build their own Microsoft Management Console (MMC) with all the tools they need to use in their environment. Since an MMC presents a unified view of the tools the administrator requires, using it is easier than navigating the Start menu every time you need a different utility. Adding System Monitor to the MMC is not as straightforward as adding most of the other snap-ins. If you look at the list of available snap-ins, you will notice that System Monitor is not included.

Once you know the following trick, adding System Monitor will be as easy as adding any other snap-in. System Monitor is actually an ActiveX control. Follow these steps to add it in to your console:

1. Open your existing console or choose Start ➢ Run and type in **MMC**.
2. Within the MMC, navigate to Console ➢ Add/Remove Snap-in.
3. In the Add/Remove Snap-in dialog box, click the Add button.
4. In the Add/Remove Snap-in selection screen, select ActiveX Control and click Add.
5. On the Insert ActiveX Control splash screen, click Next.
6. Scroll down the list, select the System Monitor Control option, and click Next.
7. Rename the control if you want, and then click Finish.
8. Click Close to close the Add/Remove Snap-in selection screen.
9. Click OK to close the Add/Remove Snap-in dialog box.
10. Verify that the System Monitor control has been added to your MMC.

When you use System Monitor, the interface tracks instances of processes running on the system. System Monitor can break down each process to a much more detailed level. The following items are available for each process: *object*, *counter*, and *instance*. During the installation of MetaFrame XP, counters are added to the system that are specific to a MetaFrame environment. Figure 14.3 shows the Add Counters screen. To reach this screen, right-click within the MMC and choose Add Counters from the context menu. In the pull-down list of performance objects available, you will see some new objects, for example, ICA Sessions.

FIGURE 14.3 Adding counters



Add Counters

○ Use local computer counters
● Select counters from computer:
\\ROSEBUD

Performance object:
Processor

○ All counters
● Select counters from list
% DPC Time
% Interrupt Time
% Privileged Time
% Processor Time
% User Time
APC Bypasses/sec
DPC Bypasses/sec

○ All instances
● Select instances from list:
_Total
0

**Object** The Performance Object section of this screen displays data that you can evaluate. The data is generated by a collection of counters known as an *object*. Each time the object performs a function, the counters associated with that function are updated. Some examples of objects are Browser, Cache, Memory, Paging File, Physical Disk, Processor, and Server objects.

**Counter** A *counter* is a component within an object. The component represents information about a certain aspect of the system or service.

**Instance** An *instance* is a single occurrence of an object, and an object may have multiple occurrences. If you want to view processor performance on a dual-processor server, you can specify instances for each processor. You can view either one processor or both processors and track the statistics for each.

There are many counters that you can use to monitor your MetaFrame server. The counters to watch in regard to monitoring and troubleshooting track statistics for memory, cache, and network performance. Here are the most important counters that you can monitor with System Monitor, listed according to type.

The memory counters include the following:

**Pages/Sec** This counter tracks the number of pages written to or read from disk when resolving hard page faults. When a process needs code or data that is located on disk rather than in physical memory, a hard page fault occurs. If this counter records a value higher than 20, your system may require a larger page file. This counter is used for troubleshooting page file problems more than for memory problems.

**Committed Bytes** This is an instantaneous counter that can be used over a period of time, along with the Memory\Available Bytes counter, to determine whether your system has a memory leak. This counter displays the number of committed bytes of virtual memory that the system is using.

**Pool Nonpaged Bytes** You can use this counter to determine whether you need additional memory installed on your system. It indicates the number of bytes that are allocated to the nonpaged pool. The nonpaged pool is a group of bytes that cannot be written to disk and must remain in physical memory. You should monitor the nonpooled page bytes and watch for increases in the number. As applications start, this number will increase, but when they end, the number should decrease. Any increase in this counter outside of application startup, or a continual increase, may indicate a memory leak.

**Pool Nonpaged Allocs** This counter helps determine whether your system has a memory leak. It reports the number of requests to allocate space in the nonpaged pool.

**Available Bytes** When a program needs additional memory, Windows 2000 uses free bytes to meet the request. When the amount of free bytes becomes low, the system takes memory from the working sets of other programs. You may need to add memory to your system if you notice a steady increase in the value for one program and a steady decrease in the value for other programs.

**Cache Bytes** You can use this counter to determine whether you need to add memory to your system. The counter monitors the number of bytes used by the system cache. The value for this counter should not rise above 4MB.

Following is the most important server counter:

**Bytes Total/Sec** This counter represents the number of bytes the system has either sent or received over the network. As your server becomes busier, you may see a dramatic increase in this number.

These counters are helpful in monitoring the physical disk:

**%Disk Time and Physical Disk\Avg. Disk Queue Length** When used with the Memory\Page Read/Sec counter, these counters can help you determine whether you have a memory shortage. An increase in queue length should be accompanied by a corresponding decrease in Memory\Page Read/Sec. If an increase in queue length does not reduce the Memory\Page Read/Sec counter, then a memory shortage does exist.

These two counters are important in monitoring the page file:

**%Usage** Every process on the server uses the page file. The system uses the page file to compensate when more memory is needed than is in RAM. This value helps you determine whether you need to make your page file larger. This counter should report no more than 99%. If the number increases to 100%, you will need to adjust your page file accordingly.

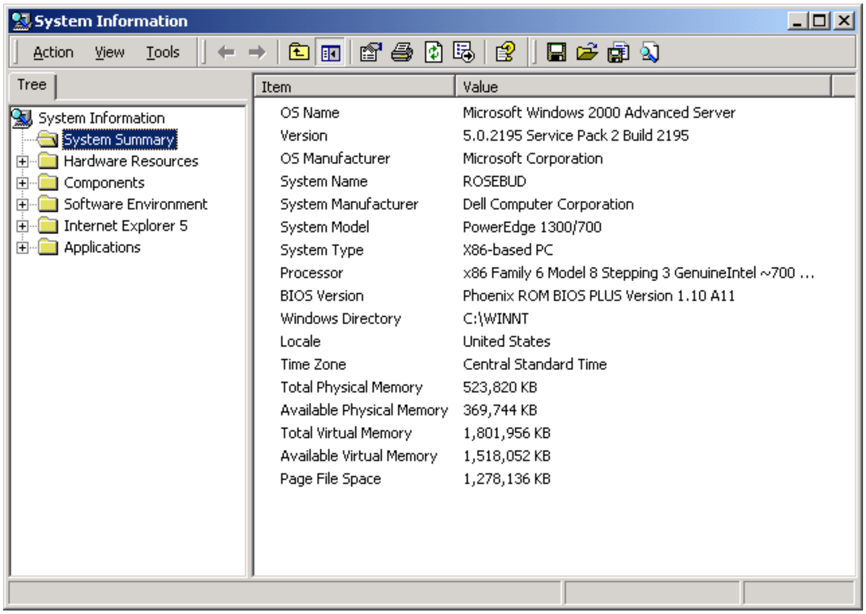
**%Usage Peak** You can also view the activity of the page file with this setting. If the counter for this object nears the maximum page file setting, you may want to increase your page file.

## System Information

System Information was known in previous versions of Microsoft operating systems as *Microsoft Diagnostics (MSD)*. The name came under fire from many administrators because the utility did not contain any diagnostic programs; it only supplied information detailing how the computer was configured. Now that it has the appropriate name for the function it performs, administrators are not so quick to admonish it. Figure 14.4 shows the System

Information main screen, which you reach by navigating through Start ➤ Programs ➤ Accessories ➤ System Tools ➤ System Information.

**FIGURE 14.4** System Information screen



| Item | Value |
|---|---|
| OS Name | Microsoft Windows 2000 Advanced Server |
| Version | 5.0.2195 Service Pack 2 Build 2195 |
| OS Manufacturer | Microsoft Corporation |
| System Name | ROSEBUD |
| System Manufacturer | Dell Computer Corporation |
| System Model | PowerEdge 1300/700 |
| System Type | X86-based PC |
| Processor | x86 Family 6 Model 8 Stepping 3 GenuineIntel ~700 ... |
| BIOS Version | Phoenix ROM BIOS PLUS Version 1.10 A11 |
| Windows Directory | C:\WINNT |
| Locale | United States |
| Time Zone | Central Standard Time |
| Total Physical Memory | 523,820 KB |
| Available Physical Memory | 369,744 KB |
| Total Virtual Memory | 1,801,956 KB |
| Available Virtual Memory | 1,518,052 KB |
| Page File Space | 1,278,136 KB |

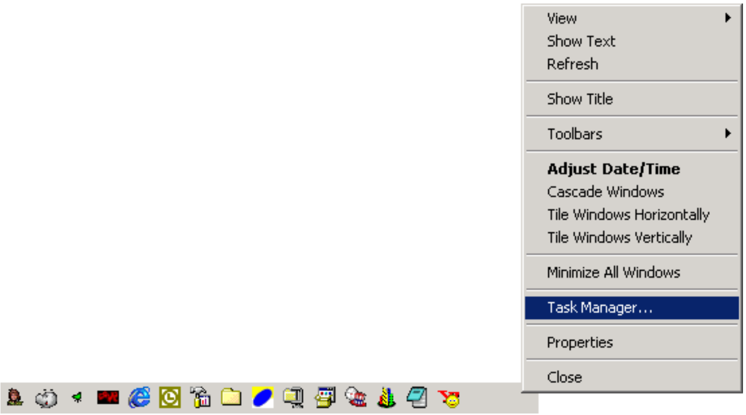
If you right-click the System Information root and choose Properties, you can select any computer within your environment, which allows you not only to view other systems in your organization but also to print out reports based on their configuration. This can be a very handy tool since you can print out the starting configuration of a system and then file it away. If one of your systems starts acting strangely, you can pull the record and check it against the current settings.

Another useful option is the ability to save the information as a file, in either text or System Information file format. Some administrators find the information presented from this tool a bit too unwieldy to print out, so they save the information on the network. They then have access to the configuration history of the system when they need it.

## Task Manager

Another tool you can use to both monitor and troubleshoot MetaFrame problems is Task Manager. System processes and CPU utilization can be monitored using this tool. Task Manager displays this information in three tabs: Applications, Processes, and Performance. To open Task Manager, you can either right-click the Start bar and select the Task Manager menu item, as shown in Figure 14.5, or you can press Ctrl+Alt+Delete while logged on to the computer. Doing so brings up the *Security dialog box*, which contains the Task Manager button.

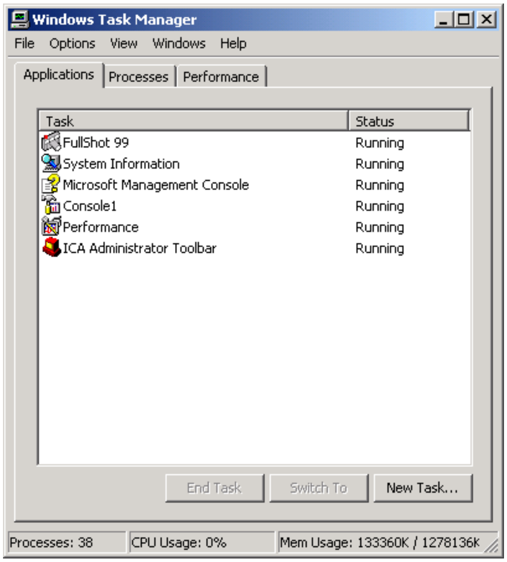
**FIGURE 14.5** Opening Task Manager from the Start bar



### Applications Tab

The *Applications tab*, shown in Figure 14.6, displays the names of the applications currently running on the server and the status of each application. The name of the application appears in the column labeled Task. The status of the application appears in the Status column. If you notice that CPU utilization is high on your system, you can check the Applications tab to see if any applications have a status of Not Responding. When an application is not responding, it can take up to 100 percent of the processor (or processors). If an application is not responding, you can end that application by highlighting it and clicking the End Task button.

FIGURE 14.6 Task Manager's Applications tab



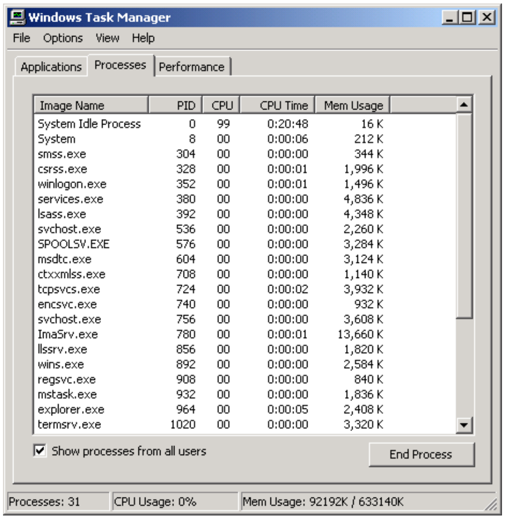
| Task | Status |
|---|---|
| FullShot 99 | Running |
| System Information | Running |
| Microsoft Management Console | Running |
| Console1 | Running |
| Performance | Running |
| ICA Administrator Toolbar | Running |

Processes: 38 | CPU Usage: 0% | Mem Usage: 133360K / 1278136K

## Processes Tab

The *Processes tab*, shown in Figure 14.7, displays detailed information about the individual processes running on the system. The Processes tab includes the following columns by default.

FIGURE 14.7 Task Manager's Processes tab



| Image Name | PID | CPU | CPU Time | Mem Usage |
|---|---|---|---|---|
| System Idle Process | 0 | 99 | 0:20:48 | 16 K |
| System | 8 | 00 | 0:00:06 | 212 K |
| smss.exe | 304 | 00 | 0:00:00 | 344 K |
| csrss.exe | 328 | 00 | 0:00:01 | 1,996 K |
| winlogon.exe | 352 | 00 | 0:00:01 | 1,496 K |
| services.exe | 380 | 00 | 0:00:00 | 4,836 K |
| lsass.exe | 392 | 00 | 0:00:00 | 4,348 K |
| svchost.exe | 536 | 00 | 0:00:00 | 2,260 K |
| SPOOLSV.EXE | 576 | 00 | 0:00:00 | 3,284 K |
| msdtc.exe | 604 | 00 | 0:00:00 | 3,124 K |
| ctxxmlss.exe | 708 | 00 | 0:00:00 | 1,140 K |
| tcpsvcs.exe | 724 | 00 | 0:00:02 | 3,932 K |
| encsvc.exe | 740 | 00 | 0:00:00 | 932 K |
| svchost.exe | 756 | 00 | 0:00:00 | 3,608 K |
| ImaSrv.exe | 780 | 00 | 0:00:01 | 13,660 K |
| llssrv.exe | 856 | 00 | 0:00:00 | 1,820 K |
| wins.exe | 892 | 00 | 0:00:00 | 2,584 K |
| regsvc.exe | 908 | 00 | 0:00:00 | 840 K |
| mstask.exe | 932 | 00 | 0:00:00 | 1,836 K |
| explorer.exe | 964 | 00 | 0:00:05 | 2,408 K |
| termsrv.exe | 1020 | 00 | 0:00:00 | 3,320 K |

☑ Show processes from all users

Processes: 31 | CPU Usage: 0% | Mem Usage: 92192K / 633140K

**Image Name** This column shows the name of the application executable or the system process that is running on the system.

**PID** The PID (Process Identification) column displays the Process Identification number that the system gives to the application executable or system process.

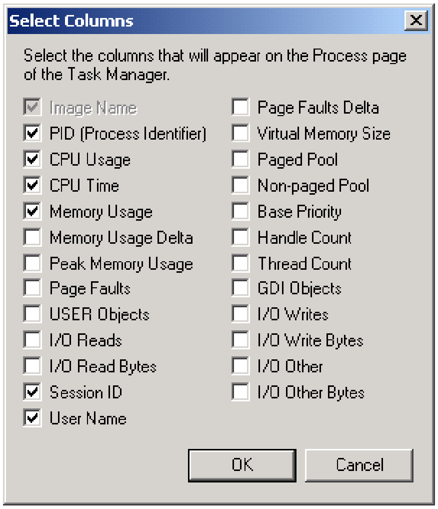
**CPU** This column displays the percentage of processor time that is being taken up by the application or system process.

