Lotus. software

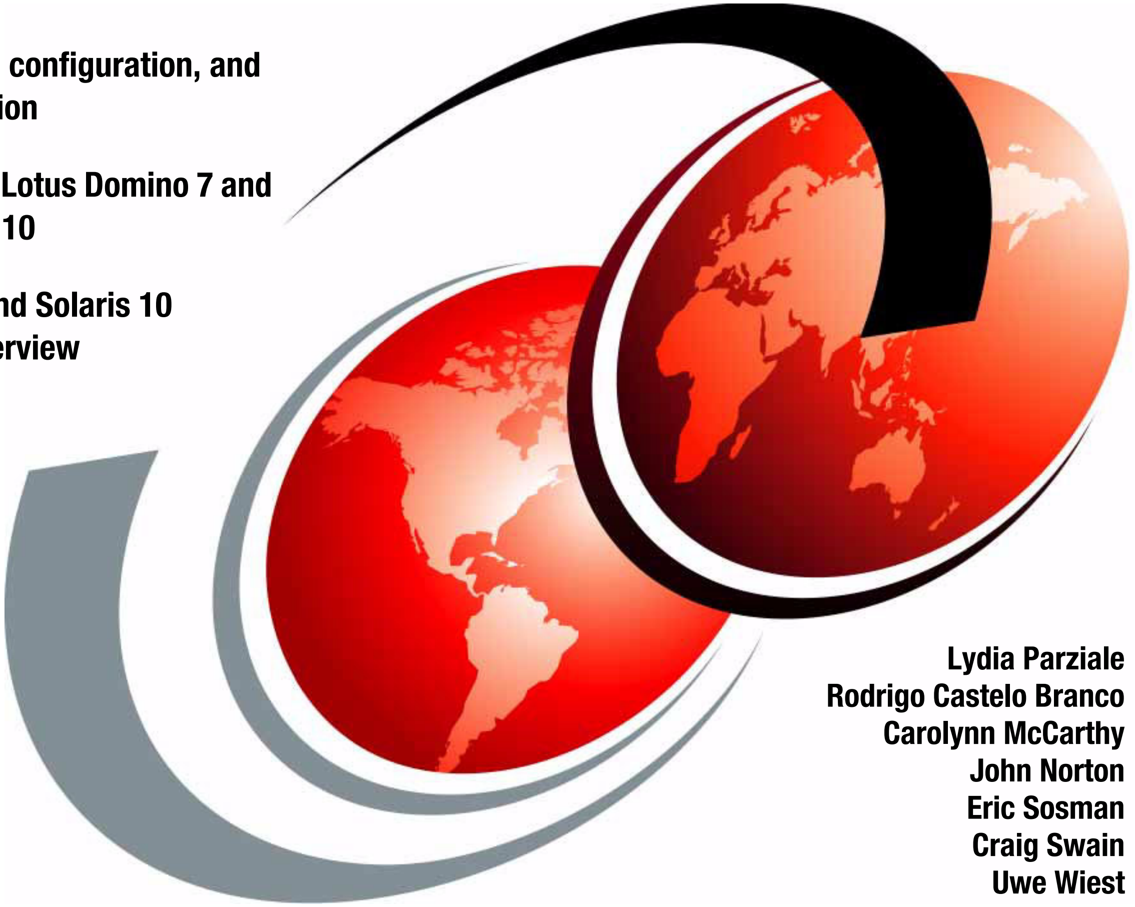
IBM

Domino 7 for Sun Solaris 10

Installation, configuration, and administration

Tuning IBM Lotus Domino 7 and Sun Solaris 10

Domino 7 and Solaris 10 security overview



Lydia Parziale
Rodrigo Castelo Branco
Carolynn McCarthy
John Norton
Eric Sosman
Craig Swain
Uwe Wiest

Redbooks

ibm.com/redbooks

International Technical Support Organization

Domino 7 for Sun Solaris 10

March 2006

SG24-7162-00

Note: Before using this information and the product it supports, read the information in “Notices” on page xiii.

First Edition (March 2006)

This edition applies to IBM Lotus Domino Version 7 and Sun Solaris Version 10.

© Copyright International Business Machines Corporation 2006. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2006. All rights reserved.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

© Copyright IBM Corp. 2006. All rights reserved.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®
AS/400®
Domino Designer®
Domino®
DB2 Universal Database™
DB2®
developerWorks®
eServer™
IBM®
iNotes™
iSeries™
i5/OS®
Lotus Enterprise Integrator®
Lotus Notes®
Lotus®
Lotusphere®
Notes®
PowerPC®
Redbooks™
Redbooks (logo) ™
S/390®
Sametime®
Tivoli Enterprise™
Tivoli Enterprise Console®
Tivoli®
WebSphere®
Workplace™
z/OS®
zSeries®

The following terms are trademarks of other companies:

IPX, Java, JavaScript, JVM, J2EE, Solaris, Solstice, Sun, Sun Enterprise, Sun Enterprise Authentication Mechanism, Sun Fire, Sun Java, Sun Microsystems, Sun StorEdge, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Outlook, Windows server, Windows NT, Windows, Win32, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

Although the IBM® Lotus® Domino® server is platform independent, each platform it runs on requires additional platform-specific knowledge and configuration to ensure that it operates efficiently and at maximum capability. This IBM Redbook explains how to run Domino 7 on the Sun™ Solaris™ 10 Operating Environment.

The primary focus is to explain the installation, configuration, and performance tuning of Domino 7 in this environment. We take you through all of the steps that are required to run a Domino 7 server on Solaris 10, from choosing the right hardware, installing Solaris and Domino, tuning the OS and the Domino server, security for the OS and Domino, and performing administrative tasks, through to problem determination and troubleshooting.

© Copyright IBM Corp. 2006. All rights reserved.

The team that wrote this book

This book was produced by a team of specialists from around the world working at the International Technical Support Organization Center at Lotus in Cambridge, Massachusetts, USA.

Figure 1 The IBM Lotus Domino 7-Sun Solaris 10 Redbooks Project Team

Lydia Parziale is a Project Leader for the ITSO team in Poughkeepsie, New York, with domestic and international experience in technology management including software development, project leadership, and strategic planning. Her areas of expertise include e-business development and database management technologies. Lydia is an IT Specialist with an MBA in Technology Management and has been employed by IBM for 23 years in various technology areas.

Rodrigo Castelo Branco joined IBM Brazil in 2004. As a system specialist, he supports IBM Lotus Domino international customers over several OS platforms. He also has published three Redpapers for ITSO (“Linux®: Why It Should Replace Your Windows® NT Domains,” “Migrate Exchange 5.5 to Domino on Linux” and “Open Your Windows with Samba on Linux”). Before joining IBM he worked at Cyberlynxx, an IBM Business Partner, as a system architect and pre-sales, leveraging Lotus sales and certifying the company as the first IBM Linux Leader in Brazil.

Carolynn McCarthy is an Advisory Software Engineer on the L3 Domino Development Team in the United States. She has 13 years of experience working on Lotus products, with 10 of those years spent working on Notes/Domino. Her areas of expertise include resolving Domino PMRs/SPRs, specifically on UNIX® platforms. She holds a Bachelor of Science in Engineering from the University of Massachusetts, Lowell.

John Norton is a Senior Engineer for G2 Associates, Inc., based in McLean, Virginia. He has more than 20 years of IT experience with a focus on mail and messaging infrastructures. He holds a Master of Science degree in Information Systems Management from Clarkson University. As an IBM/Lotus employee (1996-2002) he held a variety of senior consulting positions that focused on enterprise deployment projects, doing infrastructure planning for complex environments for large commercial and government organizations. He has helped customers to implement Domino on Solaris in the United States. His duties also include providing pre-sales and technical support for ProActive Tools by G2 Associates, Inc.

Eric Sosman is a member of the technical staff in the Market Development Engineering group of Sun Microsystems™ Inc. He has been a software engineer for nearly four decades, devoting the past seven years almost exclusively to the Sun/Lotus partnership. He has participated in and occasionally led joint IBM/Sun engineering projects. He has produced benchmarks and best practices guides, is the author of *Domino on Solaris: Common Tuning Tips* and co-author with Craig Swain of Sun's internal Domino sizing guide.

Craig Swain is a senior Solution Architect for Sun Microsystems Inc. based in Burlington, Massachusetts, supporting the Sun-IBM Software partnership. He has been a software engineer for close to 30 years and has a Bachelor of Science degree from Cornell University. Craig has been helping partners and customers architect Lotus on Sun solutions since 1995 and Notes 3.3. He is a co-author with Eric Sosman of Sun's internal Domino sizing guide and has been a speaker at Lotusphere® and other events.

Uwe Wiest is a Global Senior Architect for Sun Microsystems GmbH and is located in Kirchheim-Heimstetten, Germany. Uwe invented the Infinite Mailbox for Lotus Domino, which then was merged into the new Compliance and Content Management solution portfolio.

Thanks to the following people for their contributions to this project:

John Berglund
Project Leader, International Technical Support Organization, Cambridge Center

Phil Monson
Project Leader, International Technical Support Organization, Cambridge Center

Paul John Dwyer and Krupa Patel
Price Waterhouse Coopers

Gary Greenwood
President, G2 Associates

Shane Kilmon
Advisory Software Engineer, IBM Software Group, Lotus

Marc Luescher
IBM Global Services, Integrated Technology Services

Frank Kushmerek, Dan Parisi, Larry Allard, and Mike Nelson
Sun Microsystems Inc.

Christian Wiest
Field Support, IBM Sales and Distribution

Mel Stull
Infrastructure Team, DaimlerChrysler

Oliver Froemel
IT Consultant, Independent, Germany

Special thanks to the team who wrote *Domino R5.08 on Solaris 8*, SG24-5969, who laid the groundwork and set the pace for this Redbook team:
David Morrison, Uwe Wiest, Rudolf Utzschneider, Eric Dolce, Chris O'Donnell, Carmen Spieker and Valerie Walker.

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will team with IBM technical professionals, Business Partners, and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYJ Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

1

Introduction to IBM Lotus Domino 7 for Sun Solaris

This chapter introduces the reader to Domino 7. A general overview of Domino 7 is provided, along with a brief overview of new features and enhancements of Domino 7 over prior releases. A brief overview of Lotus Notes® 7, and its new features and enhancements, is also provided.

© Copyright IBM Corp. 2006. All rights reserved.

1.1 Domino 7 defined

IBM Lotus Domino combines security-rich messaging, calendar and scheduling capabilities with a robust platform for collaborative applications on a wide variety of operating systems. As a member of the IBM Workplace™ family, Lotus Domino can help you improve the productivity of your people and enable them to share, manage, and organize information more efficiently.

With Lotus Domino 7, IBM extends the reach of Lotus Domino messaging and collaboration solutions while continuing to leverage your IT and application investments. The new version offers capabilities to support more people with fewer servers, to simplify administration and to provide tighter integration with Web standards.

For more information about new features in Domino 7, see:

http://www.lotus.com/products/product4.nsf/wdocs/whatsnewindomino7

1.2 Lotus Notes 7 defined

IBM Lotus Notes, an integrated client option for IBM Lotus Domino server, delivers e-mail, calendar and scheduling capabilities, integrated instant messaging, personal information management (PIM) tools, discussion forums, teamrooms, and reference databases with basic workflow — along with a powerful desktop platform for collaborative applications.

Lotus Notes is available in two offerings: Lotus Notes for Messaging (access to messaging functions) and Lotus Notes for Collaboration (both messaging and applications). An integral part of the IBM Workplace family, Lotus Notes offers employees business-critical collaboration tools designed to help increase organizational productivity and responsiveness.

With Version 7, new integration with IBM Workplace products enables organizations to extend and leverage their existing infrastructure investments. Enhanced instant messaging and Web conferencing integration gives employees immediate access to the people and tools they need to do their jobs more effectively. Productivity enhancements enable users to better manage daily information and resources.

1.3 Lotus Domino 7 family of servers and clients

The Domino server family is an integrated messaging and Web application software platform for growing companies that need to improve customer responsiveness and streamline business processes.

The Domino server family is comprised of three core server licenses:

- Domino 7 Mail Server (mail use only)
- Domino 7 Application Server (mail and application use)
- Domino 7 Enterprise Server (mail, application, and clustering use)

The Domino client family is comprised of three core clients and one additional subcomponent:

- Notes client 7
- Domino Administrator 7
- Domino Designer® 7
- Domino Access for Microsoft® Outlook® and Domino Web Access 7.0 (iNotes™). iNotes is a component of the Domino server.

In addition, the Domino server supports many of the open standards available today, such as HTTP, IMAP, POP, NNTP, SMTP, and LDAP.

1.4 Terminology in Lotus Notes 7

These are some of the most important terms used in Notes/Domino.

> **Attention:** To ensure the full understanding of this book, we strongly encourage you to become familiar with these terms.

Directory Catalog

A compressed version of one or more Domino Directories, which improves the speed of name lookups and name resolution for all organizations.

Domino Directory

The Public Address Book is now referred to as the Domino Directory.

Directory Assistance

The Master Address Book is now referred to as the Directory Assistance.

Domino Enterprise Connection Services

Lotus Domino 7 includes Domino Enterprise Connection Services (DECS) for building live links between Domino pages and forms to data from relational databases.

Transactional logging

Domino allows for 24x7 online server backups and recovery support, in order to eliminate the need to shut down Domino servers for maintenance. A transactional log provides a sequential record of every operation that occurs (sequential writing on a disk is much faster than writing in various places on a disk). Logging helps to ensure complete data integrity for updates and enables you to perform incremental database backups.

Domino Off-Line Services

Domino Off-Line Services (DOLS) provides a way for browser users to take Domino Web applications offline. With a browser, an end user can easily take an application offline, make changes, and synchronize the changes with the online application.

Domino Domain Monitoring (DDM)

Domino Domain Monitoring is one of the new tools that implements great improvements in the way the administrator can monitor a Domino environment. With this new information, you can enable automatic actions to be taken on predetermined events. In other words, this feature gives your Domino server autonomic computing capabilities.

Activity Trends

This powerful analysis tool helps administrators to size system utilization and predict environment growth trends. This ensures that the company is prepared to take the proactive actions and plan projects to expand the Domino platform in order to better support new users and maintain the best uptime possible.

Policies

Policy-based administration helps the administrator maintain a consistent pattern within the organization. It defines a basic set of rules that can be used to enforce a standard configuration within the organization or subsets of it. Policies can be used to set configurations in the users' clients, to standardize user creation, to set up mail archive rules, and to manage client's security settings. New mail and calendar configuration policies were introduced in Version 7, making remote administration easier and more reliable.

1.5 New Notes Domino features

1.5.1 New features introduced in Domino 6

Many new features were introduced in Domino Version 6. For a list of new features, refer to the Lotus Notes/Domino 6 *Upgrade Guide* at:

http://www.lotus.com/ldd/doc/uafiles.nsf/docs/Domino6PR2/$File/upgrade.pdf

1.5.2 New features introduced in Domino 7

- Increased scalability and performance

  Metrics from the IBM development lab (using NotesBench workloads) and statistics from the Lotus Domino 7 beta program show significantly enhanced scalability and performance.

  IBM Lotus Domino 7 uses up to 25% less CPU resources than the Lotus Domino 6.5 server.

  Lotus Domino 7 software can support up to 80% more Lotus Notes users or up to 50% more Lotus Domino Web Access users on the same server hardware.

  For more information, refer to this IBM Lotus Domino 7 performance paper:

  ftp://ftp.lotus.com/pub/lotusweb/product/domino/Domino_7_Performance_Paper.pdf

- New diagnostic tools and autonomic capabilities

  - Domino Domain Monitoring presents a single, feature-oriented view through which administrators can see the status of multiple servers across one or more domains. It presents probable causes, offers possible solutions, and displays correlated events.
  - The Activity Trends feature provides powerful, predictive analysis tools to help administrators predict growth and sizing requirements.
  - Expanded policy-based administration -- policies can be extended to cover mail and calendar settings stored in user mail files; administrators have the option to lock down settings for users who do not need to take advantage of a customized Lotus Notes or Lotus Domino Web Access user experience.

- Security and anti-spam enhancements

  - Security APIs: application programming interfaces for manipulating secure e-mail
  - Option to use 1024-bit RSA encryption keys and 128-bit symmetric keys for Lotus Notes remote procedure call (RPC) protocol

  - Improvements to Lotus Notes ID management
  - Expanded anti-spam features, including use of Domain Name System (DNS) whitelists containing public lists of acceptable sources
  - SMTP disclaimer support for including a company disclaimer in outbound Internet messages
- Expanded interoperability and integration
  - Support to 1.4.2 Java™ VM.
  - Native support for Web services to easily extend and integrate applications with J2EE™ and Microsoft .NET environments, often with less time and effort and using existing skills.
  - Enhanced support for open standards makes for easy integration of Lotus Domino solutions with other members of the IBM Workplace family, including IBM Workplace products and IBM WebSphere® Portal software.
  - The option to use IBM DB2® Universal Database™ as an alternative to Lotus Notes storage facility (NSF) for data storage enables organizations to consolidate their data within a common DB2 store and then integrate it with other applications, including IBM Workplace applications. Using complementary enhancements to IBM Lotus Domino Designer application development tool (a separate product), developers can easily build new applications that blend collaborative services with relational data using Structured Query Language (SQL). For more information, refer to:

    `http://www.lotus.com/products/product4.nsf/wdocs/nsfdb2`
  - LDAP enhancements enable the handling of special characters and improved integration with IBM Lotus products and third-party products. Alias support enables handling of multiple IDs in the Domino Directory or third-party directories.
- Enhanced support for Linux

  Lotus Domino 7 server offers a new Linux technology-based Web administration client that runs on a Mozilla browser. This enables you to implement an end-to-end messaging and collaboration solution based on Linux, using Lotus Domino 7 server on Linux for Intel® or zSeries®, Lotus Domino Web Access 7 client on Mozilla or Firefox for Linux, and the new Linux administration client.
- Enhanced software deployment tools

  Enhancements to the Lotus Notes Smart Upgrade feature help automate the installation and upgrade processes. Administrators are notified through a mail-in database whether the installation or upgrade was successful, delayed, or unsuccessful. Other features include server cluster failover, which switches the Lotus Notes Smart Upgrade function to another server if the first is unavailable; a governor feature, which limits the number of upgrades per hour; and reporting capabilities that detail which users have upgraded to which versions.

- Improved management of rooms and resources

  Lotus Domino 7 software continues to provide enterprise organizations with an effective way to manage conference rooms and meeting resources, such as audio-visual equipment. Improvements to the centralized rooms and resources database include:

  - New Lotus Domino server task to eliminate overbookings and increase efficiency and availability of rooms and resources.
  - Simplified and streamlined templates to enhance the calendaring and scheduling user experience.
  - Enhanced functionality that enables administrators to establish an end date for future reservations.
  - Customizable reminder notices for weekly and daily meetings or events.

  For more information, refer to:

  `http://www.ibm.com/developerworks/lotus/library/rr-nd7`

- Client enhancements

  - ClientIPv6 implementation: Server IPv6 support was introduced inV6. Now clients support this version of the protocol as well.
  - New Notes 7 template: Redesigned to be more user friendly and, with its new intuitive interface, users now can perform actions using a right-click of the mouse.
  - Autosave the editing documents as drafts: This prevents users from losing their work in case of a problem with the workstation.
  - It is also possible to save your client's windows state and recover it next time the Notes client is launched.
  - Resource and Reservation user interface improved for better usability.

1.6 Available platforms

Among Domino's key competitive strengths has always been its support for multiple operating system platforms, and Domino 7 maintains and extends this tradition. The following tables summarize details about the various operating system platforms that support Notes and Domino 7.

Note: Operating system patches, service packs, and other updates are not specified in the tables that follow. Note that operating system vendors frequently release updates. For the most recent information regarding updates, see the Lotus Knowledgebase online at:

http://www.ibm.com/software/lotus/support/

or contact your local Lotus Support representative.

The platforms and operating systems listed in the following tables are applicable to the Notes/Domino 7.0 release, and might not necessarily pertain to other Notes/Domino releases.

Table 1-1 Notes client

	Microsoft Windows 2000	**Microsoft Windows XP**
Supported operating system versions	Microsoft Windows 2000 Professional (See the "Windows service pack requirements" Release Note for Service Pack information.)	Microsoft Windows XP Professional Microsoft Windows XP Tablet PC Edition (See the "Windows service pack requirements" Release Note for Service Pack information.)
Processors supported	Intel Pentium®	Intel Pentium
RAM	128 MB minimum 256 MB or more recommended	128 MB minimum 256 MB or more recommended
Disk space (The minimum amounts are the disk space required for installing default files. More disk space is required if databases are replicated locally or copied locally.)	275 MB required	275 MB required
Monitors supported	Color monitor required	Color monitor required
Protocols supported:		
NetBEUI/NetBIOS[1]	Yes	No (NetBEUI)
NetBIOS over IP[2]	Yes	Yes
NetBIOS over IPX™	Yes[3]	Yes[4]

	Microsoft Windows 2000	Microsoft Windows XP
SPX	No	No
SPXII	No	No
TCP/IP	Yes	Yes
X.PC	Yes	Yes

1. Only Microsoft NetBEUI is supported. Starting with Windows XP, Microsoft has discontinued support of the NetBEUI.
2. Only Microsoft TCP/IP is supported.
3. Both Novell NetBIOS and Microsoft NetBIOS over IPX are supported.
4. Both Novell NetBIOS and Microsoft NetBIOS over IPX are supported.

Table 1-2 Domino Administrator Client, Domino Designer(5)

Platform	**Microsoft Windows 2000**	**Microsoft Windows XP**
Supported operating system versions	Microsoft Windows 2000 Professional (See the “Windows service pack requirements” Release Note for Service Pack information.)	Microsoft Windows 2000 Professional (See the “Windows service pack requirements” Release Note for Service Pack information.)
Processors supported	Intel Pentium	Intel Pentium
RAM	128 MB minimum 256 MB or more recommended	128 MB minimum 256 MB or more recommended
Disk space (The minimum amounts are the disk space required for installing default files. More disk space is required if databases are replicated locally or copied locally)	275 MB required	275 MB required
Monitors supported	Color monitor required	Color monitor required
Protocols supported:		
NetBEUI/NetBIOS[1]	Yes	No (NetBEUI)
NetBIOS over IP[2]	Yes	Yes
NetBIOS over IPX	Yes[3]	Yes[4]

Platform	Microsoft Windows 2000	Microsoft Windows XP
SPX	No	No
SPX II	No	No
TCP/IP	Yes	Yes
X.PC	Yes	Yes

1. Only Microsoft NetBEUI is supported. Starting with Windows XP, Microsoft has discontinued support of the NetBEUI.
2. Only Microsoft TCP/IP is supported.
3. Both Novell NetBIOS and Microsoft NetBIOS over IPX are supported.
4. Both Novell NetBIOS and Microsoft NetBIOS over IPX are supported.

Table 1-3 Domino server (4)

Platform	Microsoft Windows 2000	Microsoft Windows XP
Supported operating system versions	Microsoft Windows 2000 Server Microsoft Windows 2000 Advanced Server (See the “Windows service pack requirements” Release Note for Service Pack information.)	Microsoft Windows 2003 Server Standard Edition; Microsoft Windows 2003 Server Enterprise Edition (See the “Windows service pack requirements” Release Note for Service Pack information.)
Processors supported	Intel Pentium or higher and compatibles	Intel Pentium or higher and compatibles
RAM	256 MB minimum 512 MB or more recommended per CPU	512 MB minimum 512 MB or more recommended per CPU
Disk space	1.5 GB minimum per partition	1.5 GB minimum per partition
Disk swap space	2 times the amount of physical RAM installed	2 times the amount of physical RAM installed
Monitors supported	Color monitor required	Color monitor required
Protocols supported:		
NetBEUI/NetBIOS[1]	Yes	No
NetBIOS over IP[2]	Yes	Yes
NetBIOS over IPX	Yes	Yes
SPX	No	No

Platform	Microsoft Windows 2000	Microsoft Windows XP
SPX II	No	No
TCP/IP	Yes	Yes
TCP/IP IPV6	No	Yes
X.PC	Yes	Yes

1. Only Microsoft NetBEUI is supported. Starting with Windows XP, Microsoft has discontinued support of the NetBEUI.
2. Only Microsoft TCP/IP is supported.

Table 1-4 Domino server

Platform	IBM AIX®(5)	Linux	Sun Solaris
Supported operating system versions	IBM AIX 5.2 IBM AIX 5.3 (see the “AIX patch requirements” Release Note for Service Pack information)	Novell SUSE Linux Enterprise Server (SLES) 8 Novell SUSE Linux Enterprise Server (SLES) 9 (See the “Linux patch requirements” Release Note for Service Pack information.)	Sun Solaris 9 **Sun Solaris 10** (See the “Solaris patch requirements” Release Note for Service Pack information.)
Processors supported	PowerPC®	Intel Pentium or higher and compatibles	UlraSPARC and newer
RAM	512 MB minimum; 512 MB or more recommended per CPU	512 MB minimum; 512 MB or more recommended per CPU	512 MB minimum; 512 MB or more recommended per CPU
Disk space	1.5 GB minimum 1.5 GB or more recommended	1.5 GB minimum 1.5 GB or more recommended	1.5 GB minimum 1.5 GB or more recommended
Disk swap space	Same amount as Physical memory required; recommend 2 times the amount of physical RAM installed	2 times the amount of physical RAM installed recommended	3 times the amount of physical RAM recommended
Monitors supported	Any standard display (local or remote)	Any standard display (local or remote)	Any standard display (local or remote)
Protocols supported:			
NetBEUI/NetBIOS[1]	No	No	No

Platform	IBM AIX®(5)	Linux	Sun Solaris
NetBIOS over IP[2]	No	No	No
NetBIOS over IPX	No	No	No
SPX[3]	No	No	No
SPX II	No	No	No
TCP/IP	Yes	Yes	Yes
TCP/IP IPV6	Yes	Yes	Yes
X.PC	Yes	Yes	Yes

[1] Only Microsoft NetBEUI is supported. Starting with Windows XP, Microsoft has discontinued support of the NetBEUI.
[2] Only Microsoft TCP/IP is supported.
[3] Domino clusters and partitioned server configurations do not support the IPX/SPX protocol. At this time, Lotus does not plan to provide IPX/SPX network support for future releases of these features.

> **Note:** The Domino release notes specify 3 times memory for SWAP space, which might be appropriate for a small Solaris server. See our recommendations for SWAP space in 3.4, “Disk space” on page 24.

Table 1-5 Domino server

Platform	Domino for IBM i5/OS®	IBM z/OS®	Linux on zSeries
Supported operating system versions	IBM i5/OSTM V5R3 (See the “i5/OS system requirements” Release Note for additional information.)	IBM z/OS Version 1, Release 5 and above	Novell SUSE Linux Enterprise Server (SLES) 8 on zSeries (31-bit) Novell SUSE Linux Enterprise Server (SLES) 9 on zSeries (64-bit) (See the “Domino for Linux on zSeries service pack requirements” Release Note for service pack information.)
Processors supported	IBM iSeries™ server based on PowerPC (RISC) technology eServer™ i5 model 520 or higher	Any that supports your release level of z/OS	Any that supports your release level of Linux on zSeries
RAM	288 MB minimum; 512 MB or more recommended	1 GB minimum; 2 GB or more recommended	1 GB minimum 2 GB or more recommended

Platform	Domino for IBM i5/OS®	IBM z/OS®	Linux on zSeries
Disk space	1.6 GB minimum 2 GB or more recommended	1.6 GB minimum 2 GB or more recommended	2.5 GB minimum 2.5 GB or more recommended
Disk swap space	N/A	N/A	N/A
Monitors supported	Any standard display (local or remote)	Any standard display (local or remote)	Any standard display (local or remote)
Protocols supported:			
NetBEUI/NetBIOS[1]	No	No	No
NetBIOS over IP[2]	No	No	No
NetBIOS over IPX	No	No	No
SPX[3]	No	No	No
SPX II	No	No	No
TCP/IP	Yes	Yes	Yes
TCP/IP IPV6	No	Yes	Yes
X.PC	No	No	No

1. Only Microsoft NetBEUI is supported. Starting with Windows XP, Microsoft has discontinued support of the NetBEUI.

2. Only Microsoft TCP/IP is supported.

3. Domino clusters and partitioned server configurations do not support the IPX/SPX protocol. At this time, Lotus does not plan to provide IPX/SPX network support for future releases of these features.

4. If you are running with DB2 as the Domino datastore, then you must add additional DB2 install requirements. DB2 8.2 is supported. For additional install requirements, see “Setting up and using Domino 7 and DB2” in the Domino Administrator Help.

5.The 64-bit kernel must be installed and in use on these systems, even though the OS is 32-bit. The use of the 32-bit kernel is no longer supported on these platforms. See the OS vendor documentation for questions about enabling and using the 64-bit kernel. (On Solaris, the 64-bit kernel is used by default on supported hardware; this is not the case for AIX.)

1.6.1 Domino Web Access system requirements

For the most current Domino Web Access system requirements, refer to the release note titled “Domino Web Access system requirements.” You can search for it at:

`http://www.ibm.com/`

As of this book’s publish date:

- Client operating systems
  - Microsoft Windows 2000 Professional
  - Microsoft Windows XP
- Client operating systems for Mozilla
  - Novell SUSE Linux Enterprise Server (SLES) 8
  - Novell SUSE Linux Enterprise Server (SLES) 9
- Supported browsers
  - Win32® Internet Explorer 6.0, or higher
  - Mozilla 1.4.1 and 1.7.x (Linux clients only)
  - Mozilla Firefox 1.0.x on Win32 and Linux (supported by the DWA7 mail template only; not supported by iNotes6 templates)

  Any attempt to access Lotus Domino Web Access through an unsupported browser will result in the display of an unsupported browser notice. Netscape 4.x users might see hangs or crashes when encountering the Lotus Domino Web Access unsupported browser page. If you are a Netscape 4.x user and you encounter these problems, you should open your mail file using the WebMail UI directly through the &ui=webmail switch. This is documented in the topic “Switching to WebMail” in the Lotus Domino Web Access help.

  > **Note:** Lotus Domino Web Access will not work if JavaScript™ is disabled or if session cookies are disabled.

- Certified proxy servers
  - SunOne Portal Server 6.2
  - IBM WebSphere Edge Server 2.0.2 efix 49
  - Tivoli® Access Manager 5.1
- Adobe Acrobat
- Adobe Acrobat Reader, Version 4.0, or higher, to print calendars

2

Introduction to Solaris 10

Solaris 10 is the latest version of Sun's flagship operating system, offering complete binary compatibility with earlier versions along with a wider choice of hardware platforms. Solaris 10 also enhances many features of earlier versions and introduces a large suite of entirely new capabilities. This section describes some enhancements and new features of particular interest for IBM Lotus Domino installations.

For a more comprehensive list of new features in Solaris, visit:

http://www.sun.com/software/solaris/features.jsp

© Copyright IBM Corp. 2006. All rights reserved.

2.1 What's new in Solaris 10

For general information about these and other Solaris 10 features, visit:

http://www.sun.com/software/solaris/

Additional technical information can be found at:

http://www.sun.com/bigadmin/

2.1.1 Enhanced performance

The entire TCP/IP network protocol stack has been rewritten for higher throughput and lower latency. Interactive users benefit from quicker response times, and replications and other large-volume data transfers take advantage of increased throughput.

The performance of systems with large numbers of network connectors has been improved, and support for high-bandwidth 10Gb Ethernet has been added.

Support for processors using chip multithreading (CMT) and other high-throughput enhancers has been improved. Memory placement optimization (MPO) and support for large memory pages help keep the processors busy doing computations instead of waiting for data from system memory.

Support for multi-threaded applications such as Domino has been made more efficient, continuing the progress made in Solaris 8 and Solaris 9.

2.1.2 File system enhancements

The UNIX File System (UFS) in Solaris 10 supports file systems of multi-terabyte capacity. With UFS metadata logging, a file system can be brought back online after a system crash without a file system check, thus shortening reboot time.

2.1.3 Observability

The Solaris 10 feature DTrace enables developers and system administrators to observe a system's behavior in unprecedented detail with minimal overhead and maximal convenience. Other tools exist for monitoring activities inside Domino or inside the Solaris kernel; DTrace can see into both worlds simultaneously and reveal how they interact. Thus, it makes available a wealth of new information for troubleshooting and performance tuning.

For more information, visit:

http://www.sun.com/bigadmin/content/dtrace

2.1.4 Management

Solaris 10 containers (*zones*) can isolate applications from each other and from the system as a whole. An application that misbehaves or is compromised cannot gain access to devices outside its container or write to file systems it does not own; in short, its mischief is confined to its own container.

Solaris Resource Manager can apportion system resources among containers, allowing the system administrator great control for meeting level-of-service requirements. An application that goes into an infinite loop cannot steal CPU time or network bandwidth and thus starve applications running in other containers.

Solaris' Service Management Facility (SMF) enables an application to declare what services it provides and what services it requires in order to operate. With this knowledge, Solaris can start and stop services in a controlled and coherent manner, during system boot or shutdown and in response to hardware faults.

2.1.5 Predictive Self-Healing

Sun Microsystems has developed a new architecture for building and deploying systems and services that are capable of Predictive Self-Healing. Self-healing technology enables Sun systems and services to maximize availability when software and hardware faults occur. In addition, the self-healing technology facilitates a simpler and more effective end-to-end experience for system administrators and service providers, thereby reducing costs. The first major set of new features to result from this initiative is available in the Solaris 10 OS. The Solaris 10 software includes components that facilitate self-healing for CPU, memory, I/O bus nexus components, and system services.

Specific details about the components of this new architecture are covered in "Solaris Service Manager" on page 380 and "Solaris Fault Manager" on page 380.

2.1.6 Other new features

Domino 7 supports Solaris 9 in addition to Solaris 10, so it avoids relying on some new Solaris 10 features not found in older versions. Although Domino 7 does not exploit these features as we write this book, some are under consideration for use in future Domino versions:

- Event Ports enable an application such as Domino to monitor many network connections efficiently, a task present-day Domino performs by adding modules to the Solaris kernel. If a future Domino uses event ports instead, it could run without adding super-privileged kernel code to the system.

- Process Rights Management goes beyond the traditional UNIX all-or-nothing privilege model, where the `root` user has all privileges and other user accounts have none. Fine-grained privilege control could enable Domino to operate without the set-UID privileged components it uses today.
- Secure Execution allows (among other things) digital signatures to be applied to program files and libraries, so Solaris can verify that they have not been tampered with before allowing them to execute.

Consult Domino's release notes to learn what Solaris 10 features future Domino versions support.

3

Sizing guidelines for IBM Lotus Domino Messaging Server

This chapter discusses some sizing guidelines to ensure that your organization's Domino Messaging Server provides optimum utilization and throughput.

Note that these guidelines apply only to Domino servers whose primary functions are messaging, calendaring, and scheduling — not to Domino operating as a general-purpose Web server, an application platform, and so on.

Also keep in mind the pace of development in computer architecture and implementation. Every few months brings a newer and more capable CPU, a faster network, or some other improvement. The methods discussed in this chapter remain valid, but the numbers given for CPU capacity and the like will become outmoded. Consult your Sun representative for up-to-date information about newer product offerings.

© Copyright IBM Corp. 2006. All rights reserved.

3.1 Describe the users

A Domino Messaging Server exists to handle the demands of its users, so much of the work in producing a size estimate consists of gathering information about the user population. Provide estimates of the most demanding user population the system will serve during its lifetime, which might not be the same as the load it faces at initial installation.

Experience shows that a group of users can be characterized by three pieces of information: the type of client they use (different clients make different demands on the server), the size of their mail databases (larger databases make Domino work harder and usually belong to more active users), and their concurrency (the fraction of users accessing the server simultaneously). Concurrency is perhaps the hardest of these factors to estimate. It is the fraction of users who actively use the server in a typical 15-minute period during the peak usage hours. Most users do not spend all of their time working with their mail, and they place very little load on the server at other times even if they remain logged in. Concurrency rates in office settings are typically between 30% and 40%, to which you should add another 5% or 10% as a safety margin. If in doubt, estimate 40% concurrency plus a 10% safety margin for a total of 50%.

Table 3-1 User population worksheet

Mail client type	Load factor	Light users (50-100 MB)		Medium users (100-300 MB)		Heavy users (> 300 MB)	
		Count	Load	Count	Load	Count	Load
Lotus Notes (R5 or later)	1						
Domino Web Access (iNotes)	2.5						
Microsoft Outlook	1.5						
Internet clients (IMAP or POP)	2						
Total Load:							
Concurrent Load:							

Table 3-1 is a worksheet to help you organize this information. Fill it in as follows:

1. Group the users according to their mail database sizes, which indicate the users' level of activity. Databases of 50 MB to 100 MB suggest light usage,

100 MB to 300 MB is the medium or typical range, and databases larger than 300 MB usually belong to heavy power users.

2. For each client type, fill in the number of light, medium, and heavy users in the appropriate Count column.
3. Multiply each user count by the Load Factor for its client type, and enter the product in the adjacent Load column.
4. Total the three Load columns and enter the sums in the Total Load row.
5. Multiply the three total loads by the concurrency rate and enter the products in the Concurrent Load row.

3.2 Determine CPU and memory requirements

Table 3-2 Computing resources worksheet

	Light users	Medium users	Heavy users
Concurrent Load from Table 3-1			
Load per CPU from Table 3-3			
Quotients			

Table 3-2 is a worksheet to help you determine the computational resources your user population requires. Complete it as follows:

1. Enter the Concurrent Load values from Table 3-1 on page 20 in the first row of Table 3-2.
2. Select a CPU model from Table 3-3 on page 22. (The table describes both current UltraSPARC processors and older models that might be found in existing equipment being repurposed.) Enter the Concurrent Load per CPU values from Table 3-3 on page 22 in the second row of Table 3-2.
3. Divide each of the first row's values by the corresponding value from the second row, and enter the quotients in the third row.
4. Add the three quotients. If the system is the active member of an active-standby Domino cluster (but *not* if it is a free-standing system or a standby system or a member of a load-balanced cluster), multiply the total by 1.25 to allow for cluster overhead. See 7.1, "Domino cluster components" on page 228.
5. Round the total up as needed. In some Sun machines the processors must be installed in pairs or in groups of four; your Sun representative can provide details. This is the number of CPUs of the chosen type you should configure.

6. Finally, multiply the CPU count by the Memory per CPU value from Table 3-3 for the chosen processor; this is the minimum amount of RAM that is required, in gigabytes.

This calculation yields the grand total processor count and memory size required. You may choose to install these resources in a single machine, or to apportion them among several smaller machines.

Table 3-3 UltraSPARC processor characteristics

Processor model	Concurrent load per CPU			Memory per CPU (GB)
	Light users	Medium users	Heavy users	
UltraSPARC T1, 1.2 GHz (8)[a]	17150	12840	9660	32
UltraSPARC T1, 1 GHz (8)[a]	14290	10700	8050	32
UltraSPARC T1, 1 GHz (6)[a]	10710	8010	6030	32
UltraSPARC T1, 1 GHz (4)[a]	7140	5340	4020	16
UltraSPARC IV+, 1.5 GHz[b]	3880	2920	2180	4
UltraSPARC IV, 1.35 GHz[b]	2500	1870	1410	4
UltraSPARC IV, 1.2 GHz[b]	2280	1710	1280	4
UltraSPARC IV, 1.05 GHz[b]	2000	1490	1120	4
UltraSPARC IIIi, 1.6 GHz	1510	1130	850	2
UltraSPARC IIIi, 1.5 GHz	1420	1060	800	2
UltraSPARC IIIi, 1.35 GHz	1280	960	720	2
UltraSPARC III Cu, 1.2 GHz	1240	930	700	2
UltraSPARC III Cu, 900 MHz	1030	780	580	2
UltraSPARC III, 750 MHz	860	650	480	2

a. The UltraSPARC T1 CPU is available with four, six, or eight “processor cores.”
b. Each UltraSPARC IV or UltraSPARC IV+ CPU has two “processor cores.”

3.3 Determine partition and domain counts

Table 3-4 Domino partition worksheet

	Light users	Medium users	Heavy users
Concurrent Load from Table 3-1			
Load per Domino partition	1800	1500	1200
Quotients			

There is a limit to the amount of concurrent load a single Domino instance can handle, so you might have to run multiple instances, or *Domino partitions*, to serve the user population described in the preceding section. (See Chapter 8, “Partitioning” on page 251.) Table 3-4 is a worksheet to help you compute the minimum required partition count. Complete it as follows:

1. Enter the Concurrent Load values from Table 3-1 on page 20 in the first row of Table 3-4.
2. Divide each value in the first row by the number in the second, and enter the quotients in the third row.
3. Add the three quotients and round up to the next whole number; this is the minimum number of Domino partitions your user load requires.

There are several reasons why you might want to configure more than the minimum number of Domino partitions. You might wish to separate the users along departmental bounds (so Finance, Sales, and R&D have their own partitions), or by time zone (to facilitate maintenance using a follow-the-sun approach), or to satisfy other administrative needs. Certain clustering topologies (see 7.1, “Domino cluster components” on page 228) might suggest the use of additional partitions.

A best practice is to keep the number of Domino partitions on a single Solaris instance to eight. This varies depending on the size and speed of the machine, the types of loads the Domino partitions handle, and many other factors that are hard to characterize. A conservative general rule is that eight active Domino partitions will run well on a single *Solaris domain*. It is safe to run more than eight partitions if the extras are lightly loaded: administrative servers, backup partitions, and so on do not put a lot of stress on Solaris. However, if you choose to run, say, 12 partitions, it would be prudent to divide them between at least two domains.