**CPU Time** This column displays the total accumulated processor time that the application or system process has used.

**Mem Usage** This column shows the amount of physical memory that the application is taking from RAM.

For advanced troubleshooting and monitoring, you can add other columns to the list displayed in the Processes tab. Navigate to View ➢ Select Columns to add additional columns to the Processes tab's display. Figure 14.8 shows the list of columns available. This functionality is especially useful in a terminal services environment since you can add the User Name column, which shows the processes that users running sessions on the server are utilizing. This allows you to pinpoint which user is causing problems on the system.

**FIGURE 14.8** Additional columns available



Select Columns

Select the columns that will appear on the Process page of the Task Manager.

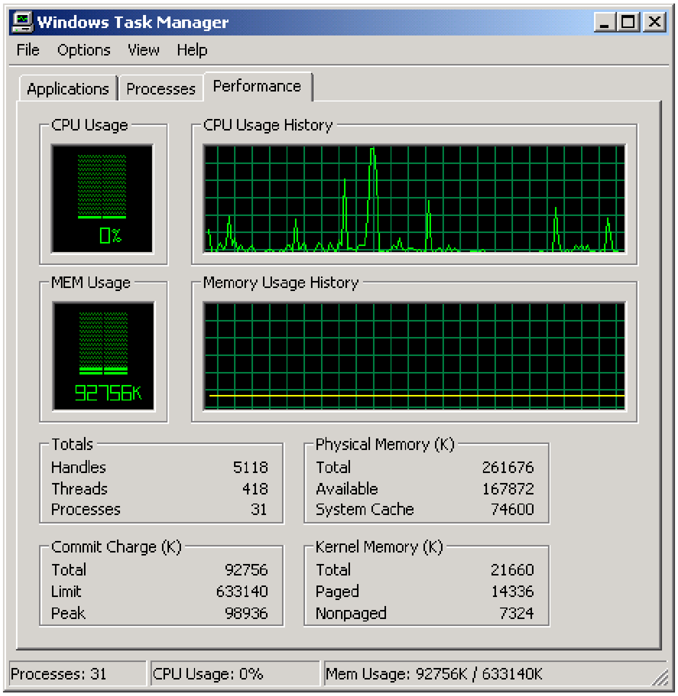
☑ Image Name
☑ PID (Process Identifier)
☑ CPU Usage
☑ CPU Time
☑ Memory Usage
□ Memory Usage Delta
□ Peak Memory Usage
□ Page Faults
□ USER Objects
□ I/O Reads
□ I/O Read Bytes
☑ Session ID
☑ User Name

□ Page Faults Delta
□ Virtual Memory Size
□ Paged Pool
□ Non-paged Pool
□ Base Priority
□ Handle Count
□ Thread Count
□ GDI Objects
□ I/O Writes
□ I/O Write Bytes
□ I/O Other
□ I/O Other Bytes

## Performance Tab

The *Performance tab*, shown in Figure 14.9, displays information about CPU and memory usage. CPU usage appears in real time within the CPU Usage window, and a running history is graphed in the CPU Usage History window. Likewise, memory usage is displayed in real time and in graphical format directly beneath the CPU windows. The lower section of this screen contains statistics for the processor and memory. For more information on these counters, see the Windows 2000 Resource Kit. You can monitor the objects listed previously in the "System Monitor" section of this chapter in the Task Manager's Performance tab.

**FIGURE 14.9** Task Manager's Performance tab



CPU Usage: 0%

MEM Usage: 92756K

| Totals | |
|---|---|
| Handles | 5118 |
| Threads | 418 |
| Processes | 31 |

| Physical Memory (K) | |
|---|---|
| Total | 261676 |
| Available | 167872 |
| System Cache | 74600 |

| Commit Charge (K) | |
|---|---|
| Total | 92756 |
| Limit | 633140 |
| Peak | 98936 |

| Kernel Memory (K) | |
|---|---|
| Total | 21660 |
| Paged | 14336 |
| Nonpaged | 7324 |

Processes: 31 CPU Usage: 0% Mem Usage: 92756K / 633140K

If system performance and response time are slow, check the Processes tab, shown previously in Figure 14.7, to see if an application or system process is taking up CPU time. You can click the CPU column name to arrange the processes in order by CPU utilization. If a process is taking up too much of the CPU, you can highlight the process and click the End Process button to kill that individual process.

# Citrix Tools

Citrix also provides tools for monitoring and troubleshooting network and application problems. Aside from the network and application problems typically encountered after a system is installed, you may experience other problems such as connectivity issues. Citrix includes the *Network Manager* and *Resource Manager* utilities with MetaFrame. They are both included when you install a MetaFrame XPe connection license on your network.

NOTE

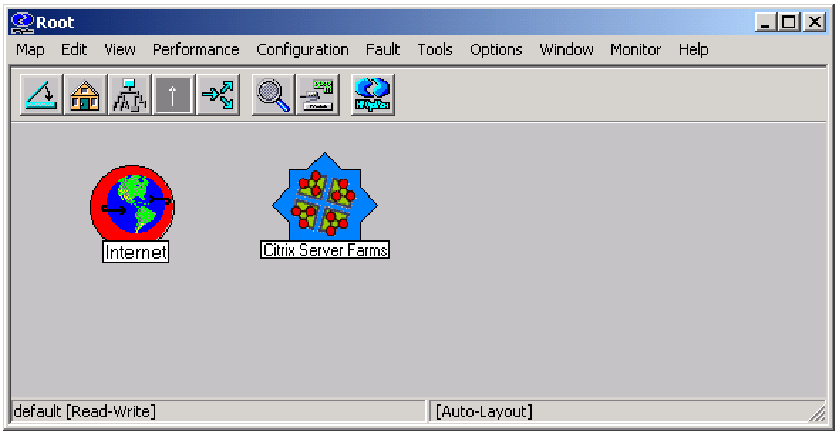
The following is a brief discussion of Network Manager and Resource Manager. While you may be asked a very basic question about these products on the Citrix Certified Administrator exam, the exam itself is not designed to be an assessment of your skill with these products. Individual exams exist for each of these products and are part of the Citrix Certified Enterprise Administrator (CCEA) certification. For more information on the CCEA certification, go to the Citrix Systems website, www.citrix.com.

## Network Manager

Network Manager 1.0 is a component that adds Simple Network Management Protocol (SNMP) functionality to your server farm and allows you to monitor MetaFrame XPe servers from third-party SNMP management consoles, such as HP OpenView and Tivoli NetView. This functionality is achieved through plug-ins for HP OpenView and Tivoli NetView and a Citrix SNMP management agent. The Network Manager plug-in, shown in Figure 14.10, interacts with the SNMP management console to perform the following functions:

- Discover MetaFrame XPe servers and gather information from those servers that have the SNMP service installed.
- Automatically update data in the management console's network map.
- Record MetaFrame XPe SNMP traps to the event log.

**FIGURE 14.10** HP OpenView showing the Citrix farm added to the management console



An administrator monitoring the network with one of the SNMP management applications can use the SNMP console to perform tasks that are normally reserved for the Citrix Management Console. From the SNMP management console, you can terminate processes on MetaFrame XPe servers, disconnect, log off, and send messages to active sessions on MetaFrame XPe servers, and shut down or restart MetaFrame XP servers remotely.

In order to install and configure Network Manager 1.0, the following requirements must be met:

- The Microsoft SNMP service must be installed on the Citrix MetaFrame XPe server.
- The Network Manager plug-in must be installed on the server running the SNMP management console software.

As an optional step, you can install the Citrix Management Console on the server running the SNMP management console software. Use the Citrix Management Console on the MetaFrame XPe server to configure the Citrix SNMP Agent. Finally, determine the startup options and login settings for the SNMP service.

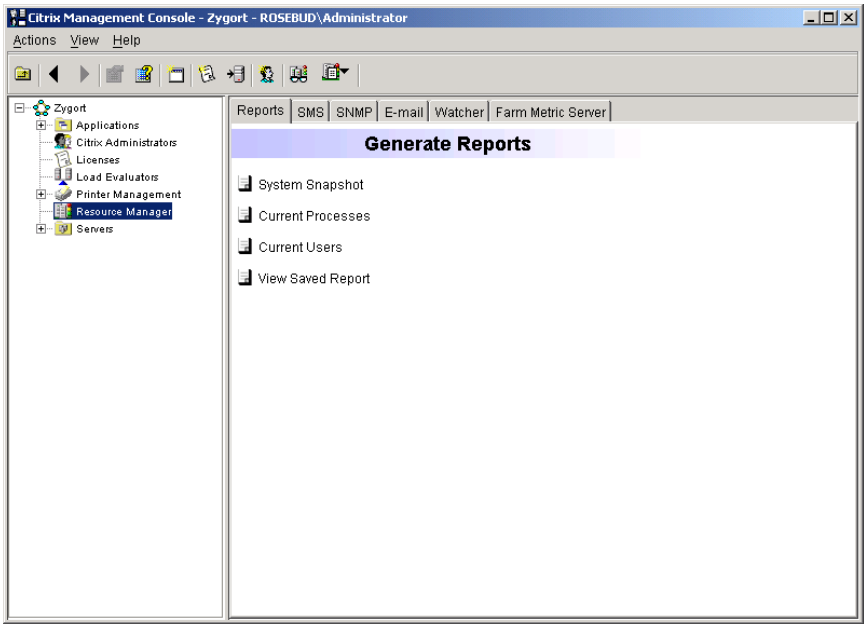
NOTE

Network Manager 1.0 supports both Tivoli NetView 5.1.2 and later and HP OpenView Network Node Manager 6.1 and later.

## Resource Manager

Resource Manager 2.0 manages, tracks, and reports server and application usage. It is an application and system management tool that works in real time and displays information in a local view and a farm view. Using the Citrix Management Console, shown in Figure 14.11, you can monitor performance and application parameters for all MetaFrame XPe servers and applications in the farm. The information received from Resource Manager can be valuable for solving problems and planning for future resource needs. Through the Citrix Management Console, an administrator can define monitoring *metrics*.

**FIGURE 14.11** Citrix Management Console with the Resource Manager plug-in in place



Metrics are units of measurement that are based on performance counters native to the local operating system. Metrics are configurable indicators that can alert an administrator to a problem over media such as e-mail, SMS, or SNMP. You can also define a custom script to run to fix a problem. Data collected by the metrics is available to the administrator in report form and is based on system statistics, processes, users, and changes made to the system. This includes all events within the past 48 hours.

An administrator can also set notification by configuring remote alerts to warn of possible problems with the Citrix servers and the farm. It's also possible to monitor published applications using Resource Manager. You can trace usage and licensing with custom metrics, making it easier for the administrator to track license usage and determine upgrade needs.

Default metrics are assigned to the system during installation. Metrics for applications must be enabled, as they are not available by default. After the metrics are added to the system, you can set thresholds and customize them for all metrics. This gives the administrator a great deal of power in configuring monitoring on their network.

# Troubleshooting

**O**ther problems you encounter may be more difficult to narrow down. Let's face it—no computer system is without faults. If they all ran without any problems, there would not be such a demand for us, the administrators. And, since humans write operating systems and applications, there will always be bugs in the process. In this section, we will look at some of the more frequent problems and how to deal with them.

## Installation Issues

During installation, you may encounter an error when trying to initialize permanent storage. This error is in response to the IMA service failing to create objects in the data store. You can determine that this is the problem by following these steps:

1. Verify ODBC connectivity to the database.
2. Verify that the user account defined for the database has the correct permissions for the database. The user should be able to create tables, stored procedures, and index objects. The Microsoft SQL user equivalent permission is `db_owner`. If you are using Oracle as the data store, the permission must be set to `resource`.
3. Verify that any previous installation of MetaFrame XP is completely removed from the server.
4. If you are using an Oracle database, verify that the system tablespace is not full.

If the installation failed, the data collector may continuously try to contact the failed server. You can compare the list of servers in the Citrix Management Console to the list of servers returned by the *`queryhr`* command. If there are servers listed in the `queryhr` results that do not show up in the Citrix Management Console, use the command `<queryhr -d servername>` to remove the server from the list. Using the `-d` option with the `queryhr` command removes a server from the farm. Do not use this command on a server that is functioning properly.

## Database Connectivity Issues

If the connection to the data store fails, the problem may be with ODBC connectivity. If you suspect ODBC connectivity problems, follow these steps:

1. Verify that the remote database server is online.
2. Check the following Registry key to verify that the correct data store file is being used: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\datasourcename`. The data store name will have an extension of `.dsn`.
3. If you are using Microsoft Access for the data store, use another database connectivity tool to test your connection. Oracle has a utility called Oracle ODBC Test that you can use to test connectivity to a database. Microsoft SQL's utility (ODBC Test) is built into the SQL driver.
4. Verify that the correct username and password for the database are being used. You can change the username and password with the command `<dsmaint config>`.
5. Reinstall the Microsoft Data Access Components (MDAC) 2.5 or install the latest version of MDAC to ensure that the latest ODBC files are installed.
6. If you are using Microsoft Access as the data store, install (or reinstall) the Jet Database Service Pack 3 or later.
7. Enable ODBC tracing.

## Misconfiguration Issues

Some frequently encountered obstacles are a result of misconfiguration. Let's examine them briefly:

**Failure to connect to the application** This error can occur when a user attempts to connect to a load-managed published application. The server may send the user's session request to a server that is not currently using a MetaFrame XPa or XPe product license.

**Program Neighborhood not displaying folders** If you created folders to organize your applications in the Citrix Management Console, these folders will not show up in Program Neighborhood. To create application folders in Program Neighborhood, right-click the application and choose Properties. Choose the Program Neighborhood Settings tab in the Properties sheet and enter a folder name in the Program Neighborhood Folder text box.

## Licensing Issues

If a MetaFrame XP server won't allow you to enter a license count, try the following technique:

1. Open the Citrix Management Console and select the server. Right-click the server and select Set MetaFrame Product Code. Verify that the correct product code is entered and is set for the server.
2. From a command prompt, enter the command **`<clicense refresh>`** on the affected server.
3. Stop and restart the IMA (Independent Management Architecture) service.

NOTE

If you skipped the licensing section of MetaFrame setup, you must set the product code in the Citrix Management Console for each server.

If the IMA service fails to start, follow these steps:

1. IMA might not be able to contact the data store. You can verify this by checking the Registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\runtime\currentlyloadingPlugin`. If this Registry key's value is blank, the IMA might not be able to contact the data

store. If the Registry key has a value, the IMA service made a successful connection to the data store. This value will also be blank if the local host cache is missing or corrupt.

2. Verify that the local host cache file (`imalhc.mdb`) exists and is not corrupt.
3. Check the Registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\DataSourceName`. Verify that the IMA service is using the correct data store (DSN) file.
4. When using direct mode to access the data store, test the connectivity of the ODBC data store file (`mf20.dsn`) with a third-party database.
5. If the IMA service reports that it failed to start, but you notice that it eventually started on its own, ignore the message. Either a high load on the database or network latency can cause the IMA service to start slowly. The Service Control Manager has a timeout of six minutes. If the IMA service takes longer than that to start, but does eventually start, this error is not a problem.
6. Check the spooler service and make sure that it is set to start up as a system account, not a user account.

## Logging Issues

Another way of troubleshooting the IMA service is to enable logging at the server level. You can configure logging to produce output to a text file or to the screen. To enable logging, follow these steps:

1. Open the system Registry by running regedt32.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\Tracer\Logging Options`.
3. Edit the following values to change the logging options:
   - Log to Debugger (REG_DWORD): 0×0 disables debug output, and 0×1 enables debug output.
   - Log to File (REG_DWORD): 0×0 disables file output, and 0×1 enables file output.
   - Log File Name (REG_SZ): Full path and filename of the output file.

An alternate way of enabling logging can be set in the HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\Tracer key. Any subsystem that has information that can be traced will have a subkey in the Tracer key listed above. By default, all subsystems in this key have tracing turned on, but specific types of messages for those subsystems are turned off. The value must be set to 1 for both the default value and the subsystem in order for tracing to be enabled.

## Data Collector Issues

Another problem you may encounter after the MetaFrame server is installed and running is a performance decline with the zone data collector. If you feel that the data collector for your zone is not performing as well as it should, you can follow these guidelines to troubleshoot and possibly fix the problem:

**Check the zone** Check the data collector's zone to find the number of servers it contains. If the number of servers in the zone is greater than 256, you will need to modify the Registry to accommodate the high number of servers in the zone.

**Check the utilization** Check the CPU utilization on the data collector server. If CPU utilization is very high, you may want to take one of these actions:

**Dedicate** Define one server as a data collector only. It should serve no other purpose in the farm other than acting as the dedicated data collector.

**Separate** Divide the zone into smaller zones so that the data collector is now managing a smaller zone.

**Upgrade the CPU** Upgrade the CPU or add another CPU to the server that is the data collector for that zone. The server may need CPU upgrades to handle the load from the farm.

**Upgrade the RAM** Upgrade the RAM in the data collector computer. All session information is stored in RAM on the data collector. Adding more RAM can decrease the amount of page file swapping that takes place. Citrix recommends the following formula when determining how much RAM to install in a data collector computer: `Bytes = (11000+(1000*Con)+(600*Discon)+(350*Apps)) * (Srvrs-1)`, where Con is the average number of connections per server, Discon is the average number of disconnected sessions per server, `Apps` is the number of published applications in the farm, and `Srvrs` is the number of servers in the farm.

**Change roles** Define a more powerful server to be the data collector for the zone.

## Fixing Common Problems

If a server has become unresponsive or is corrupt, you may need to rejoin it to the farm. To rejoin a server to a farm, follow these steps:

1. Uninstall MetaFrame XP on the server in question.
2. Open the Citrix Management Console and remove the server from the farm.
3. Reinstall MetaFrame XP on the server. Add the server to the farm during installation.

If ICA Clients cannot connect to a MetaFrame XP server, but they can communicate on the network, do the following.

- Check the connection type in the ICA Client settings. The client may be configured to use TCP/IP instead of TCP/IP+HTTP.
- If the client is configured to use TCP/IP, you must enter a server address in the address list of the application set's properties.
- If you are running a mixed-mode Citrix farm, ICA Clients may not be able log on to the application set if the domain name contains an extension, such as `domain.ctxs`. If the clients remove the extension from the domain name, they should be able to log on.

Another problem you may run into when operating in mixed mode is published applications disappearing from the Published Application Manager. There are many things you can do to fix this problem:

- Publish applications through the Citrix Management Console on MetaFrame XP servers only; do not use the Published Application Manager in MetaFrame 1.8 to publish applications.
- You can remove a Registry key so that each published application is configured only on MetaFrame 1.8 servers. The Registry key is

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\citrix\managedapplications\[`*`AppName`*`]\[`*`ServerName`*`]`. Replace *`AppName`* with the name of the published application and *`ServerName`* with the name of a MetaFrame XP server. When you find a Registry key with a server name that is an XP server, remove that key. Repeat this step for each application that has a MetaFrame XP server listed as the server name.

Problems with existing published applications can be resolved by doing the following:

1. Open the Published Application Manager. In the Properties sheet for the published application, remove all the MetaFrame XP servers from the list of configured servers and save the changes.
2. Open the Citrix Management Console. In the Properties sheet for the published application, remove all the MetaFrame XP servers from the list of configured servers and save the changes.
3. In the Citrix Management Console, open the properties of the published application and add the server back into the list of configured servers. Save the changes. This will correctly add the list of configured servers to the data store.

If you notice that the information in the Citrix Management Console is different on other servers, the local host cache may be out of sync with the data store. If you run the command `<dsmaint refreshlhc>`, the server in question will reload information from the data store.

## Connectivity Problems

The following topics cover some of the more common connectivity problems you may encounter when working in a MetaFrame XP environment and the steps to troubleshoot and correct the problems.

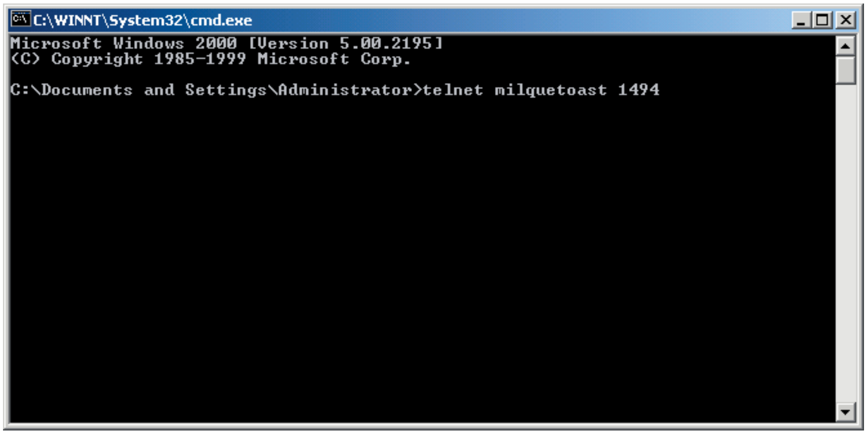
### ICA 32-Bit Connectivity Issues

To determine basic network connectivity problems, follow these steps:

1. Ping the server. If you know that ICMP packets are not filtered and you should be receiving a response, you should receive replies. If you cannot ping the server, you are having a problem at the network level.

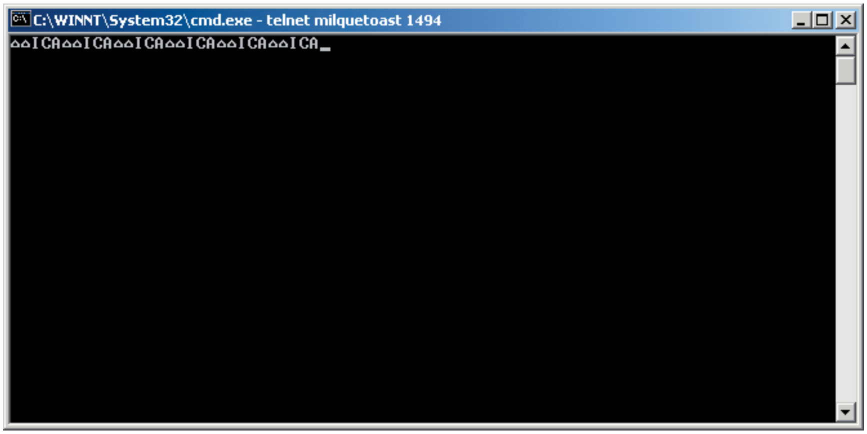
2. Open a telnet session and telnet to the address of the server. Instead of doing a telnet to the standard port, enter **1494** in the port field or at the end of the command line, as seen in Figure 14.12. When the telnet screen comes up, you should receive an ICA sounder, as shown in Figure 14.13.

**FIGURE 14.12** Initiating a telnet session to a MetaFrame XP server



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents and Settings\Administrator>telnet milquetoast 1494
```

**FIGURE 14.13** ICA sounder response