These Solaris domains can be on separate machines, or (on some models) they can run independently in a single larger machine. Consult your Sun representative for information about servers capable of hosting multiple domains.

3.4 Disk space

A Domino server requires disk space for many purposes. It is useful to consider the disk space in three broad categories:

- Disk space for Solaris itself, for Domino's program files, and for the so-called "swap" area.
- Disk space for the Domino data directories and the users' mail databases.
- Disk space for the Domino partitions' transactional log files.

The following subsections consider each of these purposes in turn, and 3.4.4, "Using RAID for data protection" on page 26 discusses the additional requirements of high-availability RAID configurations.

3.4.1 Solaris, programs, and "swap"

For a full installation of Solaris, each Solaris domain requires a minimum of 5 GB of disk space, but 12 GB is recommended. This can be reduced a bit if you decide to install less than a full installation.

Each installed Domino version needs an additional gigabyte for the program directory.

It would be possible to squeeze Solaris and the Domino programs into about 6 GB, but giving the system more breathing room will gain flexibility: easier installation of Solaris patches, the ability to install multiple Domino versions simultaneously, and so on. In addition, future releases of Solaris and Domino might take more space than the current releases. Considering the ever-diminishing cost of furnishing a gigabyte of disk storage, it should be no hardship to allocate 16 or more gigabytes for this purpose.

Each Solaris domain also requires what is still called "swap" space, although the name no longer truly describes how the space is actually used. For a Domino server, the swap space should be roughly one-third the size of the Solaris domain's physical memory, but not less than 2 GB. Thus, a machine with 4 GB of memory should have 2 GB of swap space, while a machine with 32 GB of memory should have 11 GB of swap.

Note that at the time this book was written, the Domino 7 release notes specify that swap should be three times physical memory. It has been our experience with Solaris 9 and Solaris 10 that this large amount is no longer required. It will not hurt to configure swap to three times the physical memory, but we believe that this is overkill.

3.4.2 Domino directories and databases

A Domino partition requires about 1 GB of disk space for its data directory, which contains essential server databases such as names.nsf and mail.box. This much space suffices for organizations of up to a few thousand registered users. For larger organizations, estimate an additional 25 MB per thousand users and scale up accordingly.

If you are running multiple partitions, each requires its own data directory, so multiply the per-partition space by the partition count to get the grand total space required. It is an excellent idea to keep the various partitions' data directories on different disk volumes, so that one partition's I/O traffic does not interfere with another's.

The users' mail databases also require disk space. Add up the total size of all users' mail databases (or refer to Table 3-1 on page 20 and estimate 100, 300, or 500 MB for each light, medium, or heavy user) to estimate the total space required.

Domino's data directories and databases can reside on any file system Solaris supports. The amount of space required for file system metadata differs from one file system to the next, as does the amount of slack space required for good performance. Most, though, require no more than 10% for file system metadata, and will not suffer overcrowding until the disks become more than 80% full. To allow for this expansion, multiply the total Domino space by 1.1 and divide by 0.8 (or equivalently, add three-eighths to the nominal Domino size to compute the recommended raw disk space). If you have more specific information about the particular file system you intend to use, you might be able to refine this estimate, but unless you are sizing a very large system, the difference is not likely to amount to much.

To summarize the steps to size your Domino data directory space:

1. Start with 1 GB per Domino partition plus adjustments for large user counts.
2. Add the estimated space for your users' mail files and Domino application databases.
3. Multiply by 1.1 to accommodate file system metadata.
4. Divide by .80 to ensure good file system performance by keeping the disks below 80% full.

3.4.3 Domino transactional logs

Domino transaction logs are an optional feature. Our best practices recommend that you use Domino transaction logs as it will reduce the time required to recover from an abnormal Domino shutdown.

Each Domino partition records changes to its databases in a transactional log. This enables Domino to maintain the integrity of its databases in the event of a power loss or other uncontrolled shutdown and to restart quickly after such a failure. The transactional logs can also participate in some backup strategies (see Chapter 13, “Backup strategy for IBM Lotus Domino 7 on Solaris” on page 419) to enable backups to be taken while Domino is running.

Proper configuration of transactional logs is not usually a question of space, but of I/O bandwidth. Because all database changes must flow through the transactional logs, it is clear that the logs must sustain quite a high level of activity. Think about it: all the output that is distributed across your multi-terabyte SAN configuration must first be written to the transactional log.

We include this to convince you that you should not listen to someone who says that it is wasteful to devote a 73 GB drive to 4 GB of log data. Equally, you should not listen to anyone who proposes to virtualize the log volumes by striping them across disks that are shared with other activities. The authors of this book have seen such penny-pinching at far too many installations, and have seen the misery that this false economy can cause.

The lesson, then, is simple: Use your very fastest disk subsystem for Domino’s transactional logs. A disk operates at its fastest if the access arm seldom needs to move, which is why you should dedicate a disk to each partition’s log: if the access arm is always being yanked away from where Domino needs it, everything will slow down badly. If possible, attach the log disks to the server through a dedicated controller, or at least through a controller that is not shared with the data disks.

3.4.4 Using RAID for data protection

RAID technology uses additional disk space to protect disk-resident data against disk failures and to provide higher performance than single disks can achieve. RAID configurations come in several types or *RAID levels*, three of which are commonly used with Domino servers:

- *RAID-1* or *mirroring* protects against disk failure by making two copies of all of the data, one on each disk of a *mirrored pair*. RAID-1 offers excellent data protection and some performance benefits, at the cost of doubling the number of disks required to store a given amount of data.
- *RAID-10* or *striped mirrors* (more formally known *RAID-1+0*) combines several RAID-1 mirrored pairs into a *stripe*, a sort of very large super-disk. RAID-10 offers data protection, high capacity, and high performance, but, as with RAID-1, it doubles the required number of disks.
- *RAID-5* uses one disk’s worth of parity information to protect the data of *N* disks, so the space required is only *N*+1 disks’ worth instead of the *N*+*N*

required by RAID-1 and RAID-10. RAID-5 performs well when all drives are functioning, but performance suffers when a disk fails. The performance penalty is severe if *N* is large, so RAID-5 stripes should usually be limited to no more than six or seven disks altogether, for five or six disks' worth of data storage.

Any of these RAID technologies can be *host-based*, meaning that Solaris takes responsibility for issuing the actual I/O commands to the individual disks, or *controller-based*, meaning that Solaris issues single I/O commands to a RAID-aware controller that in turn handles the individual disk I/O. Either mode is suitable for RAID-1 or RAID-10; for performance reasons it is recommended that RAID-5 be used only in controller-based configurations. For all RAID levels, controller-based RAID will offer higher performance, often significantly higher.

The disk space devoted to Solaris, programs, and swap should usually be protected with a RAID-1 mirror, either host-based or controller-based.

The Domino data directories and mail databases usually occupy a large amount of space, so economical RAID-5 is usually the appropriate solution. Use three to six disks' worth of data to one disk's worth of parity; longer stripes will perform very badly when a disk fails, and shorter stripes are not very economical. As mentioned above, RAID-5 should always be controller-based, never host-based.

If controller-based RAID-5 is not available or if the server is small enough that the economies of RAID-5 are not too urgent, you might wish to consider host-based or controller-based RAID-10 for the Domino data directories and mail databases.

We recommend dedicating a controller-based RAID-1 mirror to each partition's transactional logs. Doubling the disk requirement is not expensive because the logs are usually not large, and the high performance of a controller-based solution avoids making Domino wait for log I/O. Host-based RAID-1 is possible but far less attractive because its performance is noticeably poorer. Failing to use RAID protection is a *very* bad idea; keep in mind that after an unplanned shutdown the transactional logs hold data that has yet to be written to the databases, so that data must be protected at least as well as the databases themselves.

Putting it all together:

- Solaris will require one RAID-1 mirrored pair.
- Each Domino partition requires a RAID-1 pair for its transactional logs.
- If you use RAID-10 for the data disks, you have to provide twice as much disk space as the earlier calculations suggest.
- If you use RAID-5 for the data disks, you must provide one-sixth more disk space (for a 6+1 stripe) up to one-third more (for a 3+1 stripe).

3.5 Network I/O sizing

A Notes user connected to a Domino server over a LAN generates roughly 4 KB to 6 KB per second of network traffic while actively using the system. Some primary factors that contribute to this:

- Bandwidth requirement for initial Notes client launch
- Bandwidth requirement for steady-state Notes client usage
- Bandwidth requirement for Calendaring and Scheduling services
- Bandwidth requirement for Lotus Sametime®

Even if half of the nominal bandwidth is consumed by protocol overhead, a switched LAN running at 100 Mbps in each direction can easily sustain 12,000 or so concurrent users. In short, the bandwidth of the server's network connection is rarely a concern. You might choose to use multiple network connections on a server for fail-over purposes, but it will seldom be necessary to do so for capacity reasons.

However, it is likely that some users' communications with the server travel over slower links whose capacity might impose limits. For example:

- A shared (rather than switched) Ethernet branch with a nominal capacity of 10 Mbps can deliver only about half of its nominal rate before serious congestion sets in. Again assuming 50% protocol overhead, 600 active Notes clients would pretty much saturate this network segment.
- A wide-area network using a T1 line at a nominal 1.5 Mbps can only handle about 150-180 active Notes users, again assuming 50% overhead for network protocols.

Network topologies are extremely diverse, and it is not possible to describe them all here. As you analyze your own network or proposed network, look for the slowest link in the path between each user and the server, consider how many users share that link, and apply the 4-6 KBps per user estimate to see whether the link has adequate capacity.

If you use Domino clustering (see 7.1, "Domino cluster components" on page 228), it is a good idea to keep the server-to-server traffic on a network separate from that used to communicate with the users. This second, private network can also be useful for administrative purposes such as server monitoring, communicating with the control consoles of the servers and disk arrays, and so on. A LAN operating at 100 Mbps is more than adequate for the replication traffic in most clusters; the administrative traffic volume is negligible.

4

Solaris 10 installation, configuration, and considerations

The following steps are required set up IBM Lotus Domino on a Sun Solaris server:

1. Size the proper server and storage.
2. Define:
   a. Network host names, IP addresses, and so forth
   b. Solaris group for the Domino partitions
   c. Solaris accounts for the Domino partitions
   d. File system and directory names
3. Install the server and storage hardware.
4. Install Solaris.
5. Configure Solaris including:
   a. Installing patches
   b. Configuring file systems
   c. Configuring the network
   d. Creating a group and accounts for Domino
6. Install Domino.
7. Set up and configure Domino.

© Copyright IBM Corp. 2006. All rights reserved.

In this chapter our primary focus is items 2 on page 29 through 5 on page 29. We discuss the Solaris 10 features and configuration options that relate to Domino.

After you have selected the memory, disk space, and CPU, you must configure your system correctly to be able to work optimally with Solaris and the Domino server. We describe in detail the things that should be done prior to installing and setting up Domino.

This chapter includes the following topics:

- Pre-installation checklist information describing our Redbooks Lab for the examples
- Solaris patch considerations
- Operating system considerations
- Network configuration
- File system layout
- Creating a Solaris group and user accounts for Domino
- Setting owner and group for Domino transaction logs
- Moving applications from Windows to Solaris

4.1 Pre-installation checklist

Prior to starting the installation of Solaris and customizing the installation for your site, you need to decide several configuration items. We provide more details describing our lab examples in the sections that follow.

We want to introduce you to a summary of the kinds of things you need to know to set up your environment. Often another group within your organization can quickly provide you with the required information based on standards and policies that have been developed for all servers in the organization.

The information you need includes:

1. General Solaris settings and policies including:
   a. Time zones
   b. Language
   c. Password for and restrictions on the root account
2. Storage layout for Solaris and Domino including naming conventions, space requirements, types of file systems, and RAID levels for:
   a. Solaris operating system files
   b. Solaris account home directories
   c. Domino program directories
   d. Domino data directories and, optionally, sub-directories
   e. Domino transaction logs
3. Network topology including:
   a. Host names and IP addresses
   b. Private and public networks for users, clusters, administration, and so forth
   c. Directory services
   d. Routing
4. Solaris group for the Domino partitions
5. Solaris accounts for the Domino partitions

4.2 Brief description of installing Solaris

It is beyond the scope of this book to show all the steps involved with installing Solaris from scratch, but we want to provide an overview of the process. Refer to the documentation that came with your server and Solaris for more information. You can also find detailed documentation and help at:

`http://docs.sun.com`

`http://www.sun.com/bigadmin`

The examples in this book assume that the initial installation of Solaris has already been done and during installation a portion of the network was set up (in particular, the first host name for each server).

4.2.1 Server console

Prior to installing Solaris, you need access to the server's console. This can be accomplished several ways, depending on the specific server you have purchased. Refer to the documentation that arrived with your server or online at:

`http://docs.sun.com`

Some common methods include:

- Terminal attached to the server's serial console port
- Terminal emulator on a PC or workstation's COM port to the server's serial console port
- Graphics hardware, keyboard, mouse installed on the server
- Terminal server port to the server's console port
- Telnet session over a network to the server's Net Mgt port

4.2.2 Installing Solaris

Methods for installing Solaris include:

1. Pre-installed by Sun at the factory. When you power up the server for the first time, you have to answer several Solaris configuration questions, including:
    a. Language
    b. Time zone, date, time
    c. Network configuration
    d. Root password

2. Install from DVDs. The procedure might vary based on your server but the basic procedure is:

   a. Place the first Solaris 10 DVD in the DVD drive.

   b. At the server's console, boot the DVD with the **`boot cdrom`** command from the server's system control prompt, which is usually `OK>`.

   c. You will also have to answer questions about your disk or disks and which options you want to install.

   d. Depending on how you answer the questions, you might be prompted to insert the Solaris 10 Additional Software DVD and the Solaris 10 Documentation DVD.

3. Over the network from a Solaris install server, which is often know as a *jump start server*. In this case, a Solaris install server has been configured and set up on your network. The organization has already defined which Solaris options, patches, and other software have to be installed. The administrator will register the new server and decide which configuration profile is appropriate. Usually all you need to do is **`boot net`** from the system control prompt while at the server's console.

4. By way of a Provisioning System, which is being used by the organization to manage the installation and deployment of systems within the organization.

4.2.3 Restrictions on the root account

The root account is the Solaris Super User. This account has access to all local file systems and system administration commands. It is important that you protect the password for this account to avoid potential security issues. By default, after the initial installation of Solaris, there are restrictions on the root account. Root can only log on to the server's console and cannot be used to FTP into the server.

It is good practice to have these restrictions. We recommend that users log on to the server using their own Solaris accounts and then use the **`su`** command (become super user or another user) if they need to be the root account for some maintenance function. All successful and unsuccessful executions of **`su`** are recorded in the /var/adm/sulog file.

In this example from one of our lab servers, the user typed:

```
more /var/adm/sulog
```

The + character in the fourth column of the output indicates that the **`su`** was successful:

```
SU 10/27 15:57 + pts/7 root-sol1a
SU 10/28 10:25 + pts/1 root-sol1a
SU 10/28 10:25 + pts/1 root-root
SU 10/28 10:26 + pts/1 root-sol1a
SU 11/02 13:19 + pts/4 sol1a-root
SU 11/03 12:52 + pts/5 root-sol1a
SU 11/03 12:55 + pts/4 root-sol1a
SU 11/05 10:44 + pts/4 sol1a-root
```

You can also use the Solaris 10 user roles feature to restrict what a user can do.

Chapter 10, “Security” on page 331 has more information about security.

You might want to temporarily allow root to log on over the network:

1. Log on as the root account.
2. **cd** to `/etc/default`
3. Edit the login file to comment out the line that starts with `CONSOLE`. Place a `#` character in front of this line.

This is a segment of the /etc/default/login file with CONSOLE commented out:

```
root@dom1b # cd /etc/default
root@dom1b # more login
#ident  "@(#)login.dfl  1.14    04/06/25 SMI"
#
# Copyright 2004 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.

# Set the TZ environment variable of the shell.
#
#TIMEZONE=EST5EDT

# ULIMIT sets the file size limit for the login.  Units are disk blocks.
# The default of zero means no limit.
#
#ULIMIT=0

# If CONSOLE is set, root can only login on that device.
# Comment this line out to allow remote login by root.
#
#CONSOLE=/dev/console

# PASSREQ determines if login requires a password.
#
PASSREQ=YES
--More--(23%)
```

You might wish to temporarily allow root to use FTP. To do this:

1. Log on as root.

2. **cd** to `/etc/ftpd`
3. Edit ftpusers to comment out the root line with one or more #s.

This is how /etc/ftpd/ftpusers looks on our lab servers:

```
root@dom1a # cd /etc/ftpd
root@dom1a # cat ftpusers
# ident "@(#)ftpusers   1.5     04/02/20 SMI"
#
# List of users denied access to the FTP server, see ftpusers(4).
#
###root
daemon
bin
sys
adm
lp
uucp
nuucp
smmsp
listen
gdm
webservd
nobody
noaccess
nobody4
```

4.3 Solaris patch considerations

From time to time, Sun provides fixes and updates to Solaris and its components, both as individual patches and as clusters containing entire suites of patches. Some patches might be required by Domino for proper operation; others are recommended by Sun for reasons of performance or security. This section explains how to determine what patches are needed, how to obtain them, and how to install them.

> **Note:** If your system is covered by a Sun Service Plan, you can use the Sun Update Connection to automate many of the manual procedures described in this section. For more information about the Sun Update Connection, visit:
>
> `http://www.sun.com/service/sunupdate/`
>
> Contact your Sun representative for information about service plans.

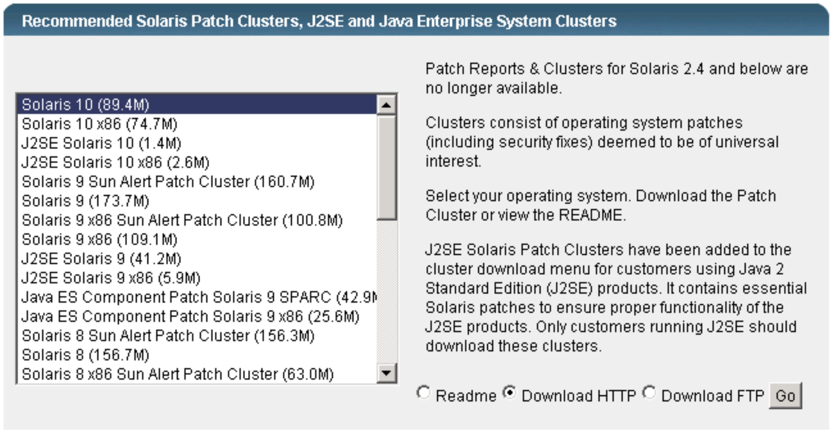
4.3.1 Patches recommended by Sun

To help ease the drudgery of keeping your system updated, Sun collects the most important and widely applicable patches into *patch clusters* that can be downloaded as a unit and installed with a single command. It is good practice to install Sun's latest recommended patch cluster before installing Domino for the first time. When the system is put into service, the choice of whether to keep it up-to-date by applying new patch clusters or by applying individual patches is a matter for your own system administration policies to decide.

To find the patch clusters that Sun recommends for all Solaris systems, visit:

`http://sunsolve.sun.com/`

1. Read and accept the terms of use, then click **Patches and Updates** on the next page and **Recommended Patch Clusters** on the following page.
2. Choose the appropriate patch cluster and download method as shown in Figure 4-1 and click **Go** to begin the download. Save the cluster archive (which usually has a name such as `10_Recommended.zip`) in any convenient directory.



Recommended Solaris Patch Clusters, J2SE and Java Enterprise System Clusters

Solaris 10 (89.4M)
Solaris 10 x86 (74.7M)
J2SE Solaris 10 (1.4M)
J2SE Solaris 10 x86 (2.6M)
Solaris 9 Sun Alert Patch Cluster (160.7M)
Solaris 9 (173.7M)
Solaris 9 x86 Sun Alert Patch Cluster (100.8M)
Solaris 9 x86 (109.1M)
J2SE Solaris 9 (41.2M)
J2SE Solaris 9 x86 (5.9M)
Java ES Component Patch Solaris 9 SPARC (42.9M
Java ES Component Patch Solaris 9 x86 (25.6M)
Solaris 8 Sun Alert Patch Cluster (156.3M)
Solaris 8 (156.7M)
Solaris 8 x86 Sun Alert Patch Cluster (63.0M)

Patch Reports & Clusters for Solaris 2.4 and below are no longer available.

Clusters consist of operating system patches (including security fixes) deemed to be of universal interest.

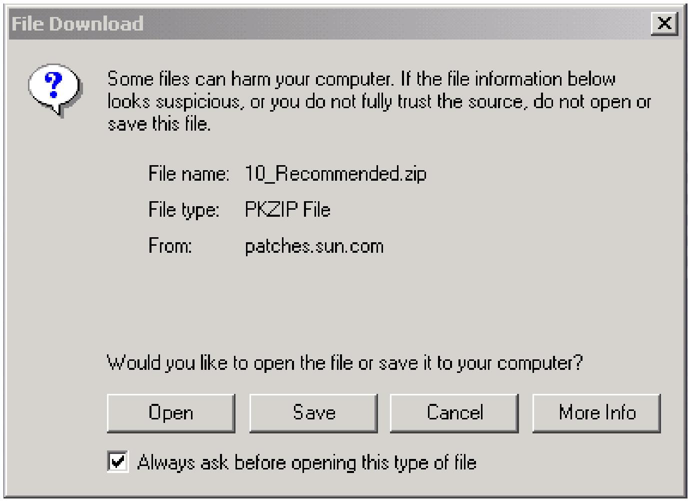
Select your operating system. Download the Patch Cluster or view the README.

J2SE Solaris Patch Clusters have been added to the cluster download menu for customers using Java 2 Standard Edition (J2SE) products. It contains essential Solaris patches to ensure proper functionality of the J2SE products. Only customers running J2SE should download these clusters.

○ Readme ● Download HTTP ○ Download FTP Go

Figure 4-1 Downloading a patch cluster

3. Select **Save** on the next window (Figure 4-2).



Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: 10_Recommended.zip

File type: PKZIP File

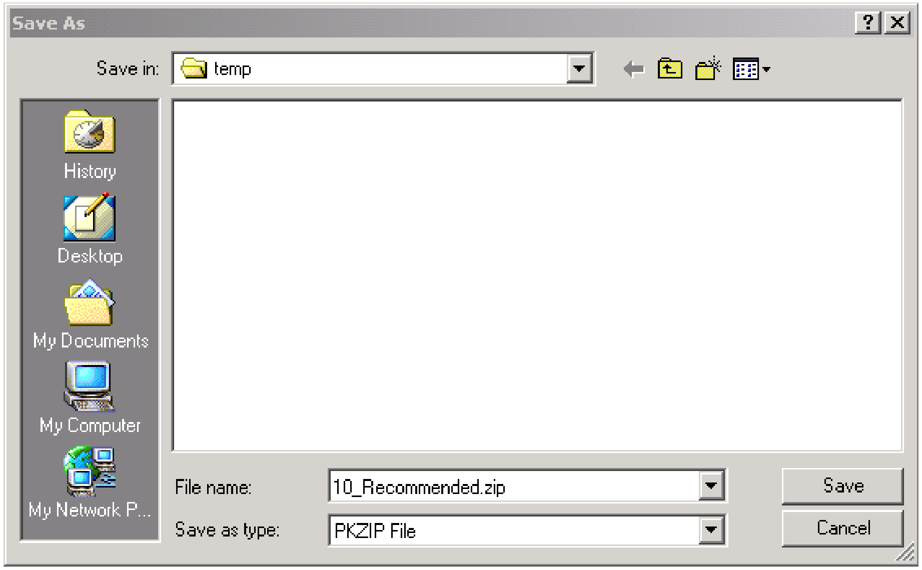
From: patches.sun.com

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

Figure 4-2 Downloading a patch cluster

4. Select a location to save the patch cluster (Figure 4-3).



Save in: temp

File name: 10_Recommended.zip

Save as type: PKZIP File

Figure 4-3 Downloading a patch cluster step 4

5. When the download completes, move it to your Solaris server if you did not directly download to the server.

6. Unpack the archive in a working directory. We picked /tmp as our working directory. `/directory` is the location of the patch cluster.

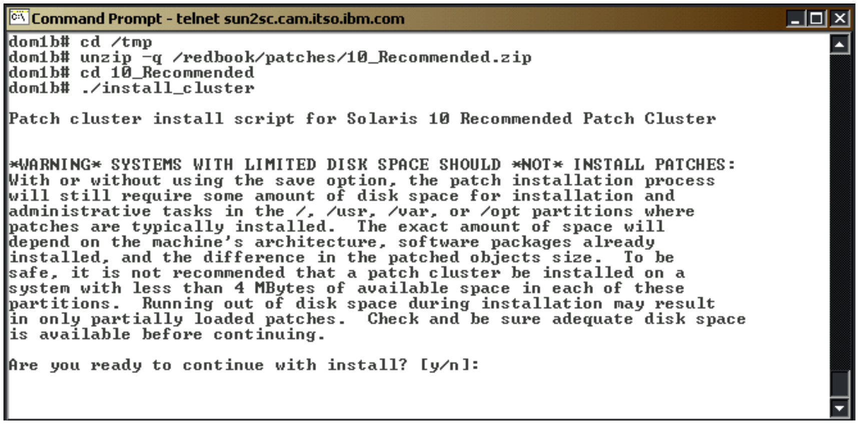
   ```
   cd /tmp
   unzip -q /directory/10_Recommended.zip
   ```

   This creates a directory named `/tmp/10_Recommended`, which contains the uncompressed patches ready for installation. There is also a CLUSTER_README file, which you should study in case there are any special instructions for installing the patches.

7. Many patches require that the system be quiescent when they are applied. Shut down Domino and any other applications, log on as `root` on the system console, and use **`init s`** to bring the system to single-user mode. Then start the patch installation:

   ```
   cd /tmp/10_Recommended
   ./install_cluster
   ```

   Figure 4-4 is displayed.



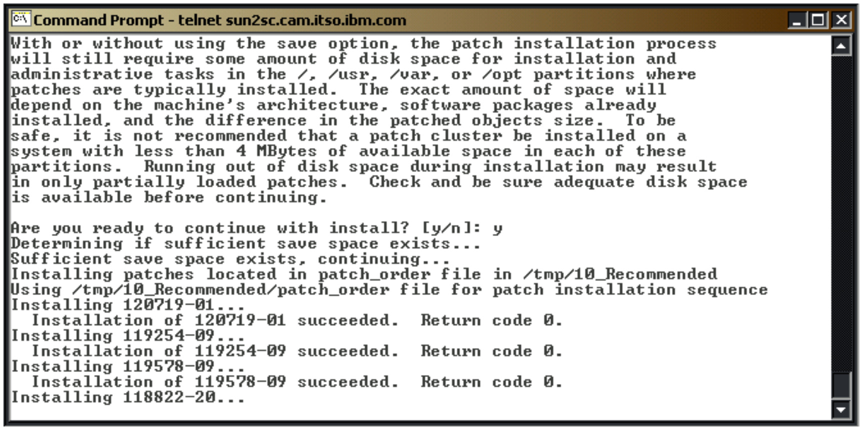
```
dom1b# cd /tmp
dom1b# unzip -q /redbook/patches/10_Recommended.zip
dom1b# cd 10_Recommended
dom1b# ./install_cluster

Patch cluster install script for Solaris 10 Recommended Patch Cluster


*WARNING* SYSTEMS WITH LIMITED DISK SPACE SHOULD *NOT* INSTALL PATCHES:
With or without using the save option, the patch installation process
will still require some amount of disk space for installation and
administrative tasks in the /, /usr, /var, or /opt partitions where
patches are typically installed.  The exact amount of space will
depend on the machine's architecture, software packages already
installed, and the difference in the patched objects size.  To be
safe, it is not recommended that a patch cluster be installed on a
system with less than 4 MBytes of available space in each of these
partitions.  Running out of disk space during installation may result
in only partially loaded patches.  Check and be sure adequate disk space
is available before continuing.

Are you ready to continue with install? [y/n]:
```

Figure 4-4 Install patches: start

8. The installation script asks for confirmation before it proceeds; read its instructions and answer `y` when you are ready to install the patches.

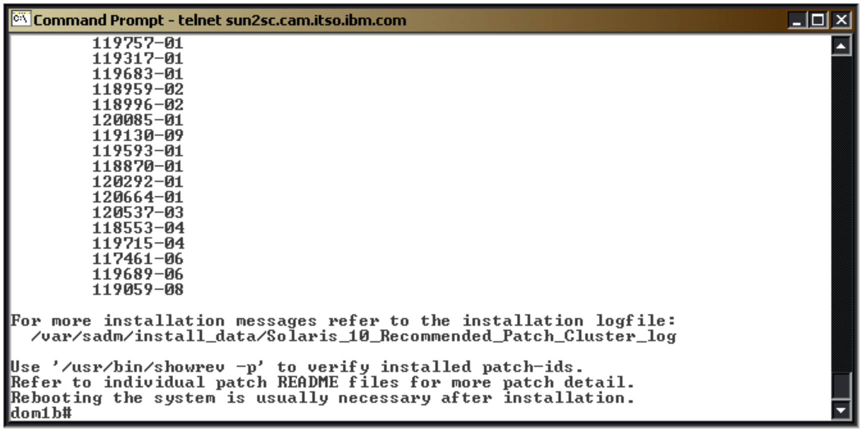
9. The script installs all of the cluster's patches without further intervention. If the cluster contains patches that are already present on the system (perhaps from installing earlier patch clusters), they will be skipped.

Figure 4-5 and Figure 4-6 show the start and end of this process.



```
With or without using the save option, the patch installation process
will still require some amount of disk space for installation and
administrative tasks in the /, /usr, /var, or /opt partitions where
patches are typically installed.  The exact amount of space will
depend on the machine's architecture, software packages already
installed, and the difference in the patched objects size.  To be
safe, it is not recommended that a patch cluster be installed on a
system with less than 4 MBytes of available space in each of these
partitions.  Running out of disk space during installation may result
in only partially loaded patches.  Check and be sure adequate disk space
is available before continuing.

Are you ready to continue with install? [y/n]: y
Determining if sufficient save space exists...
Sufficient save space exists, continuing...
Installing patches located in patch_order file in /tmp/10_Recommended
Using /tmp/10_Recommended/patch_order file for patch installation sequence
Installing 120719-01...
  Installation of 120719-01 succeeded.  Return code 0.
Installing 119254-09...
  Installation of 119254-09 succeeded.  Return code 0.
Installing 119578-09...
  Installation of 119578-09 succeeded.  Return code 0.
Installing 118822-20...
```

Figure 4-5 Patches being installed



```
        119757-01
        119317-01
        119683-01
        118959-02
        118996-02
        120085-01
        119130-09
        119593-01
        118870-01
        120292-01
        120664-01
        120537-03
        118553-04
        119715-04
        117461-06
        119689-06
        119059-08

For more installation messages refer to the installation logfile:
  /var/sadm/install_data/Solaris_10_Recommended_Patch_Cluster_log

Use '/usr/bin/showrev -p' to verify installed patch-ids.
Refer to individual patch README files for more patch detail.
Rebooting the system is usually necessary after installation.
dom1b#
```

Figure 4-6 Install patches finished

After all patches have been installed, you usually have to reboot Solaris before resuming normal operation. Enter **`init`** 6 to cause Solaris to shut down all the way, then reboot.

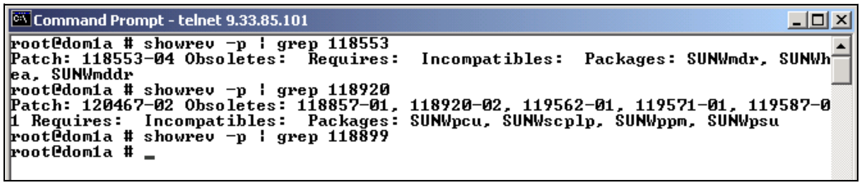
4.3.2 Patches required by Domino

Before installing or upgrading Domino, check the Domino Release Notes to see what Solaris patches are required for proper operation. You can read and download the release notes and other documentation by visiting the IBM DeveloperWorks Web site at:

http://www.ibm.com/developerworks/

Select **Lotus** → **Technical Library** → **Notes/Domino release notes**.

To learn whether a particular patch has already been installed, use the **showrev -p** command and search its output for the desired patch number. Figure 4-7 shows how to check for patches 118553-02, 118920-02, and 118899-01; each case is slightly different.



```
root@dom1a # showrev -p | grep 118553
Patch: 118553-04 Obsoletes:  Requires:  Incompatibles:  Packages: SUNWmdr, SUNWh
ea, SUNWmddr
root@dom1a # showrev -p | grep 118920
Patch: 120467-02 Obsoletes: 118857-01, 118920-02, 119562-01, 119571-01, 119587-0
1 Requires:  Incompatibles:  Packages: SUNWpcu, SUNWscplp, SUNWppm, SUNWpsu
root@dom1a # showrev -p | grep 118899
root@dom1a # _
```

Figure 4-7   Checking whether a patch has been installed

The first command in Figure 4-7 shows that the required patch has already been installed in an even newer version than the release notes call for. If it had shown an older installed version, you would have to apply a newer patch; as it is, the system already meets the release notes' requirement.

The second command shows that the desired patch is not installed, but that a completely different patch that subsumes it is present. Again, no action is required.

The final command shows that the desired patch has not been installed. You must apply the patch before running Domino.

4.3.3 Applying individual patches

To install individual patches that are not contained in patch clusters, you must download each patch as a separate file and install them individually.

1. To obtain the patch files, visit:

   http://sunsolve.sun.com/

2. Read and accept the terms of use, then click **Patches and Updates** on the next page.
3. Type the desired patch number in the PatchFinder search box (it is usually best to omit the revision number) and click **Find Patch**.
4. When the patch information page appears, click **FTP** or **HTTP** to download the patch, and save the patch file in any convenient directory.

Return to the PatchFinder page if you wish to download additional patches.

5. Unpack each patch file into a working directory; for example:

   ```
   cd /tmp
   unzip -q /directory/123456-01.zip
   unzip -q /directory/113355-04.zip
   ...
   ```

   These commands create directories /tmp/123456-01, /tmp/113355-04, and so on, ready for installation.

6. Review the README files in all directories for any special instructions, prerequisites, and the like. In particular, see whether any patches require that the system be in single-user mode, and whether any patches require a reboot.

   If any of the patches requires a quiescent system, shut down Domino and any other applications and use the **`init s`** command to bring the system to single-user mode.

7. Install the patches (check their README files to see whether a specific installation order is required) by using the **`patchadd`** command:

   ```
   cd /tmp
   patchadd 123456-01
   patchadd 113355-04
   ...
   ```

8. Finally, bring the system back to normal operation. How you do this depends on the patches' requirements and on the current system state:

   - If any patch requires a system reboot, shut down Domino and any other applications that might still be running and enter **`init 6`** to shut down and restart Solaris.
   - If a reboot is not required but the system was placed in single-user mode during the patch installation, enter **`init 3`** to return Solaris to normal operation. Then restart Domino and any other applications.

4.4 Operating system considerations

In 4.1, “Pre-installation checklist” on page 31, we discussed the information to gather to configure your Solaris system to run Domino correctly for your environment. We continue this process by discussing additional requirements that you might have for special needs in your business.

A common reason for implementing Domino on a Solaris platform is to take advantage of the reliability and scalability of the operating system. To get the most out of the features of Solaris, you might want to design special configurations that enable you to implement the large-scale configuration that Solaris can provide for the Domino servers.

In this section, we describe the services that are available with Solaris that work in conjunction with your Domino implementations. The services are:

- Disk drive configuration
- Configuring /tmp
- Default services
- sendmail and HTTP services
- /etc/system
- Domino partitioning
- Domino clustering
- Hardware clustering
- Network redirection

4.4.1 Disk drive configuration for Solaris

Part of the Solaris installation process is to select the disk drive or drives that will hold Solaris and to configure file systems for these drives.

It is a good practice to allocate and configure a pair of disks in a RAID 1 mirror for the Solaris boot disk. This provides increased availability of your server. If one disk fails, you can boot the server with the other disk and schedule replacement of the failed disk.

To configure the drive, you must partition it. Partitioning in the Solaris environment is not the same as partitioning in relation to your Domino server. When a disk is added on a Solaris system you must decide the sizes for the different file systems. A *file system* is defined as the physical or logical device that holds a collection of files and directories. This might be a hard disk drive or a partition on a disk drive.

In general, Solaris requires a minimum of two pieces of disk space: one with a file system typically labeled root and a raw piece called *swap*. In 3.4, “Disk space” on page 24, find the recommendations for the minimum sizes for this disk space.

You also need space for the home directories for the Solaris accounts you need. At a minimum you need one Solaris account per Domino partition. These home directories do not contain much data. The data for a Domino partition will be in the partition’s data directory. You might also want to create additional Solaris accounts for other reasons. For example, you might want each Domino administrator who performs some Solaris administration roles to have an account. There are a number of options as to where you may place these home directories. An organization might have home directory servers and use NFS (Network File System) to mount these across the network. It is also common for servers that are used for Domino to use local files for the home directories as we have done with the example lab servers we used for this book. Assuming that you want local home directories, the Solaris convention for this space is export/home/*login_name*, where *login_name* is the name of the Solaris account. You can either create a larger root file system or create a separate file system for the /export/home directory.

The disk partitions and files systems are created as part of the initial Solaris installation process that we described in 4.2, "Brief description of installing Solaris" on page 32.

We discuss Domino-related file systems in 4.6, "File system layout" on page 53.

4.4.2 /tmp (swap)

By default, Domino on Solaris utilizes mmap() files, which are created in /tmp and used by Domino for shared memory. In Solaris, the /tmp file system is a memory-based file system whose size is determined by physical memory plus the size of all of the swap space. Each Domino partition has its own set of files in /tmp. These files all start with the characters `.NOTESMEM_please_do_not_remove.` followed by a hexadecimal number that makes each filename unique. Note that these file names start with a dot, which indicates to Solaris that these are considered hidden files. To list the file, use the **`ls -a`** command. These files are created when Domino starts and as Domino needs more shared memory. They are removed when Domino is shut down. See 3.4.1, "Solaris, programs, and "swap"" on page 24 for a discussion about sizing the swap area.

The .NOTESMEM_* files will not be present if you configure Domino to use System V shared memory, as described in Appendix B, "Using System V shared memory" on page 521.

In addition, each Domino partition creates some files in /tmp that contain queue information useful to Lotus when analyzing problems. These files start with `.MQDnotes.*` Note that these file names start with a dot, indicating to Solaris that they are considered hidden files. To list the file, use the **`ls -a`** command.

The files in /tmp are vulnerable to well-intentioned but misguided attempts to clean up old files. If a Domino server has been running for a few weeks and a routine maintenance procedure (possibly a periodic **`cron`** job) decides to remove the "stale" .NOTESMEM_* or .MQDnotes.* files, Domino will die horribly.

4.4.3 Configuring default services

On a standard Solaris installation, several services run in the background, and you might want to disable some or all of them for security and performance reasons. Starting and stopping these services is usually controlled by the Service Management Facility (SMF) or with Run Control (RC) scripts. Starting with Solaris 10, most standard Solaris services are managed with SMF.You can use the **`man`** command to view the manual pages for SMF, svc.startd, svcadm, and svcs for more information about SMF. For more information about legacy RC scripts, use the **`man init.d`** command.

It is beyond the scope of this book to address all of these services; refer to one of the many Solaris administration and security books that cover this topic in depth, or visit:

http://www.sun.com/bigadmin

As these administration references describe, you many wish to bind these services exclusively to particular IP interfaces. If you decide to disable any Solaris services, make sure that you understand the ramifications of the services you disable. For instance, on a Domino application server you might disable FTP service running in the background due to potential security issues; however, this will disable your ability to use the FTP server to transfer files to Sun or Lotus support, for example from this server.

4.4.4 Disable Solaris sendmail and HTTP services

Two services that ship with Solaris, sendmail and HTTP, should be considered before you install Domino. Starting with Solaris 10, both of these services are managed by the Service Management Facility (SMF).

Domino and Solaris can both provide SMTP services for mail and routing. If you want to use the Solaris services, you do not want to configure the Domino services. You will have to disable Solaris sendmail, HTTP, or both if you want to use Domino's services.

To disable the Solaris sendmail service, log on to the server with the root account and execute the following command to disable the sendmail service:

```
svcadm disable sendmail
```

To disable the Solaris HTTP service, log on to the server with the root account and execute the following command to disable the HTTP service:

```
svcadm disable http
```

4.4.5 Edit Solaris system configuration (/etc/system)

Solaris kernel parameters are set in the /etc/system text file. Software applications might require that you set parameters here to override the Solaris default settings in order for the application to function. You may also set parameters here to tune the system to optimize performance.

Lotus documents any settings required in /etc/system for Domino in the release notes for the version of Domino you are installing. You can read and download the release notes and other documentation by selecting **Lotus** → **Technical Library** → **Notes/Domino release notes** at the IBM DeveloperWorks Web site:

`http://www.ibm.com/developerworks/`

As of the time of this writing, with Solaris 10 and Domino 7.0, there are no parameters that you need to set in /etc/system; however, some recommended tuning adjustments are described in Chapter 6, "Tuning and monitoring Domino servers on Solaris" on page 207.

4.4.6 Domino partitioning

Domino partitioning is when multiple instances of the Domino server run on the same machine. Currently there is no theoretical limit on the number of partitions you can run, given infinite hardware resources. However, in practical terms you will find that too many partitions on one physical box introduce complexity that might be difficult to manage. The right number of partitions for any given machine depends on available hardware and the expected load on each partition. The type and frequency of client access to the server also has to be taken into account. You can make some rough estimates using guidelines in 3.3, "Determine partition and domain counts" on page 23.