```
⌂⌂ICA⌂⌂ICA⌂⌂ICA⌂⌂ICA⌂⌂ICA⌂⌂ICA_
```

If you do not receive a response using the telnet test, you are having difficulty establishing a socketed connection to the MetaFrame server. Here are some of the reasons that you could be experiencing this problem:

- There are no idle port listeners available on the MetaFrame server, or the server is not accepting connections. You can check this by using the command `<qwinsta /debug>`. If there are no more idle port listeners available, check the Citrix Management Console to see if the listener ports are disabled. You can look in Event Viewer to see why the port listeners are down.
- A router or firewall is blocking ports 1023 and above. When an ICA Client establishes a connection, it needs to be able to establish a socket on TCP port 1494 to the Citrix server, and the Citrix server needs to respond on ports 1023 and above to the client. Check routers and firewalls between the servers to ensure that they are not blocking socketed connections of this type.

### COM Port Redirection

If you are having problems connecting to a device attached to a COM port on the client device, follow these steps to troubleshoot the issue:

1. Test the application from the server console. Test to see if the application works when the COM device is physically attached to the local COM port of the MetaFrame server.
2. If the application and device work properly from the console, make an ICA connection from the client to the server.
3. Within the client desktop session, open a command prompt. Type the command **`<net use>`** and press Enter.
4. If the redirected COM port does not show up, it was not automatically connected. Type **`<net use comx: \\client\comz`**, where ***x*** is the server's COM port number and ***z*** is the COM port number you would like to use on the local computer.

## Technical Support

When you call Citrix Technical Support for help with your problems, you may be asked to collect some information they can use to debug your system.

If you are having problems installing or uninstalling MetaFrame XP, Citrix Technical Support may ask you for installation or uninstallation logs. During installation, an IMA log and a MetaFrame XP log are created by default. Both of these logs are helpful in determining installation or uninstallation problems.

Command-line options can control the creation of these logs. You can control the installation program (setup) and the uninstall program (rmvica) with the following command-line options:

**`/trace`** Enables tracing for the installation (enabled by default and used if no option is selected).

**`/noTrace`** Disables tracing for the installation.

The IMA files (`imains<timestamp>.log` for the installation log and `ima_unins<timestamp>.log` for the uninstall log) are stored by default in the `%systemroot%\` folder. If multiple copies of the installation log exist, you can differentiate them by the timestamp.

The MetaFrame logs are stored in the `%systemroot\system32` folder. The installation log information is stored in `Icatrace.log`, and the uninstallation information is stored in `Rmvicatrace.log`. These log files are overwritten each time MetaFrame XP is installed or uninstalled.

Aside from the log files, Citrix Technical Support may ask you to capture Citrix Management Console debug output. You can launch the Citrix Management Console from the command line with a switch that writes debug information to a log file. You must run this command from the Citrix Management Console installation directory. By default, this directory is `%ProgramFiles%\Citrix\Administration`. The switch is `-debugFile:logfilename`. The log file will be written to the Citrix Management Console installation directory if no path is defined.

If the Citrix Management Console hangs or fails when starting, press Ctrl+Break in the command window to view the stack trace. You can then copy the stack trace information to a text file. Citrix Technical Support will need the stack trace and the `output.log` files to debug the problems.

Citrix Technical Support may request additional ODBC tracing information. Enabling ODBC tracing depends on the database platform in use.

To activate ODBC tracing on Microsoft SQL Server, follow these steps:

1. Run the ODBC Data Source Administrator.
2. Select the Tracing tab.
3. In the Log File Path text box, enter the path where you want to save the log file.
4. Click Start Tracing or Stop Tracing to start or stop the tracing function.

To activate ODBC tracing on an Oracle server, follow these steps:

1. Run the Net8 Assistant.
2. Choose Net8 Configuration ➢ Local ➢ Profile.
3. Select General from the drop-down list box.
4. Make the logging changes you want on the Tracing and Logging tabs.

So there you have it—monitoring and troubleshooting. While there is more to these topics than we have presented here, the information offered in this chapter is ample for what is required on the exam. If you do need more information on any of these topics, please visit the Citrix Systems website.

This is the last chapter of the study guide. We hope that you have found the material useful, and we wish you luck on the exam. We also hope that you will come back to this book from time to time since we have formatted it not only as a study guide but also as a reference. Good luck in your endeavors, and may your systems never crash and your users never complain!

# Summary

In this chapter, we presented the tools used to troubleshoot your MetaFrame XP environment. Windows 2000 has its own built-in tools that you can take advantage of. You can use Event Viewer as the first point of response when you are having problems and as a tool to monitor warnings that might escalate to problems. System Information is useful for gathering configuration information concerning your network. System

Monitor is used to monitor processes in real time on your servers. Task Manager is used to check on applications and processes—and end them if necessary.

We then looked at the Citrix tools available in MetaFrame XPe that can monitor and control your MetaFrame servers. Network Manager works in conjunction with an SNMP management system to monitor and control MetaFrame XPe systems, while Resource Manager can develop real-time reports and monitor data from all of your MetaFrame XPe servers.

Finally, we introduced some of the most common troubleshooting and repair options. From installation issues to data collector problems to connectivity issues and more, we presented the information you will need while working within your MetaFrame environment as well as that needed for the certification exam.

# Exam Essentials

**Know the Windows 2000 tools used to monitor and troubleshoot.** The tools native to Windows 2000 are Event Viewer, System Information, System Monitor, and Task Manager.

**Know what Event Viewer provides.** Event Viewer displays information, warnings, and errors that are generated from the operating system and applications.

**Know what System Information provides.** System Information generates a report detailing the configuration of the server.

**Know what System Monitor provides.** System Monitor provides real-time information about processes running on the server.

**Know what Task Manager provides.** Task Manager provides an interface for the administrator to view the applications and processes running on the system and the ability to end and start them if necessary.

**Know the Citrix utilities used to troubleshoot and monitor.** Citrix provides two utilities with the XPe version of MetaFrame: Network Manager and Resource Manager.

**Know what Citrix Network Manager provides.** Network Manager allows the server farm to be monitored by an SNMP Management Console.

**Know what Citrix Resource Manager provides.** Resource Manager 2.0 manages, tracks, and reports server and application usage.

## Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Application log
Applications tab
auditing policy
counter
Event Viewer
instance
metrics
Microsoft Diagnostics (MSD)
Network Manager
object
Performance tab
Processes tab
`queryhr`
Resource Manager
Security dialog box
Security log
System Information
System log
System Monitor
Task Manager

## Exercises

Working through the following exercises will familiarize you with the tools discussed in this chapter. You will be able to perform these from any MetaFrame XP server.

**EXERCISE 14.1**

### System Information

To view the system information and save the collected information, follow these steps:

1. Open System Information by navigating to Start ➢ Programs ➢ Accessories ➢ System Tools ➢ System Information.
2. Open any of the nodes in the Containers pane to view the information collected about the server.
3. Save the information to a file by choosing Action ➢ Save As System Information File.
4. Enter a name for the file, preferably using the server name, and click the Save button.

**EXERCISE 14.2**

### System Monitor

To add the Memory\Page Read/Sec counter to System Monitor so that you can monitor page file usage, follow these steps:

1. Choose Start ➢ Programs ➢ Administrative Tools ➢ Performance.
2. In the left pane, under Console Root, click System Monitor.
3. In the right pane, click the + icon to add a new counter.
4. In the Add Counters window, select the radio button labeled Use Local Computer Counters.
5. In the Performance Object dialog box, select Memory from the drop-down list.
6. While still in the Add Counters window, select the radio button labeled Select Counters From List.
7. In the window below Select Counters From List, select Pages/Sec.
8. Click Add to add the counter.
9. Click Close to close the Add Counters window.

## EXERCISE 14.3

### Task Manager

To use Task Manager to close a process that is taking up too much processor time, follow these steps:

1. Start the Notepad program by choosing Start ➤ Programs ➤ Accessories ➤ Notepad.
2. While logged on as an administrator, press Ctrl+Alt+Delete.
3. From the Security window, select Task Manager.
4. When the Windows Task Manager window appears, click the Processes tab.
5. Click the column labeled CPU. (Normally you would do this to see what is taking up processor time. Clicking the CPU column sorts the values in that column so you can see what is taking the most processor time. For this lab, though, we will find the Notepad process manually and end it.)
6. Click the column labeled Image Name.
7. Find the `Notepad.exe` process you started and highlight it.
8. Click the button labeled End Process.
9. Close Windows Task Manager.

# Review Questions

1. What is the name of the utility included with Windows 2000 that records log messages from the system and applications?

   A. Event Log Viewer

   B. Event Viewer

   C. Log Viewer

   D. Management Console

2. What are the three logs from which Event Viewer records errors and messages? (Choose all that apply.)

   A. System log

   B. Application log

   C. Service log

   D. Security log

3. If the IMA service on your MetaFrame server fails to start, which log would you check to see the error message?

   A. Security log

   B. System log

   C. Application log

   D. Service log

4. Which of the following items can you monitor when using the Windows 2000 System Monitor? (Choose all that apply.)

   A. Object

   B. Instance

   C. Counter

   D. Item

**5.** You are running Task Manager to view CPU utilization and notice that one of the nine instances of `winword.exe` is taking up 90–100 percent of the processor. How can you find out which user is running the process that is taking up most of the processor time?

**A.** In the Task Manager window, click View in the menu bar and choose Select Columns. Place a check in the check box labeled User Name.

**B.** In the System Monitor window, add a counter and select each username from the list of available users. Then monitor each counter in one window.

**C.** In the Task Manager window, place a check in the check box labeled Show Processes From All Users.

**D.** In the Task Manager window, select Options from the menu bar. Select Show Username.

**6.** Which license level must you have in your MetaFrame farm to run Network Manager and Resource Manager?

**A.** XPs

**B.** XPa

**C.** XPe

**D.** XP

**7.** Plug-ins for which SNMP management programs are included with Network Manager? (Choose all that apply.)

**A.** Tivoli NetView

**B.** HP NetView

**C.** HP OpenView

**D.** Compaq Insight Manager

8. Which of the following functions do the plug-ins for the SNMP management console perform? (Choose all that apply.)

   **A.** Record MetaFrame XPe SNMP traps to the Network Manager log viewer

   **B.** Automatically update data in the management console's network map

   **C.** Record MetaFrame XPe SNMP traps to the event log

   **D.** Discover MetaFrame XPe servers and gather information from those servers that have the SNMP service installed

9. Which of the following can you do from the SNMP management application? (Choose all that apply.)

   **A.** Terminate processes on MetaFrame XPe servers

   **B.** Shut down or restart MetaFrame XPe servers

   **C.** Take remote control of a user's ICA session

   **D.** Install software remotely

10. ____________________ are units of measure based on performance counters that are native to the local operating system and are configurable indicators that can alert an administrator to a problem over media such as e-mail, SMS, or SNMP.

    **A.** Counters

    **B.** Items

    **C.** Instances

    **D.** Metrics

11. What is the name of the utility that can manage, track, and report server and application usage on your MetaFrame XPe farm?

    **A.** Resource Management Services

    **B.** Resource Manager

    **C.** Server Manager

    **D.** Network Manager

**12.** You have a MetaFrame server in your farm that appears in the list of servers when you type **`queryhr`** from a command prompt but does not show up in the Citrix Management Console. What command would you type to remove this server from the list of servers that show up with the `queryhr` command?

**A.** `queryhr /r servername`

**B.** `queryhr servername /delete`

**C.** `queryhr -d servername`

**D.** `queryhr -r servername`

**13.** What command can you use to change the username and password for the data store database?

**A.** `dsmaint dstore`

**B.** `dsmaint config`

**C.** `dsmaint change dstore`

**D.** `dsmaint config dstore`

**14.** When installing MetaFrame XP on your server, you skipped adding licenses. Now that the server is installed, you find that nobody can connect to the new server, even after adding licenses. What must you do to resolve this problem?

**A.** Activate the licenses.

**B.** Add valid licenses.

**C.** Set the MetaFrame product code in the Citrix Management Console.

**D.** Stop and restart the IMA service.

**15.** When testing a connection to a MetaFrame server, which port should you telnet to in order to receive the ICA sounder response?

**A.** 21

**B.** 443

**C.** 1494

**D.** 1604

**16.** If you are having problems uninstalling MetaFrame XP, and Citrix Technical Support wants you to send them the uninstall log file, what command would you run to create this log?

**A.** `rmvica`

**B.** `rmvica /trace`

**C.** `rmvica /filename.log`

**D.** `rmvica /filename.txt`

**17.** You notice that the information displayed in the Citrix Management Console varies depending on which server you are running the Citrix Management Console. You determine that the local host cache is out of sync with the data store. What command would you run to reload the information in the local host cache from the data store?

**A.** `dsmaint refreshlhc`

**B.** `dsmaint /refreshlhc`

**C.** `dsmaint load lhc`

**D.** `dsmaint -r lhc`

**18.** When you make a connection to a MetaFrame server, you establish a socket on TCP port 1494 to the Citrix server. With which ports does the Citrix server respond to the client?

**A.** 1494 and 1604

**B.** 1023 and above

**C.** 443 and 1677

**D.** 4323 and above

**19.** You receive an error message stating that the IMA service failed to start. You check the following Registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\Runtime\CurrentlyLoadingPlugin`. You find that the key does not contain a value. What could this mean? (Choose all that apply.)

A. The IMA service could not contact the data store.