As a general rule, we recommend:

- Limiting the number of partitions to the number of CPU cores on your machine. (Some of Sun's CPU chips have more than one core.) Also keep in mind that the load on each Domino partition depends on the workload and tasks it is performing.
- Each partition requires its own data directory. Where possible, each data directory should be located on a separate physical device and file system.
- If you are using Domino transaction logs, each partition requires its own transaction log directory. Each transaction log directory should be located on separate physical device and file system.

Find more information about Domino partitions in Chapter 8, "Partitioning" on page 251.

4.4.7 Domino clustering

Domino clustering provides high availability and scalability to the Domino environment. With clustering, you can have multiple replica copies of databases on multiple servers. By adjusting the threshold on each server, the administrator can efficiently govern the maximum load against each machine in the cluster. As the demand on the cluster grows, more servers can be added easily, offering greater expendability.

The cluster replication is done over a TCP/IP connection between the partitions in the cluster. Assuming sufficient network capacity, the nodes in the cluster can be separated by some distance and provide disaster recovery capability at the same time.

The process used to cluster Domino servers is to set up one Domino partition on a server to replicate (copy) the databases to another Domino server partition on a separate server.

More information about Domino partitions and clusters can be found in Chapter 7, "Clustering" on page 227.

4.4.8 Hardware clustering

Solaris supports several hardware cluster solutions, including Sun Clusters. Currently, there are no vendor-supplied Domino modules for these clustering services. Administrators have used the scripting capabilities of these products to create custom solutions.

4.4.9 Network redirection

Certain services are available to redirect network traffic to multiple Domino servers for load balancing and availability. Not all services can be redirected because of the session type (statefull and stateless). A common example is to load balance and achieve high availability of an HTTP Web server by using an HTTP redirector. A redirector handles load balancing, failover, and sessions for the Web server.

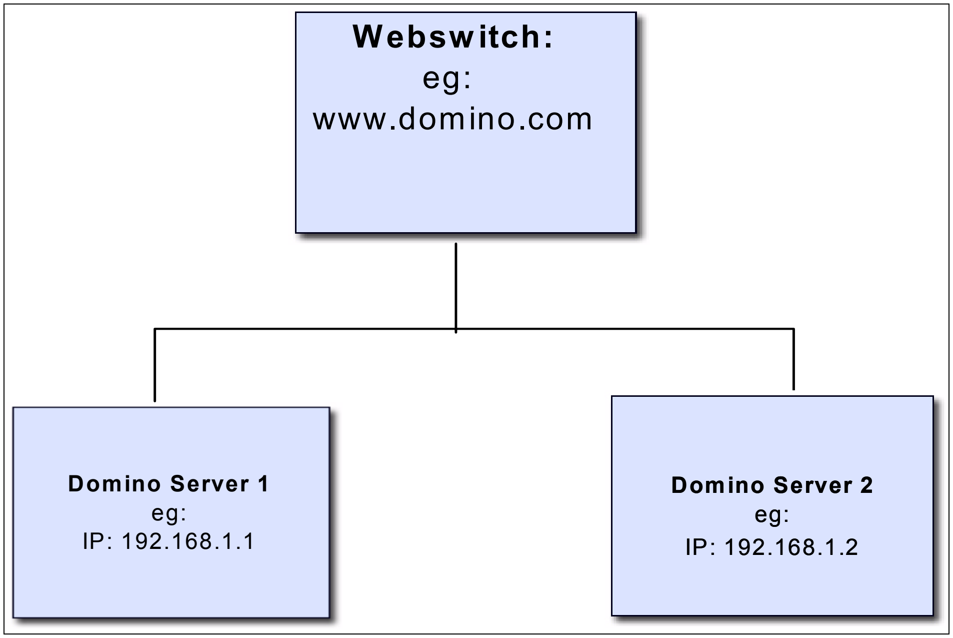


Figure 4-8 Load balancing with an HTTP redirector (Webswitch)

Users access www.domino.com and are transferred automatically to the Domino1 or Domino 2 server by the HTTP redirector, depending which of the servers is available. If both are available, the Web server with fewer sessions will be chosen by the HTTP redirector. In case of server failure, the session will be transferred automatically to the other server.

4.5 Network configuration

This section discusses some considerations for the network configuration on a Solaris system as they relate to your Domino installation.

4.5.1 Host names and IP addresses

Several scenarios can require multiple TCP/IP host names and addresses, and might require additional physical or logical network interfaces. Domino can also be configured with port mapping, which enables an IP address to be shared across partitions.

These are best practices for basic Domino servers:

- Single Domino server: Requires one IP address and host name.
  If the Domino host name is not the system's host name, an alias entry must be established tying the two together in the /etc/host file's localhost entry.
- Multiple Domino partitions: We recommend that each Domino partition has its own host name and IP address.
- Clustering: We recommend a private network between the nodes of the cluster, as well as individual host names and IP addresses for each Domino partition in the cluster.

In addition to the network connections that are required for your Domino partitions, you might need additional host names and connections for other reasons. Some organizations have an administrative network that administrators use to manage the servers and for network-based backup tools. Many of the Sun servers have system control processors running Advanced Lights Out Management (ALOM) software that can be configured to have a network connection for access to the systems console port.

With Solaris, each host name/IP address requires a network interface. This interface can either be a separate *physical* interface or multiple *logical* interfaces on a physical network card.

You might want to use a naming convention that uses a theme for the Domino servers' names as well as the host names. For example, you might want to combine location, function, and instance (such as BostonMail03 or BostonApp02) for the Domino servers' names. For host names, use the Domino server's name if only one IP address is being used. If more than one IP address is being used, name the host differently per instance. A theme can be useful here as well, such as adding a suffix to the base host name to identify each instance (cl for cluster, pr for private, or wn for WAN). Then link the Domino server's name to this host name in the remote systems name services (that is, Connection doc, Host file, DNS subdomain, or independent DNS domain) to guide the other systems to this IP address as needed.

Tip: Review RFC 1178, "Name Your Computer," for additional guidance in host naming. This material is available at:

http://www.ietf.org/rfc/rfc1178.txt

Important: Do not create host names using the underscore character because it is no longer supported in DNS/BIND 8.xx and later.

Note: The following sections describe the network we set up for our redbook examples. Much of this information might be applicable to your situation as we followed the practices described above:

- Multiple Domino partitions, each with its own host name and IP address
- Clustered across a private network and each Domino partition has its own cluster host name and IP address

We have also supplied additional information about networking options in Appendix A, "TCP/IP networking" on page 517.

4.5.2 Our Redbooks Lab topology

The following diagram and tables illustrate our Redbooks Lab topology. The servers that we used for the lab are Sun Fire™ V240s. These servers have five physical network connections; four are 10/100/1000 Mbps Ethernet ports called bge0 through bge4. Our lab design uses two of these. The fifth port is a 10 Mbps Ethernet port for the Advanced Lights Out Management (ALOM) console port. In addition, each server has a Sun StorEdge™ 3310 disk array, which has an Ethernet port for network management.

Upcoming sections describe the steps that are required to set up this lab network.

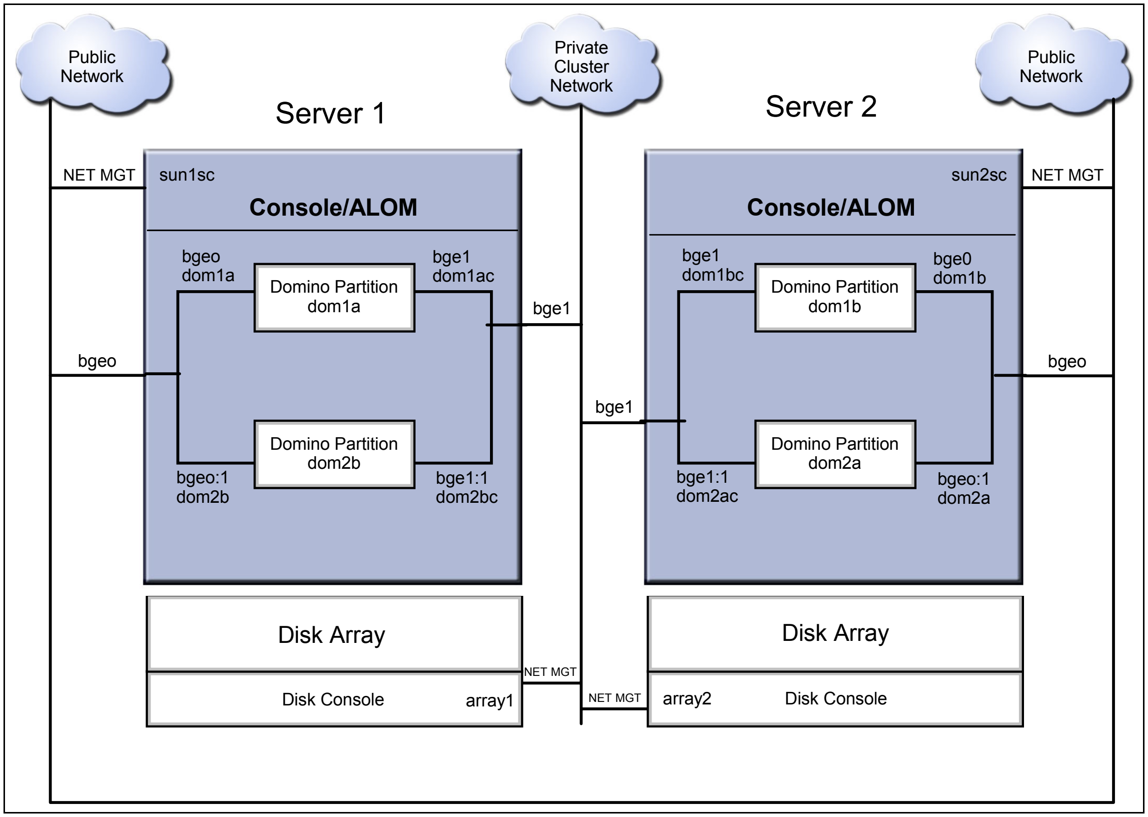


Figure 4-9 Redbooks Lab topology

Table 4-1 Redbooks Lab network

Host name	Physical connection	Solaris Interface	Public IP address	Private IP address	Notes
Server 1					
sun1sc	NET MGT		9.33.85.103		Server 1's ALOM console
dom1a	bge0	bge0	9.33.85.101		Domino partition dom1a's public connection
dom2b	bge0	bge0:1	9.33.85.102		Domino partition dom2b's public connection
dom1ac	bge1	bge1		192.168.1.101	Domino partition dom1a's cluster connection
dom2bc	bge1	bge1:1		192.168.1.102	Domino partition dom2b's cluster connection

Host name	Physical connection	Solaris Interface	Public IP address	Private IP address	Notes
array1	NET MGT			192.168.1.201	
Server 2					
sun2sc	NET MGT		9.33.85.106		Server 2's ALOM console
dom1b	bge0	bge0	9.33.85.104		Domino partition dom1b's public connection
dom2a	bge0	bge0:1	9.33.85.105		Domino partition dom2a's public connection
dom1bc	bge1	bge1		192.168.1.104	Domino partition dom1b's cluster connection
dom2ac	bge1	bge1:1		192.168.1.105	Domino partition dom2a's cluster connection
array2	NET MGT			192.168.1.202	

4.5.3 Configuring the Redbooks Lab

The following steps were used to set up the network using Server 1 as the example. We have not configured a name service such as DNS. We used the local /etc/hosts file to resolve our lab's host names and addresses. Your organization may also use a naming service. Solaris supports this configuration, but it is beyond the scope of this book to document all of the supported methods. For additional information about Solaris administration, visit:

http://www.sun.com/bigadmin

Also, you can access Sun documentation at:

http://docs.sun.com

1. Configure the first host and network interface.

   The first network interface is configured when Solaris is initially installed. See 4.2, "Brief description of installing Solaris" on page 32.

2. Edit the /etc/hosts file to define your network.

   a. Log on in as the root user.

   b. Edit the /etc/hosts file using the information we collected in Figure 4-9 on page 50 and Table 4-1 on page 50.

   Here is what the /etc/hosts file looks like on Server 1

   ```
   root@dom1a # more /etc/hosts
   ```

```
127.0.0.1       localhost
9.33.85.101     dom1a   loghost
9.33.85.102     dom2b
9.33.85.103     sun1sc
9.33.85.104     dom1b
9.33.85.105     dom2a
9.33.85.106     sun2sc
#
192.168.1.101   dom1ac
192.168.1.102   dom2bc
192.168.1.104   dom1bc
192.168.1.105   dom2ac
192.168.1.201   array1
192.168.1.202   array2
root@dom1a #
```

3. Configure the network interfaces.

   With Solaris, each host name/IP address requires a network interface. This interface can either be a separate *physical* interface or multiple *logical* interfaces on a physical network card.

   Interface name is a string in this format:

   physical-unit

   physical-unit:logical-unit

   For example: bge0 refers to the first bge physical interface, while bge0:1 refers to logical interface 1 on the first bge physical interface.

   Each network interface must know its host name and IP address. To do this, create a file called `/etc/hostname.`*`interface-name`*. This file must contain the host name to be associated with this interface name. The first network hostname file is created by the system on install.

4. Create the appropriate interface files on Server 1:

   a. Log on to Server 1 as root.

   b. Using a text editor, create the interface files and put the appropriate host name in each.

      Here are the files on our example Server 1:

      ```
      root@dom1a # cd /etc
      root@dom1a # ls -1 hostname*
      hostname.bge0
      hostname.bge0:1
      hostname.bge1
      hostname.bge1:1
      root@dom1a #
      ```

c. These commands display the contents of each of these files:

```
root@dom1a #cd /etc
root@dom1a #cat hostname.bge0
dom1a
root@dom1a # cat hostname.bge0:1
dom2b
root@dom1a # cat hostname.bge1
dom1ac
root@dom1a # cat hostname.bge1:1
dom2bc
root@dom1a #
```

5. Make sure IP forwarding is turned off.

   By default, IP forwarding and routing is disabled. The **routeadm** command is used to administer system-wide configuration for IP forwarding and routing. **routeadm** is used to enable or disable each function independently, overriding any system default setting for each function. See **man routeadm** for more information. Use **routeadm -p** to display the current status.

6. Start the network.

   You have two main options for putting your network configuration into effect:

   a. Reboot the system

      Log on as root and execute the following command:

      ```
      init 6
      ```

   b. Use a series of **ifconfig** commands, log on as root:

      ```
      /sbin/ifconfig bge1 plumb
      /sbin/ifconfig bge1 192.168.1.104 up
      /sbin/ifconfig bge1:1 192.168.1.105 up
      ```

Note: Find additional information about networking in Appendix A, “TCP/IP networking” on page 517.

4.6 File system layout

The next step in preparing for the installation of your Domino server is to set the file system layout for the Domino binary and data files. During installation of the Solaris Operating System, you set up the file systems needed for the Solaris installation. We now do the same thing for the Domino installation.

We have already discussed the considerations for the amount of disk space needed for your Domino implementation in Chapter 3, “Sizing guidelines for IBM Lotus Domino Messaging Server” on page 19.

When defining your file system layout, we recommend that you follow the guidelines listed here for performance and reliability. Note that these guidelines apply to locally attached storage; they must be adjusted for other types of storage, such as Storage Area Networks (SANs).

- Use stripes (RAID 0 or 1+0) for optimal performance.
- Protect your data (RAID 1+0, 1 or 5), even in Domino clusters.
- Use at least one file system per partition.
- Put each partition's transaction log file on a separate file system and physical disk.

4.6.1 Creating Domino file systems

If Domino's databases and logs reside on dedicated UNIX File System (UFS) volumes, there are two adjustments you should make.

When creating a file system to hold Domino server data directories or users' mail databases, you should optimize the file system for relatively large files and relatively short data transfers. Use the **`newfs`** command with parameters such as:

```
newfs -i 200000 -C 8 -c 256 -m 1 /dev/rdsk/...
```

The `-i 200000` option conditions the file system for Domino's relatively large files, and `-C 8` prevents the file system from reading ahead too aggressively for Domino's random I/O pattern. The other two options are helpful but less crucial; use the **`man newfs`** command to learn more about them and about other options you can specify, and for special instructions for multi-terabyte file systems.

Domino's transactional logs are also fairly large and also experience short data transfers, but the access pattern is primarily sequential rather than random. Create them just a little bit differently than you do the others:

```
newfs -i 200000 -C 16 -c 256 -m 1 /dev/rdsk/...
```

The `-C 16` option enables longer data transfers, which make little difference during normal Domino operation but can be helpful when a server restarts after a crash or when a backup program reads the logs.

4.6.2 Redbooks Lab Domino file systems

Figure 4-10 on page 55 illustrates the file system layout we used for our Redbooks Lab servers and the examples in this book.

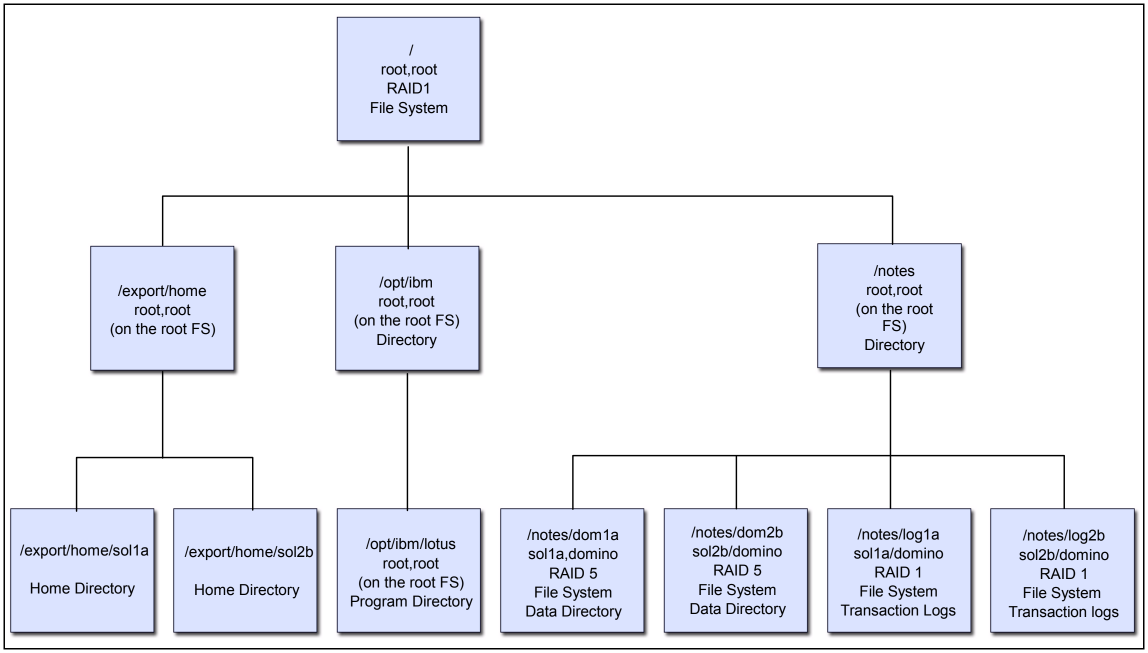


Figure 4-10 Solaris file systems used for this book

4.7 Creating a Solaris group and user accounts

Before installing Domino software, you must create a Solaris group that will be used for all Domino partitions that you plan to install. Also create a separate Solaris account and set up the Solaris environment for each Domino partition.

Solaris offers several methods to create and maintain groups and user accounts, and authenticate users. These include:

- Local files
- Network Information Name Service (NIS and NIS+)
- Lightweight Directory Access Protocol (LDAP)

It is beyond the scope of this book to document how to set up and manage NIS (or NIS+) and LDAP. We will use local files for our groups and accounts. If your company uses one of the other options, speak with your Solaris administrators to determine how to add the appropriate group and accounts.

When adding Solaris groups and accounts to the local files, you have two options:

- Using the graphical user interface (GUI) tool called the Solaris Management Console (SMC)
- From a Solaris shell using text commands

We use both of these methods in the examples that follow.

Prior to adding the Domino group and Solaris accounts, decide and document:

- The Solaris group name for the Domino partitions
- For each Solaris account:
  - Logon name
  - User ID (UID) number
  - Home directory
  - Domino data directory

For the examples used in this book, we used the configuration shown in Table 4-2.

Table 4-2 Solaris group and user configuration

Server	TCP/IP host name	Solaris account	User ID	Solaris group	Home directory	Domino data directory
sun1	dom1a	sol1a	100	domino	/export/home/sol1a	/notes/dom1a
sun1	dom2b	sol2b	101	domino	/export/home/sol2b	/notes/dom2b
sun2	dom1b	sol1b	200	domino	/export/home/sol1b	/notes/dom1b
sun2	dom2a	sol2a	201	domino	/export/home/sol2a	/notes/dom2a

4.7.1 Creating groups and accounts with SMC

The Solaris Management Console (SMC) is a graphical tool that the Solaris administrator can use to manage many aspects of a Solaris server including managing groups and accounts. The smc tool is included with Solaris.

You can find out more about SMC from the Help menu on the tool and with the **`man smc`** shell command.

SMC requires an X11 graphics display. You may meet this requirement in a number of ways, including:

- Local X11 on the server if you have installed a graphics card, keyboard, and mouse, the Solaris X11 software packages installed when you installed Solaris
- X11 on a UNIX or Linux workstation on the network with the server with the X11 installed on the workstation and the Solaris X11 software packages on the server
- X11 emulator on a Windows or other workstation and the Solaris X11 software packages on the server

For the examples used in this book, we used the VNC (Virtual Network Computing) viewer on a Windows 2000 workstation and the VNC server package plus the Solaris X11 packages on the servers. The steps that follow assume that the VNC server software has been installed on the server and that the VNC viewer software has been installed on the Windows 2000 workstation.

Use the following steps to create your Solaris group and user accounts using the smc tool.

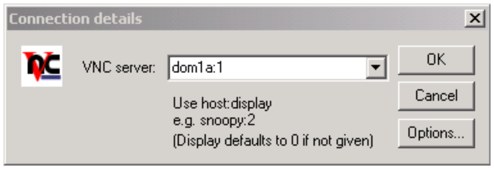
1. From the Workstation, log on to the server as the root Solaris account, and start the VNC server by typing:

   ```
   vncserver
   ```

   You should see:

   ```

   New 'X' desktop is dom1a:1

   Starting applications specified in //.vnc/xstartup
   Log file is //.vnc/dom1a:1.log

   root@dom1a #
   ```

2. At the Workstation, start the VNC viewer (**Start** → **Programs** → **VNC** → **Run VNC Viewer**).
3. Enter the host name and display number, and click **OK**.

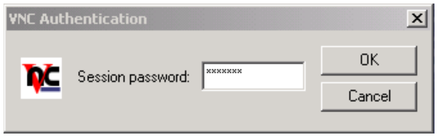

Connection details

VNC server: dom1a:1

Use host:display
e.g. snoopy:2
(Display defaults to 0 if not given)

Figure 4-11 VNC viewer (host name:display)

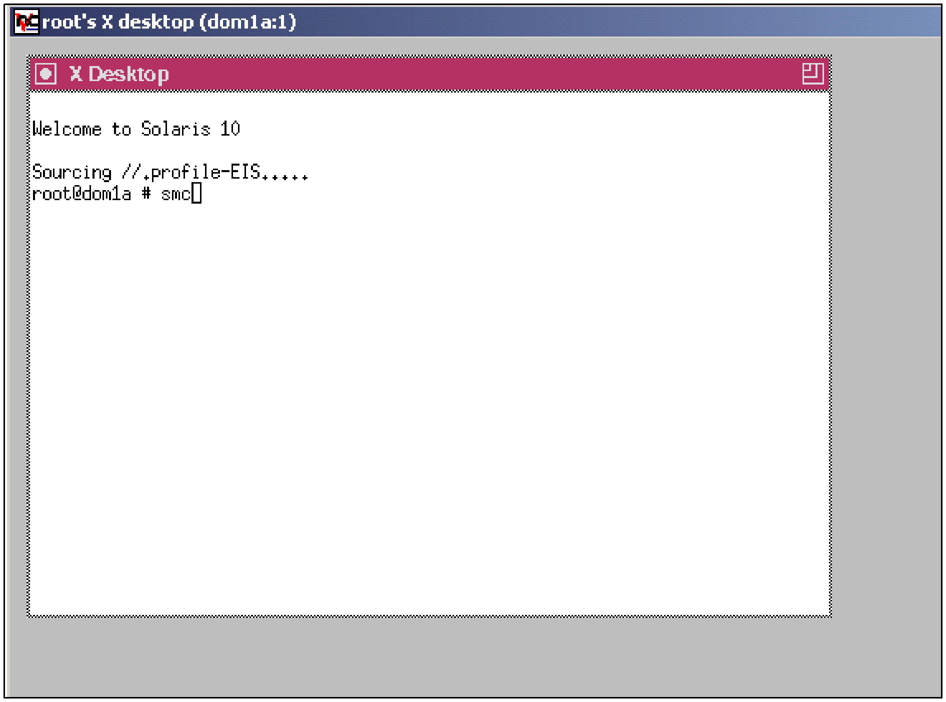
4. Enter the VNC password and click **OK**.



Session password: *******

Figure 4-12 VNC Authentication

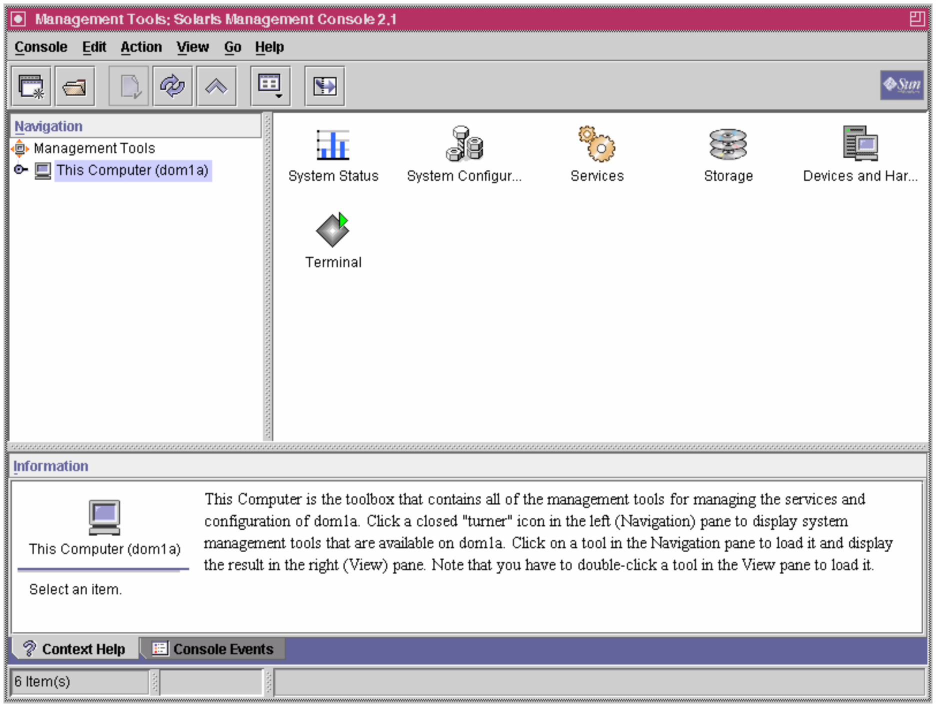
5. Start the SMC tool by entering `smc` in the VNC terminal window displayed on the workstation.



```
Welcome to Solaris 10

Sourcing //.profile-EIS.....
root@dom1a # smc
```

Figure 4-13 VNC, launch SMC

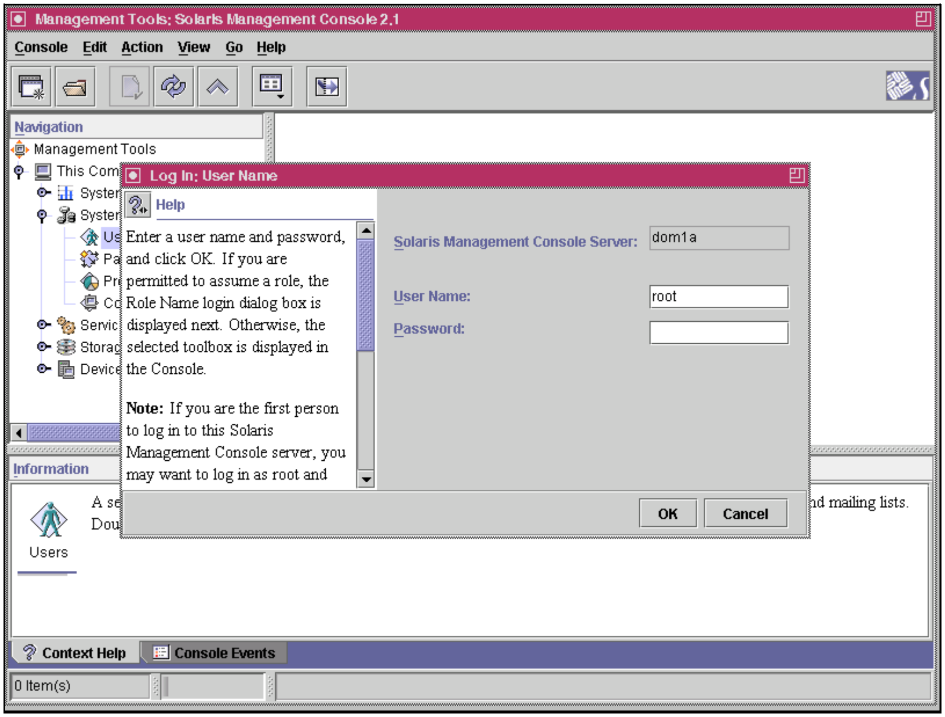
6. In the **Navigation** frame, click to expand the twisties next to **This Computer** and, under that, **System Configuration**.



This Computer is the toolbox that contains all of the management tools for managing the services and configuration of dom1a. Click a closed "turner" icon in the left (Navigation) pane to display system management tools that are available on dom1a. Click on a tool in the Navigation pane to load it and display the result in the right (View) pane. Note that you have to double-click a tool in the View pane to load it.

Figure 4-14 SMC first screen

7. Click **Users,** enter the root password, and click **OK**.



Enter a user name and password, and click OK. If you are permitted to assume a role, the Role Name login dialog box is displayed next. Otherwise, the selected toolbox is displayed in the Console.

Note: If you are the first person to log in to this Solaris Management Console server, you may want to log in as root and

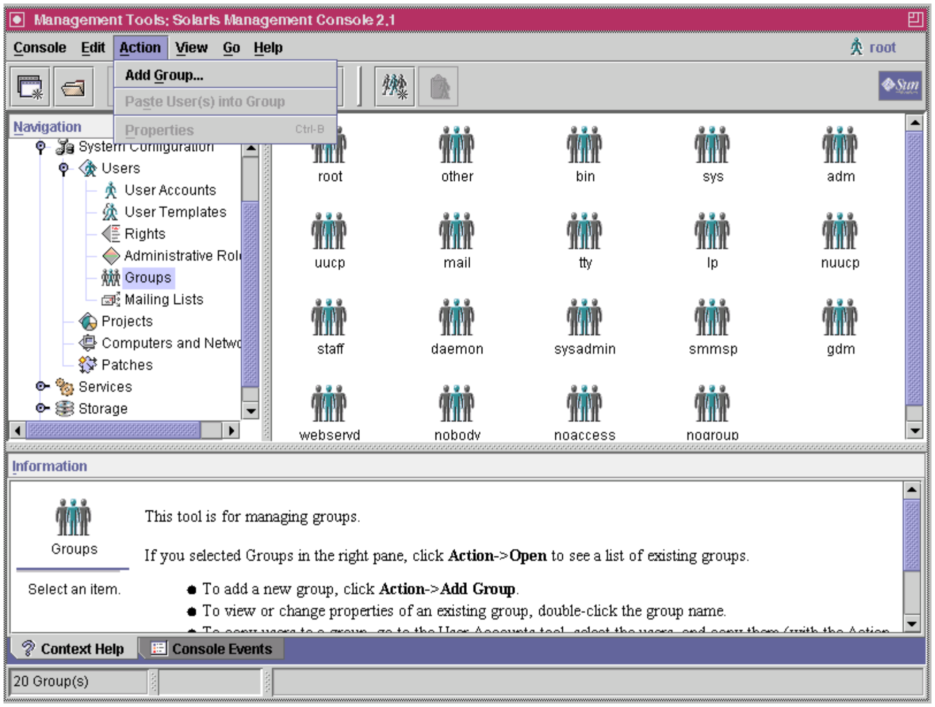
Solaris Management Console Server: dom1a

User Name: root

Password:

Figure 4-15 SMC root password

8. Click the twistie next to **Users** and click **Groups**. Select **Action** → **Add Group.**



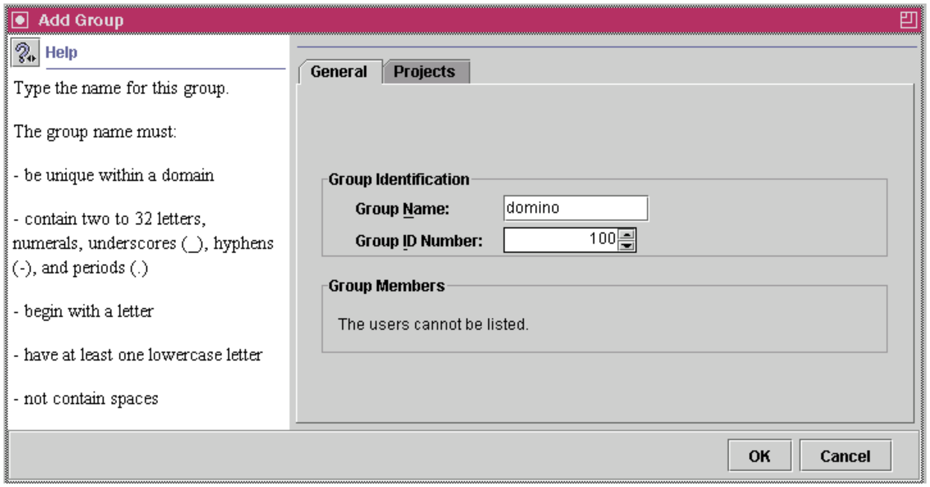
This tool is for managing groups.

If you selected Groups in the right pane, click **Action->Open** to see a list of existing groups.

- To add a new group, click **Action->Add Group**.
- To view or change properties of an existing group, double-click the group name.
- To copy users to a group, go to the User Accounts tool, select the users, and copy them (with the Action

Figure 4-16   SMC Add Group step 1

9. Enter `domino` for the Group Name and accept the Group ID Number. Click **OK**.



Type the name for this group.

The group name must:

- be unique within a domain

- contain two to 32 letters, numerals, underscores (_), hyphens (-), and periods (.)

- begin with a letter

- have at least one lowercase letter

- not contain spaces

Group Name: domino

Group ID Number: 100

The users cannot be listed.

Figure 4-17 SMC Add group called domino

10. In the Navigation frame, click **User Accounts**. Select **Action** → **Add User** → **With Wizard** as shown in **Figure 4-18**

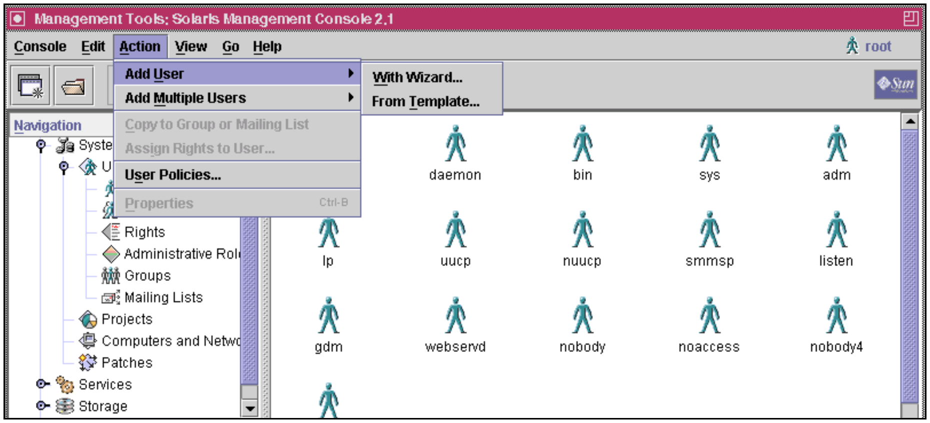
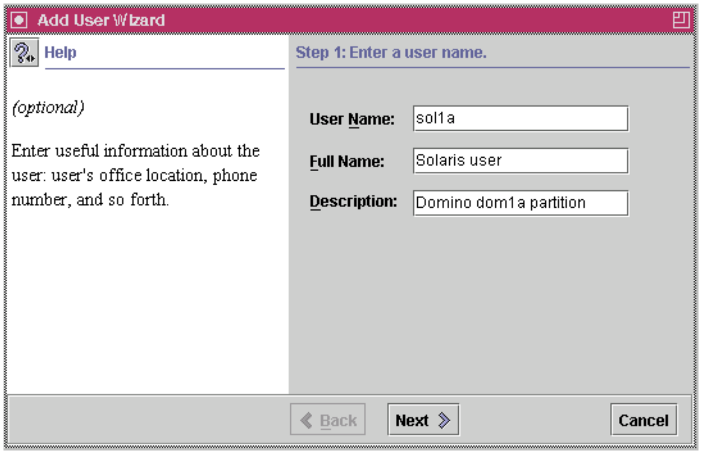


Figure 4-18 SMC Add user step 1

11. Using Table 4-2 on page 56 as a guide, enter the Solaris account name for the first Domino partition on this server in the User Name field of the Add User Wizard. Optionally, you may fill in the Full Name and Description fields. Click **Next**.



(optional)

Enter useful information about the user: user's office location, phone number, and so forth.

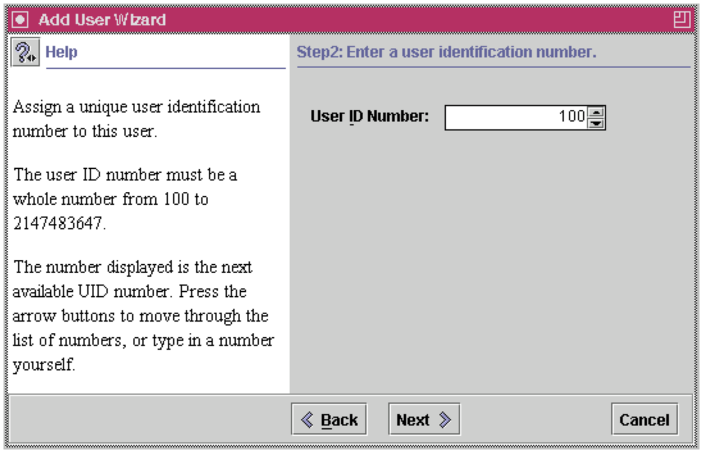
User Name: sol1a

Full Name: Solaris user

Description: Domino dom1a partition

Figure 4-19 SMC, User Name

12. Enter the User ID Number (100 in our example), and click **Next**.



Assign a unique user identification number to this user.

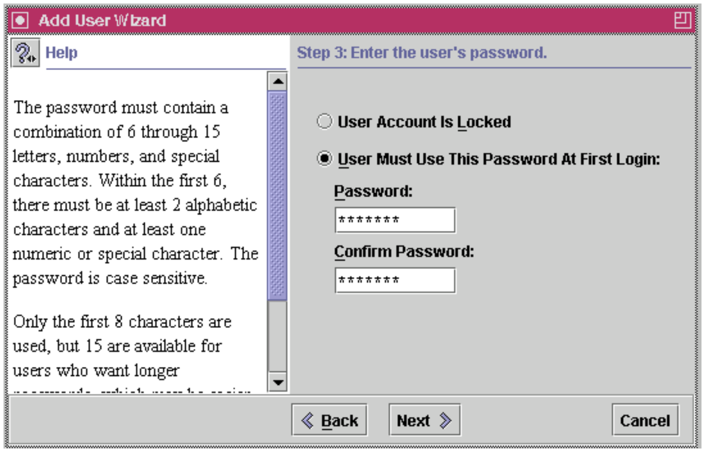
The user ID number must be a whole number from 100 to 2147483647.

The number displayed is the next available UID number. Press the arrow buttons to move through the list of numbers, or type in a number yourself.

User ID Number: 100

Figure 4-20 SMC, User ID

13. Select **User Must Use This Password At First Login**. Enter the password in the Password field and confirm it. Click **Next**.



Step 3: Enter the user's password.

The password must contain a combination of 6 through 15 letters, numbers, and special characters. Within the first 6, there must be at least 2 alphabetic characters and at least one numeric or special character. The password is case sensitive.

Only the first 8 characters are used, but 15 are available for users who want longer

○ User Account Is Locked

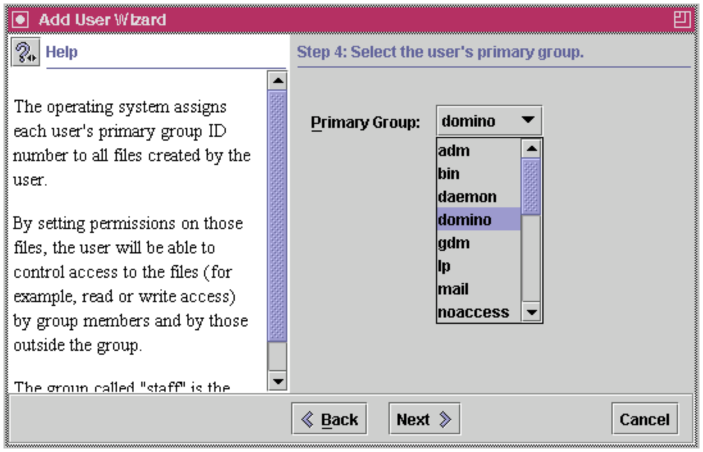
● User Must Use This Password At First Login:

Password: *******

Confirm Password: *******

Figure 4-21 Setting up the first login password

14. From the pull-down menu, select **domino** for the user's Primary Group and click **Next**.



Step 4: Select the user's primary group.

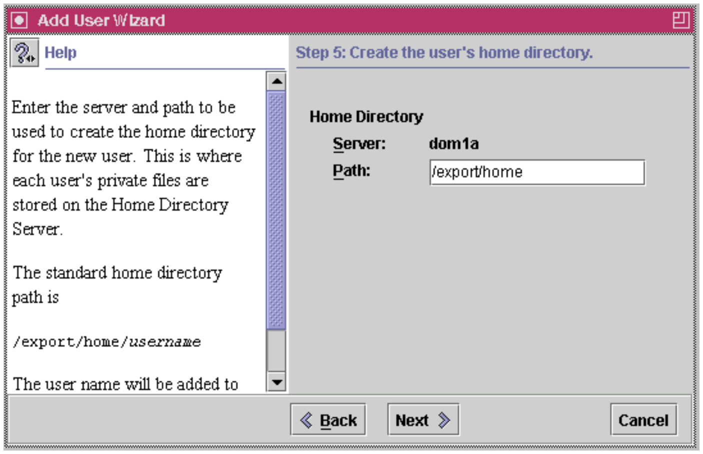
The operating system assigns each user's primary group ID number to all files created by the user.

By setting permissions on those files, the user will be able to control access to the files (for example, read or write access) by group members and by those outside the group.

Primary Group: domino

Figure 4-22 SMC, primary group

15.Accept the default Home Directory path of /export/home, and click **Next**.



Add User Wizard

Help

Enter the server and path to be used to create the home directory for the new user. This is where each user's private files are stored on the Home Directory Server.

The standard home directory path is

`/export/home/`*`username`*

The user name will be added to

Step 5: Create the user's home directory.

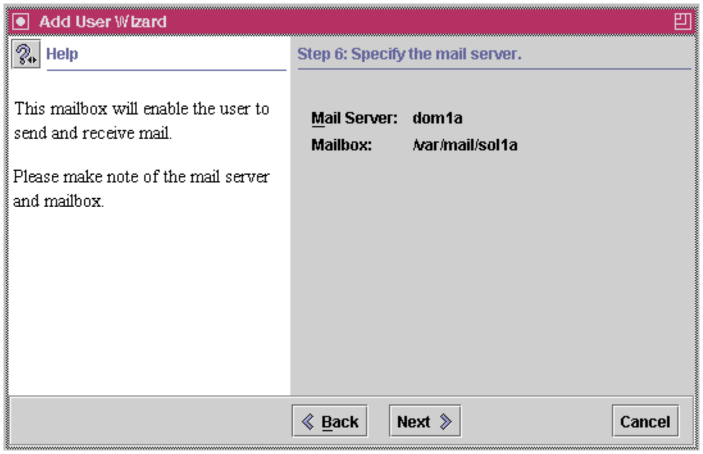
Home Directory

Server: dom1a

Path: /export/home

Figure 4-23 SMC, Home Directory

16.Click **Next** on the Mail Server window.



Add User Wizard

Help

This mailbox will enable the user to send and receive mail.

Please make note of the mail server and mailbox.

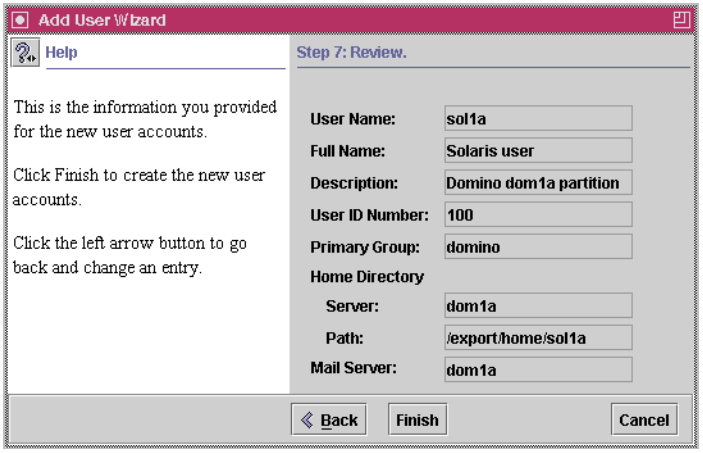
Step 6: Specify the mail server.

Mail Server: dom1a

Mailbox: /var/mail/sol1a

Figure 4-24 SMC, Mail Server

17. Review the information for the new account, and click **Finish** if it is correct.



This is the information you provided for the new user accounts.

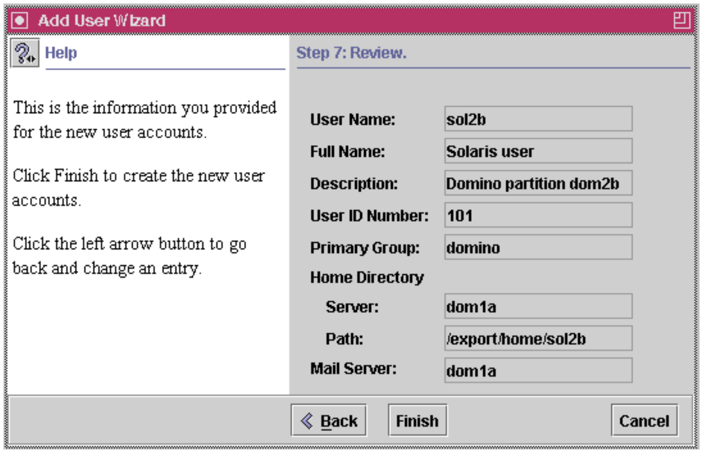
Click Finish to create the new user accounts.

Click the left arrow button to go back and change an entry.

User Name:	sol1a
Full Name:	Solaris user
Description:	Domino dom1a partition
User ID Number:	100
Primary Group:	domino
Home Directory	
Server:	dom1a
Path:	/export/home/sol1a
Mail Server:	dom1a

Figure 4-25 SMC, Review and Finish

18. Repeat steps 10 on page 62 through 17 to create a Solaris account for each Domino partition being set up on this server. For the examples used in this book, we added the second Solaris account, called dom2b. (See Table 4-2 on page 56 for the account information.) Figure 4-26 shows is the last window for creating user sol2b.



This is the information you provided for the new user accounts.

Click Finish to create the new user accounts.

Click the left arrow button to go back and change an entry.

User Name:	sol2b
Full Name:	Solaris user
Description:	Domino partition dom2b
User ID Number:	101
Primary Group:	domino
Home Directory	
Server:	dom1a
Path:	/export/home/sol2b
Mail Server:	dom1a

Figure 4-26 SMC, add sol2b account

4.7.2 Creating a group and accounts with shell commands

Solaris supports the use of shell commands to create and administer Solaris groups and accounts. These commands include:

groupadd	Add a group
groupdel	Delete a group
groupmod	Modify a group
useradd	Add an account
userdel	Delete an account
usermod	Modify an account

You can get online help with the **man *command*** utility. For example, for help with the **useradd** command, enter **man useradd** at any shell prompt while logged on to the server. Example 4-1 shows the output from **man useradd**.

Example 4-1 man useradd output

```
Reformatting page.  Please Wait... done

System Administration Commands                        useradd(1M)

NAME
     useradd - administer a new user login on the system

SYNOPSIS
     useradd [-c comment] [-d dir] [-e expire]  [-f inactive]  [-
     g group]  [  -G group  [  , group...]] [ -m [-k skel_dir]] [
     -u uid  [-o]]  [-s shell]  [-A  authorization   [,authoriza-
     tion...]]  [-P profile  [,profile...]] [-R role  [,role...]]
     [-p projname] [-K key=value] login

     useradd  -D  [-b base_dir]  [-e expire]   [-f inactive]   [-
     g group] [-A authorization  [,authorization...]] [-P profile
     [,profile...]]  [-R  role   [,role...]]  [-p  projname]  [-K
     key=value]

DESCRIPTION
     useradd adds a new user to the /etc/passwd  and  /etc/shadow
     and /etc/user_attr files. The -A and -P options respectively
     assign authorizations and  profiles  to  the  user.  The  -R
--More--(8%)
```

Use the following steps to create your Solaris group and user accounts using shell commands. As with the smc procedure, refer to Table 4-2 on page 56 for information about the Solaris accounts. In the example below, we use commands to create the group and two Solaris accounts on the second server.

1. Log on to the server as the root user and be at a shell prompt.

2. Referring to Table 4-2 on page 56 for the information about the Solaris group, add the group using the following command:

   ```
   root@dom1b # groupadd -g 100 domino
   ```

   – `-g 100` is the group number (100) you want to add.

   – `domino` is the name of the group.

3. The following command lists the contents of the /etc/group/ file:

   ```
   root@dom1b # more /etc/group
   root::0:
   other::1:root
   bin::2:root,daemon
   sys::3:root,bin,adm
   adm::4:root,daemon
   uucp::5:root
   mail::6:root
   tty::7:root,adm
   lp::8:root,adm
   nuucp::9:root
   staff::10:
   daemon::12:root
   sysadmin::14:
   smmsp::25:
   gdm::50:
   webservd::80:
   nobody::60001:
   noaccess::60002:
   nogroup::65534:
   domino::100:
   ```

4. Referring again to Table 4-2 on page 56 for information about the Solaris accounts, add the two accounts using the following commands:

   ```
   root@dom1b # useradd -d /export/home/sol1b -m -s /bin/sh \
   root@dom1b > -g domino -u 200 sol1b
   64 blocks
   root@dom1b # useradd -d /export/home/sol2a -m -s /bin/sh \
   root@dom1b > -g domino -u 201 sol2a
   64 blocks
   ```

   – `-d` *`directory path`* defines the home directory.

   – `-m` indicates that if the home directory does not exist, create it.

   – `-s /bin/sh` means the account's shell will be /bin/sh (the Bourne shell).

   – `-g` domino sets the account's primary group membership to the domino group.

   – `-u` *nnn* sets the account's user id to *nnn*.

Tip: Command continuation: Typing \ and pressing the Enter key enables you to continue a shell command on the next line.

5. After creating the accounts, use the **passwd** command to set the account's password:

   ```
   passwd sol1b
   ```

   This is the output:

   ```
   New Password:
   Re-enter new Password:
   passwd: password successfully changed for sol1b
   root@dom1b # passwd sol2a
   New Password:
   Re-enter new Password:
   passwd: password successfully changed for sol2a
   ```

Note: The **passwd** command will not echo anything when you type in the passwords.

4.7.3 Configure the Solaris environment for the Solaris accounts

After you have created the domino group and Solaris accounts, configure the Solaris environment for the Solaris accounts. These steps are the same for accounts added with the Solaris Management Console. (See 4.7.1, "Creating groups and accounts with SMC" on page 56 or, if you used shell commands, see 4.7.2, "Creating a group and accounts with shell commands" on page 67.)

The Solaris environment defines the way the Solaris accounts work when you log on to the Solaris system. It defines where to search for executables, what your default time zone is, where to send mail, and so on. There are default settings that will not be used for an account that is used for a Domino partition. A Solaris account that owns a Domino partition requires some non-default settings, which we describe in this section.

We used the default setting of the Bourne shell (/bin/sh) when we added accounts via SMC. We explicitly picked the Bourne shell for the users added via the shell command line. The examples below are for the Bourne shell. If you are using another shell such as c, bash, or korn, modify this for your shell's configuration files.

1. The PATH environment variable is the list of directories to search for executable programs and scripts when using the Bourne shell. Edit each account's .profile configuration file to have a PATH statement that includes the binary directory for the Domino software. Also, as we will be using X11 during

the Domino setup steps in 5.3, “Setting up Domino servers” on page 109, add the necessary X11 directories to the PATH.

For our example we use /opt/ibm/lotus for our Domino program directory. We added /opt/ibm/lotus/bin, which is the Domino executables directory to the PATH. We also added /user/openwin/bin and /usr/dt/bin, which are the two X11 graphics directories we want on the PATH.

Make the account’s home directory your current directory with the **cd** command:

```
cd /export/home/sol1a
```

Edit the .profile file with a text editor such as **vi**.

```
vi .profile
```

You can display the edited file with the **cat** or **more** command:

```
cat .profile
```

This is the output:

```
# Copyright (c) 2001 by Sun Microsystems, Inc.
# All rights reserved.
#
# ident "@(#)local.profile      1.10    01/06/23 SMI"
stty istrip
PATH=/usr/bin:/usr/ucb:/etc:/opt/ibm/lotus/bin:/usr/openwin/bin:/usr/dt/
bin:.
export PATH
```

2. We create a file called `.hushlogin` in each account’s home directory. The existence of this file disables the Solaris notification messages when a user logs on. While still in the accounts home directory, enter the following commands:

   ```
   cd /export/home/sol1a
   touch .hushlogin
   ```

3. We also want the make sure that these files are owned by the solaris account and have domino as the group setting. Use the **chown** command to adjust these settings:

   ```
   chown sol1a:domino .hushlogin
   ```

4. To display the list of files in the account’s home directory, including the permissions, use the **ls** command with the a and l options:

   ```
   cd /export/home/sol1a
   ls -al
   ```

This is the output:

```
total 18
drwxr-x---   2 sol1a    domino       512 Oct 31 16:27 .
drwxr-xr-x   6 root     root         512 Oct 27 15:41 ..
-rw-------   1 sol1a    domino       432 Oct 28 13:53 .bash_history
-rw-r--r--   1 sol1a    domino       136 Oct 27 14:57 .cshrc
-rw-r--r--   1 sol1a    domino         0 Oct 28 08:06 .hushlogin
-rw-r--r--   1 sol1a    domino       157 Oct 27 14:57 .login
-rw-r--r--   1 sol1a    domino       222 Oct 31 12:18 .profile
root@dom1a #
```

4.8 Setting owner and group for Domino transaction logs

A Solaris application requires permission to access a file or directory. The permissions are Read, Write, and Execute. Each file and directory has three sets of these permissions, organized as:

User The Solaris account that owns the file. Defines the access rights of the file's owner.

Group A Solaris group name. Defines the access rights for a Solaris account in that group.

Other Defines the access rights for all Solaris accounts that are not the owner or in the group.

The **ls -l** command lists the files in a directory and displays the "long listing" for each file. For example:

```
cd /notes
ls -l
```

This is the output:

```
total 40
drwxr-xr-x  14 sol1a    domino      4608 Nov  2 13:14 dom1a
drwxr-xr-x  13 sol2b    domino      4096 Nov  2 13:14 dom2b
drwxr-xr-x   3 root     root         512 Oct 26 15:12 log1a
drwxr-xr-x   3 root     root         512 Oct 26 15:13 log2b
```

The first column shows the permissions. The left-most letter indicates whether this is a directory or a file. (A dash in the left position indicates that it is a file; a directory is designated by the letter d.) The next nine letters indicate the access rights to the file for the owner, group, and other, given in three-character segments. From left to right, the permissions in each segment are read access, write access, and execute access. Therefore, an entry of rwx means that read, write, and execute access is granted. If any of the letters has a dash in its place, then that permission is not allowed. For example, r-x means that read and execute access is given but write access is not.

The owner is the user ID that owns the file, which is indicated by the third column. The owner's permissions are read from the first three permission characters in column 1 (following the file or directory indicator).

The group is identified in the fourth column. The group's permissions are identified in the next three characters in column 1.

"Other" is anyone else who has a logon access to this system. Their permissions are specified in the last three characters of column 1.

The Domino installation sets the proper owner and group to the Solaris account that will run the partition for the Domino data directory. There might be other directories that Domino will have to access that you have to set manually. The two most common directories to be changed are:

- Domino Transaction Log directory.
- File system mount points for subdirectories under the main Domino data directory. For example, you may have multiple file systems mounted under the Mail directory.

For our example, we need to change the owner and group for the file systems we plan to use for our Domino transaction logs.

For the sun1 server:

- For partition dom1a's transaction logs, set Solaris account `sol1a` as the owner and `domino` as the group for /notes/log1a.
- For partition dom2b's transaction logs, set Solaris account `sol2b` as the owner and `domino` as the group for /notes/log2b.
- Log on as root and execute the following commands:

  ```
  cd /notes
  ls -l
  ```

  This is the output:

  ```
  total 40
  drwxr-xr-x  14 sol1a    domino      4608 Nov  2 13:20 dom1a
  drwxr-xr-x  13 sol2b    domino      4096 Nov  2 13:20 dom2b
  drwxr-xr-x   3 root     root         512 Oct 26 15:12 log1a
  drwxr-xr-x   3 root     root         512 Oct 26 15:13 log2b
  ```

```
chown sol1a:domino log1a
chown sol2b:domino log2b
ls -l
```

This is the output:

```
total 40
drwxr-xr-x  14 sol1a    domino      4608 Nov  2 13:22 dom1a
drwxr-xr-x  13 sol2b    domino      4096 Nov  2 13:22 dom2b
drwxr-xr-x   3 sol1a    domino       512 Oct 26 15:12 log1a
drwxr-xr-x   3 sol2b    domino       512 Oct 26 15:13 log2b
```

We need a similar change on the sun2 server:

- Log on as root and execute the following commands:

```
cd /notes
ls -l
```

This is the output:

```
total 32
drwxr-xr-x  14 sol1b    domino      4096 Nov  2 14:22 dom1b
drwxr-xr-x  14 sol2a    domino      4096 Nov  2 14:22 dom2a
drwxr-xr-x   3 root     root         512 Oct 26 16:43 log1b
drwxr-xr-x   3 root     root         512 Oct 26 16:43 log2a
root@dom1b # chown sol1b:domino log1b
root@dom1b # chown sol2a:domino log2a
root@dom1b # ls -l
total 32
drwxr-xr-x  14 sol1b    domino      4096 Nov  2 14:23 dom1b
drwxr-xr-x  14 sol2a    domino      4096 Nov  2 14:23 dom2a
drwxr-xr-x   3 sol1b    domino       512 Oct 26 16:43 log1b
drwxr-xr-x   3 sol2a    domino       512 Oct 26 16:43 log2a
```

4.9 Moving applications from Windows to Solaris

Domino databases are *platform independent*, meaning that you can copy files from one Domino server to Domino running on Solaris and open the database without any kind of change to the file format.

However, keep in mind a few considerations regarding the differences in the environment. To ensure that your application will be compatible, consider the following questions before moving an application to Solaris:

1. Is your Domino application “self contained?”
2. Did you use CASE (Computer Aided Software Engineering) tools?
3. Does it use OS platform exploitation?

Is your Domino application “self-contained?”

A self-contained application runs entirely inside the Domino server without any explicit references to files, without external calls, and without importing or exporting data. An explicit reference to a file, such as c:\domino\data\NAMES.NSF, does not work on Solaris and must be replaced with the Solaris path to the database (for example, /notes/dom1a/names.nsf). Solaris does not support the \ character for specifying paths; it uses the / character. Solaris is case sensitive when specifying paths and file names; operating systems such as Windows are not. Case sensitivity can also be a problem anywhere an external script call, link, or hotspot is used; be sure to check that the correct case is used.

Did you use CASE tools?

CASE tools might be helpful, but many of these tools were created with non-UNIX operating systems in mind and their output code might not be compatible with Solaris. Be sure to check with the manufacturer for compatibility before using these tools.

Does your application use OS platform exploitation?

Anything in the application that might be platform specific could fail in the Solaris environment. For example, Windows-specific services such as Active-X controls, or compilers that rely on platform-specific libraries to compile the application, cause problems when the application is moved to Solaris.

4.9.1 Moving the application to the Solaris server

We use Windows 2000 as our source server in the example that follows. You may use a similar procedure when moving from other platforms.

Files can be transferred from Windows to Solaris using many methods. FTP, transfer via CDRW, Iomega Jazz drives, or other media, and NFS are all good ways of moving the data. For this example we use FTP because it is the most common tool used in the field.

FTP servers are installed by default on the Solaris server and might not be enabled on the Windows server™, so it is usually easier to open an FTP session from the Windows server and connect to the Solaris server.

1. On the Windows box, open a command prompt by selecting **Start** → **Programs** → **Accessories** → **Command Prompt**.
   a. Change directory to the server’s data directory with this command:

      ```
      cd \lotus\domino\data
      ```

   b. Start an FTP session with the command **`ftp`** ***`servername`***.

2. Change directory on the Solaris box to the data directory by using the command **`cd /notes/dom1a`** (or any other data dir).

   Switch to binary transfer mode by issuing the command **`bin`**.

3. Transfer the databases by issuing the **`put names.nsf`** command, or transfer multiple files at once using wildcards with the command **`mput *.nsf`**.

> **Important:** Never add or remove databases from the OS level while the Domino server is up and running. Domino caches the data directory listing, and unpredictable behavior can occur if you modify the data directory while the server is running. This could result in a server crash or hang.

Ensuring that permissions are correct

After the transfer is complete, make certain that permissions are correct on the Solaris server. Log on to the Solaris server, change to the data directory (**`cd /notes/dom1a`**) and check the permissions on the transferred file using **`ls -l *.nsf`**. An example of the permissions line is:

```
ls -l *.nsf
-rw-r--r--   1 sol1a    domino   15204352 Nov  4 16:13 mydata.nsf
```

Interpret this record as follows:

The first column shows the permissions. The left-most letter indicates whether this is a directory or a file. A dash in the left position indicates that it is a file; a directory is designated by the letter d. The next nine letters indicate the access rights to the file for the owner, group, and other, given in three-character segments. From left to right, the permissions in each segment are read access, write access, and execute access. Therefore, an entry of rwx means that read, write, and execute access is granted. If any of the letters has a dash in its place, then that permission is not allowed. For example, r-x means that read and execute access is given but write access is not.

The owner is the user ID that owns the file, which is indicated by the third column. The owner's permissions are read from the first three permission characters in column 1 (following the file or directory indicator).

The group is identified in the fourth column. In this case it is the `domino` group. The group's permissions are identified in the next three characters in column 1.

"Other" is anyone else who has logon access to this system. Their permissions are specified in the last three characters of column 1.

The following commands are used to adjust the ownership and permissions:

- **`chown`** ***`accountname filename`*** changes the file's owner.

- **chown** ***accountname:groupname filename*** changes the files owner and group.
- **chgrp** ***groupname filename*** changes the file's group.
- **chmod** ***permission filename*** changes the file's permissions. See **man chmod** for the details.

Checking for case sensitivity

In some operating systems such as Windows, file names are not case sensitive, but in Solaris they are. If your scripts call for the file log.nsf and the file is listed as LOG.NSF at the OS level, the file will not be found when the script runs. After the FTP completes, check to ensure that the file names are in lowercase unless your application is specifying otherwise.

```
ls -l *.nsf
-rw-r--r--   1 solla    domino   15204352 Nov  4 16:13 MYDATA.NSF
mv MYDATA.NSF mydata.nsf
ls -l *.nsf
-rw-r--r--   1 solla    domino   15204352 Nov  4 16:13 mydata.nsf
```

Important: There are two modes of file transfer in FTP: binary and ASCII. Binary transfers are an exact copy, and no reformatting of the file is done by FTP. ASCII transfer assumes that the file you are transferring is a text file and, when transferring between platforms, attempts to reformat the file to the native text format of the destination machine. If you are in ASCII mode when transferring a database, the database will be unreadable by Domino on the destination machine. Some versions of FTP start in ASCII mode, so you should always type **bin** on the FTP command line to ensure that you are in binary mode *before* transferring any databases or templates.

5

Installing Lotus Domino 7 on Sun Solaris 10

In this chapter we describe the installation of IBM Lotus Domino 7 on Sun Solaris 10.

In the first part of the chapter we review the steps necessary to prepare your Sun Solaris environment. Next, we take you step-by-step through the installation of the Domino server code, describe how to set up the Domino server, and finally, discuss various methods for starting and stopping the Domino server.

In brief, setting up Domino 7 on your Solaris server requires the following steps:

1. Set up the hardware.
2. Install and patch Solaris. (Refer to Domino release notes for required patches.)
3. Set up and test the network.
4. Add and set up the Solaris group and user accounts for Domino.
5. Install the Domino software from a tar file.
6. Set up and configure Domino.

© Copyright IBM Corp. 2006. All rights reserved.

5.1 Prerequisites checklist

Before starting your Domino server installation, you have to:

- Install and configure the Solaris environment.
- Prepare the Domino installation.

In this section we provide a checklist for each of these processes. Use them to ensure that you have completed all of the steps that are needed for a successful Domino installation. See Chapter 4, “Solaris 10 installation, configuration, and considerations” on page 29 for a detailed discussion of the preparation process.

5.1.1 Install and configure the Solaris environment

1. Check your hardware configuration.
2. Check patch level; if necessary, install the latest patches. You can use **`showrev -p`** to view the latest patches.

   During installation, the Domino install script will notify you if your OS has the required patches.
3. Check the kernel parameters. See the Domino release notes for the revision of Domino that you are installing by selecting **Technical Library** → **Product Documentation** at:

   http://ibm.com/developerworks/lotus

   > **Attention:** Always refer to the current Domino release notes on the IBM Web site for important installation and configuration guidance.

4. Check services. Disable unnecessary services (sendmail, http, and so forth).
5. Adapt Solaris configuration files:
   - /etc/inetd.conf
   - /etc/defaultrouter
   - /etc/hosts
   - /etc/system
   - /(userhome)/.profile
6. Prepare TCP/IP.
   - Hostnames (Domino server’s common name)
   - TCP/IP address (or addresses)
   - Network mask
   - Domain name server (DNS)
   - Default gateway
   - Static routes (if necessary)
7. Configure network.

5.1.2 Prepare the Domino installation

1. Determine the number of Domino Partitions (DPARs).
2. Prepare the Solaris file systems. Determine the Domino data directories and mount an appropriate Solaris file system for each partition.
3. Determine the destination disk for the Domino binaries (program files). Make sure you have enough disk space. This is an important planning consideration when supporting different versions of Domino on the same physical server. (See 5.2.1, “Installing different versions of Domino on one physical server” on page 106.)
4. Reserve additional space for transactional logs. As discussed previously, transactional log files must be installed on a separate physical disk. (See 3.4, “Disk space” on page 24 for details.)
5. Determine the Solaris user account and group names for every Domino partition. For security reasons, we recommend that you not use `notes` (the default) for the Solaris account name. For convention reasons we also recommend using something other than `notes` (the default) for the Solaris group name. In our example we use `domino`.
6. Create a common group for the Solaris users that will be used to run a Domino partition.
7. Create a Solaris user account that corresponds with the Domino server. Create additional Solaris user accounts when running partitioned Domino servers. Make the Solaris user accounts members of the same Solaris group.
8. Configure the Solaris user environment for Domino users. Put Domino data and program directories into the Solaris user account’s path environment variable. Use the .profile discussed in the previous chapter. Additionally, edit the .profile or .cshrc, depending on which UNIX shell you have selected, and the .hushlogin files.
9. Decide on a Domino naming convention for your Domino domain (if new), organizational units, organizations, and servers. (For example, BosMail01/Sales/Acme in the Acme domain.)
10. Register Domino servers (create the Domino server IDs) in advance for all Domino server partitions being installed (additional Domino servers only). Do not set a Domino server ID password if you plan to automate starting your Domino servers, or, if you do set a Server ID password, you will need to accommodate a password-entry requirement in your scripts that automate Domino server startup.

11.Review the latest version of Sun’s technical document “Domino on Solaris: Common Tuning Tips.” This can be found on the Technical Documentation page of the Sun Microsystems Web site at:

`http://www.sun.com/lotus`

> **Note:** For more information, see Chapter 3, “Sizing guidelines for IBM Lotus Domino Messaging Server” on page 19.

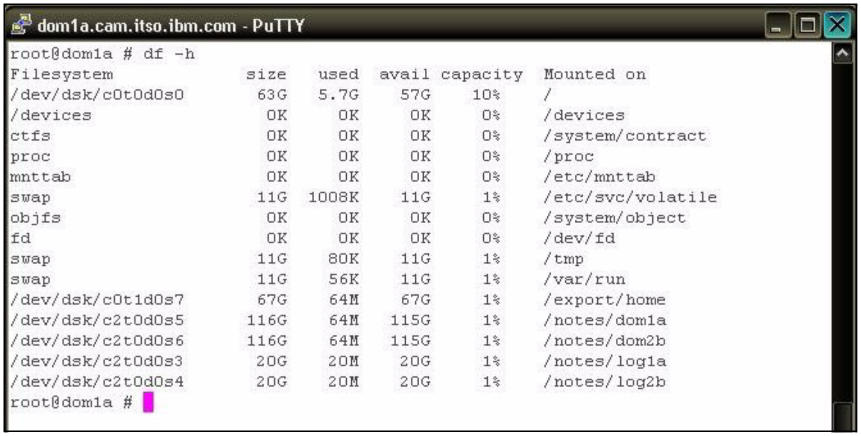
5.2 Install Domino server code

There are two parts to installing Lotus Domino on Sun Solaris. The first part is to install the Domino server code, which is done at the server console. This section provides the steps to install the code. The second part is to configure the server, which is typically done using the Remote Server Setup utility that communicates with the Domino server after the software installation has completed. This process is described in 5.3, “Setting up Domino servers” on page 109.

To run the UNIX program to install the Domino server, perform these steps:

1. Log on to Solaris as the privileged user `root`. Review file systems and available disk resources. (For security reasons we recommend that you disable telnet and use ssh instead.)

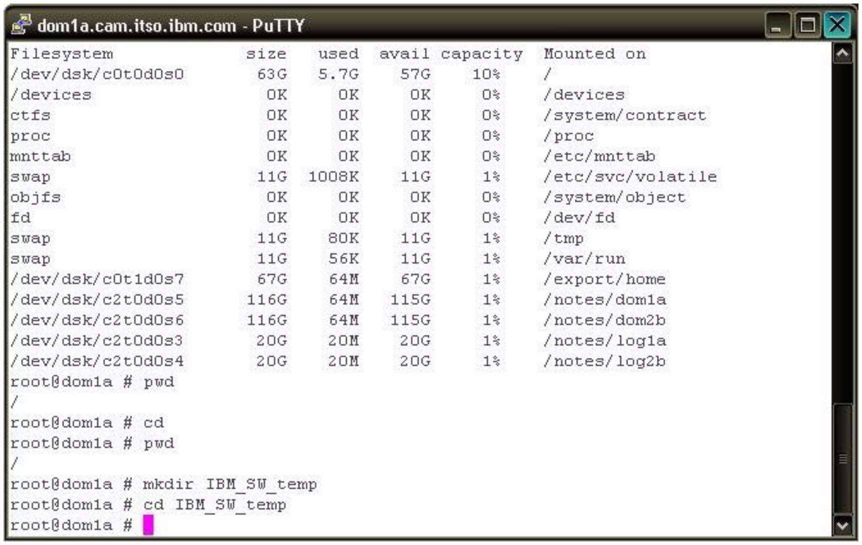
   You log in as `root` because the files in your Domino Program directory (default path: /opt/ibm/lotus) must be owned by root*.* Review the Solaris disk resources and file system layout as defined when you prepared the Solaris environment (Figure 5-1).



```
root@dom1a # df -h
Filesystem             size   used  avail capacity  Mounted on
/dev/dsk/c0t0d0s0       63G   5.7G    57G    10%    /
/devices                 0K     0K     0K     0%    /devices
ctfs                     0K     0K     0K     0%    /system/contract
proc                     0K     0K     0K     0%    /proc
mnttab                   0K     0K     0K     0%    /etc/mnttab
swap                    11G  1008K    11G     1%    /etc/svc/volatile
objfs                    0K     0K     0K     0%    /system/object
fd                       0K     0K     0K     0%    /dev/fd
swap                    11G    80K    11G     1%    /tmp
swap                    11G    56K    11G     1%    /var/run
/dev/dsk/c0t1d0s7       67G    64M    67G     1%    /export/home
/dev/dsk/c2t0d0s5      116G    64M   115G     1%    /notes/dom1a
/dev/dsk/c2t0d0s6      116G    64M   115G     1%    /notes/dom2b
/dev/dsk/c2t0d0s3       20G    20M    20G     1%    /notes/log1a
/dev/dsk/c2t0d0s4       20G    20M    20G     1%    /notes/log2b
root@dom1a #
```

Figure 5-1 Review Solaris disk resources and file system layout

2. Next, define a UNIX directory where the Domino server installation code will be staged temporarily. IBM now provides the Domino Installer in a UNIX tar file. Be sure to have enough disk space available for the temporary decompression of the Domino tar file, as it will use about 700 MB. In our example we defined a new location called `IBM_SW_temp` (Figure 5-2).



```
Filesystem             size   used  avail capacity  Mounted on
/dev/dsk/c0t0d0s0       63G   5.7G    57G    10%    /
/devices                 0K     0K     0K     0%    /devices
ctfs                     0K     0K     0K     0%    /system/contract
proc                     0K     0K     0K     0%    /proc
mnttab                   0K     0K     0K     0%    /etc/mnttab
swap                    11G  1008K    11G     1%    /etc/svc/volatile
objfs                    0K     0K     0K     0%    /system/object
fd                       0K     0K     0K     0%    /dev/fd
swap                    11G    80K    11G     1%    /tmp
swap                    11G    56K    11G     1%    /var/run
/dev/dsk/c0t1d0s7       67G    64M    67G     1%    /export/home
/dev/dsk/c2t0d0s5      116G    64M   115G     1%    /notes/dom1a
/dev/dsk/c2t0d0s6      116G    64M   115G     1%    /notes/dom2b
/dev/dsk/c2t0d0s3       20G    20M    20G     1%    /notes/log1a
/dev/dsk/c2t0d0s4       20G    20M    20G     1%    /notes/log2b
root@dom1a # pwd
/
root@dom1a # cd
root@dom1a # pwd
/
root@dom1a # mkdir IBM_SW_temp
root@dom1a # cd IBM_SW_temp
root@dom1a #
```

Figure 5-2   Create a temporary location for the Domino installer code

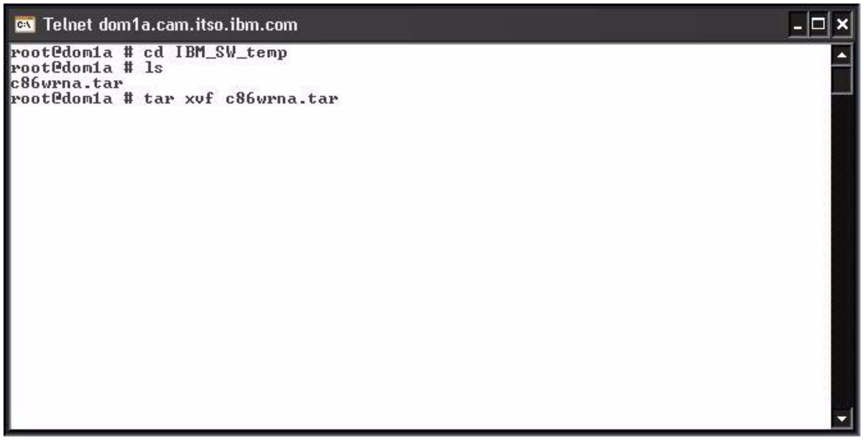
3. As mentioned previously, the Domino for Solaris server installation code is commonly provided as a UNIX tar file. As we write this book, the Domino 7 for Solaris installer file is called:

   ```
   c86wrna.tar
   ```

   If you have downloaded the installer to a Windows workstation, you can perform a binary mode FTP to transfer it to the desired Solaris directory location we created for it: /IBM_SW_temp.

   From the root user, make the /IBM_SW_temp directory current, confirm that the Domino installer tar file is located there, and invoke the Solaris command to unpack the installer file (Figure 5-3 on page 82).

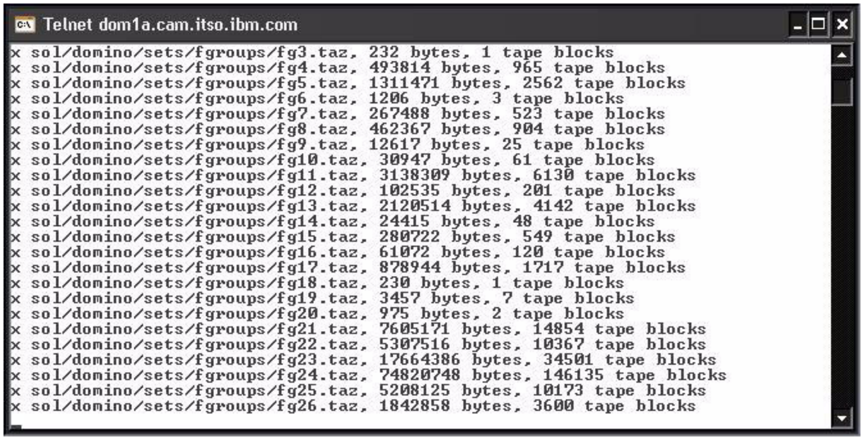
> **Note:** We used Telnet in the next series of screens, despite a prior recommendation that you use ssh instead of telnet. This decision was made for the sake of expediency in installing and configuring the lab environment for this book.



```
root@dom1a # cd IBM_SW_temp
root@dom1a # ls
c86wrna.tar
root@dom1a # tar xvf c86wrna.tar
```

Figure 5-3 Preparing to unpack the Domino installer file

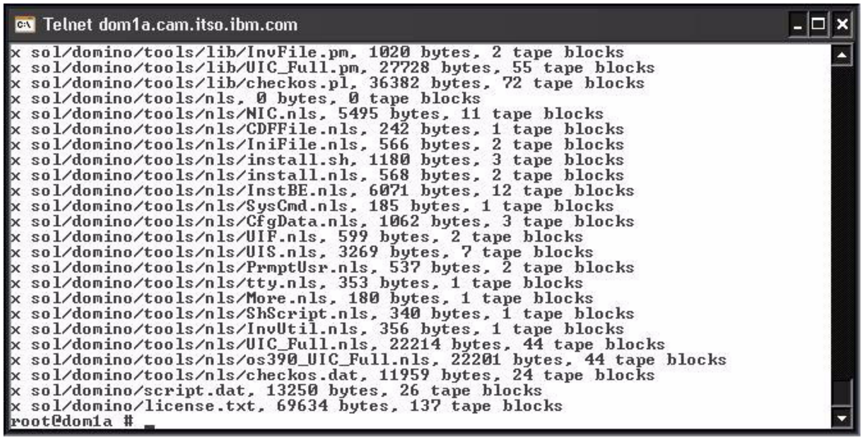
4. Type `tar xvf c86wrna.tar` and the Domino Installer begins unpacking (Figure 5-4).



```
x sol/domino/sets/fgroups/fg3.taz, 232 bytes, 1 tape blocks
x sol/domino/sets/fgroups/fg4.taz, 493814 bytes, 965 tape blocks
x sol/domino/sets/fgroups/fg5.taz, 1311471 bytes, 2562 tape blocks
x sol/domino/sets/fgroups/fg6.taz, 1206 bytes, 3 tape blocks
x sol/domino/sets/fgroups/fg7.taz, 267488 bytes, 523 tape blocks
x sol/domino/sets/fgroups/fg8.taz, 462367 bytes, 904 tape blocks
x sol/domino/sets/fgroups/fg9.taz, 12617 bytes, 25 tape blocks
x sol/domino/sets/fgroups/fg10.taz, 30947 bytes, 61 tape blocks
x sol/domino/sets/fgroups/fg11.taz, 3138309 bytes, 6130 tape blocks
x sol/domino/sets/fgroups/fg12.taz, 102535 bytes, 201 tape blocks
x sol/domino/sets/fgroups/fg13.taz, 2120514 bytes, 4142 tape blocks
x sol/domino/sets/fgroups/fg14.taz, 24415 bytes, 48 tape blocks
x sol/domino/sets/fgroups/fg15.taz, 280722 bytes, 549 tape blocks
x sol/domino/sets/fgroups/fg16.taz, 61072 bytes, 120 tape blocks
x sol/domino/sets/fgroups/fg17.taz, 878944 bytes, 1717 tape blocks
x sol/domino/sets/fgroups/fg18.taz, 230 bytes, 1 tape blocks
x sol/domino/sets/fgroups/fg19.taz, 3457 bytes, 7 tape blocks
x sol/domino/sets/fgroups/fg20.taz, 975 bytes, 2 tape blocks
x sol/domino/sets/fgroups/fg21.taz, 7605171 bytes, 14854 tape blocks
x sol/domino/sets/fgroups/fg22.taz, 5307516 bytes, 10367 tape blocks
x sol/domino/sets/fgroups/fg23.taz, 17664386 bytes, 34501 tape blocks
x sol/domino/sets/fgroups/fg24.taz, 74820748 bytes, 146135 tape blocks
x sol/domino/sets/fgroups/fg25.taz, 5208125 bytes, 10173 tape blocks
x sol/domino/sets/fgroups/fg26.taz, 1842858 bytes, 3600 tape blocks
```

Figure 5-4 Domino Installer file unpacking

5. When the Domino Installer finishes unpacking you return to the Solaris command prompt.



```
x sol/domino/tools/lib/InvFile.pm, 1020 bytes, 2 tape blocks
x sol/domino/tools/lib/UIC_Full.pm, 27728 bytes, 55 tape blocks
x sol/domino/tools/lib/checkos.pl, 36382 bytes, 72 tape blocks
x sol/domino/tools/nls, 0 bytes, 0 tape blocks
x sol/domino/tools/nls/NIC.nls, 5495 bytes, 11 tape blocks
x sol/domino/tools/nls/CDFFile.nls, 242 bytes, 1 tape blocks
x sol/domino/tools/nls/IniFile.nls, 566 bytes, 2 tape blocks
x sol/domino/tools/nls/install.sh, 1180 bytes, 3 tape blocks
x sol/domino/tools/nls/install.nls, 568 bytes, 2 tape blocks
x sol/domino/tools/nls/InstBE.nls, 6071 bytes, 12 tape blocks
x sol/domino/tools/nls/SysCmd.nls, 185 bytes, 1 tape blocks
x sol/domino/tools/nls/CfgData.nls, 1062 bytes, 3 tape blocks
x sol/domino/tools/nls/UIF.nls, 599 bytes, 2 tape blocks
x sol/domino/tools/nls/UIS.nls, 3269 bytes, 7 tape blocks
x sol/domino/tools/nls/PrmptUsr.nls, 537 bytes, 2 tape blocks
x sol/domino/tools/nls/tty.nls, 353 bytes, 1 tape blocks
x sol/domino/tools/nls/More.nls, 180 bytes, 1 tape blocks
x sol/domino/tools/nls/ShScript.nls, 340 bytes, 1 tape blocks
x sol/domino/tools/nls/InvUtil.nls, 356 bytes, 1 tape blocks
x sol/domino/tools/nls/UIC_Full.nls, 22214 bytes, 44 tape blocks
x sol/domino/tools/nls/os390_UIC_Full.nls, 22201 bytes, 44 tape blocks
x sol/domino/tools/nls/checkos.dat, 11959 bytes, 24 tape blocks
x sol/domino/script.dat, 13250 bytes, 26 tape blocks
x sol/domino/license.txt, 69634 bytes, 137 tape blocks
root@dom1a # _
```

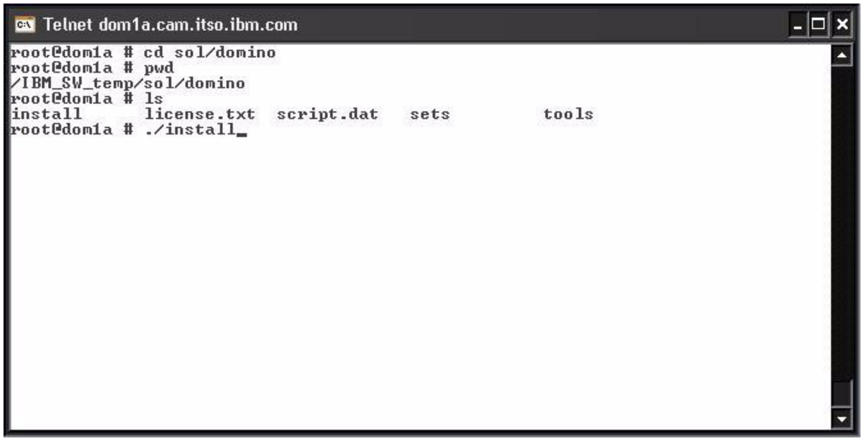
Figure 5-5 Domino Installer unpacked

After this tar file is unpacked, its component files will be stored in a new temporary location; in our example, this is /IBM_SW_temp/sol/domino.