B. The IMA service is configured to start with a local user account instead of a system account.

C. The local host cache is missing or corrupt.

D. The local host cache is not in sync with the data store.

20. What does MetaFrame XP name the data store file?

A. `lhcdb.mdb`

B. `mfxp.dsn`

C. `mf20.dsn`

D. `mfxp.mdb`

# Answers to Review Questions

1. B. Event Viewer reports errors that the system or applications encounter and also reports warnings that can aid in preventing future problems.

2. A, B, D. The messages are written to one of the three logs that make up the Event Viewer database: the Application log, the Security log, and the System log.

3. B. System components that fail during startup record events in the System log.

4. A, B, C. System Monitor is a utility that is used to track certain processes on a Windows 2000 system. System Monitor is a real-time monitoring system that displays its results graphically and consists of three items: object, counter, and instance.

5. A. When viewing CPU utilization with Task Manager, you can see which processes are taking up processor time. If you add the column labeled User Name from the Select Columns window, you can see which user is running the process that is taking up the bulk of the processor time.

6. C. The utilities that Citrix includes with MetaFrame are Network Manager and Resource Manager. They are both included when you install a MetaFrame XPe connection license on your network.

7. A, C. Plug-ins for HP OpenView, Tivoli NetView, and a Citrix SNMP management agent make up Network Manager.

8. B, C, D. The plug-ins interact with the SNMP management console to perform the following functions: discover MetaFrame XPe servers and gather information from those servers that have the SNMP service installed; automatically update data in the management console's network map; and record MetaFrame XPe SNMP traps to the event log.

9. A, B. An administrator monitoring the network with one of the SNMP management applications can use the SNMP console to perform the following tasks: terminate processes on MetaFrame XPe servers; shut down or restart MetaFrame XPe servers; and disconnect, log off, and send messages to active sessions on MetaFrame XPe servers.

**10.** D. Metrics are units of measure based on performance counters that are native to the local operating system. Metrics are configurable indicators that can alert an administrator to a problem over media such as e-mail, SMS, or SNMP.

**11.** B. Resource Manager 2.0 manages, tracks, and reports server and application usage.

**12.** C. If there are servers listed in the `queryhr` results that do not show up in the Citrix Management Console, use the command `<queryhr -d servername>` to remove the server from the list.

**13.** B. You can change the username and password to the data store with the command `<dsmaint config>`.

**14.** C. Open the Citrix Management Console and select the server. Right-click the server and select Set MetaFrame Product Code. Enter the correct product code for the server.

**15.** C. Open a telnet session with the MetaFrame server, but connect to port 1494 instead of the standard telnet port. When the telnet screen comes up, you should receive an ICA sounder.

**16.** B. Command-line options can control the creation of these logs. The installation program (setup) and the uninstall program (rmvica) can be controlled with the following command-line options: `/trace`, which enables tracing for the installation (enabled by default and used if no option is selected) and `/notrace`, which disables tracing for the installation.

**17.** A. If you notice that the information in the Citrix Management Console is different on other servers, the local host cache may be out of sync with the data store. If you run the command `<dsmaint refreshlhc>`, the server in question will reload information from the data store.

**18.** B. When an ICA Client establishes a connection, it needs to be able to establish a socket on TCP port 1494 to the Citrix server, and the Citrix server needs to respond on ports 1023 and above to the client.

19. A, C. If the `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\runtime\CurrentlyLoadingPlugin` Registry key's value is blank, the IMA might not be able to contact the data store. If the Registry key has a value, the IMA service made a successful connection to the data store. This value will also be blank if the local host cache is missing or corrupt.

20. C. During setup, MetaFrame creates the data store and names the file `mf20.dsn`.

# Appendix Feature Release 1

Software is never perfect. As much as we like to think that we have created the ultimate piece of software that contains no bugs, we know it is not true. Software companies are constantly testing and revising the software they publish. Citrix Systems is no different. They issue service packs for problems that are discovered after the software ships. Usually, service packs are a culmination of several hotfixes that were issued to correct problems in the software code. All of the hotfixes are tested to make sure that they are compatible with one another before they are combined into a service pack.

Citrix also realizes that their software is ever evolving. Additional features are not included in service packs; they are added to the system through a feature release. Feature releases add or modify components within your MetaFrame XP servers. A feature release for MetaFrame XP is meant for that platform only. Of course, you are not required to implement the feature release. You can use your system with only the components that ship with MetaFrame XP, but many of the added features give the system new functionality. Of course, you should test any software before implementing it within your production environment. There are many administrators who have been burned by software incompatibilities.

NOTE

As of this writing, Citrix has issued Feature Release 1 for MetaFrame XP. As other feature releases are issued, you will be able to check out the features that have been added or changed by going to our website at `www.sybex.com`.

# New Features in Feature Release 1

We have provided this information so that you will have a reference to look at when you encounter the new features. Citrix has not included any of these features on their exam, so you do not have to worry about learning them as you did the rest of this study guide. Since we want you to utilize this study guide as a reference, we are including the latest information. In the following sections, we will discuss the new features available with Feature Release 1.

WARNING

The new features added to your MetaFrame server farm are not available unless the server farm is running in native mode. They are not supported on MetaFrame 1.8 or MetaFrame XP servers if the server farm is running in mixed mode.

## Automatic Reconnection to ICA Sessions

If a user's connection to a MetaFrame XP server is dropped, and if they are an ICA Win32 client, they can now automatically reconnect to the session they were accessing. The user will not have to reconnect manually, nor will they have to re-authenticate or restart their applications. ICA Java clients (in embedded mode) can also take advantage of this feature. However, the ICA Java client software does not support automatic re-authentication; the user will have to log back into the session.

NOTE

Automatic reconnection is not supported with anonymous sessions.

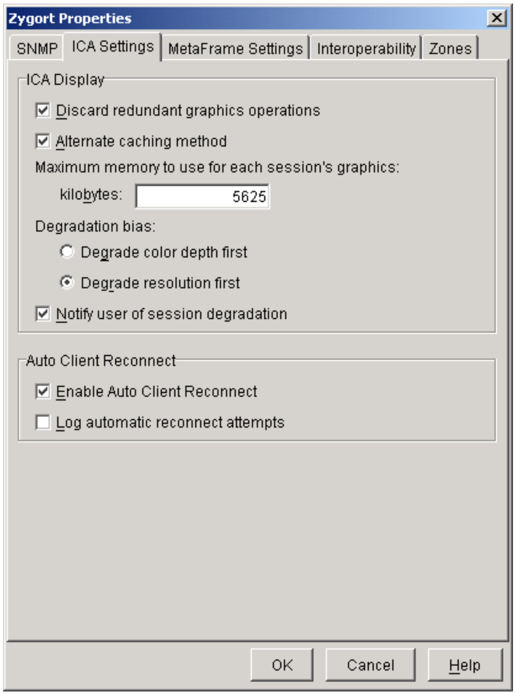
When a client detects a dropped connection, it tries to reconnect to the server based on the number of retries that have been configured. By default, the client will attempt reconnection three times. The user is presented with a message box stating that there will be a reconnection attempt. It is not necessary for the user to act unless they want to reconnect immediately or cancel the action.

MetaFrame XP servers will place the user's session in a disconnected state when the server detects that the connection has been broken. This allows the user to reconnect to their session and minimizes the possibility of another session being created. A timeframe of five minutes is granted to allow the session to reconnect. If the server does not detect the broken connection, the session is not placed in a disconnected state and the server does not begin the autoreconnect timing value. In other words, if the client disconnects normally, the server does not allow automatic reconnections.

## Server Reconnection Settings

You can configure reconnection settings at the server farm or individual server level. If you configure these settings at the server farm level, as seen in Figure A.1, all of the servers will inherit the configuration settings.

**FIGURE A.1** Configuring client reconnection settings at the server farm level



Zygort Properties

ICA Display

☑ Discard redundant graphics operations

☑ Alternate caching method

Maximum memory to use for each session's graphics:

kilobytes: 5625

Degradation bias:

○ Degrade color depth first

● Degrade resolution first

☑ Notify user of session degradation

Auto Client Reconnect

☑ Enable Auto Client Reconnect

□ Log automatic reconnect attempts

To configure reconnection settings at the server farm level, follow these steps:

1. Open Citrix Management Console.
2. Right-click the Server Farm node and select Properties.
3. From the Server Farm Properties sheet, select the ICA Settings tab.

4. Click the Enable Auto Client Reconnect check box to toggle between turning the feature on or off.
5. Click OK to close the Server Farm Properties sheet.

You can configure servers to override the server farm settings by following these steps:

1. Open Citrix Management Console.
2. Expand the Servers node.
3. Right-click the server you are going to configure and select Properties.
4. Select the ICA Settings tab from the server's Properties sheet.
5. Deselect the Use Farm Settings option.
6. Click the Enable Auto Client Reconnect check box to toggle between turning the feature on or off.
7. Click OK to close the server's Properties sheet.

You can also configure MetaFrame XP servers with the `Acrcfg` command. Running this command from the command prompt or from within a script allows you to perform the same functions as using the option within Citrix Management Console.

## Client Reconnection Settings

To configure reconnection settings for the client, all the administrator has to do is make sure that the connection and user settings are configured to disconnect a session when it has timed out or has been dropped. You can do so in two places: Citrix Connection Configuration and the user's profile properties. If you want to control this for every user that connects to the server, you can edit the settings within Citrix Connection Configuration as shown below:

1. Open Citrix Connection Configuration.
2. Double-click the connection you wish to configure and select Properties.
3. In the Edit Connection screen, click the Advanced button.
4. Within the Advanced Connection Settings screen, deselect the (Inherit User Config) check box for On A Broken Or Timed-out Connection.
5. Select Disconnect from the pull-down menu.

If you want to control the reconnection settings on a user-by-user basis, follow the same steps listed above, but first make sure that the (Inherit User Config) check box is selected. Then follow these steps:

If you're using Windows 2000:

1. Open Computer Management.
2. Expand the Users And Groups node.
3. Click the Users container.
4. Double-click the user account you wish to configure.
5. Click the Sessions tab.
6. Click Disconnect From Session in the When A Session Limit Is Reached Or Connection Is Broken section.

If you're using Windows NT Server 4.0, Terminal Server Edition:

1. Open User Manager.
2. Double-click the user account you wish to configure.
3. Click Config.
4. Within the User Configuration screen, select Disconnect from the On A Broken Or Timed-out Connection pull-down menu.

## Content Publishing

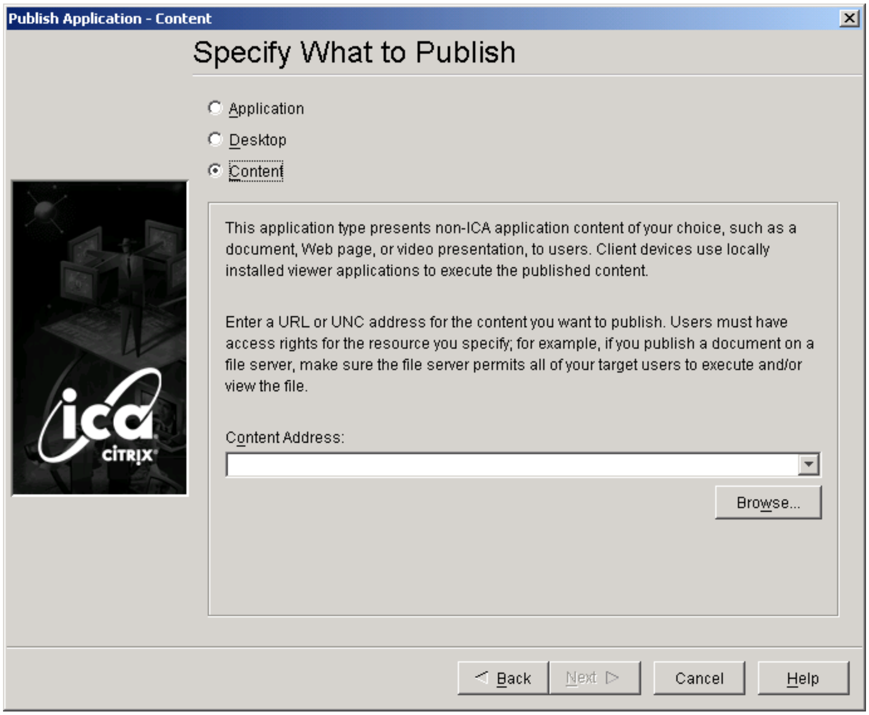
Prior to Feature Release 1, administrators could publish applications for use by selected users. Once Feature Release 1 is loaded onto a MetaFrame XP server, administrators can publish any file to a user's client device. Once a file is published, local applications are used to display the file. You can use any of the standard publishing practices when using content publishing: Program Neighborhood will display the file within the application set, you can push the icon to the user's desktop, and NFuse will display the file on the NFuse web page. For content publishing to work, you must have Feature Release 1 installed on your server, and you must add Feature Release 1 connection licenses so that users can take advantage of this feature.

After you have published content, when a user double-clicks the filename, the name and path to the file are sent to the application that will access the file. In order for this to work, the application must be associated with the appropriate file type. Since the ICA Client software does not actually access the file but only passes the file information to the associated application, the client software is not responsible for running the application.

You use Citrix Management Console to publish the content. You start the Published Application Wizard just as if you were publishing an application, but now that Feature Release 1 is installed, the Content option appears below the Desktop and Application radio buttons, as shown in Figure A.2. Once you choose Content, you can supply the path to the file. This path can be any of the following:

- HTML website address
- Document file on a web or FTP server
- Directory on an FTP server
- UNC path to a directory or file

**FIGURE A.2** Choosing to publish content



Publish Application - Content

Specify What to Publish

○ Application
○ Desktop
● Content

This application type presents non-ICA application content of your choice, such as a document, Web page, or video presentation, to users. Client devices use locally installed viewer applications to execute the published content.

Enter a URL or UNC address for the content you want to publish. Users must have access rights for the resource you specify; for example, if you publish a document on a file server, make sure the file server permits all of your target users to execute and/or view the file.

Content Address:

## Connection Control

By default, when you enable logons to your MetaFrame XP server, users have no limit as to the number of sessions they can have running. While in most environments this is probably the optimal setting, you may need to limit the number of connections a user ties up when running sessions on the server. With the Connection Control feature of Feature Release 1, you can control the number of sessions a user can establish by limiting either the concurrent connections to the server farm or the concurrent connections to a published application instance.

NOTE Connection Control is available only on MetaFrame XPa and XPe servers.