6. Now we can install Domino server software on this physical Solaris server.

   Subject to your requirements and the system resources of your server, you will be able to install one or multiple Domino instances on this server. When there are multiple instances of Domino on a physical server, each individual instance is typically called a *Domino Partition* or abbreviated as *DPAR*.

   Now that the Domino Installer code has been unpacked, let's go to the directory where it is located (Figure 5-6). While still working as the root user, begin the installation by typing `./install`.

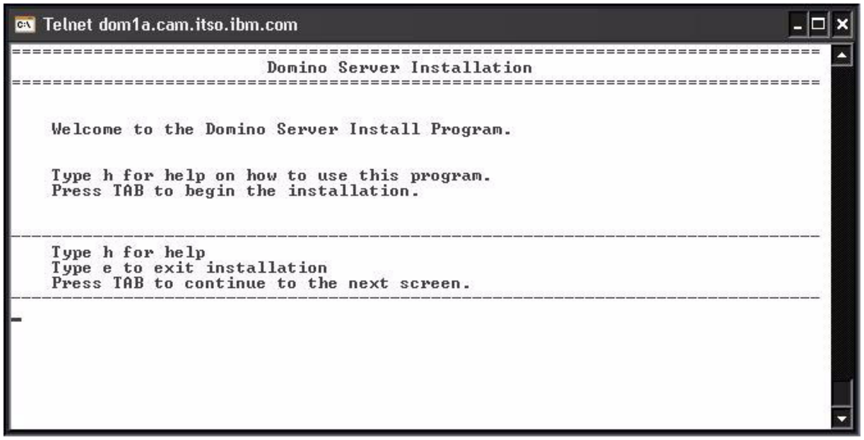


```
root@dom1a # cd sol/domino
root@dom1a # pwd
/IBM_SW_temp/sol/domino
root@dom1a # ls
install      license.txt  script.dat   sets         tools
root@dom1a # ./install_
```

Figure 5-6 Launch Domino installation program

Note: Organizations that use the Common Desktop Environment (CDE) or Sun Java™ Desktop can access these directories and files using the corresponding file management graphical interface. Where this is available, you can launch the Domino Installation program by double-clicking it in the file list.

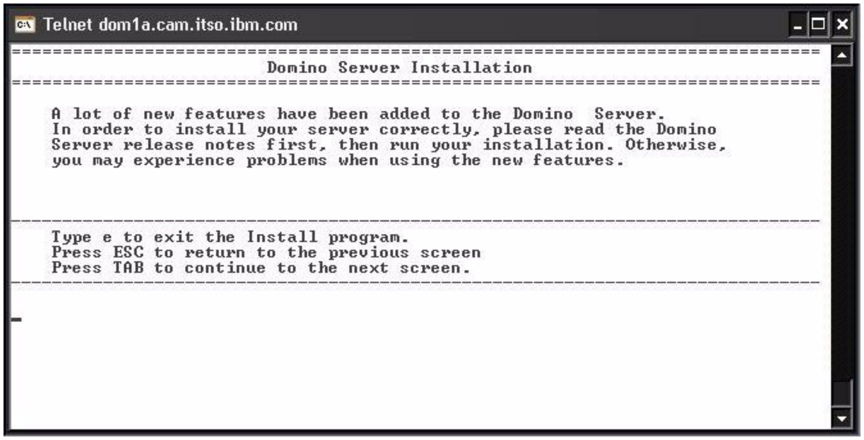
7. Several screens display, prompting you for information that you collected in earlier preparatory steps of this manual (Figure 5-7). Press Tab to continue.



```
===============================================================================
                          Domino Server Installation
===============================================================================


    Welcome to the Domino Server Install Program.


    Type h for help on how to use this program.
    Press TAB to begin the installation.


-------------------------------------------------------------------------------
    Type h for help
    Type e to exit installation
    Press TAB to continue to the next screen.
-------------------------------------------------------------------------------
_
```

Figure 5-7 Welcome screen

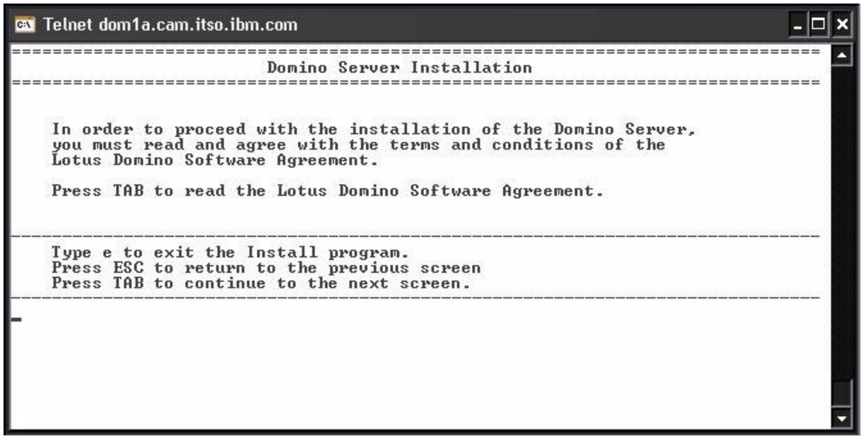
8. Press Tab to continue.



```
===============================================================================
                          Domino Server Installation
===============================================================================

    A lot of new features have been added to the Domino  Server.
    In order to install your server correctly, please read the Domino
    Server release notes first, then run your installation. Otherwise,
    you may experience problems when using the new features.


-------------------------------------------------------------------------------
    Type e to exit the Install program.
    Press ESC to return to the previous screen
    Press TAB to continue to the next screen.
-------------------------------------------------------------------------------

_
```

Figure 5-8 Review the release notes

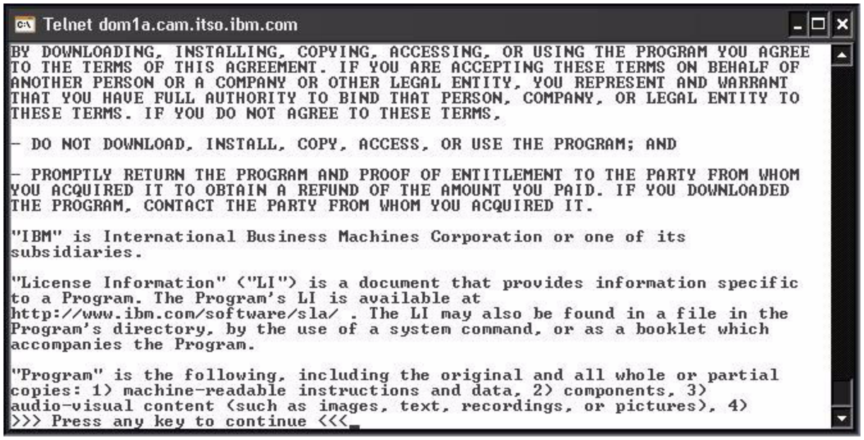
9. Press Tab to continue.



```
==============================================================================
                          Domino Server Installation
==============================================================================


    In order to proceed with the installation of the Domino Server,
    you must read and agree with the terms and conditions of the
    Lotus Domino Software Agreement.

    Press TAB to read the Lotus Domino Software Agreement.


------------------------------------------------------------------------------
    Type e to exit the Install program.
    Press ESC to return to the previous screen
    Press TAB to continue to the next screen.
------------------------------------------------------------------------------
_
```

Figure 5-9 Review the software agreement

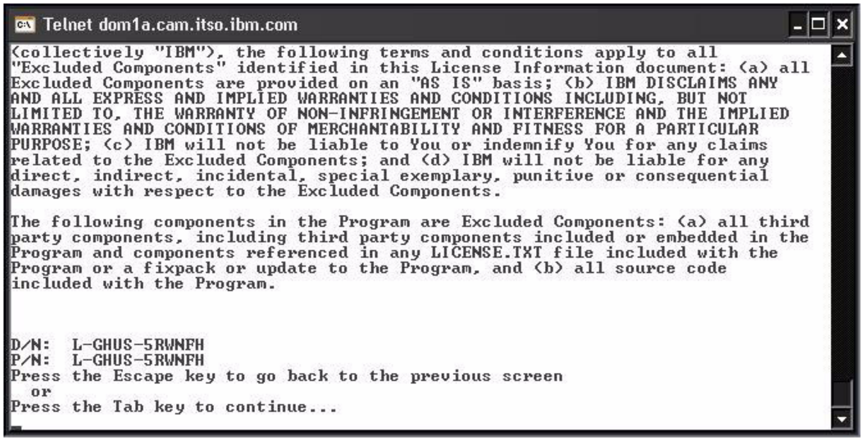
10. The Domino Software License Agreement displays next (Figure 5-10).



```
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE
TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF
ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT
THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO
THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND

- PROMPTLY RETURN THE PROGRAM AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM
YOU ACQUIRED IT TO OBTAIN A REFUND OF THE AMOUNT YOU PAID. IF YOU DOWNLOADED
THE PROGRAM, CONTACT THE PARTY FROM WHOM YOU ACQUIRED IT.

"IBM" is International Business Machines Corporation or one of its
subsidiaries.

"License Information" ("LI") is a document that provides information specific
to a Program. The Program's LI is available at
http://www.ibm.com/software/sla/ . The LI may also be found in a file in the
Program's directory, by the use of a system command, or as a booklet which
accompanies the Program.

"Program" is the following, including the original and all whole or partial
copies: 1) machine-readable instructions and data, 2) components, 3)
audio-visual content (such as images, text, recordings, or pictures), 4)
>>> Press any key to continue <<<_
```

Figure 5-10 Domino Software License Agreement

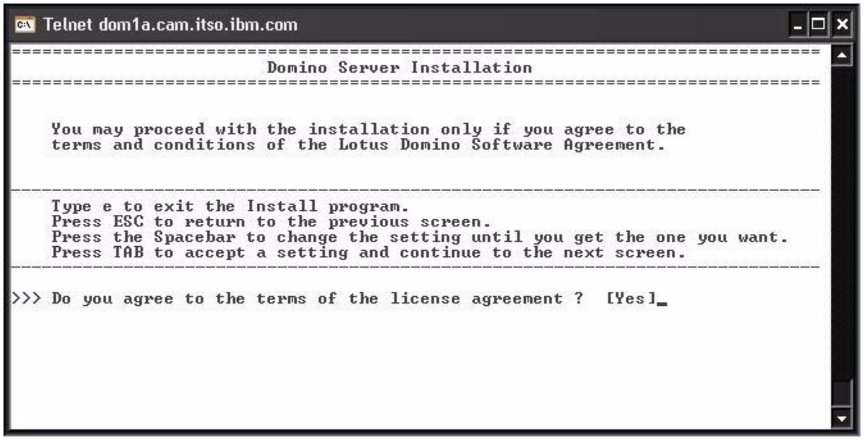
11. Advance through *many* screens to reach the end of the Software License Agreement. When you reach the end, you can continue the Domino Installation process. When you reach the bottom of the Domino Software License Agreement, press Tab to continue.



```
(collectively "IBM"), the following terms and conditions apply to all
"Excluded Components" identified in this License Information document: (a) all
Excluded Components are provided on an "AS IS" basis; (b) IBM DISCLAIMS ANY
AND ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS INCLUDING, BUT NOT
LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OR INTERFERENCE AND THE IMPLIED
WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE; (c) IBM will not be liable to You or indemnify You for any claims
related to the Excluded Components; and (d) IBM will not be liable for any
direct, indirect, incidental, special exemplary, punitive or consequential
damages with respect to the Excluded Components.

The following components in the Program are Excluded Components: (a) all third
party components, including third party components included or embedded in the
Program and components referenced in any LICENSE.TXT file included with the
Program or a fixpack or update to the Program, and (b) all source code
included with the Program.


D/N:  L-GHUS-5RWNFH
P/N:  L-GHUS-5RWNFH
Press the Escape key to go back to the previous screen
  or
Press the Tab key to continue...
```

Figure 5-11 End of Domino Software License Agreement

12. To accept the terms of the Software License agreement, press Tab to continue.

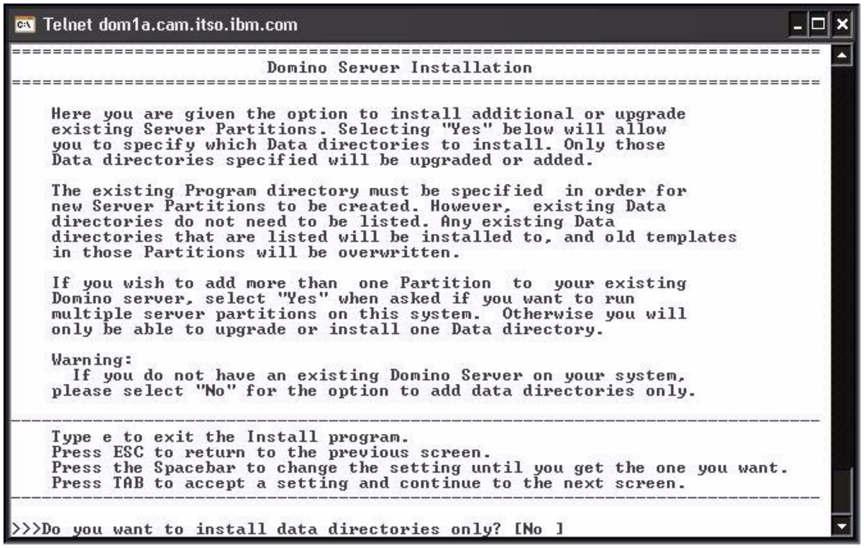


```
===============================================================================
                         Domino Server Installation
===============================================================================


    You may proceed with the installation only if you agree to the
    terms and conditions of the Lotus Domino Software Agreement.


-------------------------------------------------------------------------------
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press the Spacebar to change the setting until you get the one you want.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

>>> Do you agree to the terms of the license agreement ?  [Yes]_
```

Figure 5-12 Accept the license agreement

13. In our example, we are installing Domino Program files and Domino Data directories. Therefore, when asked if we want to install *only* the Domino Data directories, we use the default answer `no`.

    Press Tab to continue.



Telnet dom1a.cam.itso.ibm.com

```
================================================================================
                        Domino Server Installation
================================================================================

    Here you are given the option to install additional or upgrade
    existing Server Partitions. Selecting "Yes" below will allow
    you to specify which Data directories to install. Only those
    Data directories specified will be upgraded or added.

    The existing Program directory must be specified  in order for
    new Server Partitions to be created. However,  existing Data
    directories do not need to be listed. Any existing Data
    directories that are listed will be installed to, and old templates
    in those Partitions will be overwritten.

    If you wish to add more than  one Partition  to  your existing
    Domino server, select "Yes" when asked if you want to run
    multiple server partitions on this system.  Otherwise you will
    only be able to upgrade or install one Data directory.

    Warning:
      If you do not have an existing Domino Server on your system,
    please select "No" for the option to add data directories only.

--------------------------------------------------------------------------------
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press the Spacebar to change the setting until you get the one you want.
    Press TAB to accept a setting and continue to the next screen.
--------------------------------------------------------------------------------

>>>Do you want to install data directories only? [No ]
```

Figure 5-13 Data directories

14. Decide which types of Domino servers you require. When you install a Domino server, you must select one of the following installation options:

    – Domino Utility Server: Installs a Domino server that provides Application services only, with support for Domino clusters but *no* support for messaging services. The Domino Utility Server is a new installation type for Lotus Domino 7 that removes client access license requirements. See full licensing text for details.

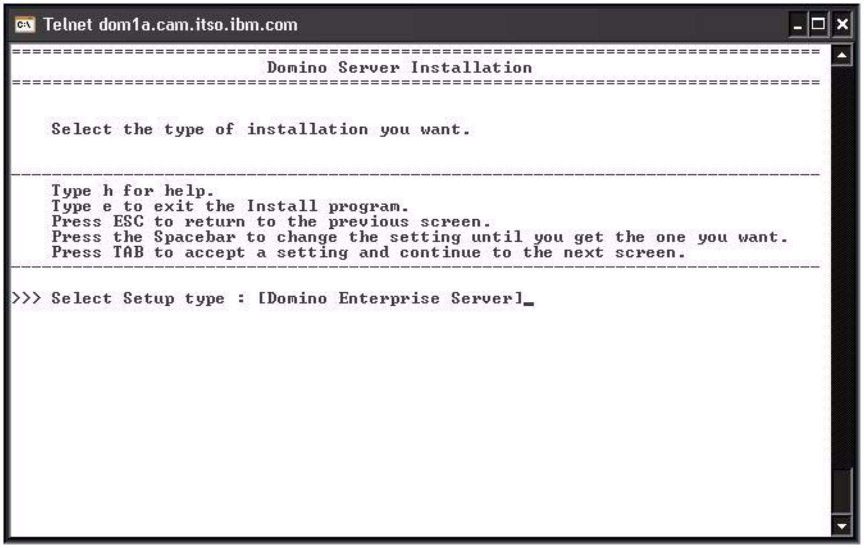
    – Domino Messaging Server: Installs a Domino server that provides Messaging services only, with *no* support for Domino clusters or Application services.

    – Domino Enterprise Server: Installs a Domino server that provides *both* Messaging and Application services, with support for Domino clusters.

    Note: All three types of installations support Domino partitioned servers. Only the Domino Enterprise Server supports a service provider (xSP) environment.

For Domino Clustering to be made available at Domino Installation time, we specify the `[Domino Enterprise Server]` setup type (Figure 5-14).

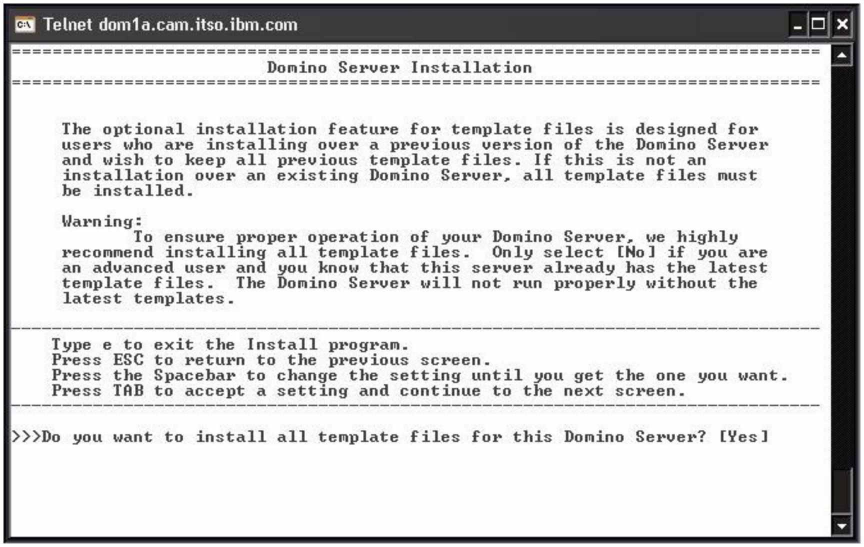
If necessary, press the Spacebar to make your selection, and press Tab to continue.



```
===============================================================================
                          Domino Server Installation
===============================================================================


    Select the type of installation you want.


-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press the Spacebar to change the setting until you get the one you want.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

>>> Select Setup type : [Domino Enterprise Server]_
```

Figure 5-14 Server setup type

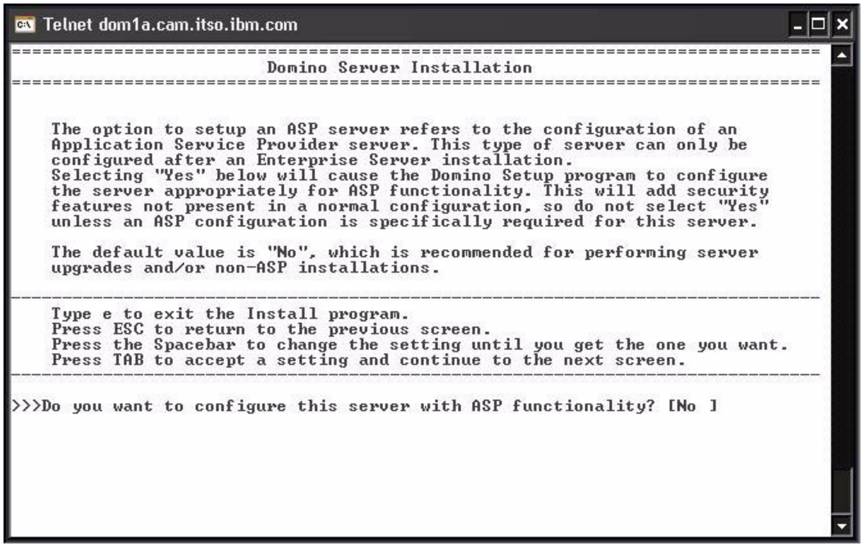
15. Because we are installing a new Domino 7 server, we want to install all of the new Domino 7 template files. Press Tab to continue.



```
================================================================================
                          Domino Server Installation
================================================================================


     The optional installation feature for template files is designed for
     users who are installing over a previous version of the Domino Server
     and wish to keep all previous template files. If this is not an
     installation over an existing Domino Server, all template files must
     be installed.

     Warning:
            To ensure proper operation of your Domino Server, we highly
     recommend installing all template files.  Only select [No] if you are
     an advanced user and you know that this server already has the latest
     template files.  The Domino Server will not run properly without the
     latest templates.

--------------------------------------------------------------------------------
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press the Spacebar to change the setting until you get the one you want.
    Press TAB to accept a setting and continue to the next screen.
--------------------------------------------------------------------------------

>>>Do you want to install all template files for this Domino Server? [Yes]
```

Figure 5-15 Template files

16. Although some organizations require ASP functionality, we believe that this server capability is used by a shrinking population of organizations that use Domino. In our example, we used the default of `no` (Figure 5-16). Press Tab to continue.



```
================================================================================
                          Domino Server Installation
================================================================================


    The option to setup an ASP server refers to the configuration of an
    Application Service Provider server. This type of server can only be
    configured after an Enterprise Server installation.
    Selecting "Yes" below will cause the Domino Setup program to configure
    the server appropriately for ASP functionality. This will add security
    features not present in a normal configuration, so do not select "Yes"
    unless an ASP configuration is specifically required for this server.

    The default value is "No", which is recommended for performing server
    upgrades and/or non-ASP installations.

--------------------------------------------------------------------------------
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press the Spacebar to change the setting until you get the one you want.
    Press TAB to accept a setting and continue to the next screen.
--------------------------------------------------------------------------------

>>>Do you want to configure this server with ASP functionality? [No ]
```

Figure 5-16 ASP functionality

Note: See Domino 7 Administrator Help for more information about Domino server ASP functionality. Search on “Installing the first server or additional servers for hosted environments.”

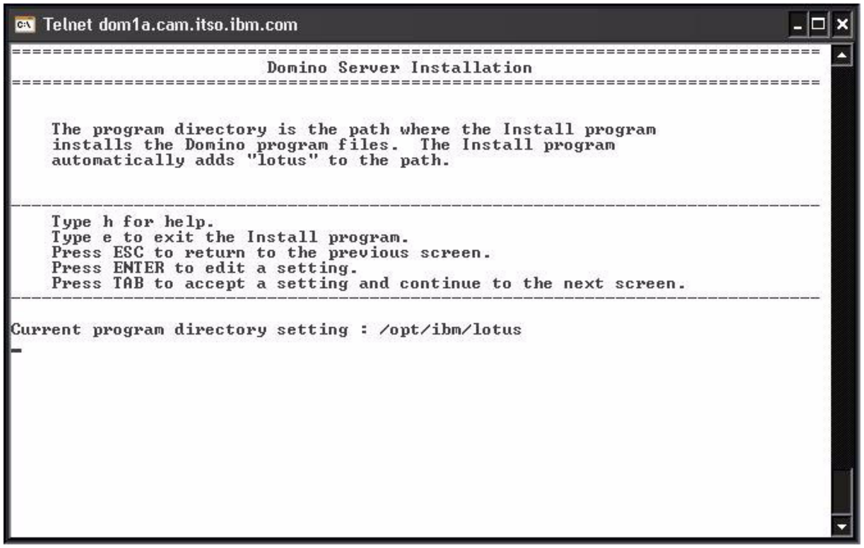
17. Figure 5-17 shows where you are prompted to enter the Domino program directory location. This is where the Domino 7 server code will reside.

Note: The default location in Domino 7 is different from the Domino R5 and Domino 6 default (/opt/lotus).

Attention: When installing a different version of Domino server software on this server, this is where you would enter the version-specific location to install the Domino program files. For more about this, see 5.2.1, “Installing different versions of Domino on one physical server” on page 106.

Follow the instructions if you want to specify a different location for the Domino program files. Our example uses the default location, /opt/ibm/lotus.

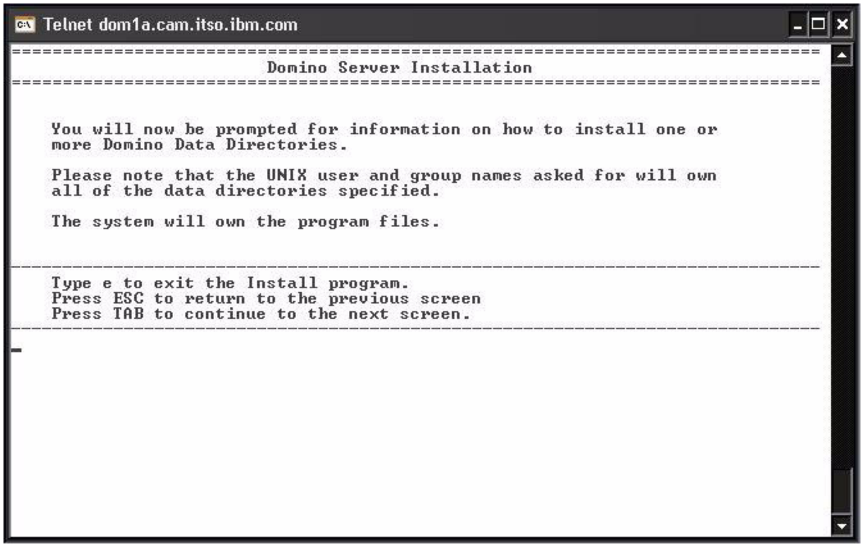
Press Tab to continue.



```
================================================================================
                           Domino Server Installation
================================================================================


    The program directory is the path where the Install program
    installs the Domino program files.  The Install program
    automatically adds "lotus" to the path.


--------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
--------------------------------------------------------------------------------

Current program directory setting : /opt/ibm/lotus
_
```

Figure 5-17 Specify the Domino program directory

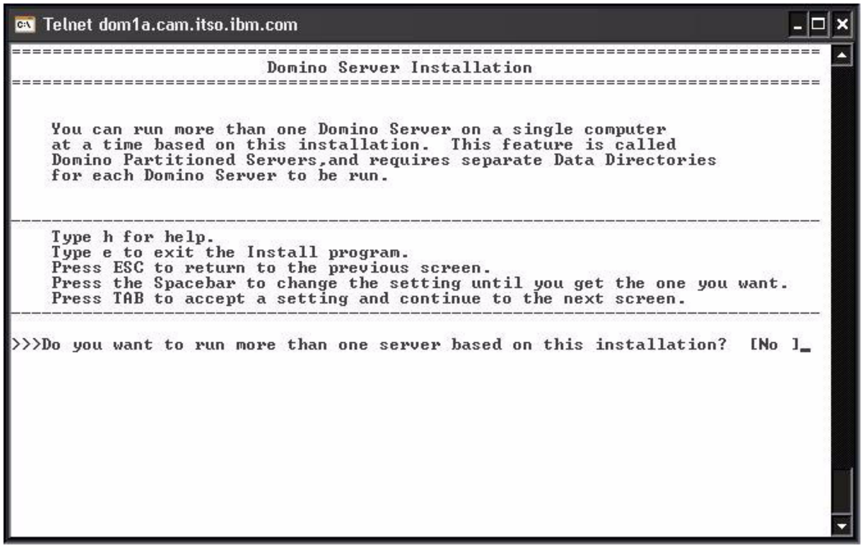
18. Press Tab to continue.



```
Telnet dom1a.cam.itso.ibm.com
===============================================================================
                          Domino Server Installation
===============================================================================


    You will now be prompted for information on how to install one or
    more Domino Data Directories.

    Please note that the UNIX user and group names asked for will own
    all of the data directories specified.

    The system will own the program files.


-------------------------------------------------------------------------------
    Type e to exit the Install program.
    Press ESC to return to the previous screen
    Press TAB to continue to the next screen.
-------------------------------------------------------------------------------
_
```

Figure 5-18 Information screen

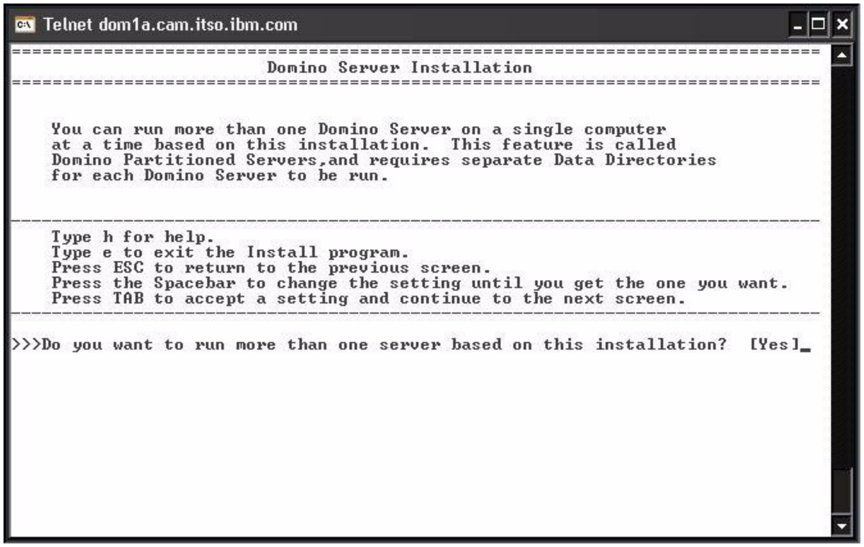
19. In Figure 5-19, the Domino server Installation program has the default expectation that only one instance of this version of Domino will be installed.



```
Telnet dom1a.cam.itso.ibm.com
===============================================================================
                          Domino Server Installation
===============================================================================


    You can run more than one Domino Server on a single computer
    at a time based on this installation.  This feature is called
    Domino Partitioned Servers,and requires separate Data Directories
    for each Domino Server to be run.


-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press the Spacebar to change the setting until you get the one you want.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

>>>Do you want to run more than one server based on this installation?  [No ]_
```

Figure 5-19 Single Domino Partition (default)

20. In an effort to reflect what real-world organizations would do, we change this value as shown in Figure 5-20. Press Tab to continue.

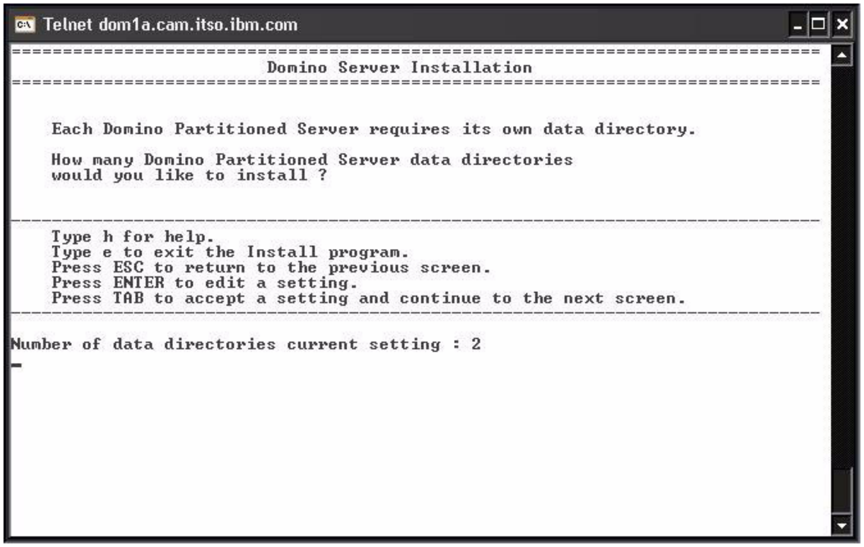


```
==============================================================================
                          Domino Server Installation
==============================================================================


    You can run more than one Domino Server on a single computer
    at a time based on this installation.  This feature is called
    Domino Partitioned Servers,and requires separate Data Directories
    for each Domino Server to be run.


------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press the Spacebar to change the setting until you get the one you want.
    Press TAB to accept a setting and continue to the next screen.
------------------------------------------------------------------------------

>>>Do you want to run more than one server based on this installation?  [Yes]_
```

Figure 5-20 Specifying multiple partitions

21. The Domino server Installation program prompts for the number of Domino partitions that will run on this Sun server (Figure 5-21). Follow the instructions to enter the correct number of Domino partitions for your environment, and press Tab to continue.

    We used the default value, 2, it in our example environment.



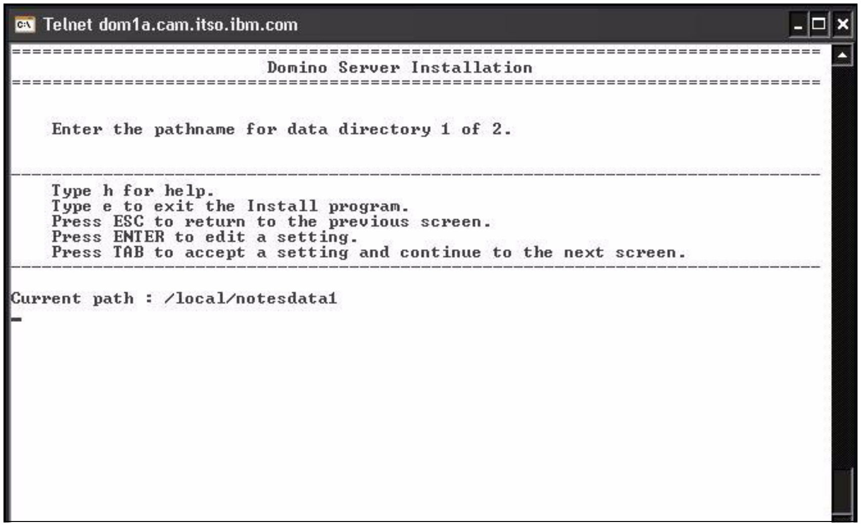
```
===============================================================================
                          Domino Server Installation
===============================================================================


    Each Domino Partitioned Server requires its own data directory.

    How many Domino Partitioned Server data directories
    would you like to install ?


-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

Number of data directories current setting : 2
_
```

Figure 5-21 Two Domino partitions specified

22. The next screen (Figure 5-22) shows the default path to Partition #1's data directory on Solaris (`/local/notesdata1`). You can expect to change this and other settings.

    We are prompted to enter information about the first of two Domino partitions. Most, if not all, organizations will use a different value that conforms to the naming conventions of their environment. In our lab environment, we defined these file systems for the Domino data directories on this physical server:

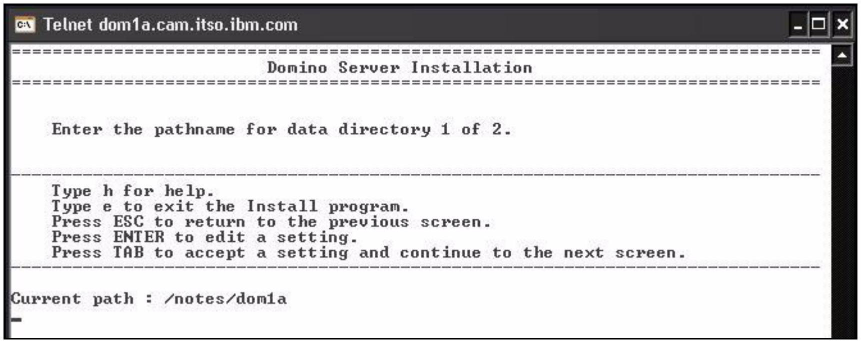
    – Partition #1 will have its Domino data directory in /notes/dom1a.
    – Partition #2 will have its Domino data directory in /notes/dom2b.



```
===============================================================================
                          Domino Server Installation
===============================================================================


    Enter the pathname for data directory 1 of 2.


-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

Current path : /local/notesdata1
_
```

Figure 5-22   Default path to Partition #1 data directory

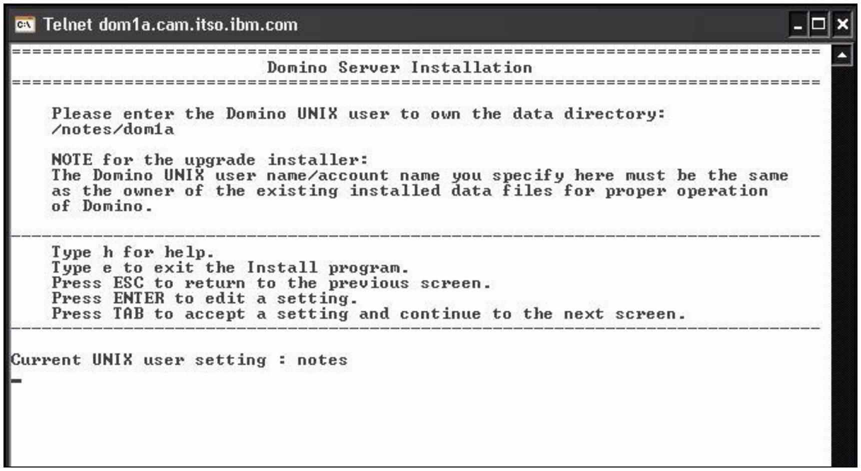
We follow the instructions to make the required change (Figure 5-23). Make the necessary changes to conform to the path name of your Domino Data directory, and press Tab to continue.



```
===============================================================================
                          Domino Server Installation
===============================================================================


    Enter the pathname for data directory 1 of 2.


-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

Current path : /notes/dom1a
_
```

Figure 5-23   Partition #1 path to data directory

23. Enter the Solaris user who will own this Domino partition from the Solaris perspective. As a matter of security, we advise *replacing* the default Solaris user name `notes` with a more meaningful Solaris user name that is similar or identical to the name of the Domino server that will run in its partition.



```
Telnet dom1a.cam.itso.ibm.com
==============================================================================
                         Domino Server Installation
==============================================================================

    Please enter the Domino UNIX user to own the data directory:
    /notes/dom1a

    NOTE for the upgrade installer:
    The Domino UNIX user name/account name you specify here must be the same
    as the owner of the existing installed data files for proper operation
    of Domino.

------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
------------------------------------------------------------------------------

Current UNIX user setting : notes
_
```

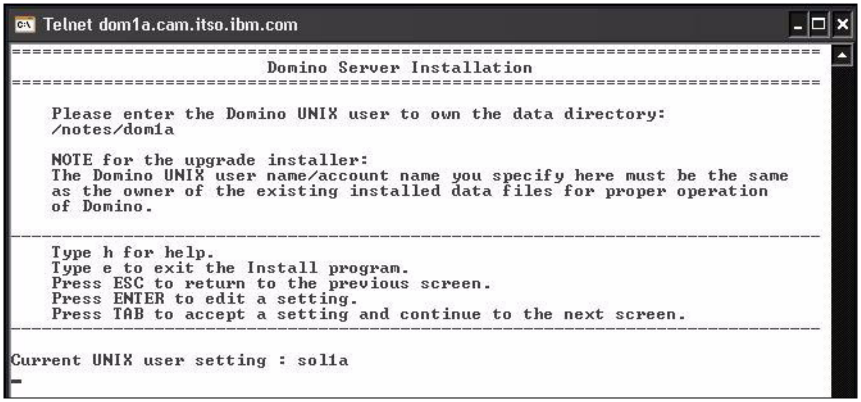
Figure 5-24 Default Solaris user associated with Partition #1

For your environment, follow the instructions to enter the appropriate Solaris user name for your Domino partition and press Tab to continue.