Administrators are usually exempt from the limits you set, but you can include them in the mix if you want. In doing so, however, you may hamper their ability to perform their tasks, such as shadowing or connecting to multiple server desktops to perform administrative functions.

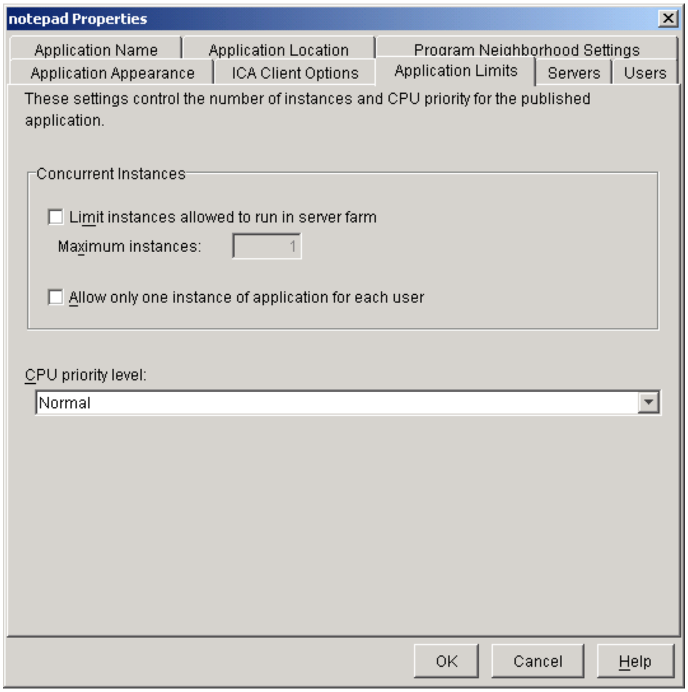
NOTE Connection Control requires that a Feature Release 1 product license and Feature Release 1 connection licenses be added to the server farm.

When publishing applications on which you want to place connection limitations, or if you are configuring applications that are already published, you will find an additional configuration section, Concurrent Instances. Two options appear in this section, as shown in Figure A.3.

**Limit Instances Allowed To Run In Server Farm** When you select this option, you can enter the number of instances of this application that can run within the server farm. If you select this option and enter 25, for example, only 25 instances of the application can run. This is a very handy option if you have licensing limits on a software package.

**Allow Only One Instance Of Application For Each User** As the name implies, each user can run only one instance of the application. Configured alone, this option limits the number of times a user can launch an application. Configured with the previous option, you can maintain the number of times that an application can be accessed by a user and also limit the number of times that the application can be launched. Therefore, no one user can monopolize a licensed application.

**FIGURE A.3** Application-level restrictions



These settings control the number of instances and CPU priority for the published application.

Concurrent Instances

□ Limit instances allowed to run in server farm

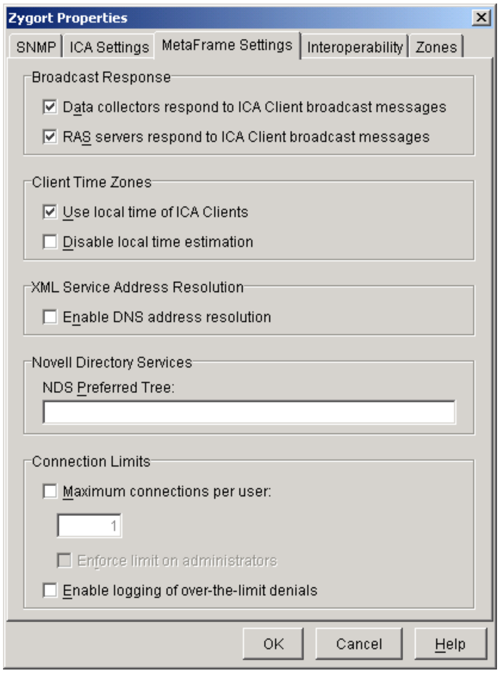
Maximum instances: 1

□ Allow only one instance of application for each user

CPU priority level: Normal

If you want to control the number of connections a user can establish within your server farm, you can configure the Maximum Connections Per User option within the Connections Limits section of the MetaFrame Settings tab in the server farm's Properties sheet, shown in Figure A.4. Once you set this option, all users will be restricted from making more connections within the farm than you have specified. These limits will be applied only to users unless you also select the Enforce Limit On Administrators option.

**FIGURE A.4** Connection limits within the server farm



Broadcast Response

☑ Data collectors respond to ICA Client broadcast messages

☑ RAS servers respond to ICA Client broadcast messages

Client Time Zones

☑ Use local time of ICA Clients

□ Disable local time estimation

XML Service Address Resolution

□ Enable DNS address resolution

Novell Directory Services

NDS Preferred Tree:

Connection Limits

□ Maximum connections per user:

1

□ Enforce limit on administrators

□ Enable logging of over-the-limit denials

## Prioritizing CPU Access by Applications

Certain applications may require a higher priority than other applications within your server farm. Prior to Feature Release 1, the only way to control the application's processor access to the server was to publish mission-critical applications on dedicated servers and other applications on separate servers.

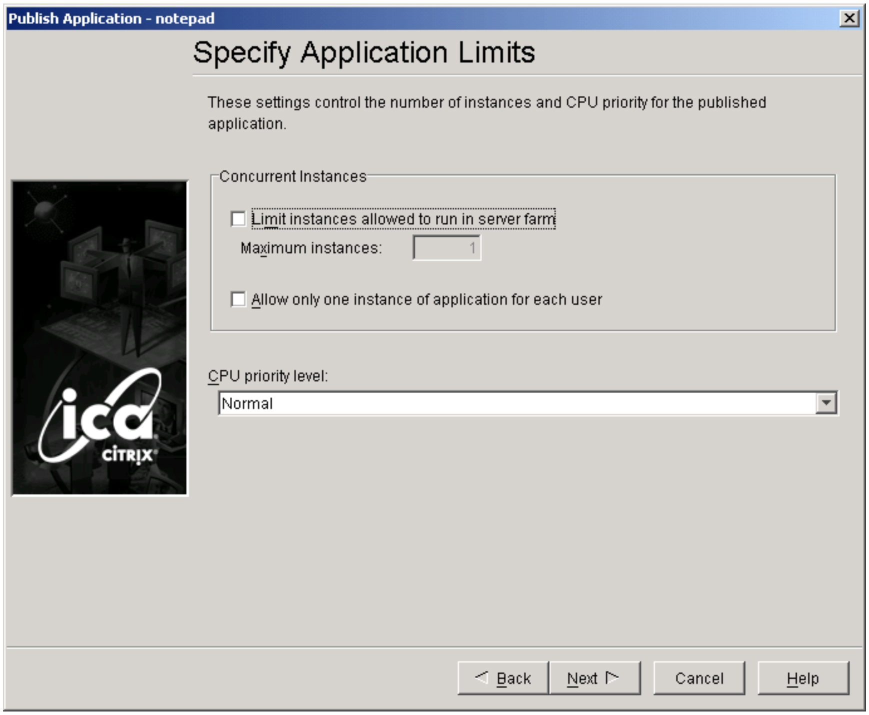
NOTE

CPU priority settings are available only on MetaFrame XP running on Windows 2000 Servers.

By configuring CPU access priority, you can control how often the scheduler allows the process to execute. The higher the priority, the more often the process executes. If you have applications that are published on a server and you want to make sure that one of them does not consume too many resources, causing the others to languish, you can change the priority on the properties of the published application. Five levels are available: low, below normal, normal, above normal, and high. Use caution when assigning the high priority to an application. Using this setting could cause the published application to consume nearly every processing cycle, which could in turn cause the operating system to bog down.

You configure the priority level the same way as you configure the concurrent instance settings for a published application. The CPU Priority Level section appears at the bottom of the Application Limits tab in the published application Properties sheet or within the Application Publishing Wizard shown in Figure A.5. The pull-down menu in this section allows you to select one of the five settings. This setting is applied to every instance of the published application within your server farm. If you want to control the CPU priority so that certain users have a higher priority while running an application than another group, you will need to publish the application twice and set the priorities accordingly on both.

**FIGURE A.5** Controlling the CPU priority level



Publish Application - notepad

Specify Application Limits

These settings control the number of instances and CPU priority for the published application.

Concurrent Instances

☐ Limit instances allowed to run in server farm

Maximum instances: 1

☐ Allow only one instance of application for each user

CPU priority level: Normal

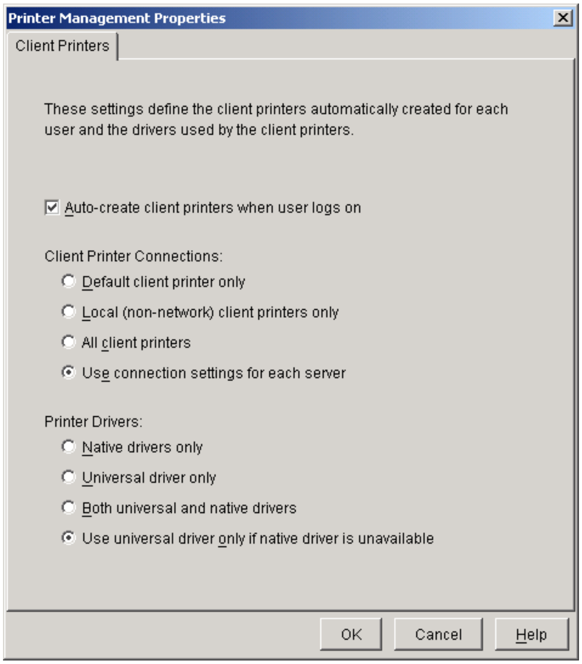
## Universal Printer Driver

Probably the most welcome feature within Feature Release 1, the Universal Printer Driver (UPD) can render print jobs into a format that every printer can use, whether a PCL, PostScript, or Windows printer. When you select the UPD, the MetaFrame XP server uses a PCL4 interpreter to convert the file to an image file that is sent to the client's printer, which then uses the local print driver to format the image to be sent to the print device.

The image that is sent to the client device does have some limitations. Color is not supported, and all of the images are rendered in 300 dots per inch (dpi) black and white. Special print device options are not supported either.

To use the UPD, you need only configure the printer options within Citrix Management Console. The UPD is installed by default when you install Feature Release 1. To configure when the UPD is used, open the Printer Management Properties sheet, shown in Figure A.6. This is a new properties page that appears only on servers with Feature Release 1 installed.

**FIGURE A.6** Configuring the printer auto-creation and driver options



Printer Management Properties

Client Printers

These settings define the client printers automatically created for each user and the drivers used by the client printers.

☑ Auto-create client printers when user logs on

Client Printer Connections:

○ Default client printer only
○ Local (non-network) client printers only
○ All client printers
● Use connection settings for each server

Printer Drivers:

○ Native drivers only
○ Universal driver only
○ Both universal and native drivers
● Use universal driver only if native driver is unavailable

Notice that the Auto-create Client Printers When User Logs On option is selected by default. If you deselect this option, users will have to manually connect to the printers they want to use. Leaving it selected will allow MetaFrame XP to create the connections to the users' printers when they log on.

You can choose from four options under the Auto-create Client Printers When User Logs On section:

**Default Client Printer Only** If you select this option, the session will create only a client printer to the user's default printer on their client device.

**Local (Non-network) Client Printers Only** This option specifies that print devices that are connected directly to the user's client device will be created within the session.

**All Client Printers** As the name suggests, all of the printers that are installed on the client device will be created within the user's session.

**Use Connection Settings For Each Server** Client printers are created within the user's session based on the settings within Citrix Connection Configuration.

The lower section of this screen allows you to choose which drivers are used when a client printer is created. It is here that you choose whether you will use the UPD or the native drivers for the print device:

**Native Drivers Only** The UDP is disabled and only the native drivers are available for use within user sessions.

**Universal Driver Only** The UPD is enabled and used for all client printers whether the native driver is available or not.

**Both Universal And Native Drivers** Client printers are created for each driver type. If you select this option, users will have two client printers created, one using the native driver and the other using the UPD. Use this option only if you have users who will understand the significance of both printers. The UPD will create only generic print jobs, while the native driver will take advantage of the special functions of the print device.

**Use Universal Driver Only If Native Driver Is Unavailable** If you select this default option, any client printer that is created will use the native driver unless that driver is unavailable.

## NDS Support

Feature Release 1 provides support for authentication through Novell Directory Services (NDS). Citrix recognizes that NDS is prevalent in many enterprise network environments and that administrators need to use NDS applications within the server farm. The steps for configuring the servers to interoperate with NDS are too extensive for inclusion in this book. If you want to use this feature, please see the MetaFrame XP Administrator's Guide that ships on the MetaFrame XP CD.

## SSL Support for ICA

Support for SSL connections within your server farm has been available to web clients, but with the new clients that ship with Feature Release 1, ICA Clients that can support SSL can take advantage of SSL connections. Once SSL Relay is configured, any client that is SSL capable can utilize SSL encryption.

NOTE

For more information on SSL Relay, see Chapter 8, "Security."

## Web-Based Administration

For the administrator who is on the go or must administer a remote MetaFrame XP server, Feature Release 1 offers web-based administrative capabilities. One of the options from the splash screen (shown in Figure A.7) that appears when the Feature Release 1 CD autostarts is to install the Citrix Web Console. While this does not really offer a new administrative tool, it does add new web pages to the Citrix web directory beneath your default website. These new pages enable administration over the Internet or your intranet when using a web browser. This added functionality allows you to use a web connection to monitor your server instead of starting an ICA session to access Citrix Management Console. Although you do not get the full range of functionality that Citrix Management Console provides, you are able to log off, disconnect, and shadow sessions as well as send messages to users. Figure A.8 shows the Citrix Web Console.

**FIGURE A.7** Feature Release 1 splash screen

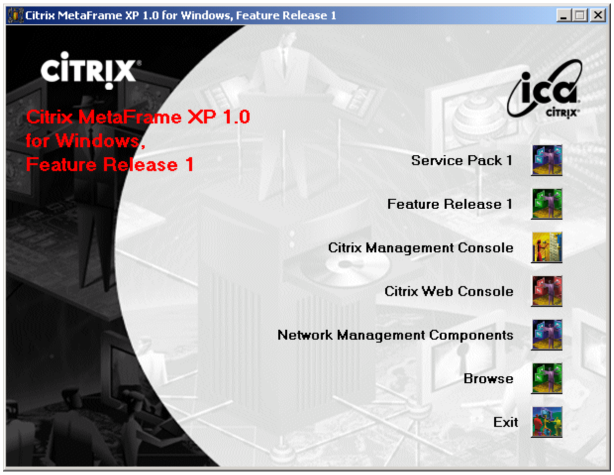
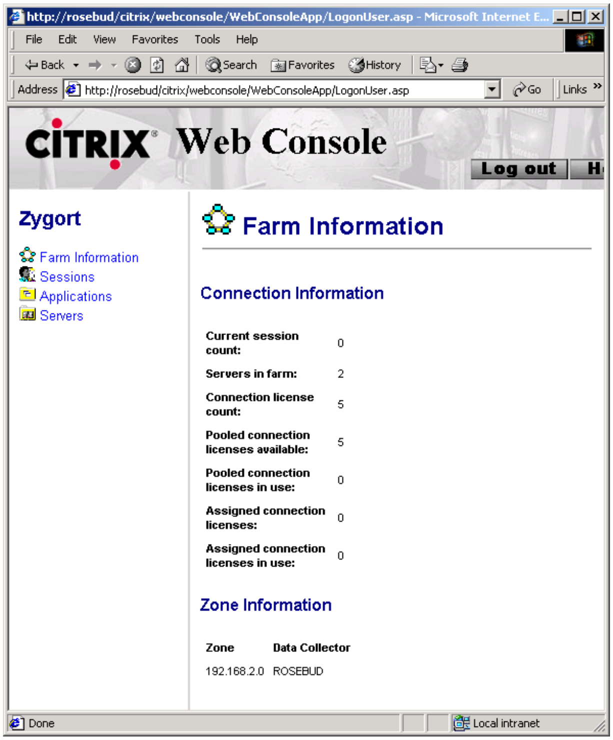


**FIGURE A.8** Citrix Web Console


http://rosebud/citrix/webconsole/WebConsoleApp/LogonUser.asp - Microsoft Internet E...
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://rosebud/citrix/webconsole/WebConsoleApp/LogonUser.asp
Go Links
CITRIX Web Console
Log out
H
Done
Local intranet

Zygort

- Farm Information
- Sessions
- Applications
- Servers

Farm Information

Connection Information

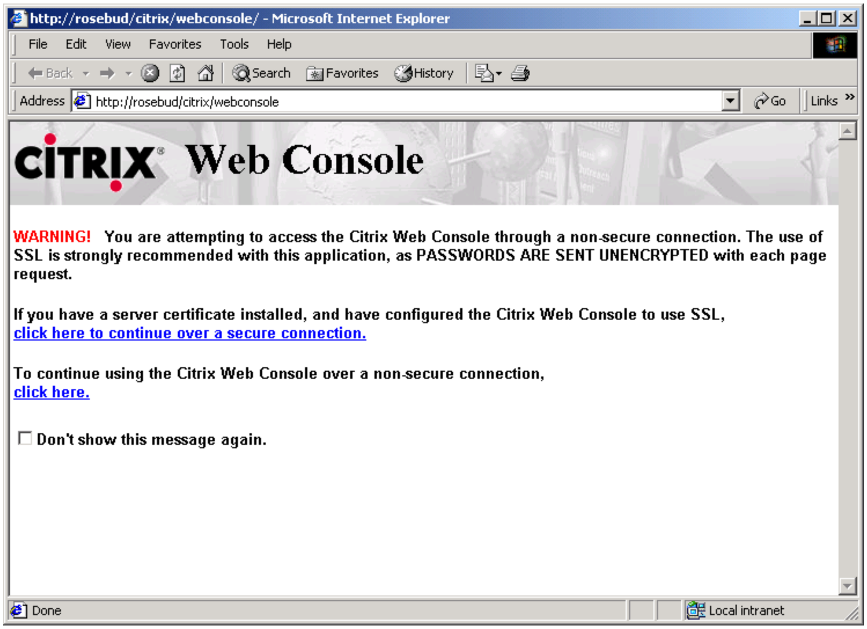
| | |
|---|---|
| Current session count: | 0 |
| Servers in farm: | 2 |
| Connection license count: | 5 |
| Pooled connection licenses available: | 5 |
| Pooled connection licenses in use: | 0 |
| Assigned connection licenses: | 0 |
| Assigned connection licenses in use: | 0 |

Zone Information

| Zone | Data Collector |
|---|---|
| 192.168.2.0 | ROSEBUD |

Since the Citrix Web Console works only in conjunction with IIS 5.0, you must use Windows 2000 as your web server. You will also have to install Service Pack 1 and Feature Release 1 before you install the Citrix Web Console. Once they are installed, you can reach the console by accessing your web server through a browser using the path `http://webserver/Citrix/WebConsole`. You will be presented with the page shown in Figure A.9.

**FIGURE A.9** Connection selection page for Citrix Web Console



http://rosebud/citrix/webconsole/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://rosebud/citrix/webconsole
Go Links
CiTRIX Web Console
Done
Local intranet

WARNING! You are attempting to access the Citrix Web Console through a non-secure connection. The use of SSL is strongly recommended with this application, as PASSWORDS ARE SENT UNENCRYPTED with each page request.

If you have a server certificate installed, and have configured the Citrix Web Console to use SSL, click here to continue over a secure connection.

To continue using the Citrix Web Console over a non-secure connection, click here.

☐ Don't show this message again.

You will be prompted to choose between a secure connection, for use if you have a certificate installed, and a non-secure connection. Of course, you will want to use SSL to make this connection; otherwise, information about your MetaFrame XP environment could be compromised.

## MetaFrame XPe Components

Adding Feature Release 1 to your MetaFrame XP server provides enhancements to Network Manager and Resource Manager. For more information on each of these products and the enhancements, download the white papers available on the Citrix Systems website at `www.citrix.com`.

## ICA Session Monitoring

When Feature Release 1 is installed, additional counters are added to the system so that you can monitor sessions from Performance/System Monitor. The new counters allow you to view bandwidth and compression counters for ICA sessions and servers, bandwidth counters for virtual channels, and latency counters for ICA sessions. You can access these counters the same way you would load any other counter into Performance/System Monitor.

NOTE Unless you are using MetaFrame XPe, the only counters that are available are latency related.

## Citrix Management Console Improvements

You can view additional Feature Release 1–specific information from Citrix Management Console. To be able to see this information, you must update Citrix Management Console on all of the computers that access the MetaFrame XP servers. You can perform this operation by installing the new Citrix Management Console from the Feature Release 1 CD. For more information on the new information available within Citrix Management Console, see the online help from within Citrix Management Console.

## Extended Parameter Passing

Just as you can publish a file and have a local application start to present or process that file, you can associate a published application to start when a file is accessed on the user's local system. When the user double-clicks the file, its path and filename are passed to the MetaFrame XP server, which will start the associated application and present the data in a session.

To configure this feature, you will need to make changes to the server and the client device. On the server, you need to add a placeholder parameter so that the application will accept parameters passed to it. For MetaFrame XP with Feature Release 1 added, the placeholder is simply the characters %*. Open the properties of the published application, and within the Command Line text box, enter the path to the executable for the application and add the placeholder at the end. For example, to allow Notepad to open when a text file is passed to the server, you would enter the following information in the Command Line text box:

```
C:\winnt\notepad.exe %*
```

Once the server is configured to allow parameters to pass to the published application, you will need to configure the client device to pass the parameters to the MetaFrame XP server. To do this, you will need to configure the file extension association so that when the file is opened, the ICA Client will pass the parameters to the server. Since each operating system is different when it comes to setting file associations, check the documentation for your operating system to determine how to assign the association.

# Glossary

**`%systemroot%\ICA\ClientDB`** The default location where MetaFrame XP installs the ICA Client update database (`dbconfig.ini`).

**`%systemroot%\system32\Clients\ICA`** The default location where MetaFrame XP installs ICA Client files.

**activation code** The alphanumeric code generated from the Citrix Activation System web page after you enter the license number generated for the server farm.

**Active** Within the Citrix Management Console, one of the states in which a connection will appear. This state appears when a user is logged on and accessing a session. See also *Conn*, *ConnQ*, *Disc*, and *Idle*.

**Active Server Pages** An extension to Internet Information Server that enables you to run server-side scripts written in JScript or VBScript; those scripts return dynamically created HTML documents based on user input or other variables.

**ActiveX** Microsoft's control plug-in technology for web browsers that allows HTML documents to reference compiled controls and to automatically download and install them if they are not already plugged into the web browser.

**Add/Remove Programs** When Terminal Services is installed, this utility switches the system from execute to install mode and tracks individual settings as they are applied when an application is installed.

**administrative plug-in** A management feature that enhances the Citrix Management Console, such as Resource Manager or Network Manager.

**`adminpak.msi`** The Microsoft installer file that adds domain-level management tools to a Windows 2000 member server or workstation.

**advanced evaluator** An evaluator that is installed by default with load management that evaluates load based upon a predetermined configuration of a single-CPU system with 192MB of RAM and a single SCSI Ultra Wide controller.

**Allow Explicit Logins** This option specifies whether users are allowed to authenticate. When this option is selected for an NFuse website, all users are required to authenticate if the Allow Anonymous option is not also selected.

**anonymous account** A user account that gives users access to the server farm without explicit authentication.

**Any Client Device** A goal of Digital Independence that allows any client device to access a Citrix MetaFrame server.

**Any Network Connection** A goal of Digital Independence that allows any physical network connection type to access a Citrix MetaFrame server.

**Any Network Protocol** A goal of Digital Independence that allows any network protocol to access a Citrix MetaFrame server.

**application compatibility script** A script file that corrects incompatibility issues between applications that were not written for a multiuser environment and a MetaFrame XP server.

**application deployment file** A script file generated when you use Installation Manager to install and configure an application that will be automatically installed on other MetaFrame XP servers in your server farm.

**application embedding** The term used to describe an application that is tied to a web page when using Citrix web-based technologies. If the user leaves the web page or closes the browser, the application session ends.

**application installation mode** When you issue the command `chgusr /install` or use the Add/Remove Programs utility, the server is placed in this mode and tracks the changes made to the system when an application is installed. The user-specific settings are then applied to any account accessing that application.

**application launching** The term used to describe an application that is started in its own window when invoked from a web page using Citrix web-based technologies. The session window is then independent of the web browser, and the user can continue browsing other web pages and even close the browser without affecting the session.

**Application Launching and Embedding (ALE)** A feature that allows clients to access published applications from a web browser without having to rewrite any of the application code.

**Application log** A log that tracks those events that are related to applications running on the computer. The Application log can be viewed in the Event Viewer utility.

**application name** A text string that identifies a published application within the server farm.

**Application Save Position** A feature that remembers an application's size and location within the user's session so that the application appears the same way when the user accesses it again.

**Application Savings** A feature of MetaFrame that allows control and management of applications from a central location.

**application set** The view of the applications to which a user has been granted access within a server farm.

**Application Set Manager** A level within Program Neighborhood that controls access to one or more MetaFrame server farms.

**Application User Load** A rule used in a load evaluator that controls the number of users that can connect to a published application.

**Applications node** The node within Citrix Management Console that is used to publish applications and configure published applications.

**asymmetric encryption** Uses two different, yet mathematically related keys to encrypt and decrypt messages.

**audit policy** Determines which user events you wish to track for security reasons. Audit policy can track the success or failure of specified security events.

**auto-created client printers** Client printers that are defined on the server to be automatically created when a user starts a session. This feature allows an administrator to define the printers that a user will have access to without having to define them at the user's workstation.

**automatic client update** A feature that allows ICA Client software to be updated automatically when a newer version of the ICA Client becomes available.

**auto-replication** Allows an administrator to replicate print drivers to all servers within the server farm.

**`autoroot.exe`** A program that allows an administrator to start the MetaFrame installation. It is located at the root of the MetaFrame XP CD.

**baseline** A snapshot of your computer's current performance statistics that can be used for performance analysis and planning purposes.

**Basic** An encryption level that is Base64 encoded. It should not be used if data needs to be secured.

**Boolean** A rule type used in load balancing that controls access to a server based on true or false results. If the rule evaluates to True, the connection is allowed; if the rule evaluates to False, the connection is denied.

**browser election** The process that determines which Citrix server becomes the master ICA or backup browser on the network.

**Cache tab** The tab in the Program Neighborhood settings that allows you to customize the amount of disk space on the client device to use for caching bitmap images.

**Centralized Data Storage** A feature of MetaFrame that allows information about users, connections, and server configurations to be stored within a centralized database.

**Certificate Authority** A server that controls the issuance and use of digital certificates for users and computers in a particular group.

**Certified Novell Engineer** A Novell certification that is achieved after successfully completing multiple Novell networking exams.

**checklist** A document that specifies the information to be included and the items required for the installation of a server.

**`chgusr /execute`** The command that puts the server into multi-user execution mode.

**`chgusr /install`** The command that places the server into a state that allows software installations to be made globally for all users.

**ciphersuite** An encryption/decryption algorithm used with SSL Relay. When a user attempts a connection through web technologies using SSL, the client and server negotiate which ciphersuite will be used for the session.

**Citrix Administrators node** The node within Citrix Management Console where user accounts are added in order to run Citrix Management Console. Once added, the user is able to control and manage the server farm.

**Citrix Certified Administrator** The certification that is achieved after successfully passing a Citrix MetaFrame Administration exam.

**Citrix ICA Client Distribution Wizard** The wizard used to populate the ICA Client images and the ICA Client Update Database and to install the ICA pass-through Client on the server.

**Citrix Management Console** The main administrative tool used to manage and monitor your MetaFrame XP server farm.

**Citrix Server Administrator** A utility included with MetaFrame 1.8 that allows administration of MetaFrame 1.8 server farms or administration of MetaFrame 1.8 features in a server farm running in mixed mode.

**Citrix WinFrame** An early version of the Citrix operating system built on the MultiWin technology.

**Citrix XML service** The service that provides an HTTP interface to the ICA browser. It uses port 80, by default, to pass information using TCP as the transport protocol.

**Client Auto Update** A feature of MetaFrame that allows ICA Clients to be automatically updated with ICA Client files upon logon.

**client device** Any hardware device capable of running ICA Client software.

**Client Device Licensing** The feature that allows a license to be associated with a client device and not a user session on a server. It benefits the user by consuming only one license for every connection to MetaFrame XP servers within the server farm, regardless of the number of server connections made.

**Client Device Mapping** The feature that allows client devices such as hard drives, printers, and COM ports to be utilized by an application running within a session.

**Client Download Mode** This option, found in the Client Update Database Settings, defines how the client will receive the automatic update.

**Client Drive Mapping** The feature that allows sessions to access hard drives on the client device as though they were local to the session.

**client printer** Any printer that is set up in Windows, including locally connected printers, printers connected on a network, and virtual printers.

**client printing** Allows a client to print to network printers, local printers, or printers attached to a MetaFrame server.

**client/server** A network architecture that dedicates certain computers, called *servers*, to act as service providers to other computers, called *clients*, which users operate to perform work. Servers can be dedicated to provide one or more network services such as file storage, shared printing, communications, e-mail, and web response.

**Client Update Database** The database of all ICA Client files that are stored on the server and the version number. When a client connects to a MetaFrame server, the client version number is checked against this database to see if it is current.

**clientname#\printername** The name of a locally attached client printer as it appears in the Citrix ICA session.

**COM port redirection** A feature that allows applications running within a session to access devices connected to the COM ports on the client device.

**Command Byte** A portion of the ICA Packet; the only required byte. It indicates a command that should be issued at the server or client.

**Command Data** A portion of the ICA Packet that carries the actual data.

**compression** The process of storing data in a form that takes less space than the uncompressed data.

**Conn** Within the Citrix Management Console, one of the states in which a connection will appear. This state appears when the session is being connected to, but the user has not yet logged in. See also *Active*, *ConnQ*, *Disc*, and *Idle*.

**connection** An ICA session that is running on a Citrix MetaFrame server.

**connection license** The license that allows a client device to access a MetaFrame XP server within the server farm in order to run a remote desktop or published application.

**connection migration license** The license installed on a MetaFrame XP server that allows MetaFrame 1.*x* user licenses to be used within your server farm.

**Connection tab** Found in the License node of Citrix Management Console; all connection licenses installed on the server appear here.

**connection upgrade pack** A license number that allows you to upgrade your connection license to a higher level of MetaFrame XP.

**ConnQ** Within the Citrix Management Console, one of the states in which a connection will appear. This state appears as the connection goes from idle and is queued for connection. See also *Active*, *Conn*, *Disc*, and *Idle*.

**Contents** Found within the Load Evaluators node, it displays all of the load evaluators available to assign to a server or published application.

**Contents tab** The tab that displays lower-level nodes and objects. You can view any object in this tab by double-clicking it.

**Context Switches** A rule in Load Manager that allows the load evaluator to calculate a load based on the number of CPU context switches. A context switch occurs every time the operating system switches from one executing process to another.

**Copy to Custom Connections** An option in the application set that allows you to configure different settings for an application session than the default settings provided by the application set.

**counter** Used with Performance Monitor, a counter is a component within an object. The component represents information about a certain aspect of the system or service.

**CPU Utilization** The CPU Utilization rule allows the load evaluator to calculate a load based on CPU usage.

**Create Desktop Shortcut** An option in the application set that allows you to quickly create a shortcut to the connection on the desktop.

**current sessions** Connected and disconnected sessions within the server farm.

**Custom ICA Connections** The level within Program Neighborhood that allows an administrator or user to create new connections to servers or published applications that are not available from the user's application set.

**Custom install** Installation option that allows control over the program options to be installed.

**data collector** The MetaFrame XP server that stores configuration information for its zone.

**data collector zone** A predetermined zone (usually a subnet) where a data collector is responsible for gathering and storing information.

**`DBConfig.ini`** The file that stores the Client Auto Update settings.

**decryption** The act of restoring encrypted data back to its original state using a decryption key.

**default evaluator** The load evaluator that is assigned to all MetaFrame XP servers within the server farm when load balancing is enabled. This evaluator is based on the number of concurrent connected users.

**Diffie-Hellman key agreement algorithm** The algorithm used to generate a public/private key pair between two entities.

**direct cost** When you calculate the Total Cost of Ownership (TCO), the direct costs are those that are tangible, such as the cost of hardware and software.

**Disc** Within the Citrix Management Console, one of the states in which a connection will appear. This state appears when the user's session is disconnected. See also *Active*, *Conn*, *ConnQ*, and *Idle*.

**Disk Data I/O** In Load Manager, the Disk Data I/O rule allows the load evaluator to calculate (in kilobytes) a load based on the disk I/O throughput.

**Disk Operations** In Load Manager, the Disk Operations rule allows the load evaluator to calculate a load based on the number of disk operations per second.

**Display Friendly Name** When you configure the SSL Relay Agent, this option specifies that the certificate's friendly name will be used if available.

**downtime** Any amount of time that a server or system is not available to clients.

**drive mapping** Associating client and server drives with the logical drive letter.

**driver compatibility** The feature that allows an administrator to control which print drivers can be used within the server farm.

**dynamic pages** Web pages that are created based upon certain criteria, such as the logon name.

**election criteria** A set of predetermined rules that decides which computer will win if an election is forced.

**embedded** Applications that run within a web page.

**encryption** The process of translating data into code that is not easily accessible in order to increase security. Once data has been encrypted, a user must have a password or key to decrypt the data.

**encryption level** The setting that controls the strength of the encryption required between a client and the MetaFrame XP server when accessing remote desktops and published applications.

**Evaluators node** The node used to control which load evaluators are assigned to servers and published applications. It is available only with MetaFrame XPa or XPe.

**event logging** The process of tracking and recording information about the computer's hardware and software, as well as security events. This information is stored in three log files: the Application log, the Security log, and the System log.

**Event Viewer** The utility that tracks information about the computer's hardware and software, as well as security events. This information is stored in three log files: the Application log, the Security log, and the System log.

**execution mode** The mode of MetaFrame XP server that allows clients to connect to and start sessions. The server enters this mode when the Add/Remove Programs utility is ended after an application is loaded or the `chgusr /execute` command is issued.

**Farm node** The node that controls the settings for the entire server farm. This is where you set the server farm for native or mixed mode and allocate licenses to subnets.

**Find New Application Set** Run from Program Neighborhood on the client, it tells Program Neighborhood to query the data collector for newly defined application sets.

**firewall** A network device that secures a network from intruders.

**Frame Head** Part of the ICA Packet that is used in stream-oriented communications to frame the data for reconstruction at the receiving computer.

**Frame Trail** Completes the ICA Packet for stream-oriented communications.

**framed protocols** Network protocols that have the functionality of building their own frame set.

**Greater Color Depth** Provides extended color support that allows applications to utilize high-color (65,535) and true-color (16.7 million) sessions.

**Greater Resolution** Allows a session to take advantage of resolutions up to the current maximum of 2700×2700.

**hotkeys** Key combinations used from within a session to mimic the key combinations used within an operating system. For example, the Ctrl+F1 sequence replaces the Ctrl+Alt+Delete sequence within the session to bring up the Security dialog box.

**HTML file** A file used to create a web page from which users can access a published application.

**HTML for IIS** Used with the Web Site Wizard if you would like to use tag-based web pages and you are running Microsoft Internet Information Server (IIS).

**HTML for Servlets** Used with the Web Site Wizard if you would like to use tag-based web pages and you are running Apache or a web server other than Microsoft IIS.

**ICA browsing** Used with MetaFrame 1.8 to enable ICA Clients to locate MetaFrame servers. MetaFrame XP now uses a centralized database and IMA.

**ICA Client** Software that acts as the front end to a session running on the MetaFrame server.

**ICA Client Administrator's Guides** Downloadable PDF format guides that contain configuration options for ICA Clients.

**ICA Client CD** The CD that comes with the Citrix MetaFrame media pack. It is used to install ICA Client files and databases.

**ICA Client Creator** The utility that allows an administrator to create ICA Client installation disks for distribution to client devices where the ICA Client can be installed.

**ICA Client Distribution Location** Specifies where the ICA Client Distribution Wizard installs the ICA Client files, `%systemroot%\system32\clients\ICA` by default.

**ICA Client Distribution Wizard** A wizard that assists the administrator in installing the ICA Client files on the server.

**ICA Client Installation** A step within the ICA Client Distribution Wizard that prompts for a typical or custom installation of the ICA Client files.

**ICA Client Printer Configuration** The utility used to create and connect client printers on DOS and Windows CE clients.

**ICA Client Update Configuration** The utility used to update the ICA Client Update Database with ICA Client images and control how those images are distributed to client devices.

**ICA file** A text file containing the information required to start an ICA session for a published application.

**ICA pass-through Client** Client software added to the MetaFrame server that allows non-Win32 clients to start a session that contains a published Program Neighborhood, which gives them the same access to application sets as Win32 clients have.

**ICA protocol** The protocol used in a MetaFrame environment that allows user input and screen updates to be sent between client devices and the MetaFrame XP server.

**ICA session** The environment created on the MetaFrame server that processes the user's remote desktop and applications. It is created as the user initiates a connection and ended when the user logs off from the session.

**ICA session shadowing** The ability to view and control a remote user's session from within another session. It is used mainly for troubleshooting purposes. The level of access to the session can be controlled. The session being shadowed can be notified of the impending shadow session, and the session can be controlled by the user shadowing the session.

**ICA Settings** Found on the Tools menu of Program Neighborhood, this option controls global settings within Program Neighborhood.

**`icaweb` directory** ICA Web Client installation files are located in the `icaweb` directory on the ICA Client CD.

**Idle** Within the Citrix Management Console, one of the states in which a connection will appear. This state appears when no sessions are connected to the connection. See also *Active*, *Conn*, *ConnQ*, and *Disc*.

**idle sessions** Sessions created for the purpose of allowing a user to connect to the server and start their session faster. The two idle sessions are full sessions that are created but not used until the listener port passes a session request to them.

**Import Network Print Server** The feature that allows a print server's printer configuration to be added to the server farm so that users will be able to access those printers as client printers.

**Incremental** A rule type that determines the maximum number that can be obtained by a rule.

**Independent Computing Architecture (ICA)** Citrix's platform that allows the application logic to be separated from the user interface. All of the application logic is processed at the server, while the client device sends only keystrokes and mouse information to the server and receives screen updates from the server.

**Independent Management Architecture (IMA)** Citrix's server-to-server infrastructure that uses a centralized data repository, known as the *data store*, which contains configuration information about every server within the server farm.

**indirect costs** Intangible costs that are calculated when figuring the Total Cost of Ownership (TCO), for example, the cost of an administrator's time spent troubleshooting issues within the server farm.

**install mode** The mode that the server is in when multiple users are accessing the server to run sessions.

**installation disks** The disks that are created by the ICA Client Creator. The disks can be used to install the ICA Client on a system that has a floppy drive.

**Installation Management** A service that allows an administrator to create application installation packages to distribute to other MetaFrame servers that are running Installation Management. The installation files are sent to the other servers along with a script.

**Installation Manager** Administrative plug-in to the Citrix Management Console that allows Citrix administrators to manage and control application installations on MetaFrame XP servers.

**Installer service** A component of Installation Manager installed on a MetaFrame XP server that controls the installation of software packaged by the packager system.

**instance** An individual version of a counter. A dual-processor computer contains two instances of processor object counters.

**Integrated Security** Built into the MetaFrame XP product are 40-, 56-, and 128-bit data encryption and 128-bit authentication encryption.

**interoperability** The ability to have MetaFrame XP and MetaFrame 1.8 servers work within the same server farm; also known as *mixed mode*.

**IP Range** A Boolean rule used in a load evaluator that controls access to the MetaFrame XP server by the subnet on which the user's client device is located.

**Java** Sun's trademark for a set of technologies used when creating and safely running software programs in both stand-alone and networked environments.

**Java Runtime Environment 1.3 (JRE 1.3)** Software required to load the Citrix Management Console on a server or workstation. It is loaded by default as part of the MetaFrame XP installation and as an additional component when Citrix Management Console is added to a user's workstation.