In our example environment, on this physical server:

– `sol1a` is the Solaris user account that owns dom1a (Partition #1), so we changed the user setting on this screen to `sol1a` (Figure 5-25).

– `sol2b` is the Solaris user account that owns dom2b (Partition #2). See step 26 on page 100.



```
Telnet dom1a.cam.itso.ibm.com
==============================================================================
                         Domino Server Installation
==============================================================================

    Please enter the Domino UNIX user to own the data directory:
    /notes/dom1a

    NOTE for the upgrade installer:
    The Domino UNIX user name/account name you specify here must be the same
    as the owner of the existing installed data files for proper operation
    of Domino.

------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
------------------------------------------------------------------------------

Current UNIX user setting : sol1a
_
```

Figure 5-25 Specifying our Solaris user associated with Partition #1

Important: Pay close attention to the screen displays in Figure 5-24 on page 96 and Figure 5-26 on page 98, as they are very similar. The first one prompts you for the Solaris *user* name, and the second one prompts you for the Solaris *group* name.

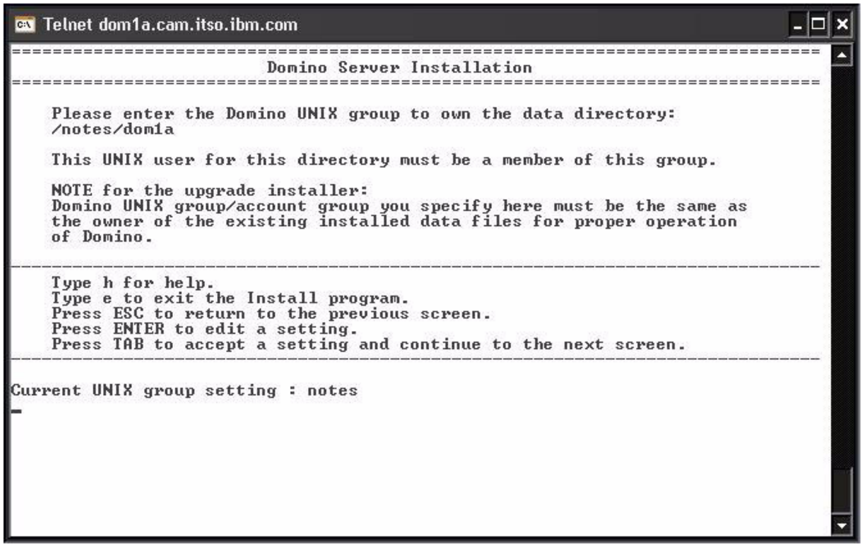
Both screens specify the *same default value*: `notes`.

Do not mistakenly change the default Solaris group name to your chosen Solaris *user* name, or change the default Solaris user name to your chosen Solaris *group* name.

Confusing these screens causes the Domino Server Installation program to specify the wrong Solaris user and group permissions at install time. If this occurs, delete the erroneous installation and relaunch the Domino install program.

24. Enter the Solaris group that your Solaris users (Domino partition owners) will be members of. This default should be changed as well. As a matter of convention, we advise replacing the default group name `notes` with a more meaningful name, such as `domino`.

    For your environment, follow the on-screen instructions to enter the appropriate Solaris group name associated with your Solaris user name and press Tab to continue.

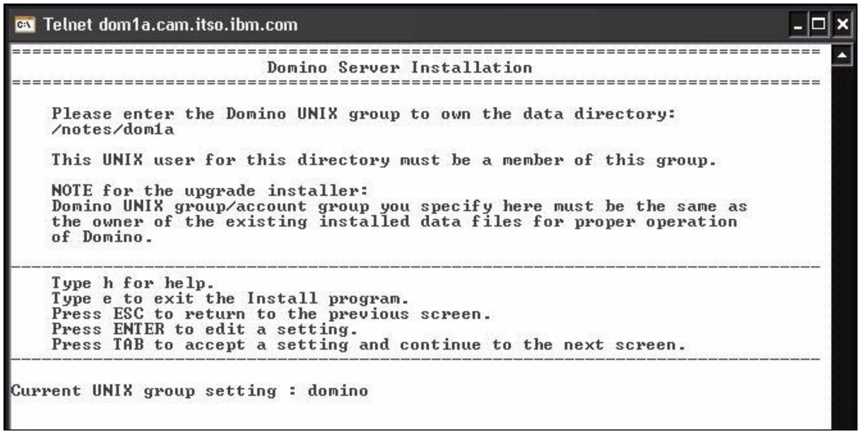


Telnet dom1a.cam.itso.ibm.com

```
===============================================================================
                            Domino Server Installation
===============================================================================

    Please enter the Domino UNIX group to own the data directory:
    /notes/dom1a

    This UNIX user for this directory must be a member of this group.

    NOTE for the upgrade installer:
    Domino UNIX group/account group you specify here must be the same as
    the owner of the existing installed data files for proper operation
    of Domino.

-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

Current UNIX group setting : notes
_
```

Figure 5-26 Default Solaris group for this physical server

For our example (Figure 5-26), we changed it to `domino`.



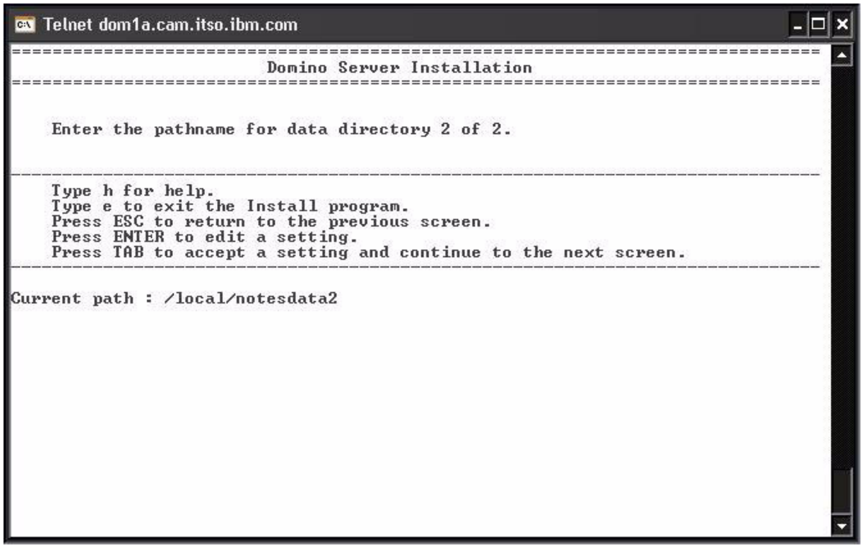
Telnet dom1a.cam.itso.ibm.com

```
===============================================================================
                            Domino Server Installation
===============================================================================

    Please enter the Domino UNIX group to own the data directory:
    /notes/dom1a

    This UNIX user for this directory must be a member of this group.

    NOTE for the upgrade installer:
    Domino UNIX group/account group you specify here must be the same as
    the owner of the existing installed data files for proper operation
    of Domino.

-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

Current UNIX group setting : domino
```

Figure 5-27 Specifying the Solaris group

25. Enter information about the second of the two Domino partitions on this server. The default value for this partition's path to the Domino Data directory on Solaris (`/local/notesdata2`, as shown in Figure 5-28) should be changed.

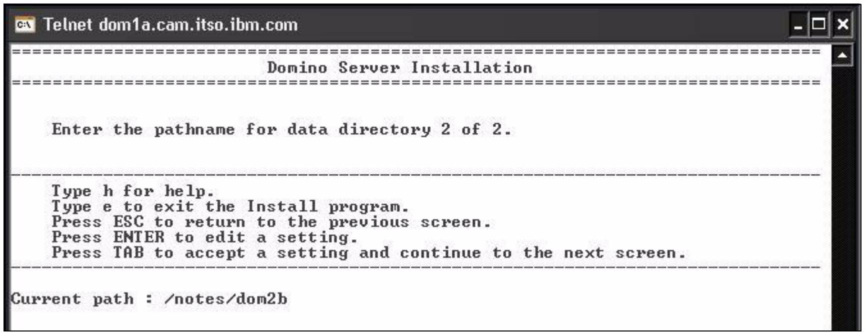
    Make the necessary changes to conform to the path name of your Domino Data directory, and press Tab to continue.



```
===============================================================================
                          Domino Server Installation
===============================================================================


    Enter the pathname for data directory 2 of 2.


-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

Current path : /local/notesdata2
```

Figure 5-28 Default path to Partition #2 data directory

Because we are being prompted for Partition #2 information here, we followed the on-screen instructions to make the required change. For our example, we entered `/notes/dom2b` (Figure 5-29).

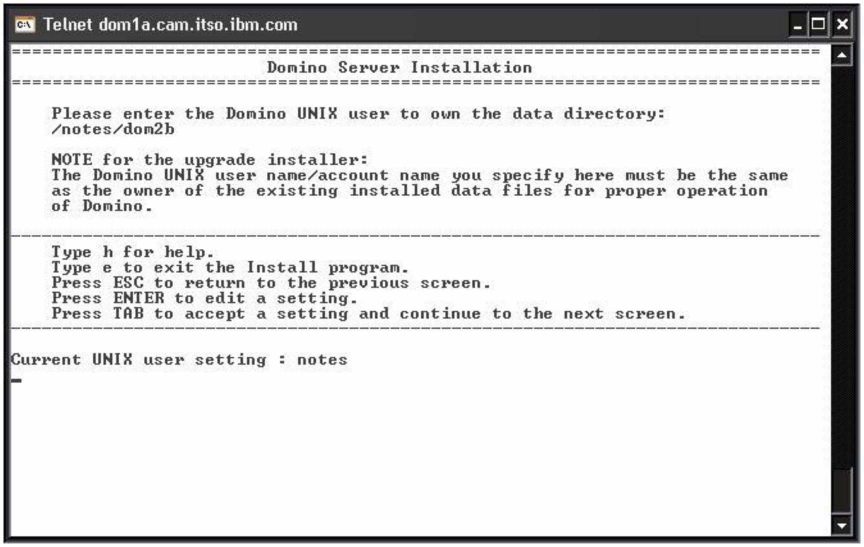


```
===============================================================================
                          Domino Server Installation
===============================================================================


    Enter the pathname for data directory 2 of 2.


-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

Current path : /notes/dom2b
```

Figure 5-29 Partition #2 path to data directory

26. Enter the name of the Solaris user who will own this Domino partition from the Solaris perspective. As a matter of security we advise replacing the default Solaris user name `notes` with a more meaningful name that is similar or identical to the name of the Domino server that will run in its partition.

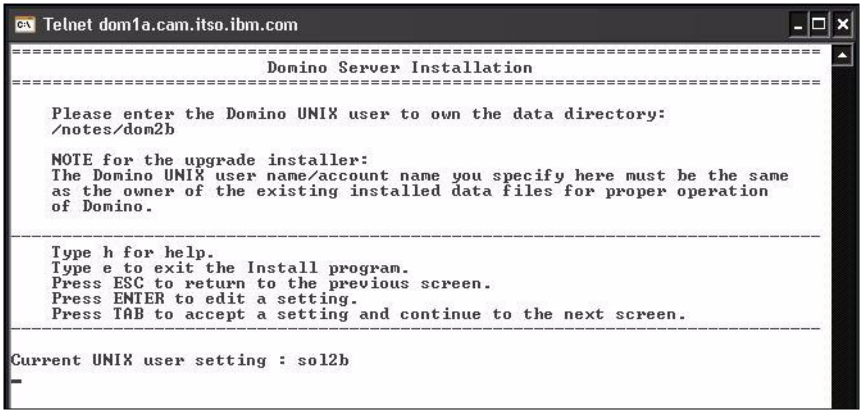
    For your environment, follow the instructions to enter the appropriate Solaris user name for your Domino partition, and press Tab to continue.



```
===============================================================================
                          Domino Server Installation
===============================================================================

    Please enter the Domino UNIX user to own the data directory:
    /notes/dom2b

    NOTE for the upgrade installer:
    The Domino UNIX user name/account name you specify here must be the same
    as the owner of the existing installed data files for proper operation
    of Domino.
-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

Current UNIX user setting : notes
_
```

Figure 5-30 Default Solaris user associated with Partition #2

For our example, we changed it to `sol2b` (Figure 5-31).

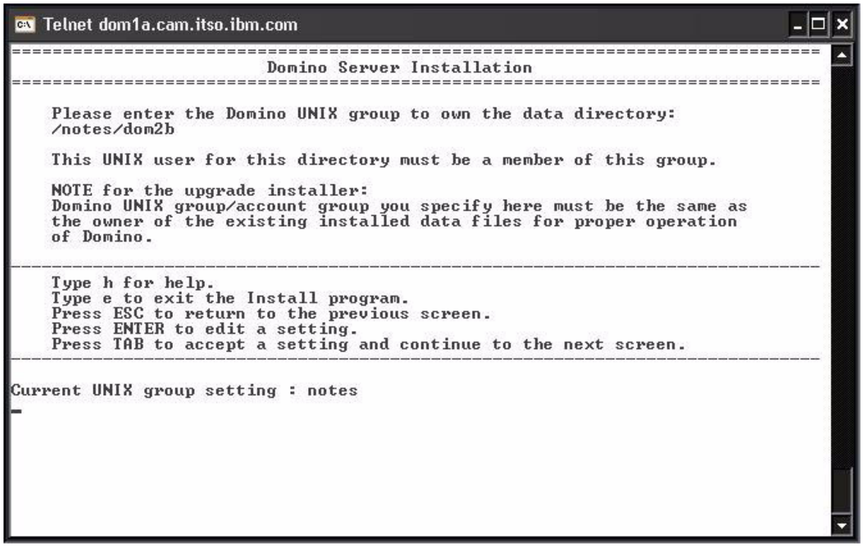


```
===============================================================================
                          Domino Server Installation
===============================================================================

    Please enter the Domino UNIX user to own the data directory:
    /notes/dom2b

    NOTE for the upgrade installer:
    The Domino UNIX user name/account name you specify here must be the same
    as the owner of the existing installed data files for proper operation
    of Domino.
-------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
-------------------------------------------------------------------------------

Current UNIX user setting : sol2b
_
```

Figure 5-31 Specifying our Solaris user associated with Partition #2

27. Enter the name of the Solaris group that your Solaris user will belong to. As a matter of convention we advise against using the default group name `notes`. Instead we recommend using a more meaningful group name of `domino`.

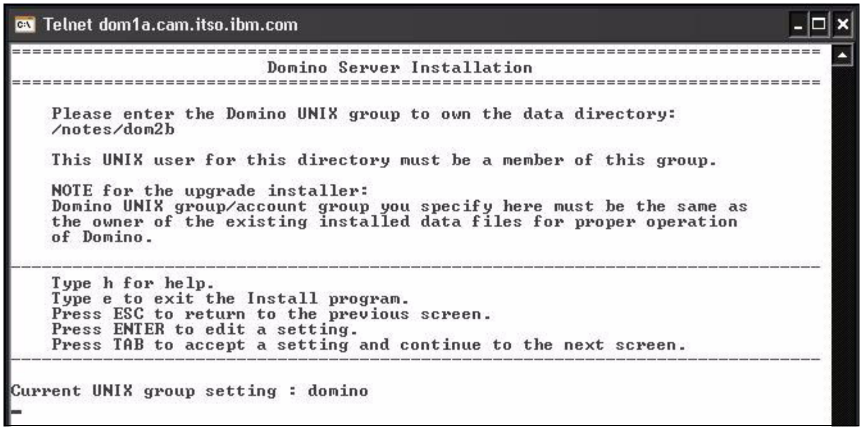
    For your environment, follow the instructions to enter the appropriate Solaris group name associated with your Solaris user name, and press Tab to continue.



```
==============================================================================
                          Domino Server Installation
==============================================================================

    Please enter the Domino UNIX group to own the data directory:
    /notes/dom2b

    This UNIX user for this directory must be a member of this group.

    NOTE for the upgrade installer:
    Domino UNIX group/account group you specify here must be the same as
    the owner of the existing installed data files for proper operation
    of Domino.
------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
------------------------------------------------------------------------------
Current UNIX group setting : notes
_
```

Figure 5-32 Default Solaris group for this physical server

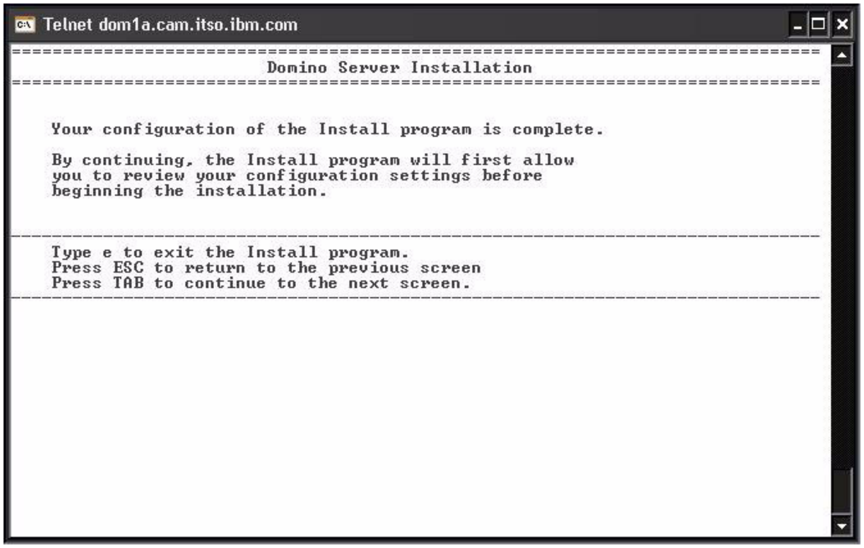
For our example, we changed it to the same group we specified for the previous Solaris user (partition owner), `domino`, as shown in Figure 5-33.



```
==============================================================================
                          Domino Server Installation
==============================================================================

    Please enter the Domino UNIX group to own the data directory:
    /notes/dom2b

    This UNIX user for this directory must be a member of this group.

    NOTE for the upgrade installer:
    Domino UNIX group/account group you specify here must be the same as
    the owner of the existing installed data files for proper operation
    of Domino.
------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
------------------------------------------------------------------------------
Current UNIX group setting : domino
_
```

Figure 5-33 Specifying the Solaris group

28. Figure 5-34 shows a message signifying that configuration of the installation program is complete. Press Tab to review your configuration settings.

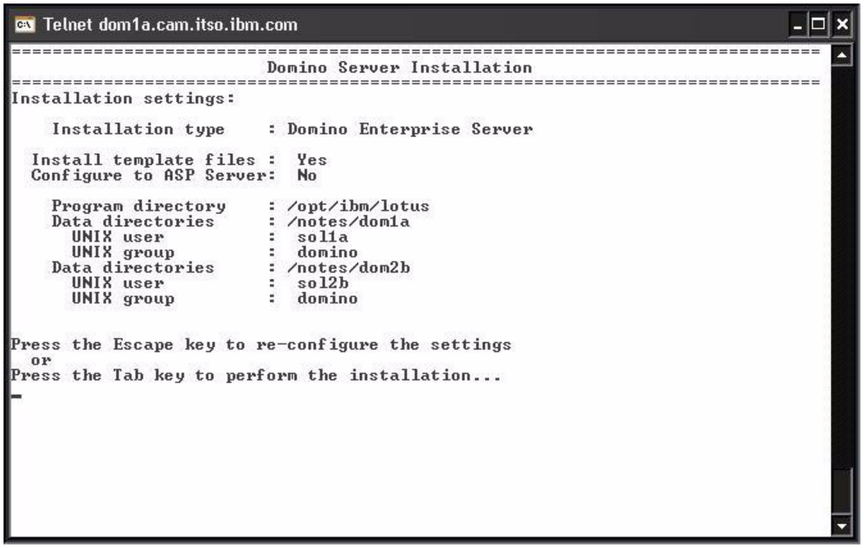


```
===============================================================================
                          Domino Server Installation
===============================================================================


    Your configuration of the Install program is complete.

    By continuing, the Install program will first allow
    you to review your configuration settings before
    beginning the installation.


-------------------------------------------------------------------------------
    Type e to exit the Install program.
    Press ESC to return to the previous screen
    Press TAB to continue to the next screen.
-------------------------------------------------------------------------------
```

Figure 5-34 Information screen

29.The Domino Server Installation program displays all of the parameters you specified to configure your installation of Domino on this Sun server (Figure 5-35).

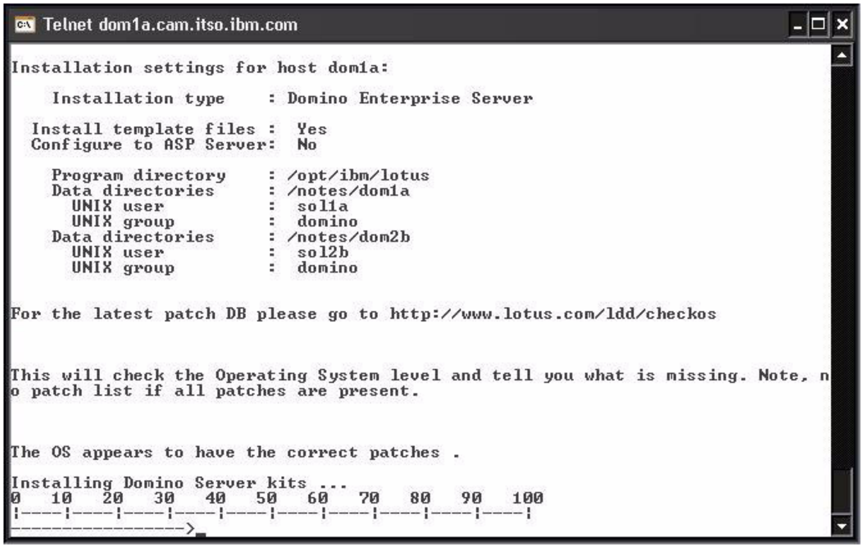
- If you detect errors, follow the on-screen instructions to go back and reconfigure your Domino Installation settings.
- If the information looks correct, then press Tab to begin the installation.



```
===============================================================================
                         Domino Server Installation
===============================================================================
Installation settings:

    Installation type    : Domino Enterprise Server

  Install template files :  Yes
  Configure to ASP Server:  No

    Program directory    : /opt/ibm/lotus
    Data directories     : /notes/dom1a
      UNIX user          :  sol1a
      UNIX group         :  domino
    Data directories     : /notes/dom2b
      UNIX user          :  sol2b
      UNIX group         :  domino


Press the Escape key to re-configure the settings
  or
Press the Tab key to perform the installation...
_
```

Figure 5-35 Review installation settings

30. Figure 5-36 shows the Domino Server Installation program while in progress.



```
Installation settings for host dom1a:

    Installation type    : Domino Enterprise Server

  Install template files :  Yes
  Configure to ASP Server:  No

    Program directory    : /opt/ibm/lotus
    Data directories     : /notes/dom1a
      UNIX user          :  sol1a
      UNIX group         :  domino
    Data directories     : /notes/dom2b
      UNIX user          :  sol2b
      UNIX group         :  domino

For the latest patch DB please go to http://www.lotus.com/ldd/checkos


This will check the Operating System level and tell you what is missing. Note, n
o patch list if all patches are present.


The OS appears to have the correct patches .

Installing Domino Server kits ...
0    10   20   30   40   50   60   70   80   90   100
|----|----|----|----|----|----|----|----|----|----|
------------------>_
```

Figure 5-36 Installation program running

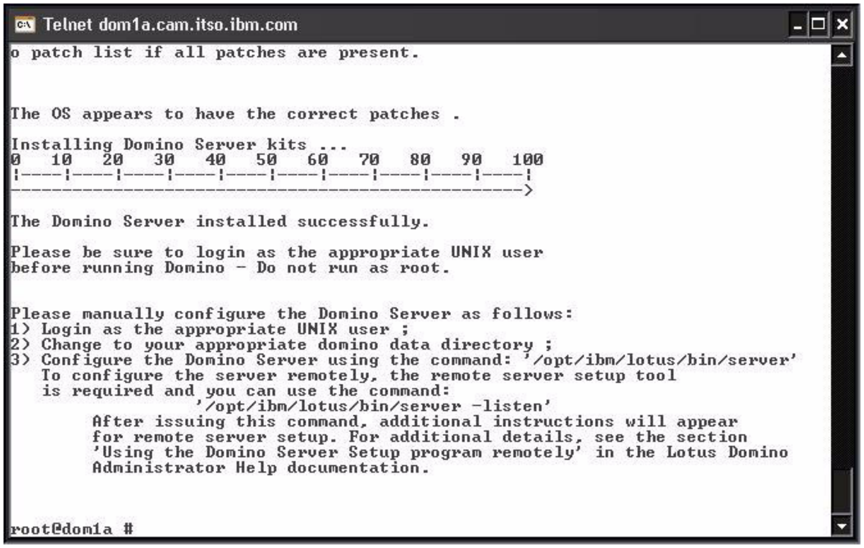
Note: The Installation program for Domino 7 introduces a progress bar feature that enables you to monitor installation progress. This is very reassuring because, depending on several factors, this stage of the installation process can take anywhere from 30 seconds to 5 minutes to complete.

The Installation program for Domino 6.x (Solaris 8 and Solaris 9) lacks this progress bar feature. When you reach this stage of a Domino 6.x installation you might have to wait from 30 seconds to 5 minutes, with no way to determine what, if anything, is happening on the server. This can be very unsettling.

Be patient when you reach this stage of the Domino 6.x installation for Solaris.

31. Figure 5-37 shows what you will see at the successful completion of the Domino Server Installation program.

    This display also describes available Domino Server Setup alternatives.



```
o patch list if all patches are present.


The OS appears to have the correct patches .

Installing Domino Server kits ...
0   10   20   30   40   50   60   70   80   90   100
|----|----|----|----|----|----|----|----|----|----|
--------------------------------------------------->

The Domino Server installed successfully.

Please be sure to login as the appropriate UNIX user
before running Domino - Do not run as root.


Please manually configure the Domino Server as follows:
1) Login as the appropriate UNIX user ;
2) Change to your appropriate domino data directory ;
3) Configure the Domino Server using the command: '/opt/ibm/lotus/bin/server'
   To configure the server remotely, the remote server setup tool
   is required and you can use the command:
                  '/opt/ibm/lotus/bin/server -listen'
        After issuing this command, additional instructions will appear
        for remote server setup. For additional details, see the section
        'Using the Domino Server Setup program remotely' in the Lotus Domino
        Administrator Help documentation.


root@dom1a #
```

Figure 5-37 Successful completion

The next step is to set up your Domino server.

Important: Running a Domino server partition as root is not supported.

The files in the /opt/ibm/lotus directory should be owned by root. This is the reason why you change to the root user ID to install the Domino Program code.

The Domino Data directory files must be owned by the Solaris user account that was created for that Domino partition. For example, in our example environment, /notes/dom1a is owned by Solaris user sol1a, and /notes/dom2b is owned by Solaris user sol2b.

In preparation for Domino Server Setup, you must log off root and log on as one of your new Solaris users who owns a Domino partition.

5.2.1 Installing different versions of Domino on one physical server

Note: This discussion is specific only to *adding* new Domino server partitions. It does not address the issue of upgrading a Domino partition to Domino 7 from earlier releases of Domino.

For information about upgrading to Notes and Domino 7, see:

- Appendix G, “Moving to IBM Lotus Notes and Domino 7” on page 567
- The IBM Lotus Web site: `http://www.ibm.com/software/lotus/`
- The IBM Redbooks Web site: `http://www.redbooks.ibm.com/`
- Domino Admin 7 Help

Beginning with Domino 6, certain vendors’ platform implementations of Domino introduced the ability to support multiple versions of Domino on a single physical server. This was true with Domino 6.x for Solaris, and remains true with Domino 7 for Solaris.

Note: This raises an interesting issue regarding certified Domino and Solaris OS combinations. As we write this book, the only officially certified combinations are:

- Domino 6.x on Solaris 8 and 9 (requires a minimum of Solaris 8)
- Domino 7 on Solaris 9 and 10 (requires a minimum of Solaris 9)

Another Domino/Solaris OS combination might warrant consideration by some organizations: Domino 6.x on Solaris 10. This combination is not yet certified, and its certification future is unclear at the time of this writing.

If implementing Domino 6.x on Solaris 10 is an important issue for your organization, we recommend that you contact your IBM Lotus Support Manager (LSM), or search the IBM Web site for the latest information on Lotus Domino Software platform support.

From what we have already described in this book, it should be clear that it is easy to implement multiple Domino server instances, or Domino partitions, on a physical Sun server. The number of Domino partitions you implement on a Sun server is a function of requirements versus physical resources on the server.

However, starting with Domino 6.x and continuing with Domino 7, these partitions can each run different, independent versions of Domino server software.

Not only can all Domino partitions on a physical server share one common version of Domino server software, but now *every* Domino partition can run its own unique version of Domino server code on the physical server.

The ability to support multiple versions of Domino software on a single server, in addition to the ability to support multiple Domino partitions on a single server, demonstrates the power and flexibility of Solaris as a strategic enterprise platform for Domino.

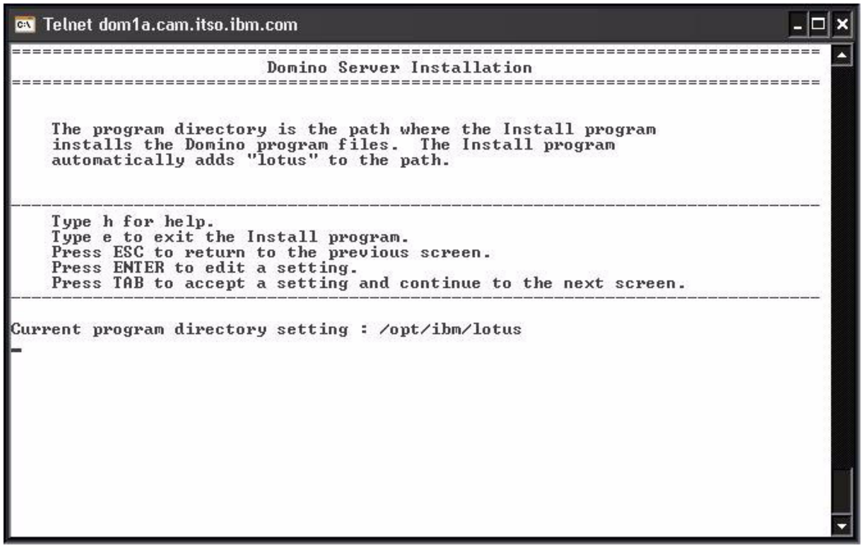
Note: If you add new Domino partitions to Solaris when other partitions already exist, it is very important to review the Solaris configuration settings to ensure that they are properly set or modified to accommodate new partitioned Domino server instances.

Refer to the appropriate sections in the following chapters:

- Chapter 3, “Sizing guidelines for IBM Lotus Domino Messaging Server” on page 19
- Chapter 4, “Solaris 10 installation, configuration, and considerations” on page 29
- Chapter 8, “Partitioning” on page 251

At the heart of this flexibility is the point during the Domino Software Installation process where you specify the Solaris file system location for the Domino Program directory.

We now take another look at the location we specified for the Domino Program Directory when we installed the Domino server software (Figure 5-38).



```
==============================================================================
                              Domino Server Installation
==============================================================================


    The program directory is the path where the Install program
    installs the Domino program files.  The Install program
    automatically adds "lotus" to the path.


------------------------------------------------------------------------------
    Type h for help.
    Type e to exit the Install program.
    Press ESC to return to the previous screen.
    Press ENTER to edit a setting.
    Press TAB to accept a setting and continue to the next screen.
------------------------------------------------------------------------------

Current program directory setting : /opt/ibm/lotus
_
```

Figure 5-38 Prompt for program directory location

The default location for the Domino 7 program directory is /opt/ibm/lotus.

> **Note:** The Domino 6.x default location for the Domino program directory is: /opt/lotus.

Note that we can specify any value we want for the Domino program directory, as long as we specify a Solaris file system location with sufficient disk space to accommodate a separate, version-specific copy of the Domino Program files.

> **Important:** The Domino Server Installation program appends `/lotus` to the end of any directory path you specify for the Domino program directory.
>
> For example, if you specify a new program directory, /opt/ibm/domino7, the Domino Server Installation program will append /lotus to the end, making your *actual* program directory: /opt/ibm/domino7/lotus.

The process of installing a new version of Domino on your Solaris server (without affecting previous versions) is to:

1. Create a new Solaris group (optional). You can do this if you want to have Domino version-specific Solaris groups. You should be able to use the existing Solaris group defined for the user accounts that own your Domino partitions, regardless of the Domino version they run.
2. Create and configure a new Solaris user account for every new Domino partition that will run the new Domino server code.
3. Make the necessary Solaris filesystem changes to provision sufficient disk space for each new partition's Domino data directory.
4. Make the necessary Solaris filesystem changes to provision sufficient disk space to hold a new copy of version-specific Domino program files. Determine the filesystem naming convention you want to use for the version-specific Domino program files, and remember that /lotus will be appended to whatever filesystem path you specify.
5. As root, run the Domino installation program as though you are installing a new Domino server partition (or partitions), being careful to specify your new version-specific Domino program directory.

   > **Attention:** Do *not* specify an existing Domino program directory as this will affect every Domino partition currently using that Domino program directory!

6. When the Domino Server Installation process completes, proceed with the normal Domino Server Setup process, start your servers, and configure them per your organization's requirements.

Important: This approach for installing and maintaining different versions of Domino on the same physical Solaris server can also be used to install and maintain independent versions of Domino that each run from their own, potentially identical versions of Domino.

For example, you can use this approach to install and support multiple Domino 7 partitions on a physical server, and each partition can run from its own, distinct set of Domino program files (binaries), even if each independent copy is the same version of Domino 7.

This approach is gaining popularity with some organizations because it provides partitioning with the benefit of being able to make partition-specific changes that do not affect other partitions, such as occurs in a traditional shared-binaries configuration.

5.3 Setting up Domino servers

In this section we describe how to set up your Domino servers. The Domino Server Setup program guides you through the choices you make to configure a Domino server. Setting up the first Domino server in a domain establishes a framework that consists of the Domino Directory, ID files, and documents. When you set up additional servers, you build on this framework.

The setup for the first Domino server will be different than it will be for subsequent, additional Domino servers in your environment. Procedures for setting up first and additional Domino servers are included here.

Note: During server setup, you can use an existing certifier ID instead of creating a new one. The certifier ID that you specify cannot have multiple passwords assigned to it. Attempting to use a certifier ID with multiple passwords generates an error message and causes server setup to halt.

5.3.1 Domino Server Setup methods

Several methods can be used for setting up your Domino server:

- Remote Server Setup
- Local Server Setup
- Server Setup using a Setup Profile

Remote Server Setup

After you install the program files for a Domino server on a system, you can use either a Windows client system or another Domino server to run the Server Setup program remotely. Running the Server Setup program from a Windows client is easier if the client has Domino Administrator installed; to run the program from a client without Domino Administrator, you need the Java Runtime Environment plus some files from the program directory of an installed Domino server.

The Server Setup program asks a series of questions and guides you through the setup process.

Note: In this book, we illustrate the process of performing Remote Server Setup of the first Domino server and the second Domino server.

We recommend this method because it can be very easy and straightforward. However, be aware that this method, by default, expects port 8585 to be available for communication between the Remote Setup utility and the Domino server. If firewall restrictions prevent port 8585 access, then consider Local Server Setup as an alternative. If port 8585 is not enabled in your network, you can easily change the port by using the command `server -listen portnumber` (e.g. 5555).

Local Server Setup

After installing the Domino server program files on a server, you can run the Domino Server Setup program locally by starting the server. The Server Setup program asks a series of questions and guides you through the setup process. Online Help is available during the process.

Note: In this book, we illustrate the process of performing Local Server Setup of the third Domino server.

This method requires X.11 terminal access to the Setup process running on Solaris. There are many ways to provide X.11 terminal access, and we offer one approach for doing this in our illustrated example.

Server setup using a setup profile

You can use a server setup profile at the server you are setting up, or from a client system. Using a server setup profile from a Windows client is easier if the client has Domino Administrator installed; to use a profile from a Windows or Solaris client without Domino Administrator, you need the Java Runtime Environment plus some files from the program directory of an installed Domino server.

When you use a setup profile, you choose whether to view the setup screens as you run the profile. Running a profile without viewing the screens is sometimes referred to as a *silent* setup.

Note: This book does not include Server Setup using a setup profile. See Domino 7 Administrator Help for more information about using a setup profile to set up your Domino server.

We illustrate each method in the next sections as follows:

- Remote Server Setup of the first Domino server (dom1a)
- Remote Server Setup of the second Domino server (dom2b)
- Local Server Setup of the third Domino server (dom2a).

Note: There was once a free, unsupported Domino R5 Server Setup utility called the *domsetup* program. The domsetup program, now obsolete, was an application for installing a Domino server in a UNIX environment that lacked a graphical monitor. This program was not supported by Lotus or Sun.

This *domsetup* program remains unsupported with Domino 6.x and Domino 7, and is no longer available in either event.

Installations that still have access to this utility from past Domino R5 implementations on Solaris are advised against attempting to use this utility to set up Domino 6.x or Domino 7.

5.3.2 Setting up the first Domino server

This section shows how to set up the first Domino server in an organization. Your certifier ID and Domino hierarchical naming conventions are established during this stage.

In 5.3.3, “Setting up additional Domino servers” on page 137, we show how to add an additional server in an existing Domino domain.

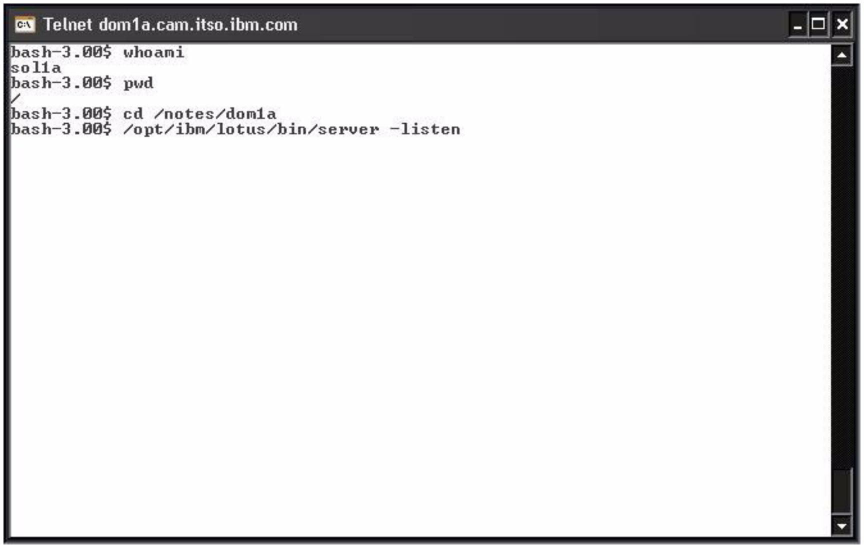
After installing the Domino server program files you must set up the Domino server. The method we recommend for setting up your Domino server is the Remote Server Setup utility, a companion utility that is installed with the Domino Administrator client.

Remote Server Setup communicates with the Server Setup program on Solaris. The Domino server is placed in a listening state on port 8585, awaiting communication from the Remote Server Setup utility, which is typically on a Windows client.

Perform the following steps to run the setup program:

1. Log on to the system as the Solaris account for the partition you are setting up. In our example it is `sol1a`.
2. Change to the Domino Data directory for the partition you are setting up. In our example it is `/notes/dom1a`.
3. Type the following line on the command line and press Enter:

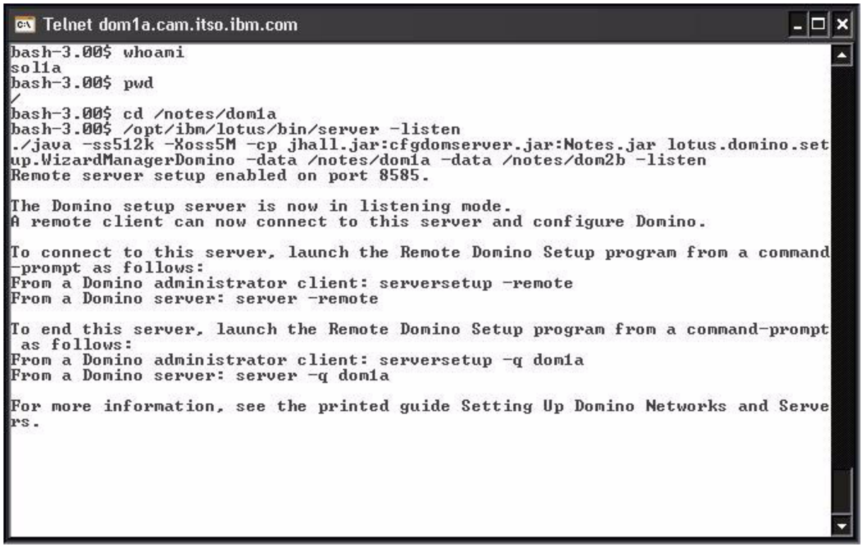
```
/opt/ibm/lotus/bin/server -listen
```



```
bash-3.00$ whoami
sol1a
bash-3.00$ pwd
/
bash-3.00$ cd /notes/dom1a
bash-3.00$ /opt/ibm/lotus/bin/server -listen
```

Figure 5-39 Preparing for Domino Remote Server Setup

4. The screen in Figure 5-40 appears, saying that the Domino setup server is in listening mode.



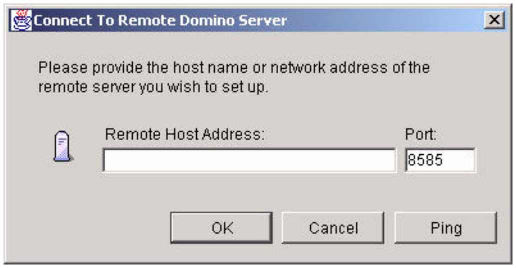
```
bash-3.00$ whoami
sol1a
bash-3.00$ pwd
/
bash-3.00$ cd /notes/dom1a
bash-3.00$ /opt/ibm/lotus/bin/server -listen
./java -ss512k -Xoss5M -cp jhall.jar:cfgdomserver.jar:Notes.jar lotus.domino.set
up.WizardManagerDomino -data /notes/dom1a -data /notes/dom2b -listen
Remote server setup enabled on port 8585.

The Domino setup server is now in listening mode.
A remote client can now connect to this server and configure Domino.

To connect to this server, launch the Remote Domino Setup program from a command
-prompt as follows:
From a Domino administrator client: serversetup -remote
From a Domino server: server -remote

To end this server, launch the Remote Domino Setup program from a command-prompt
 as follows:
From a Domino administrator client: serversetup -q dom1a
From a Domino server: server -q dom1a

For more information, see the printed guide Setting Up Domino Networks and Serve
rs.
```

Figure 5-40 Domino Partition #1 listening for Remote Setup Client

The Domino server dom1a is now listening on port 8585, waiting for the Remote Server Setup utility to communicate with it.

5. At this time go to the Windows workstation where you have a Domino Administrator client installed. From the Windows Start menu, select **Programs** → **Lotus Applications** → **Remote Server Setup**.

6. When Remote Server Setup launches, it prompts you for the remote host address of the Domino server to set up (Figure 5-41). Enter the IP address or host name of the server you want to connect to and click **Ping** to test the connection.



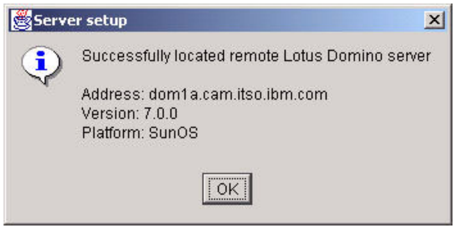
Please provide the host name or network address of the remote server you wish to set up.

Remote Host Address:

Port: 8585

Figure 5-41 Server connection dialog box

7. If you specified a valid address you will see a confirmation dialog (Figure 5-42). Click **OK** to return to the Server Connection dialog box.



Server setup

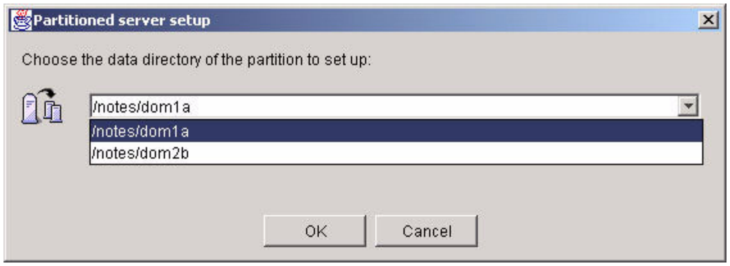
Successfully located remote Lotus Domino server

Address: dom1a.cam.itso.ibm.com
Version: 7.0.0
Platform: SunOS

Figure 5-42 Pinging the remote Domino server

8. Click **OK** again to continue to the next window.
9. The Domino partitions that are available for Remote Setup on the physical server you've connected to appear in a pull-down list (Figure 5-43). We have two partitions to choose from. We are setting up the first Domino partition, dom1a, as our first Domino server, so we select its Domino Data directory: **/notes/dom1a**.

   Click **OK** to continue.



Partitioned server setup

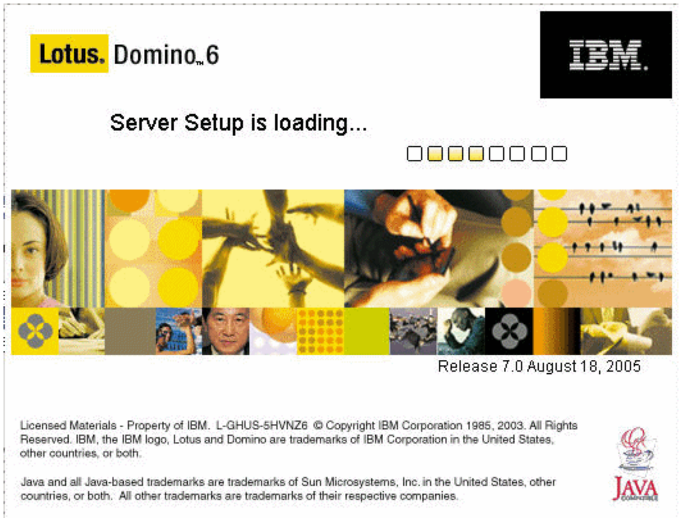
Choose the data directory of the partition to set up:

/notes/dom1a
/notes/dom1a
/notes/dom2b

Figure 5-43 Remote Domino Server Setup - choose the Domino partition

10. The Domino Server Setup splash screen displays (Figure 5-44 on page 115).

> **Tip:** We used a Domino 6 version of the Remote Server Setup utility for Remote Setup of the first Domino 7 server. If you do not have the Notes 7 clients installed yet, you can use older versions of the Remote Server Setup utility when setting up your new Domino 7 server.



Server Setup is loading...

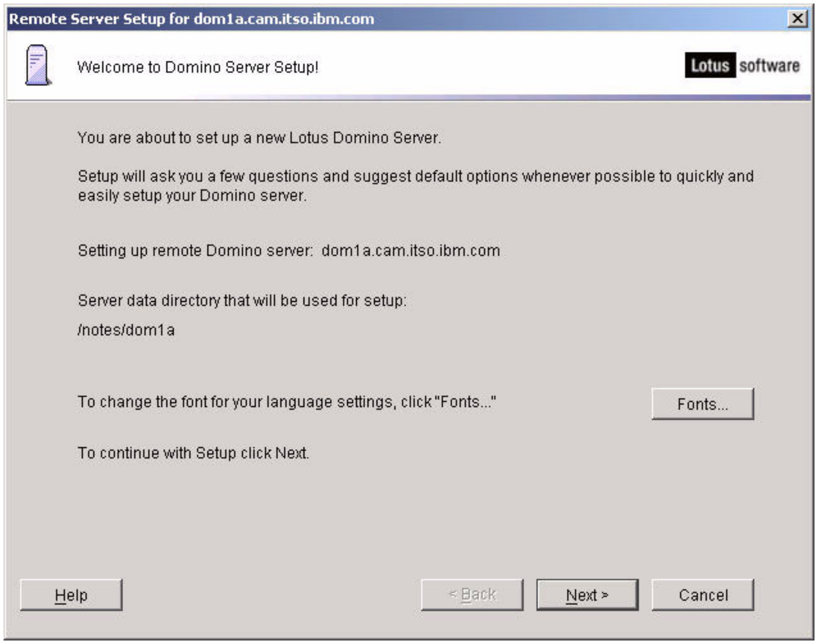
Release 7.0 August 18, 2005

Licensed Materials - Property of IBM. L-GHUS-5HVNZ6 © Copyright IBM Corporation 1985, 2003. All Rights Reserved. IBM, the IBM logo, Lotus and Domino are trademarks of IBM Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. All other trademarks are trademarks of their respective companies.

Figure 5-44 Server Setup splash screen

11. The splash screen disappears and the Remote Server Setup Welcome window appears (Figure 5-45). The Remote Server Setup utility gives you the option to change the font for your language settings. Click **Fonts**.



Welcome to Domino Server Setup!

You are about to set up a new Lotus Domino Server.

Setup will ask you a few questions and suggest default options whenever possible to quickly and easily setup your Domino server.

Setting up remote Domino server: dom1a.cam.itso.ibm.com

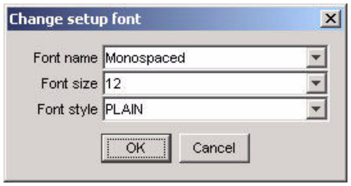
Server data directory that will be used for setup:
/notes/dom1a

To change the font for your language settings, click "Fonts..."

To continue with Setup click Next.

Figure 5-45 Welcome window

12. In the Setup Fonts dialog box (Figure 5-46), make changes, if necessary, and click **OK**.



Change setup font

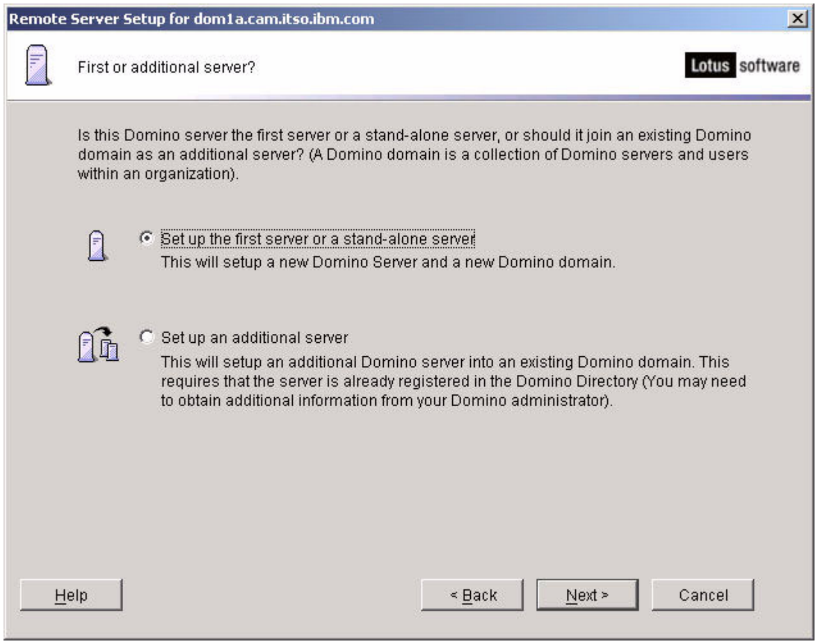
Font name: Monospaced
Font size: 12
Font style: PLAIN

Figure 5-46 Setup Fonts dialog box

13. This returns you to the Remote Server Setup Welcome window, click **Next** to continue.

14. In our example we are setting up the first server in our Domino domain. This is also the default choice when we first see Figure 5-47.

    Click **Next** to continue.



Remote Server Setup for dom1a.cam.itso.ibm.com

First or additional server?

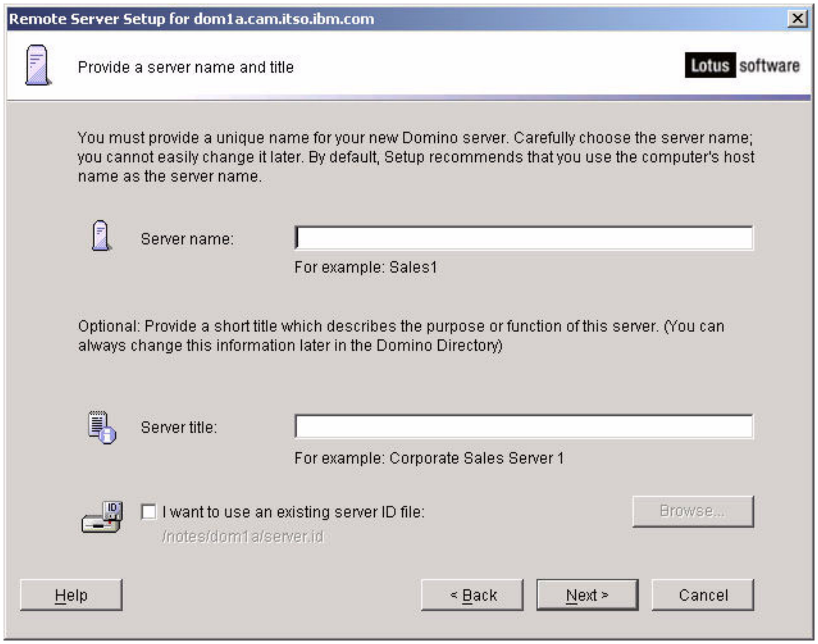
Is this Domino server the first server or a stand-alone server, or should it join an existing Domino domain as an additional server? (A Domino domain is a collection of Domino servers and users within an organization).

● Set up the first server or a stand-alone server
This will setup a new Domino Server and a new Domino domain.

○ Set up an additional server
This will setup an additional Domino server into an existing Domino domain. This requires that the server is already registered in the Domino Directory (You may need to obtain additional information from your Domino administrator).

Figure 5-47 Setting up the first server in the Domino domain

15. The window in Figure 5-48 prompts for the name and title of the Domino server we are setting up. Enter information that pertains to your environment.



Remote Server Setup for dom1a.cam.itso.ibm.com

Provide a server name and title

You must provide a unique name for your new Domino server. Carefully choose the server name; you cannot easily change it later. By default, Setup recommends that you use the computer's host name as the server name.

Server name:

For example: Sales1

Optional: Provide a short title which describes the purpose or function of this server. (You can always change this information later in the Domino Directory)

Server title:

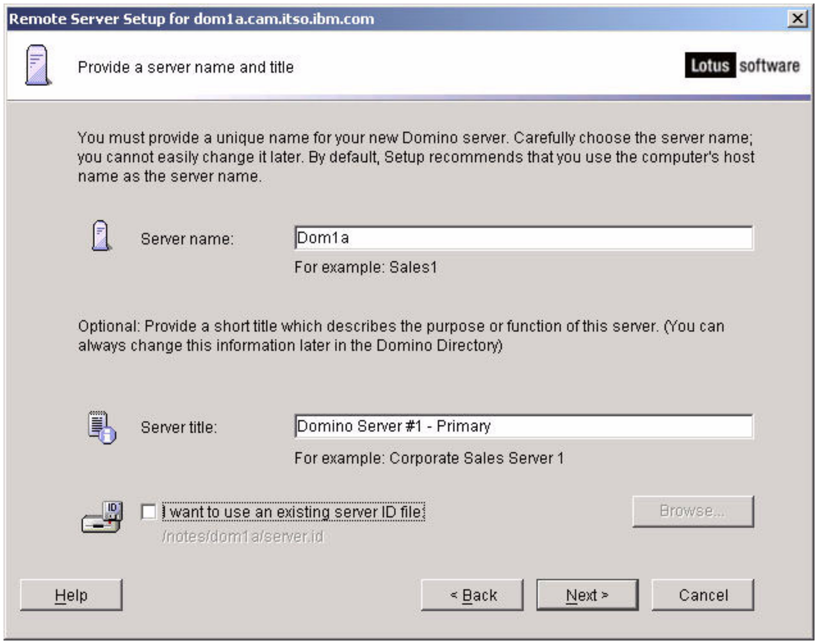
For example: Corporate Sales Server 1

□ I want to use an existing server ID file:

/notes/dom1a/server.id

Figure 5-48 Prompt for Domino server name and title

Figure 5-49 shows the values we specified in our example. Click **Next** to continue.



Remote Server Setup for dom1a.cam.itso.ibm.com

Provide a server name and title

You must provide a unique name for your new Domino server. Carefully choose the server name; you cannot easily change it later. By default, Setup recommends that you use the computer's host name as the server name.

Server name: Dom1a

For example: Sales1

Optional: Provide a short title which describes the purpose or function of this server. (You can always change this information later in the Domino Directory)

Server title: Domino Server #1 - Primary

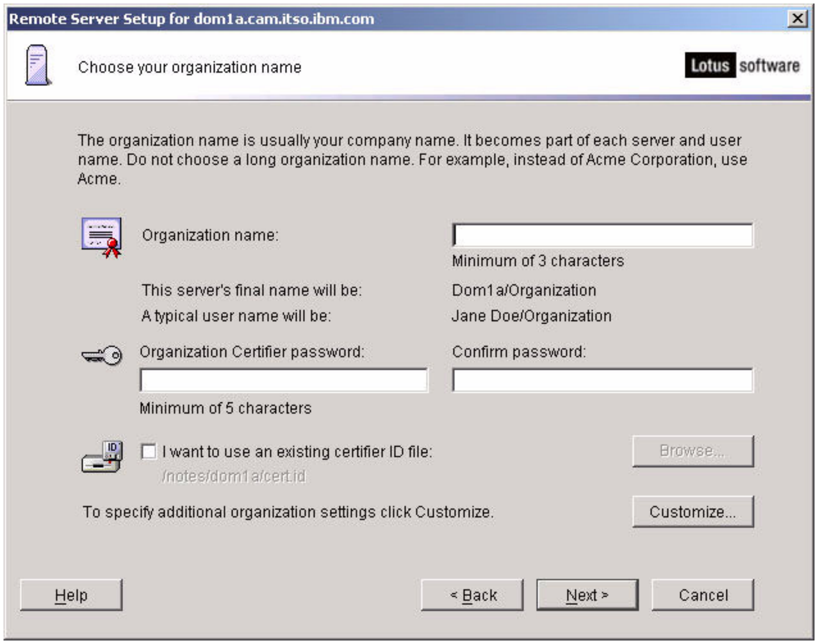
For example: Corporate Sales Server 1

□ I want to use an existing server ID file

/notes/dom1a/server.id

Figure 5-49 Specify server name and title

16. Enter the required information and click **Customize** to specify additional parameters that might apply to your environment.



Remote Server Setup for dom1a.cam.itso.ibm.com

Choose your organization name

The organization name is usually your company name. It becomes part of each server and user name. Do not choose a long organization name. For example, instead of Acme Corporation, use Acme.

Organization name:

Minimum of 3 characters

This server's final name will be: Dom1a/Organization

A typical user name will be: Jane Doe/Organization

Organization Certifier password:

Minimum of 5 characters

Confirm password:

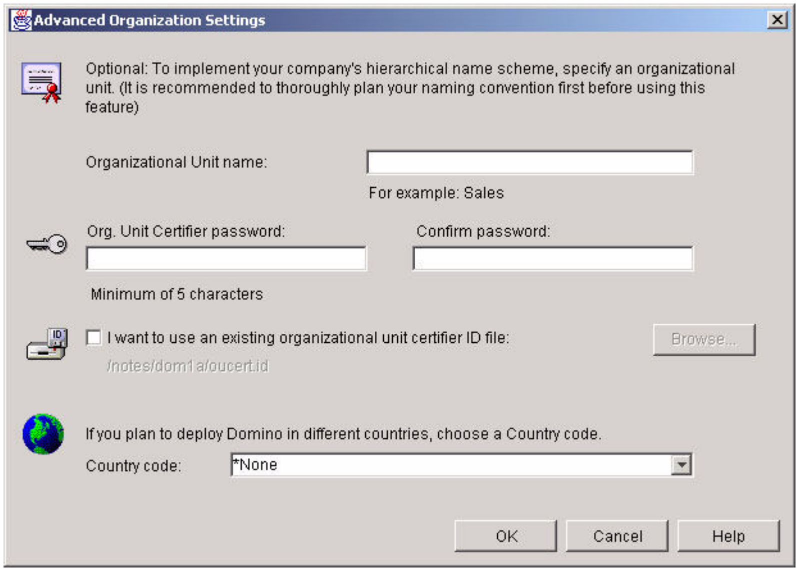
□ I want to use an existing certifier ID file: /notes/dom1a/cert.id

To specify additional organization settings click Customize.

Figure 5-50 Prompt for organization details

17. Figure 5-51 shows the Advanced Organization Settings window that displays after you click the Customize button. If applicable, enter the Organization Unit information that corresponds to the requirements of your Domino environment. Click **OK** to return to the prior window.

    In our example we did not specify Organization Units, leaving the defaults in effect. We also did not use any existing Organization, nor Organization Unit, certifier ID files. We let Domino create new IDs for our example environment.



Advanced Organization Settings

Optional: To implement your company's hierarchical name scheme, specify an organizational unit. (It is recommended to thoroughly plan your naming convention first before using this feature)

Organizational Unit name:

For example: Sales

Org. Unit Certifier password:

Confirm password:

Minimum of 5 characters

□ I want to use an existing organizational unit certifier ID file:

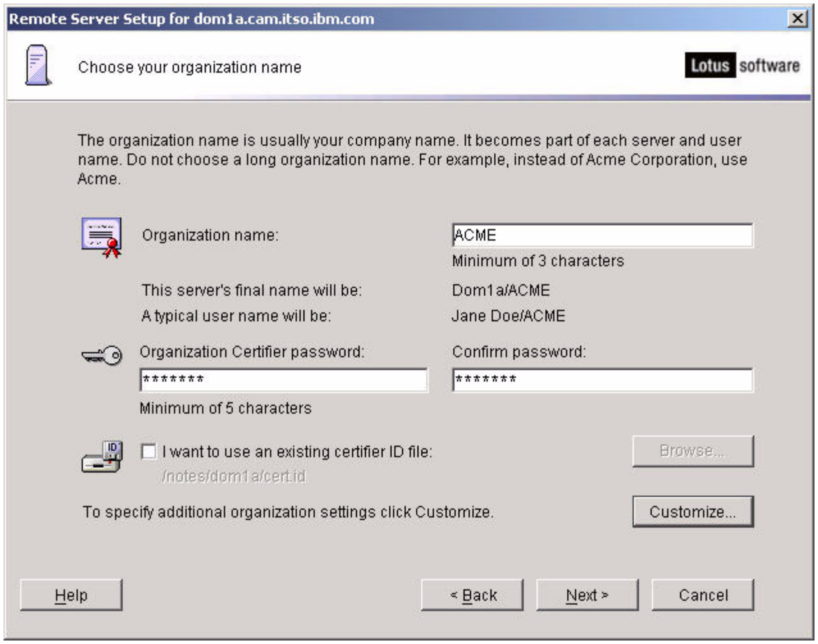
/notes/dom1a/oucert.id

If you plan to deploy Domino in different countries, choose a Country code.

Country code: *None

Figure 5-51 Organization - Advanced Settings

18.Now, the Organization settings window (Figure 5-52) contains the information from our sample environment. If you detect errors here, make the necessary changes now. If the information looks correct, click **Next** to continue.



Remote Server Setup for dom1a.cam.itso.ibm.com

Choose your organization name

The organization name is usually your company name. It becomes part of each server and user name. Do not choose a long organization name. For example, instead of Acme Corporation, use Acme.

Organization name: ACME

Minimum of 3 characters

This server's final name will be: Dom1a/ACME

A typical user name will be: Jane Doe/ACME

Organization Certifier password: *******

Confirm password: *******

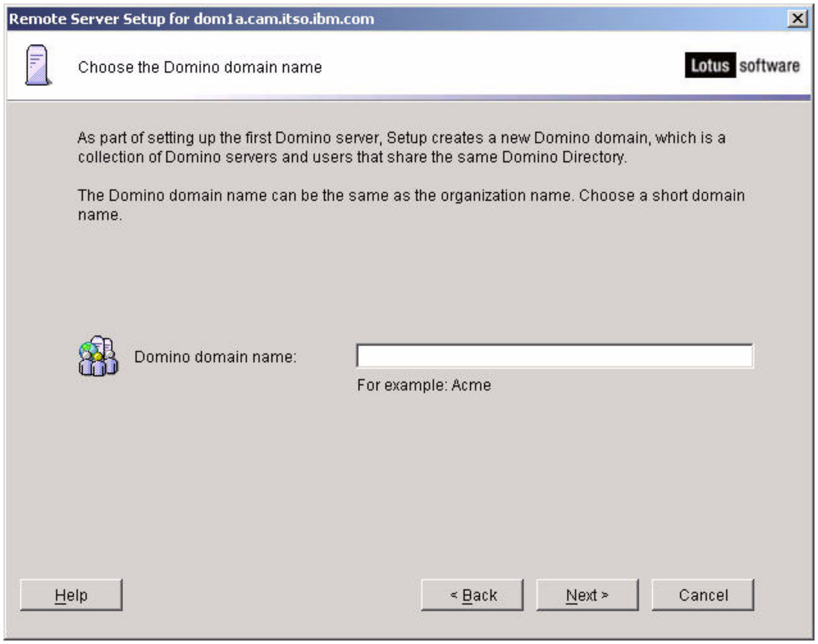
Minimum of 5 characters

□ I want to use an existing certifier ID file: /notes/dom1a/cert.id

To specify additional organization settings click Customize.

Figure 5-52 Organization setup complete

19. The Remote Server Setup program prompts for the name of your new Domino domain. Enter your Domino domain name. If you detect errors here, make the necessary changes now. If the information looks correct, click **Next** to continue.



Remote Server Setup for dom1a.cam.itso.ibm.com

Choose the Domino domain name

As part of setting up the first Domino server, Setup creates a new Domino domain, which is a collection of Domino servers and users that share the same Domino Directory.

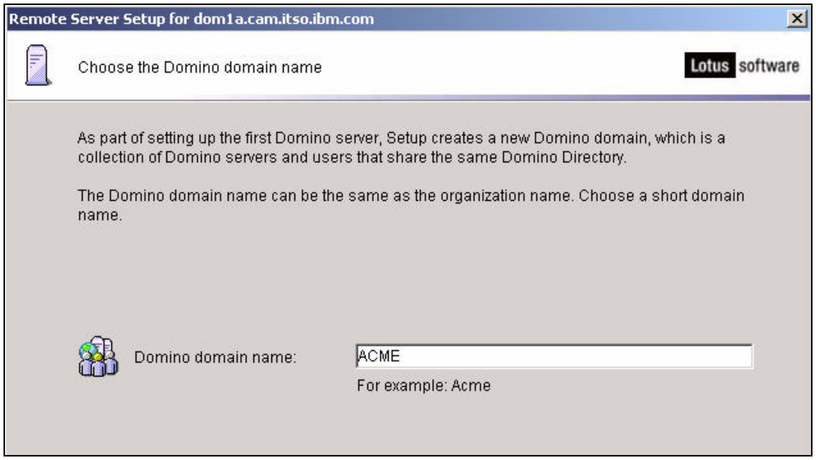
The Domino domain name can be the same as the organization name. Choose a short domain name.

Domino domain name:

For example: Acme

Figure 5-53 Prompt for Domino domain name

In our example (Figure 5-54) we specified `ACME`.



Remote Server Setup for dom1a.cam.itso.ibm.com

Choose the Domino domain name

As part of setting up the first Domino server, Setup creates a new Domino domain, which is a collection of Domino servers and users that share the same Domino Directory.

The Domino domain name can be the same as the organization name. Choose a short domain name.

Domino domain name: ACME

For example: Acme

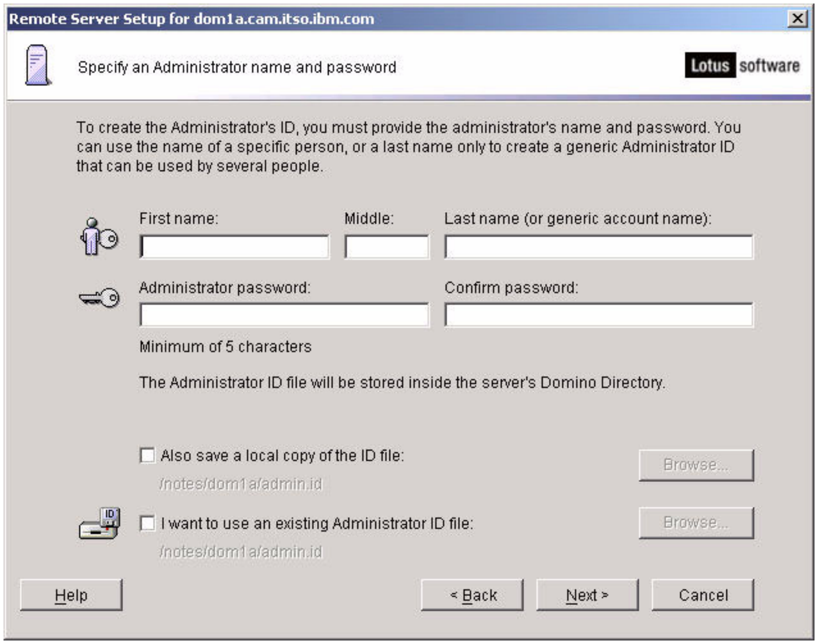
Figure 5-54 Domino domain name specified

Note: The Domino domain name is specific to Domino, and is defined by the contents of the Domino Directory database, names.nsf. The current official term for names.nsf is the *Domino Directory*.

Other terms are used to refer to the Domino Directory. Early in its history, this database was called the Name and Address Book and is often abbreviated as NAB. This database is also sometimes called the Notes Directory. These terms all refer to names.nsf on the Domino server.

Similarly, what we now call the Domino domain began as the Notes Domain. In practical usage, these terms mean the same thing.

20. In Figure 5-55 you are prompted to enter your Domino Administrator name and password. Enter the information that pertains to your organization. If you detect errors here, make the necessary changes now. If the information looks correct, click **Next** to continue.



Remote Server Setup for dom1a.cam.itso.ibm.com

Specify an Administrator name and password

To create the Administrator's ID, you must provide the administrator's name and password. You can use the name of a specific person, or a last name only to create a generic Administrator ID that can be used by several people.

First name:

Middle:

Last name (or generic account name):

Administrator password:

Confirm password:

Minimum of 5 characters

The Administrator ID file will be stored inside the server's Domino Directory.

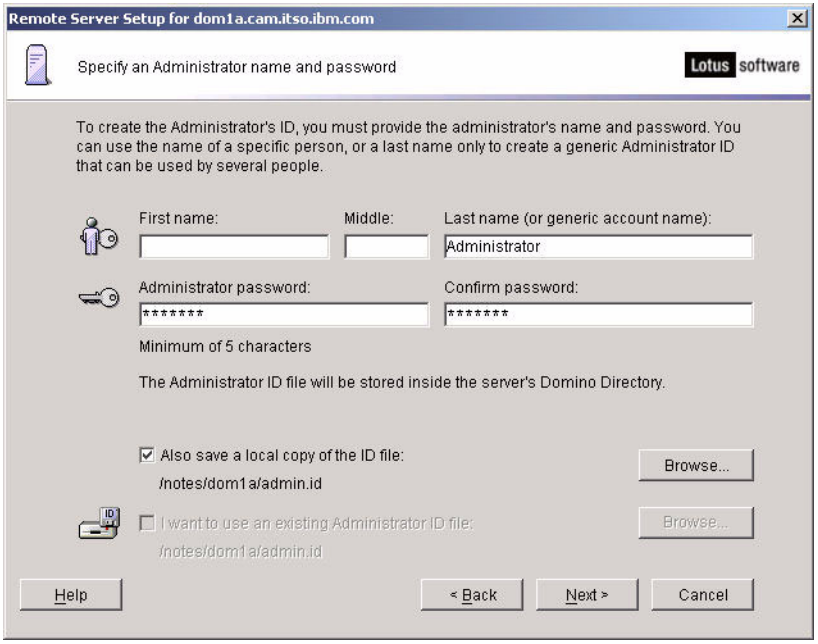
□ Also save a local copy of the ID file:
/notes/dom1a/admin.id

□ I want to use an existing Administrator ID file:
/notes/dom1a/admin.id

Figure 5-55 Prompt for Administrator details

Tip: You might not want to specify the real name of an individual in your organization here. Instead, consider specifying a generic name that really represents the Domino Administrator *role*.

In our example (Figure 5-56), we specified only the last name `Administrator`, and we chose to save the Administrator ID file for easy retrieval later.


Remote Server Setup for dom1a.cam.itso.ibm.com

Specify an Administrator name and password

To create the Administrator's ID, you must provide the administrator's name and password. You can use the name of a specific person, or a last name only to create a generic Administrator ID that can be used by several people.

First name:

Middle:

Last name (or generic account name): Administrator

Administrator password: *******

Confirm password: *******

Minimum of 5 characters

The Administrator ID file will be stored inside the server's Domino Directory.

☑ Also save a local copy of the ID file:
/notes/dom1a/admin.id

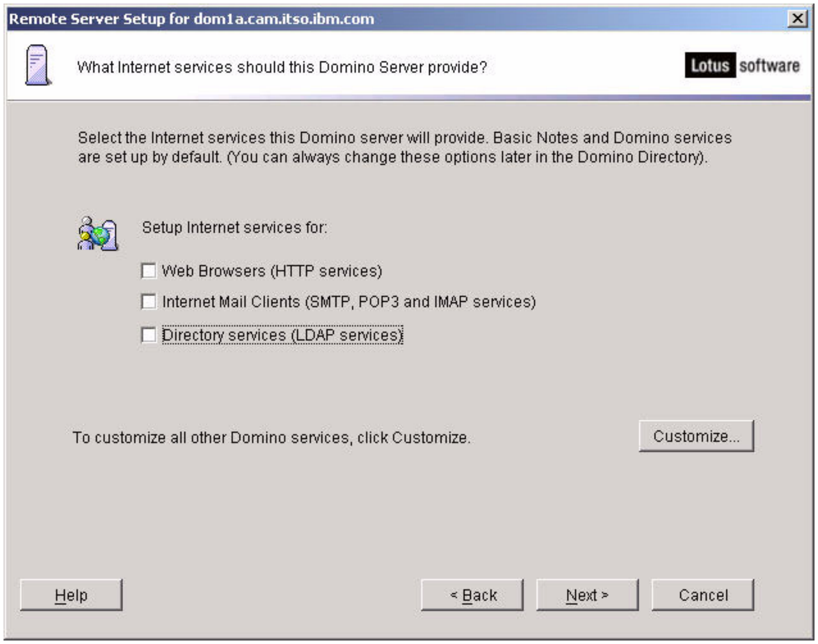
☐ I want to use an existing Administrator ID file:
/notes/dom1a/admin.id

Figure 5-56 Administrator details chosen

> **Important:** Keep the administrator password safe. When you begin to administer your Domino environment you will be prompted for this administrator password in order to use the Administrator ID file.

21. In Figure 5-57 you are prompted to select the Internet services you want to support on this Domino server. If necessary, enable/disable Domino tasks to customize this server's functions.

    To see a complete list (Figure 5-58 on page 126 and Figure 5-59 on page 126) of the Domino server tasks that you can choose to enable or disable, click **Customize**.


Remote Server Setup for dom1a.cam.itso.ibm.com

What Internet services should this Domino Server provide?

Select the Internet services this Domino server will provide. Basic Notes and Domino services are set up by default. (You can always change these options later in the Domino Directory).

Setup Internet services for:

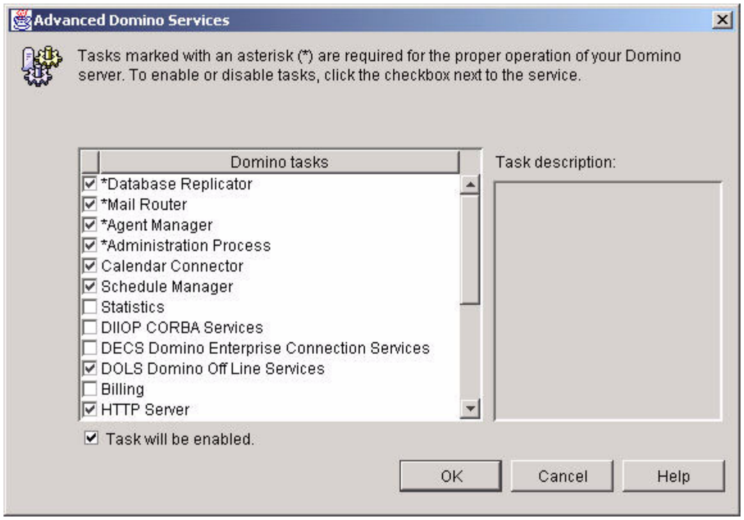
□ Web Browsers (HTTP services)

□ Internet Mail Clients (SMTP, POP3 and IMAP services)

□ Directory services (LDAP services)

To customize all other Domino services, click Customize.

Figure 5-57 Prompt for Internet services and other Domino server tasks

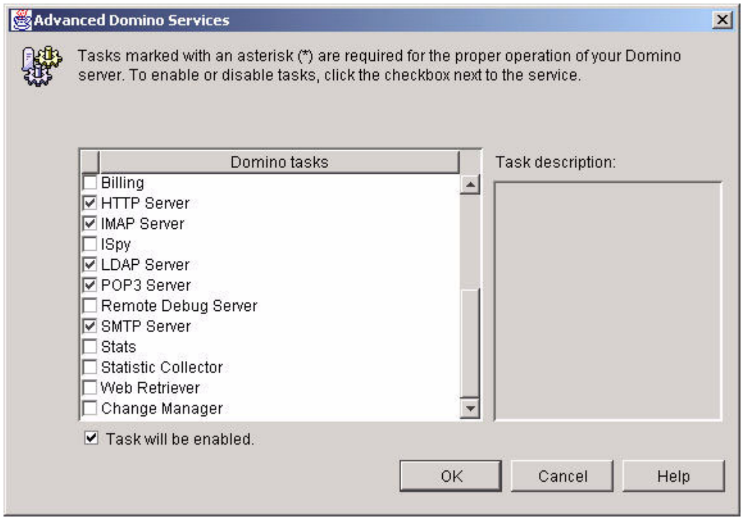


Tasks marked with an asterisk (*) are required for the proper operation of your Domino server. To enable or disable tasks, click the checkbox next to the service.

- ☑ *Database Replicator
- ☑ *Mail Router
- ☑ *Agent Manager
- ☑ *Administration Process
- ☑ Calendar Connector
- ☑ Schedule Manager
- ☐ Statistics
- ☐ DIIOP CORBA Services
- ☐ DECS Domino Enterprise Connection Services
- ☑ DOLS Domino Off Line Services
- ☐ Billing
- ☑ HTTP Server

☑ Task will be enabled.

Figure 5-58 Advanced Domino Services (upper half of Domino server tasks list)



Tasks marked with an asterisk (*) are required for the proper operation of your Domino server. To enable or disable tasks, click the checkbox next to the service.

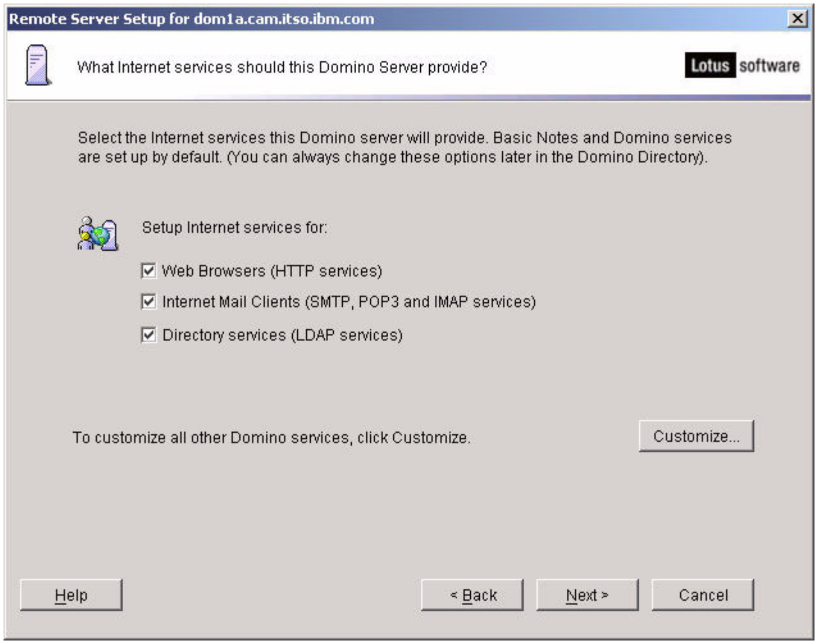
- ☐ Billing
- ☑ HTTP Server
- ☑ IMAP Server
- ☐ ISpy
- ☑ LDAP Server
- ☑ POP3 Server
- ☐ Remote Debug Server
- ☑ SMTP Server
- ☐ Stats
- ☐ Statistic Collector
- ☐ Web Retriever
- ☐ Change Manager

☑ Task will be enabled.

Figure 5-59 Advanced Domino Services (lower half of Domino server tasks list)

22. After you have made your Domino Server Task selections (in our example environment we kept the defaults), click **OK**.

23.This returns you to the initial Internet Services window (Figure 5-60). If you detect errors here, make the necessary changes now. If the information looks correct, click **Next**.



Remote Server Setup for dom1a.cam.itso.ibm.com

What Internet services should this Domino Server provide?

Select the Internet services this Domino server will provide. Basic Notes and Domino services are set up by default. (You can always change these options later in the Domino Directory).