**JavaServer Pages** Web technology that uses template data, custom elements, scripting languages, and server-side Java objects to return dynamic content to a client.

**Key Store Location** Specifies the location of the certificate used to validate the identity of the relay to web servers that are NFuse-enabled. The default location of the certificate store is `%systemroot%\SSLRelay\keystore`.

**keys** Stored at both the sender and receiver, keys can be either public or private. Keys are used to encrypt and decrypt data.

**Launched** This option creates an independent session when the application is started from a web page.

**license count** The number of licenses that a license pack allows after it has been added to the server farm.

**License node** The node in Citrix Management Console where license information is managed and monitored.

**license number** The code that appears within the License node of Citrix Management Console. After you add the license information from the license pack, the system generates the unique code from the server information. This code is used to generate the activation code from the Citrix Activation System web page.

**license pooling** The feature that allows an administrator to combine the licenses for use by any MetaFrame server within the server farm.

**License Threshold** The rule used by load evaluators that allows an administrator to control the number of connections made to a server by the number of licenses used.

**licensing** A MetaFrame XP feature that provides single-point license installation and activation with support for license pooling.

**listener port** A virtual port on the MetaFrame server that monitors for ICA session requests and then passes those requests to idle sessions to create the session. One listener port exists for every protocol on the server.

**load balancing** The ability to control where session requests are sent based on the resource consumption of the server. The ideal is to have the session request sent to the least-busy server in the server farm that can handle the request.

**load evaluator** The tool used to control load balancing within the server farm. The administrator can create custom evaluators, made up of rules, to control access to each server.

**Load Evaluators node** The node within the Citrix Management Console containing the load evaluators that exist within the server farm and the servers and published applications to which the evaluators are assigned.

**Load Manager** An add-in product available for use with the XPa and XPe versions of MetaFrame XP. Load Manager enables load balancing of the servers within the server farm.

**Load Manager Monitor** Provides a graphical view of the load evaluators assigned to servers and published applications and of the rules that make up the evaluator.

**local host cache** The memory area within a MetaFrame XP server that holds configuration information about that server and other servers and published applications within the server farm.

**local printers** Printers that are connected directly to MetaFrame XP servers within the same farm.

**local text echo** The feature that allows text fields to be populated within a user's session prior to the server responding with the updated screen information.

**Log tab** Found within the Load Evaluators node in Citrix Management Console, the Log tab displays information as events occur with the evaluators used in the farm.

**logging of shadowing** When shadow logging is enabled on a MetaFrame XP server, the shadow session information is written to the System log of Event Viewer.

**lower threshold** When you create rules, the lower threshold defines the value at which the server reports that it is experiencing no load.

**Management Console** Within an SNMP-monitored network, the Management Console is the device that receives trap information from the SNMP agents and reports the information.

**Memory Usage** In Load Manager, the Memory Usage rule allows the load evaluator to calculate a load based on memory utilization.

**MetaFrame XP License Agreement** A legal document that specifies what rights and restrictions a company has in using MetaFrame XP.

**metrics** When you use Resource Manager on MetaFrame XPe, metrics are the units of measure based on performance counters native to the local operating system. Metrics are configurable indicators that can alert an administrator to a problem over media such as e-mail, SMS, or SMTP.

**Microsoft Access** A Microsoft database program that utilizes the Jet database engine; it can be used as the data store.

**Microsoft Certified Systems Engineer** A Microsoft certification that is achieved after successfully passing a series of exams.

**Microsoft Diagnostics** The former version of the System Information utility that displays information obtained from the operating system.

**Microsoft Java Virtual Machine (JVM)** Microsoft's "execution engine" that executes the byte codes in Java-class files.

**Microsoft SQL Server** Microsoft's Structured Query Language database application; it can be used for the data store.

**Microsoft Terminal Services** The service based on MultiWin technology that runs on a Windows 2000 Server or Windows NT Server 4.0, Terminal Server Edition operating system and that allows a user to execute a client/server session.

**minimum requirements** The lowest level of hardware that will support the software being installed on the computer.

**mixed mode** The server farm must be in mixed mode when it contains both MetaFrame XP and MetaFrame 1.8 servers that need to interoperate.

**modules** The software being accessed from within a user's session. This information can be found within the Citrix Management Console.

**mouse click feedback** Changes the mouse pointer into an hourglass until the server can send the screen update, illustrating that the user clicked the mouse button.

**Moving Average** Rules based on this criterion use a percentage of the resource over a predefined period of time.

**Moving Average Compared To High Threshold** Rules based on this criterion use a percentage based on the values specified in the high and low threshold fields. The values that can be used with such a rule fall within the range 0–2,147,483,647.

**Multi-Monitor Support** Allows a session to take advantage of a client device that has multiple monitors on one desktop.

**Multi-Vendor Support** Allows client devices running operating systems other than a Windows platform to run client sessions on the server.

**multiple session support** Feature of MetaFrame XP that allows 16-bit ICA Clients to run multiple sessions.

**MultiWin** The technology that allows a server to run multiple instances of a user session within the operating system.

**native mode** The server farm can be placed in native mode when there are no MetaFrame 1.8 servers with which the MetaFrame XP servers need to interoperate.

**Netscape plug-in** Software that allows web-based ICA access to the MetaFrame server when using a Netscape browser.

**Network Address Translation (NAT) device** An IP router that has the ability to translate the IP address and TCP/UDP port numbers of packets as they are forwarded.

**Network Manager** The administrative add-in to Citrix Management Console that allows the MetaFrame XP server farm to participate in an SNMP-monitored network. It is available only in the XPe version of MetaFrame.

**network printers** Printers that are connected to print servers or MetaFrame XP servers that are not part of the same farm.

**network share** An access point on a server that allows users to connect to a specified directory to access subdirectories and files.

**NFuse** Citrix's premier web technology that enables administrators to easily manage web-based access to the server farm.

**NFuse Java objects** Software objects added to the NFuse web server. These objects perform functions on behalf of the client including authenticating the user to the server farm, modifying the properties of an application before presenting the application to the user, retrieving the application set for the user to see, and creating and sending ICA files that are necessary to start an ICA session.

**object** A component of Performance/System Monitor that captures data on system components as the system performs tasks.

**Open Database Connectivity (ODBC) driver** Industry-standard software driver that allows an application to interact with database software such as Microsoft SQL Server or Oracle.

**Open Systems Interconnection (OSI) model** A model defined by the International Organization for Standardization (ISO) to categorize the process of communication between computers in terms of seven layers. The seven layers are Application, Presentation, Session, Transport, Network, Data Link, and Physical.

**Oracle** An enterprise-level database server that can be used as the data store for the MetaFrame XP server farm.

**packager** The system used to install, and monitor the installation of, applications that will be pushed out to other servers in the server farm.

**Page Fault** A rule used within a load evaluator that controls access to the server based on the number of page faults that occur on the server.

**page files** A temporary storage location on the hard drive of a computer that is reserved for storing data from memory when there is not enough physical memory (RAM).

**Page Swap** A rule used within a load evaluator that controls the access to the server based on the number of page swaps that occur on the server.

**Panning and Scaling** The feature that allows you to view a full-size desktop that exceeds the screen size of the client through the use of scroll bars at the edges of the screen (panning) or through resizing the screen to the user's preference (scaling).

**pass-through authentication** The ability to send the user's current credentials from the profile that they are logged on with to the MetaFrame XP server for authentication.

**Performance Logs and Alerts** A Microsoft Management Console snap-in that creates performance logs.

**Performance Monitor** A utility found within Windows NT that monitors performance counters on the server.

**Performance tab** A tab found within Task Manager that displays performance data for the computer. Information displayed on this tab includes processor and memory information.

**Pooled License** A feature of MetaFrame XP that allows licenses to be used on any server within the server farm.

**port** A logical connection point within a TCP/IP address that allows multiple protocols to communicate with a single host at the same time.

**Presentation layer** The sixth layer of the OSI model; responsible for formatting data exchange such as graphic commands and conversion of character sets. Also responsible for data compression, data encryption, and data stream redirection. See also *Open Systems Interconnection (OSI) model*.

**print device** The hardware that accepts print jobs from a printer and creates the document.

**print server** A computer that acts as a repository for printers and accepts print jobs from clients on the network.

**printer** Software installed on a client device that acts as the intermediary between applications and the print device.

**Printer Bandwidth tab** The tab within the Servers node of Citrix Management Console that controls the amount of network bandwidth that print jobs consume.

**printer driver** Software that structures print jobs sent from applications into a format that print devices understand.

**printer management** A feature of MetaFrame XP that allows printer driver configuration and replication through the server farm.

**Printer Management node** The node within Citrix Management Console used to control print drivers used within the server farm and printers that are defined for user sessions.

**printer mapping** The association made between a legacy printer driver used on a Windows *9x* platform and the driver used on Windows NT or Windows 2000 when the drivers are named differently.

**printer replication** The feature that allows printer driver configuration information to be replicated to other servers within the server farm.

**private key** A technology in which both the sender and the receiver have the same key. A single key is used to encrypt and decrypt all messages. See also *public key*.

**processes** The programs and system software that are running within a user's session.

**Processes tab** A tab found within the Citrix Management Console that displays all of the processes running within the server and which session they are running in.

**product code** A character string that identifies a MetaFrame XP server with the appropriate version of MetaFrame XP that it will use. MetaFrame XPs, XPa, and XPe, as well as evaluation and not-for-resale versions, all use different product codes.

**product license** The software license that enables MetaFrame XP versions.

**Product tab** A tab found within the Citrix Management Console that displays the product licenses that are installed within the server farm.

**Program Neighborhood** The user interface to the server farm. Used with Windows 32-bit operating systems and ICA Java Clients, it gives users their application set, which contains the published applications that they have permission to use within the server farm.

**proxy server** A type of server that makes a single Internet connection and services requests on behalf of many users.

**public key** A technology that uses two keys to facilitate communication, a public key and a private key. The public key is used to encrypt a message to a receiver. See also *private key*.

**published application** An application that is made available to clients when they access Program Neighborhood. You configure published applications to run on specified servers within the server farm, and you can specify which users can access them.

**publishing** The act of making an application that is installed on MetaFrame servers available to users.

**queryhr** The utility used to display a list of MetaFrame servers within the server farm.

**RC5 (128 bit)** The 128-bit version of the RSA RC5 algorithm. See also *RSA RC5 algorithm*.

**RC5 (128 bit) logon only** The version of the RSA RC5 algorithm that allows logons to use 128-bit encryption but does not provide data encryption. See also *RSA RC5 algorithm*.

**RC5 (40 bit)** The 40-bit version of the RSA RC5 algorithm. See also *RSA RC5 algorithm*.

**RC5 (56 bit)** The 56-bit version of the RSA RC5 algorithm. See also *RSA RC5 algorithm*.

**Relay Credentials tab** A tab found within the SSL Relay Agent that allows you to define the password for the server certificate used to decrypt the packets.

**relay listening port** The TCP port that monitors the network for SSL connections from a web server.

**Reliable** Part of the ICA Packet, the Reliable header is used in connectionless protocols to provide reliable, error-free delivery.

**Resource Mapping and Redirection** A feature of MetaFrame that allows a client's session to interact with the client's local device.

**Resource Manager** The administrative add-in to Citrix Management Console that allows an administrator to monitor the MetaFrame XP server farm and generate detailed reports.

**RSA RC5 algorithm** The security algorithm used by MetaFrame to encrypt the information that is sent between the server and clients when Secure ICA is used. See also *Secure ICA*.

**rule** The piece of the load evaluator that controls the connections made to servers and published applications.

**Scheduling** The rule used in a load evaluator that controls access to the MetaFrame XP servers based on time constraints set by the administrator.

**seamless desktop integration** The ability to make applications appear as though they are running as part of the local user profile instead of within a user session.

**Secure ICA** An encryption add-on to the MetaFrame 1.*x* product that is now included as part of MetaFrame XP.

**Secure Socket Layer (SSL)** An encrypted transmission protocol that uses TCP/IP to implement a secure, public-key-encrypted data channel between a client and a server.

**security** The science of configuring computers and networks so that only authorized individuals are able to access the information and hardware within the systems.

**Security dialog box** The dialog box that appears after the Ctrl+Alt+Del key sequence is pressed on a Windows NT 4.0 or Windows 2000 operating system.

**Security log** A log that tracks events related to Windows 2000 auditing. The Security log can be viewed through the Event Viewer utility.

**Server Certificate** A file used with public key encryption that verifies the identity of the server.

**server farm** A group of MetaFrame servers that are grouped together for administrative purposes and that share the same IMA data store.

**Server IP address** When you configure the SSL Relay Agent, this field is populated with the IP addresses of the servers that will have data relayed to them after the SSL Relay has decrypted the original information.

**Server Location** The setting within the ICA Client software that determines which server will be contacted when a user attempts to start a published application.

**Server User Load** The rule used with load evaluators to control the number of users allowed to access the server.

**Servers node** The node within Citrix Management Console that allows monitoring and management of individual servers within the server farm.

**Set As Default** An option from the context menu that determines which application set will be connected to when Program Neighborhood is started.

**shadow** To monitor and interact with another user's session from within your own session.

**shadowed session** Session that is shadowed from another session.

**Shadow Indicator** A dialog box that appears in the upper-left corner of the session window when the session is being shadowed. It appears only if shadow notification is enabled.

**Shadow taskbar** The taskbar that can be used to control multiple shadowed sessions from the server desktop.

**Simple Network Management Protocol (SNMP)** An Internet protocol that manages network hardware such as routers, switches, servers, and clients from a single client on the network.

**Simple Network Management Protocol (SNMP) Agent** Software added to a client device that allows it to interact with an SNMP Management Console such as HP OpenView.

**SpeedScreen** The technology that controls the screen refresh information sent to an ICA Client device. If the screen information is not updated, the screen is not repainted. Also, if the information is hidden behind a window, it is not transferred across the network to the client device.

**SpeedScreen Latency Reduction** Technologies used to reduce user interface discrepancies when there is a delay in transferring the screen updates between a server and the ICA Client.

**Sun Java Runtime Environment (JRE)** A subset of the Java Development Kit that includes the Java virtual machine, the Java core classes, and supporting files. It is available as a free download for end users and developers who want to redistribute the runtime environment alone.

**symmetric encryption** A form of encryption that uses the same key to encrypt and decrypt the data.

**System Information** The Windows 2000 utility that displays resource configuration information about the operating system and computer system on which it is run.

**System log** A log that tracks events that relate to the Windows 2000 operating system. The System log can be viewed through the Event Viewer.

**System Monitor** A Windows 2000 utility used to monitor real-time system activity or view data from a log file.

**Task Manager** An application that you can use to manually view and close running processes or to view CPU and memory statistics. Press Ctrl+Alt+Delete to access the Security dialog box, and then click the Task Manager button to launch Task Manager. From within a session, you can press Ctrl+F1 to launch Task Manager.

**TCP-based ICA Browsing** A feature of MetaFrame XP that allows browsing to use TCP as the transport protocol instead of UDP. This allows browsing to function through routers and other network devices.

**template** A published application that is used to generate other published applications. When a template is used, the servers and users that have access to the template are copied into the new published application, making publishing an application easier for an administrator.

**temporary files directory** A directory used to store files that are used by an application but are not needed after the application exits.

**terminal services** Technology that allows a user's session to run on a server while the user accesses the session from a thin client application on their desktop. The client software sends keystrokes and mouse movements and clicks to the server, and the screen updates are delivered back to the client software to be displayed on the client device.

**thin client technology** A term used to describe the act of having a server process information on behalf of a client system.

**ticketing** Used with web technologies to replace the user credentials with text strings that identify the user. Tickets have a short time-to-live and are not available after the ticket expires.

**transform file** A file used in conjunction with a Windows Installer file that allows different options to be installed automatically.

**triggers** Events that force updates of the server load to be sent to the data collector within the zone.

**Typical install** The installation option that installs the most widely used features of an application.

**unassociated applications** Applications that are published under the NT domain scope within a MetaFrame 1.*x* server farm.

**upper threshold** When you create rules, the upper threshold defines the value at which the server reports that it is experiencing 100 percent, or full, load.

**Usage Reports tab** A tab found within the Citrix Management Console that displays the evaluators that are assigned to servers and published applications.

**User Connect/Disconnect** A trigger used to control the load on a server when load balancing is enabled using MetaFrame XPa and XPe. The data collector uses this trigger to adjust the load whenever a user is in a connected or disconnected state so that a true load value can be reported to user session requests.

**User Logon/Logoff** A trigger used to control the load on a server when load balancing is enabled using MetaFrame XPa and XPe. The data collector uses this trigger to momentarily increment the load value for the server until the actual value is reported from the server.

**Users** The entry found within the Citrix Management Console that shows the account that is logged in and accessing a session.

**Users tab** Found within the Citrix Management Console, this tab displays the users that are currently connected to the MetaFrame server and running a session.

**version checking** A feature of ICA Clients that allows them to report their version number to the ICA Client Update Database. If a different version is detected, the database configuration controls how the ICA Client is updated.

**web-based ICA Client install** The deployment method used to allow web-based download and setup of ICA Clients. Once a user accesses the website, they can automatically download and install the client files.

**web browser** Software installed on a computer that allows a client to access a web server and retrieve information using web technologies.

**web server** A server that is used to provide access to data when utilizing web technologies.

**Web Site Wizard** The wizard that is used to create websites to be used in an NFuse environment. The entire web interface can be created with this wizard.

**web technologies** Tools used to enable web-based access to MetaFrame sessions.

**`WebInst` directory** The directory that is created when the web-based ICA Clients are installed on a web server. It is used to automatically install and update web-based ICA Client software.

**`wfcname.ini`** The file used to store the ICA Client name. This name is sent to MetaFrame XP servers and is seen in the Citrix Management Console when the user has a session running.

**Windows 2000 Server** Microsoft's premier server operating system that has Terminal Services as one of its services. Citrix's MetaFrame XP can be installed to provide enterprise-level Terminal Services.

**Windows Installer package** A file with an `.msi` extension that is used to control the installation of software within a Microsoft operating system.

**Windows NT Server 4.0, Terminal Server Edition** Microsoft's first version of an operating system that is used to run the MultiWin kernel that was licensed from Citrix.

**Windows NT Server 3.51** The first operating system that Citrix used to develop and run the MultiWin kernel.

**WOW (Win16 On Win32)** A program that is used to control and manage Win16 applications on a Windows NT or Windows 2000 Server.

**`wtsprnt.inf`** A file that resides on each server used to save the printer information within the server farm.

**`www.citrix.com/downloads`** The web page where the Citrix ICA Client software can be downloaded.

**XPa** The advanced version of MetaFrame XP that includes load balancing.

**XPe** The enterprise version of MetaFrame XP that includes load balancing, Network Manager, Installation Manager, and Resource Manager.

**XPs** The standard version of MetaFrame XP; it consists of only the MetaFrame software, with no additional add-in pieces.

**zone** A grouping of MetaFrame XP servers, usually by subnet. All MetaFrame XP servers within the zone communicate directly with the zone's data collector to send and retrieve configuration information.