Setup Internet services for:

☑ Web Browsers (HTTP services)

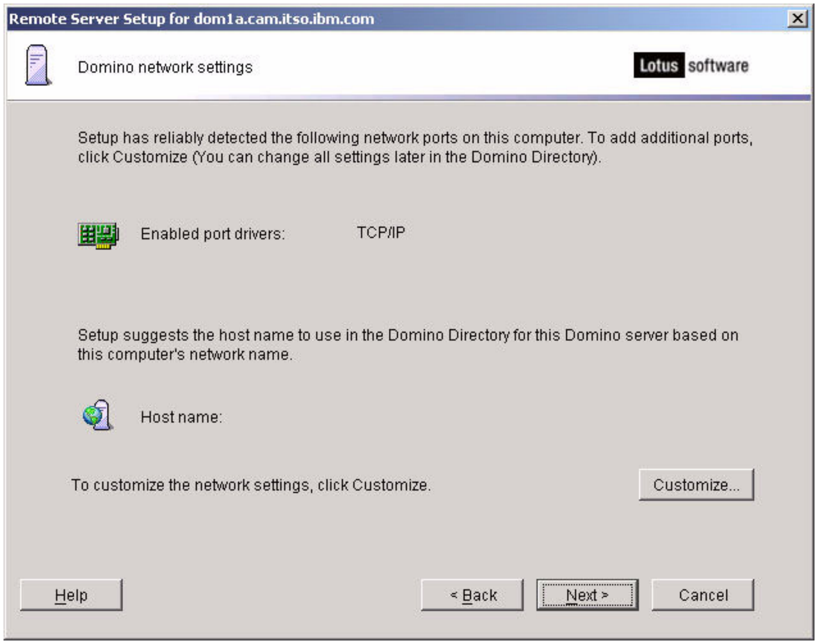
☑ Internet Mail Clients (SMTP, POP3 and IMAP services)

☑ Directory services (LDAP services)

To customize all other Domino services, click Customize.

Figure 5-60 Internet services specified

24. You are prompted for your Domino Server Network Settings (Figure 5-61). Click **Customize**.



Remote Server Setup for dom1a.cam.itso.ibm.com

Domino network settings

Setup has reliably detected the following network ports on this computer. To add additional ports, click Customize (You can change all settings later in the Domino Directory).

Enabled port drivers: TCP/IP

Setup suggests the host name to use in the Domino Directory for this Domino server based on this computer's network name.

Host name:

To customize the network settings, click Customize.

Figure 5-61 Prompt for network settings

25. This opens the Advanced Network Settings window (Figure 5-62), which prompts for network configuration details specific to this Domino Server.

    Note the fields that are `Editable` (see column headings). You can specify:

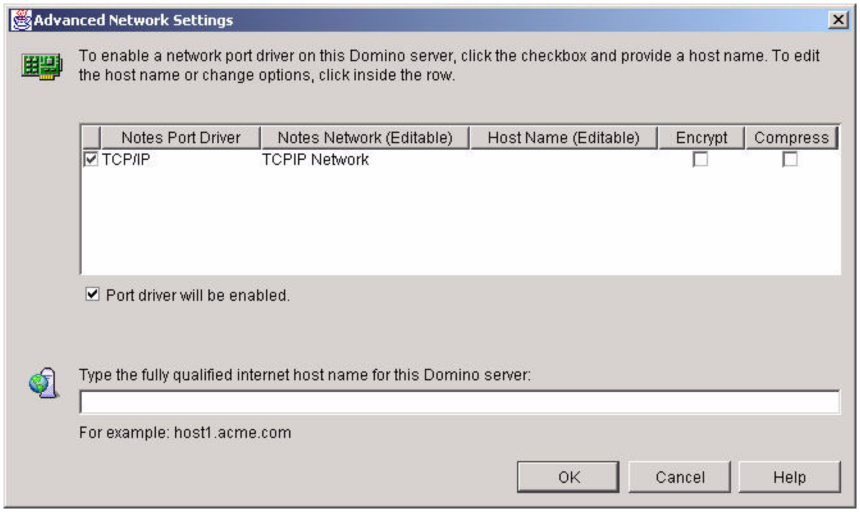
    – The name of your TCP/IP network if different from the default value.

    – Your Domino server SMTP host name. This can be the local part of the Domino server's host name or its IP address. We encourage using SMTP host names whenever possible in order to avoid potential network issues when IP addresses change.

    – Whether to enable Domino server encryption and network compression.

    – The fully qualified SMTP host name of this Domino server.

    Click **OK**. (Figure 5-63 shows the information for our lab environment.)



Advanced Network Settings

To enable a network port driver on this Domino server, click the checkbox and provide a host name. To edit the host name or change options, click inside the row.

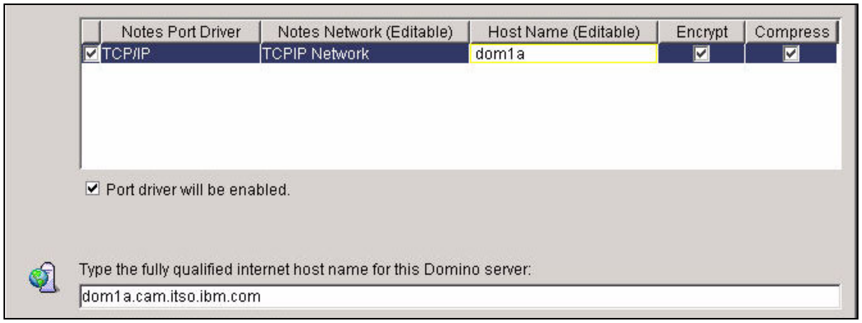
	Notes Port Driver	Notes Network (Editable)	Host Name (Editable)	Encrypt	Compress
☑	TCP/IP	TCPIP Network		□	□

☑ Port driver will be enabled.

Type the fully qualified internet host name for this Domino server:

For example: host1.acme.com

Figure 5-62 Prompt for Advanced Network Settings



	Notes Port Driver	Notes Network (Editable)	Host Name (Editable)	Encrypt	Compress
☑	TCP/IP	TCPIP Network	dom1a	☑	☑

☑ Port driver will be enabled.

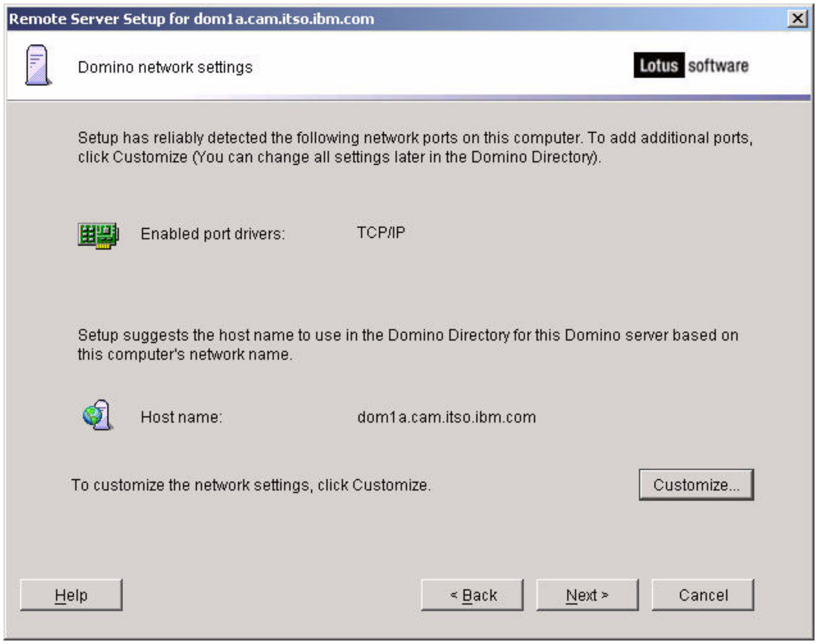
Type the fully qualified internet host name for this Domino server:

dom1a.cam.itso.ibm.com

Figure 5-63 Advanced Network Settings specified

26. This returns you to the initial Network Settings window (Figure 5-64), which is now populated with information you entered in the Advanced Network Settings window.

If you detect errors here, make the necessary changes now. If the information looks correct, click **Next** to continue.



Remote Server Setup for dom1a.cam.itso.ibm.com

Domino network settings

Setup has reliably detected the following network ports on this computer. To add additional ports, click Customize (You can change all settings later in the Domino Directory).

Enabled port drivers: TCP/IP

Setup suggests the host name to use in the Domino Directory for this Domino server based on this computer's network name.

Host name: dom1a.cam.itso.ibm.com

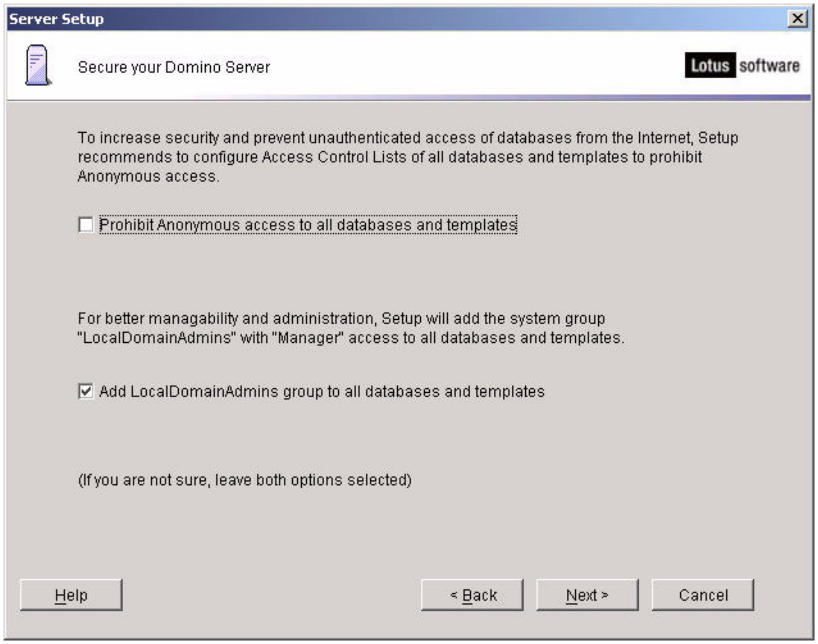
To customize the network settings, click Customize.

Figure 5-64 Network Settings completed

27. Specify your Domino server's initial Security Settings (Figure 5-65).

Unless you have a specific requirement to allow Anonymous access to all databases and templates on your Domino server, we strongly encourage you to select the option to *prevent* this access. Domino gives you the ability to change your security settings later, after your server is up and running.

Select the Security Settings that pertain to your environment. If you detect errors here, make the necessary changes now. When the information looks correct, click **Next** to continue.



Server Setup

Secure your Domino Server

To increase security and prevent unauthenticated access of databases from the Internet, Setup recommends to configure Access Control Lists of all databases and templates to prohibit Anonymous access.

□ Prohibit Anonymous access to all databases and templates

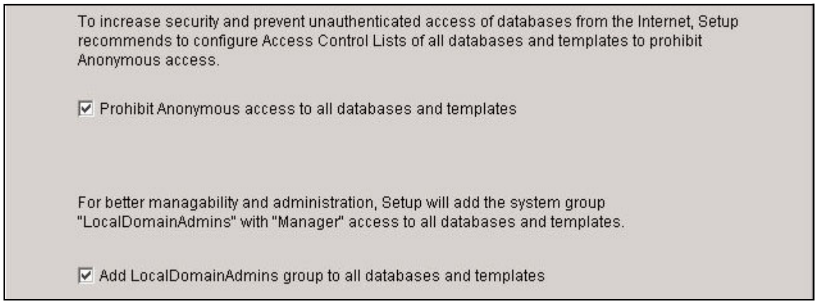
For better managability and administration, Setup will add the system group "LocalDomainAdmins" with "Manager" access to all databases and templates.

☑ Add LocalDomainAdmins group to all databases and templates

(If you are not sure, leave both options selected)

Figure 5-65 Prompt for Security Settings

In our example environment (Figure 5-66) we selected both security options.



To increase security and prevent unauthenticated access of databases from the Internet, Setup recommends to configure Access Control Lists of all databases and templates to prohibit Anonymous access.

☑ Prohibit Anonymous access to all databases and templates

For better managability and administration, Setup will add the system group "LocalDomainAdmins" with "Manager" access to all databases and templates.

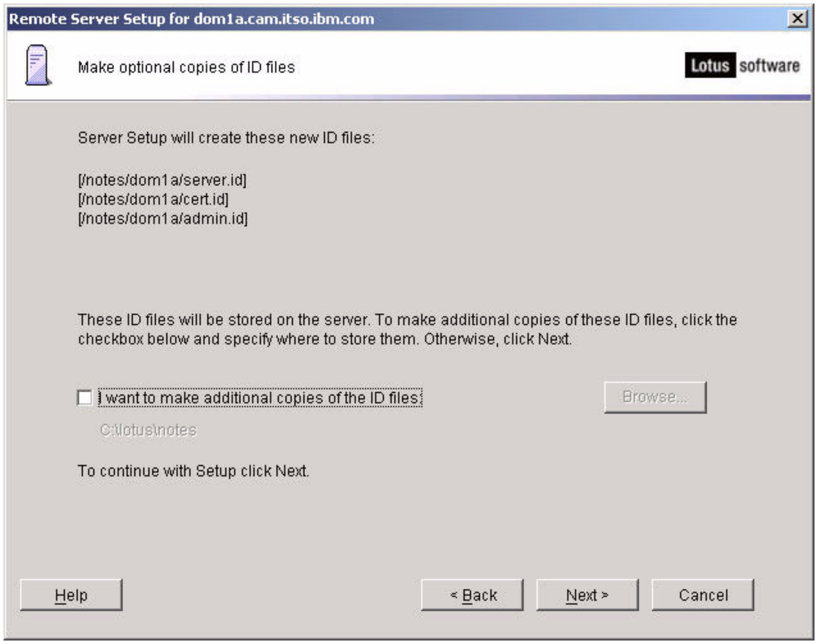
☑ Add LocalDomainAdmins group to all databases and templates

Figure 5-66 Security Settings specified

28. In Figure 5-67 the Remote Server Setup program gives you the option to make copies of the ID files created as part of the setup process.

    In our example we did not make optional copies of the ID files.

    Make the selection that is appropriate for your environment. If you detect errors here, make the necessary changes now. If the information looks correct, click **Next** to continue.



Remote Server Setup for dom1a.cam.itso.ibm.com

Make optional copies of ID files

Server Setup will create these new ID files:

[/notes/dom1a/server.id]
[/notes/dom1a/cert.id]
[/notes/dom1a/admin.id]

These ID files will be stored on the server. To make additional copies of these ID files, click the checkbox below and specify where to store them. Otherwise, click Next.

☐ I want to make additional copies of the ID files:

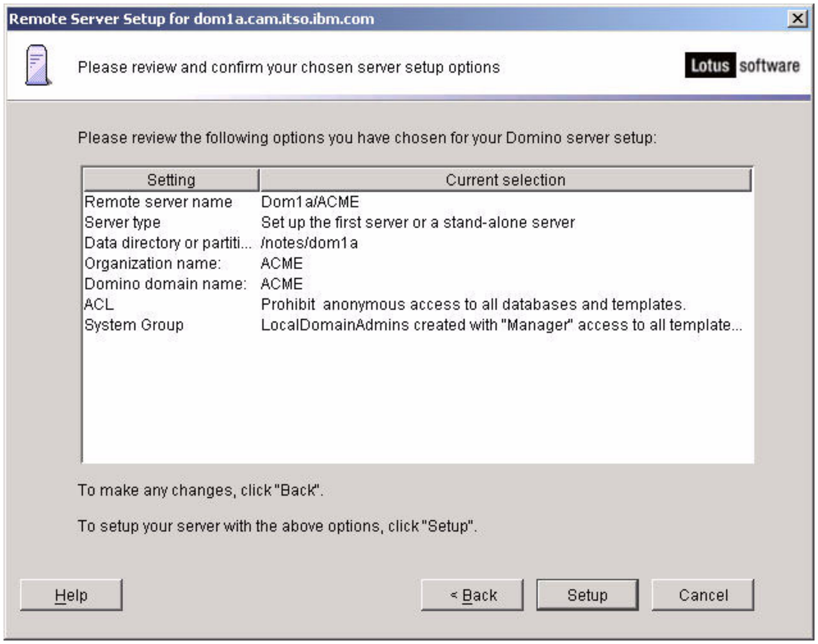
C:\lotus\notes

To continue with Setup click Next.

Figure 5-67 Optional copies of ID files

29. Review your server settings (Figure 5-68). Note that only a subset of all your selections and choices are actually shown here.

If you find errors with the settings shown in this display, use the Back button to step back through the Remote Server Setup screens until you reach the part you need to fix. Then click Next to advance through the Remote Server Setup screens until you return to this display to confirm your settings again. When all appears correct, click **Setup** to launch the Domino Server Setup process.



Remote Server Setup for dom1a.cam.itso.ibm.com

Please review and confirm your chosen server setup options

Please review the following options you have chosen for your Domino server setup:

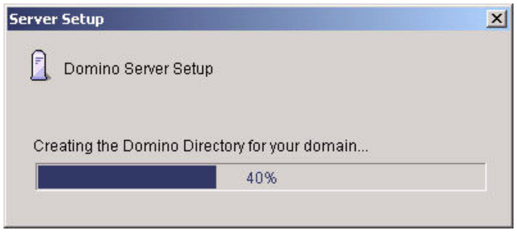
Setting	Current selection
Remote server name	Dom1a/ACME
Server type	Set up the first server or a stand-alone server
Data directory or partiti...	/notes/dom1a
Organization name:	ACME
Domino domain name:	ACME
ACL	Prohibit anonymous access to all databases and templates.
System Group	LocalDomainAdmins created with "Manager" access to all template...

To make any changes, click "Back".

To setup your server with the above options, click "Setup".

Figure 5-68 Confirm your server settings

30. The Domino Server Setup progress bar displays (Figure 5-69).



Server Setup

Domino Server Setup

Creating the Domino Directory for your domain...

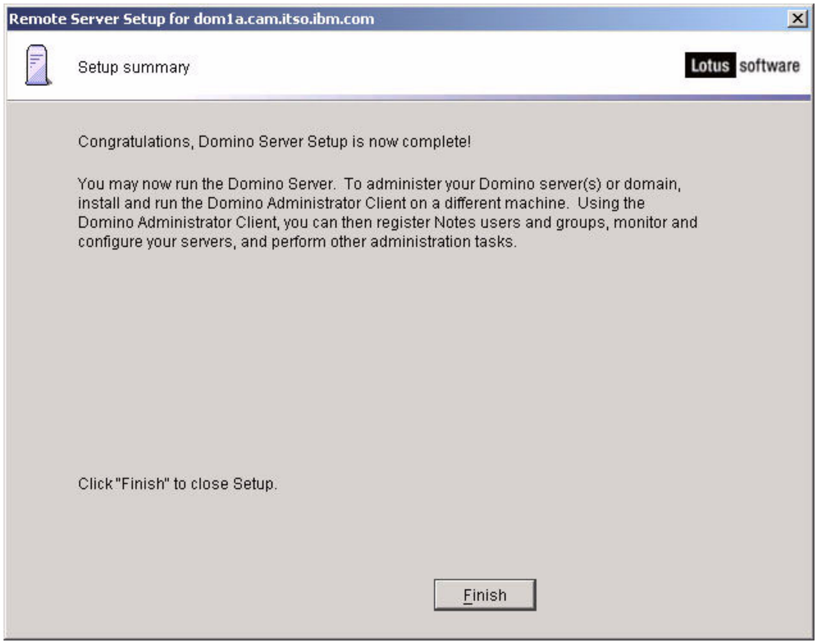
Figure 5-69 Progress bar, Setup running

Normally this process completes without stopping unless unexpected issues arise. Here are examples of errors that can occur (typically associated with the setup of *additional* Domino servers, not the first server), with suggestions about how to address them:

- If progress stops at *20%*: This normally happens only when setting up an additional server in the Domino domain, not a first server. It can occur when the new Domino server that is being set up *cannot* access the existing Domino server that has the Domino Directory. If this occurs, you can click **Back** to return to the Settings Review window. Check network and Access Control settings as potential causes. When network access is restored, restart Remote Server Setup by clicking **Submit**.
- If progress stops at *50%*: This normally happens only when setting up an additional server in the Domino domain, not a first server. It can occur when the new Domino server that is being set up *can* access the existing Domino server that has the Domino Directory, but cannot read the Domino Directory. If this occurs, you can click **Back** to return to the Settings Review window. Check Access Control settings as potential causes. When Domino Directory access is restored, restart Remote Server Setup by clicking **Submit**.
- If progress stops at *85%*: This normally happens only when setting up an additional server in the Domino domain, not a first server. This can occur when there is already a Domino Directory (names.nsf) file in the data directory of the Domino server being set up. This rogue Domino Directory might have gotten there if one was FTPed from an existing Domino server to the new server beforehand, and there might be UNIX ownership issues or other issues with this file. If this occurs, you can click **Back** to return to the Settings Review window. Log on to your Solaris server, check to see whether a names.nsf file already exists in the data directory of the server being set up. If one exists, rename it for subsequent investigation. Restart Remote Server Setup by clicking **Submit**.

Tip: In case of a setup failure, you can find reasons for possible errors logged in the Domino server's notes.ini file, which is in the server's Domino data directory.

31. After the progress bar successfully reaches 100%, it disappears and the window in Figure 5-70 displays. Click **Finish** to close the Domino Remote Server Setup utility.



Remote Server Setup for dom1a.cam.itso.ibm.com

Setup summary

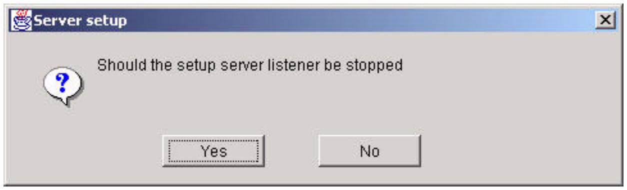
Congratulations, Domino Server Setup is now complete!

You may now run the Domino Server. To administer your Domino server(s) or domain, install and run the Domino Administrator Client on a different machine. Using the Domino Administrator Client, you can then register Notes users and groups, monitor and configure your servers, and perform other administration tasks.

Click "Finish" to close Setup.

Figure 5-70 Server Setup completed

32. You will be asked whether to shut down the listener task on the remote Domino server that you just set up (Figure 5-71). Click **Yes**.

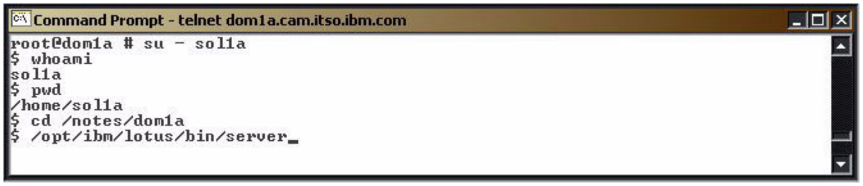


Server setup

Should the setup server listener be stopped

Figure 5-71 Prompt about Listener task on remote server

33. You can launch the new Domino 7 server, the first server in this Domino domain, on Solaris 10. Return to the Solaris display where your Solaris user was running the new Domino server in Listening mode (Figure 5-72)



```
root@dom1a # su - sol1a
$ whoami
sol1a
$ pwd
/home/sol1a
$ cd /notes/dom1a
$ /opt/ibm/lotus/bin/server_
```

Figure 5-72 Manually launch Domino

34. In our example, the first Domino server is dom1a, owned by Solaris account sol1a. To make this Domino partition's data directory current, type the following command as sol1a:

```
cd /notes/dom1a
```

To launch this Domino server, type:

```
/opt/ibm/lotus/bin/server
```

Note that this fully qualified command can be shortened to just **`server`** when you are already in the directory PATH of the owning Solaris user (in our example, this is `sol1a`).

> **Note:** Because your first Domino server is starting for the first time, network and port-specific error messages typically will not appear among the Domino server console information that begins to scroll by, but depending on your specific environment, such errors are possible.
>
> Such issues and errors are addressed in Domino Administration steps in 5.4.1, "Partitioned server networking considerations" on page 181.

> **Important:** There are many ways to start your Domino server, and what we have shown you here is the most basic approach. We suggest that you refer to the following sections for additional information:
>
> - 5.5, "Starting Domino and the server controller console" on page 194
> - 9.4.1, "Domino Server Controller" on page 322
> - 9.4.2, "Domino (Java) Console" on page 325

Leave this Domino server up and running.

Now we turn our attention to setting up additional Domino servers in your environment.

5.3.3 Setting up additional Domino servers

This section describes how you can set up additional Domino servers in your environment.

Getting the Administrator ID

Before starting the setup process for additional Domino servers, you must first register and certify these additional servers with the appropriate certifier ID. If you have just set up the first server, then the Domino Administrator ID (admin.id) and the Domino Certifier ID (cert.id) will be stored in the data directory of the first Domino server. To access these ID files:

1. Log onto a Windows workstation that has the Domino Administrator client installed. Install the Domino Administrator client now if you have not done this already. Follow your organization's policies for ID management to determine a safe location to store the Administrator ID and Certifier ID.
2. From this same Windows workstation, FTP to the Solaris server and log in as the owning Solaris account of the first Domino server. In our example, this is Solaris user `sol1a`.
3. Change directory to this Domino server's data directory. In our example, this is `/notes/dom1a`.
4. Perform a binary mode file transfer of **admin.id** and **cert.id** from the Solaris server to the location you chose on the Windows workstation.
5. Launch the Domino Administrator client and specify the location of the Administrator ID to use for administering our Solaris-resident Domino servers. You can ensure that the Domino Administrator client is using the correct ID file (admin.id) using **File** → **Security** → **Switch ID** to specify the correct Administrator ID file to use.
6. Enter the Administrator ID password specified during Remote Server Setup.

Registering a new server

When you have both the admin.id and cert.id files, you can register the second and additional servers.

The figures and procedures that follow are performed with the Domino 7 Administrator client.

Recall that our example Domino environment has four Domino servers (two Domino partitions each on two Sun Solaris servers). The steps that follow depict the process of registering the remaining three additional servers for our sample environment.

To register additional Domino servers:

1. Launch the Domino Administrator client.

Release 7.0 August 18, 2005 L-GHUS-5RWNHM

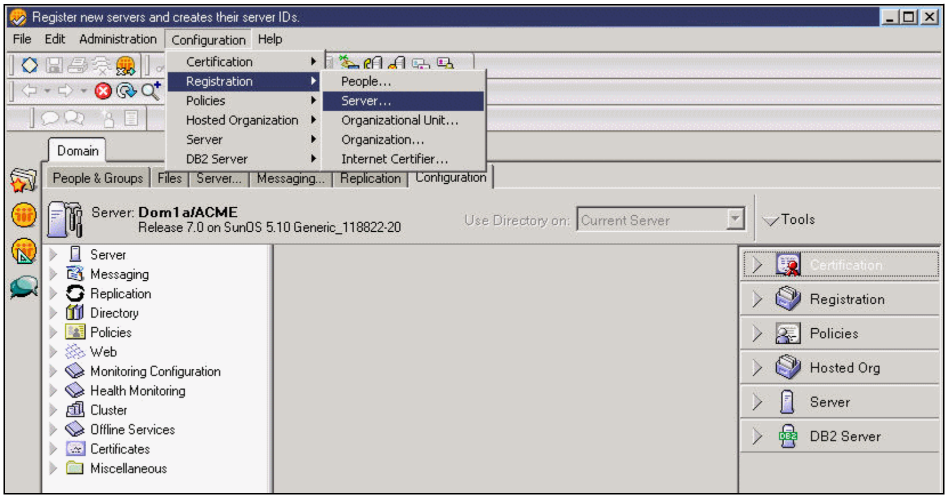
Licensed Materials - Property of IBM. © Copyright IBM Corporation 1985, 2005. All Rights Reserved. IBM, the IBM logo, Lotus and Notes are trademarks of IBM Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product or service names may be trademarks or service marks of others.

Figure 5-73 The Lotus Domino 7 Administrator client

2. If necessary, switch to the new Administrator's ID file by selecting **File** → **Security** → **Switch ID** from the menu. If prompted, enter the Administrator password.

3. Click the **Configuration** tab and select **Registration** → **Server** (Figure 5-74).

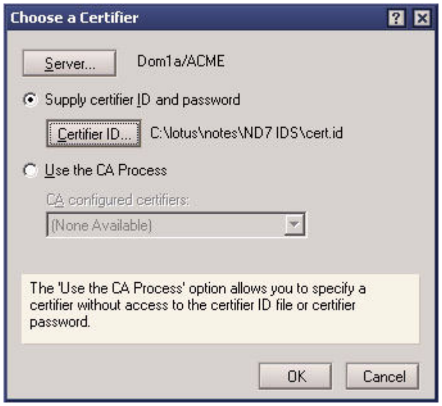


Server: Dom1a/ACME
Release 7.0 on SunOS 5.10 Generic_118822-20

Figure 5-74 Getting started

4. The Choose a Certifier dialog box appears. Click **Server** and enter the name of the first server. (In our example, it is `dom1a/ACME`.) Select **Supply certifier ID and password** and click **Certifier ID** to specify the location of the Certifier ID file.

   When you have provided all of the required Certifier information, the dialog box will resemble Figure 5-75. Click **OK**.



Choose a Certifier

Server... Dom1a/ACME

● Supply certifier ID and password

Certifier ID... C:\lotus\notes\ND7 IDS\cert.id

○ Use the CA Process

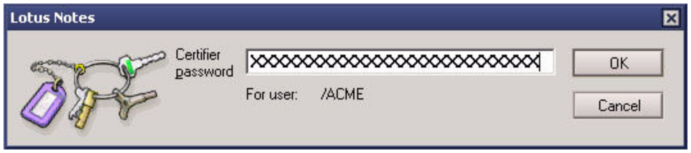
CA configured certifiers: (None Available)

The 'Use the CA Process' option allows you to specify a certifier without access to the certifier ID file or certifier password.

OK Cancel

Figure 5-75 Specifying the Certification Server and Certifier ID

5. When prompted, enter the Certifier password you specified when you configured the first server and click **OK** (Figure 5-76).



Lotus Notes

Certifier password XXXXXXXXXXXXXXXXXXXXXXXXXX

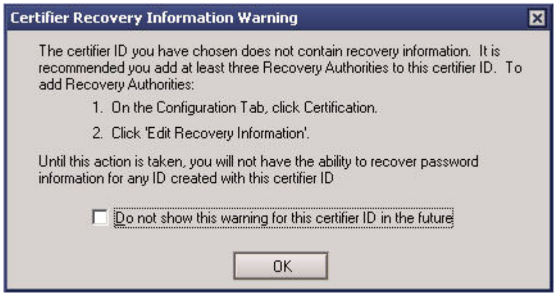
For user: /ACME

OK

Cancel

Figure 5-76 Enter the Certifier ID password

6. Specify Recovery Authorities for this Certifier ID and click **OK** (Figure 5-77). This is recommended for most Domino environments, but is not covered in this book.



Certifier Recovery Information Warning

The certifier ID you have chosen does not contain recovery information. It is recommended you add at least three Recovery Authorities to this certifier ID. To add Recovery Authorities:

1. On the Configuration Tab, click Certification.
2. Click 'Edit Recovery Information'.

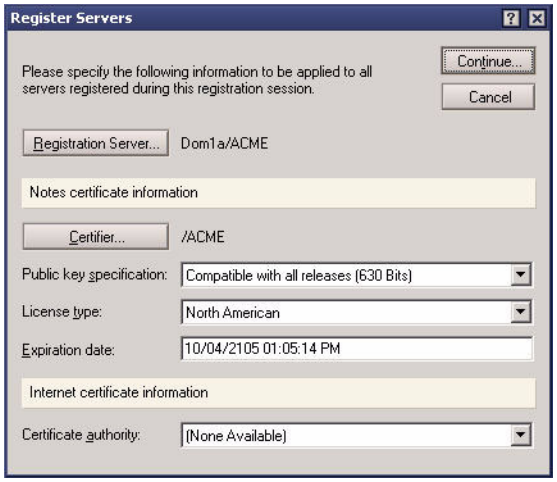
Until this action is taken, you will not have the ability to recover password information for any ID created with this certifier ID

□ Do not show this warning for this certifier ID in the future

Figure 5-77 Certifier Recovery Warning

7. Figure 5-78 shows the Registration profile we applied to all of our additional Domino servers. We used the default settings.

   Click **Continue**.



Register Servers

Please specify the following information to be applied to all servers registered during this registration session.

Dom1a/ACME

Notes certificate information

/ACME

Public key specification: Compatible with all releases (630 Bits)

License type: North American

Expiration date: 10/04/2105 01:05:14 PM

Internet certificate information

Certificate authority: (None Available)

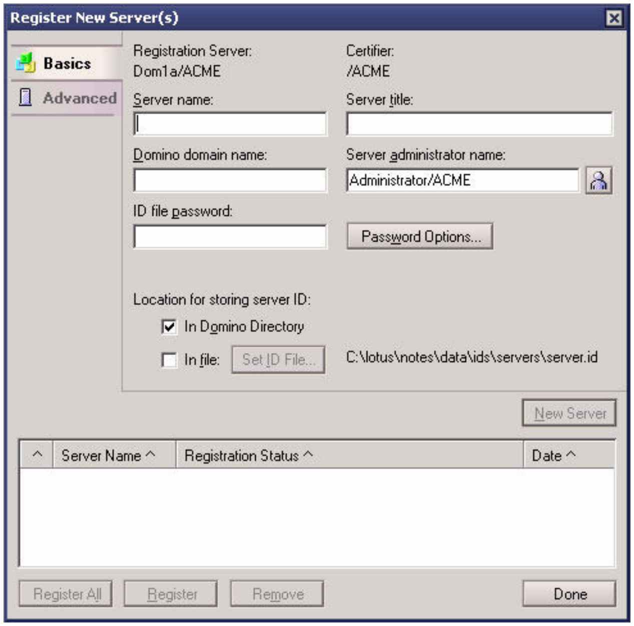
Figure 5-78 Registration profile that we applied to all servers

8. In the Register New Servers window (Figure 5-79), enter specific information about each of the additional Domino servers to register in your environment. With this interface you can register one or many additional Domino servers. In our example, we register *all* of our additional Domino servers at this time.

   Enter the following information for your first additional server (actually the second server in your Domino domain):

   – Server name
   – Server title
   – Domino domain name
   – Server administrator name (already populated)
   – Server ID file password and password options

   Click **Password Options**.



Register New Server(s)

Registration Server: Dom1a/ACME

Certifier: /ACME

Server name:

Server title:

Domino domain name:

Server administrator name: Administrator/ACME

ID file password:

Location for storing server ID:

☑ In Domino Directory

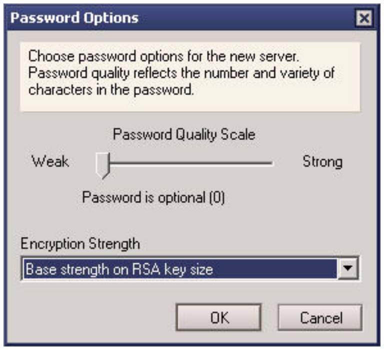
□ In file: C:\lotus\notes\data\ids\servers\server.id

Server Name	Registration Status	Date

Figure 5-79 Prompt for details of additional servers

Important: Unless your organization’s security policies require a password for your Domino server IDs, do not specify a Domino server ID password if you will automate the launch of your Domino server partitions in Solaris; otherwise, you will have to accommodate a password-entry requirement in your scripts that automate Domino server startup, and your Domino server will not launch unless the password is provided.

9. Figure 5-80 shows how to prevent the Domino server ID file from having a password. Use the sliding indicator on the Password Quality Scale to specify **Password is optional (0)**. Unless your organization requires a Server ID password, ensure that the Domino server does not have a password; this simplifies automating Domino server launch in Solaris. Click **OK**.



Password Options

Choose password options for the new server. Password quality reflects the number and variety of characters in the password.

Password Quality Scale

Password is optional (0)

Encryption Strength

Base strength on RSA key size

Figure 5-80 Password Options

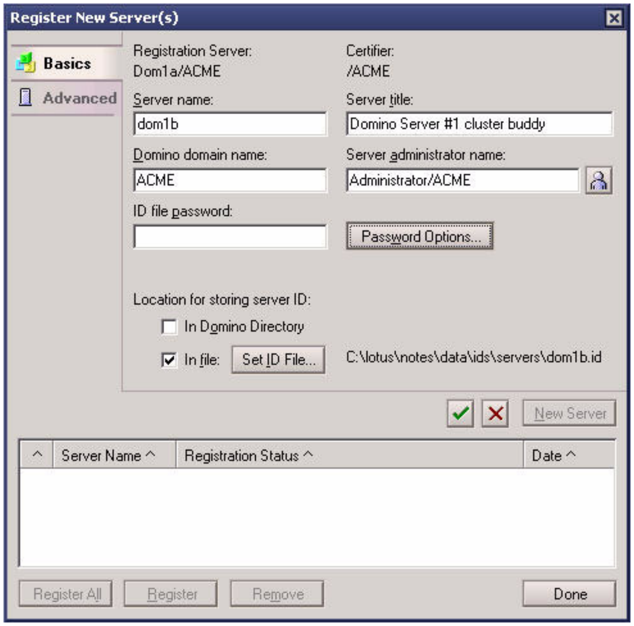
> **Note:** To remove the password from the ID file, see Appendix D, “Removing a password from a server ID file” on page 545.

10. Back at the Register New Servers window (Figure 5-81), server information is now complete, but note one *important* option we have changed from the original defaults: You must save your server ID either as a file in a folder or as an attachment in a server document in the Domino Directory (names.nsf).

    If you choose to store the new server ID file in the Domino Directory, then you must set a Server ID password. In our example, we save the server ID files to a folder and avoid the requirement of having a Server ID password.

    > **Important:** To facilitate automating the start of your Domino servers, we recommend that you register your new Server IDs files, securely store them on the file system, and do not assign a password.

    If you detect errors here, make the necessary changes now. If the information looks correct, click the green check mark button to place this server in the Registration Queue.



Register New Server(s)

Registration Server: Dom1a/ACME

Certifier: /ACME

Server name: dom1b

Server title: Domino Server #1 cluster buddy

Domino domain name: ACME

Server administrator name: Administrator/ACME

ID file password:

Location for storing server ID:

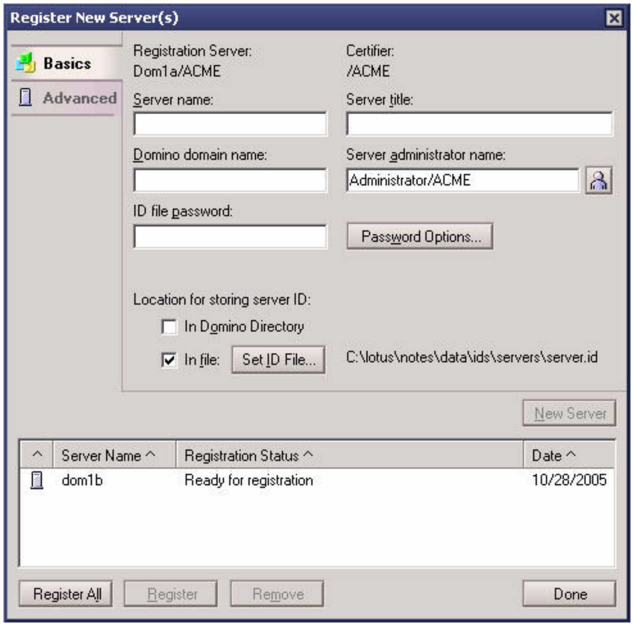
□ In Domino Directory

☑ In file: C:\lotus\notes\data\ids\servers\dom1b.id

Server Name	Registration Status	Date

Figure 5-81 First additional server ready to stage in Registration work queue

The following figures show the registration of our remaining additional Domino servers.



Registration Server: Dom1a/ACME

Certifier: /ACME

Server name:

Server title:

Domino domain name:

Server administrator name: Administrator/ACME

ID file password:

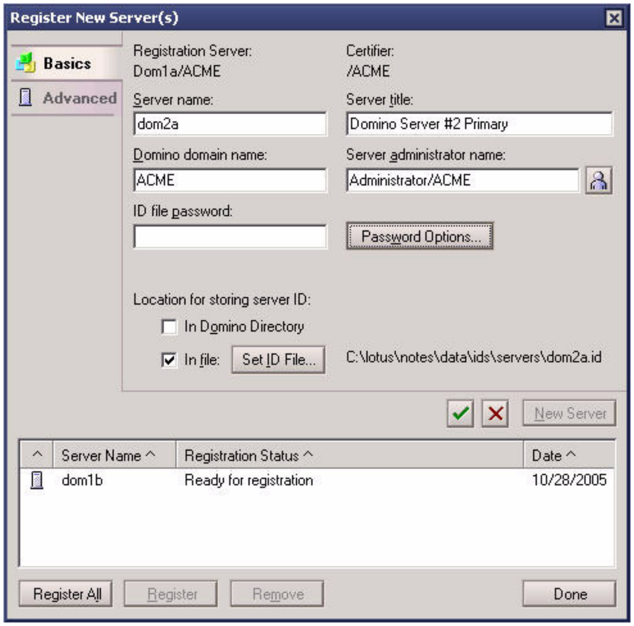
Location for storing server ID:

☐ In Domino Directory

☑ In file: C:\lotus\notes\data\ids\servers\server.id

Server Name	Registration Status	Date
dom1b	Ready for registration	10/28/2005

Figure 5-82 First additional server moved to Registration work queue



Registration Server: Dom1a/ACME

Certifier: /ACME

Server name: dom2a

Server title: Domino Server #2 Primary

Domino domain name: ACME

Server administrator name: Administrator/ACME

ID file password:

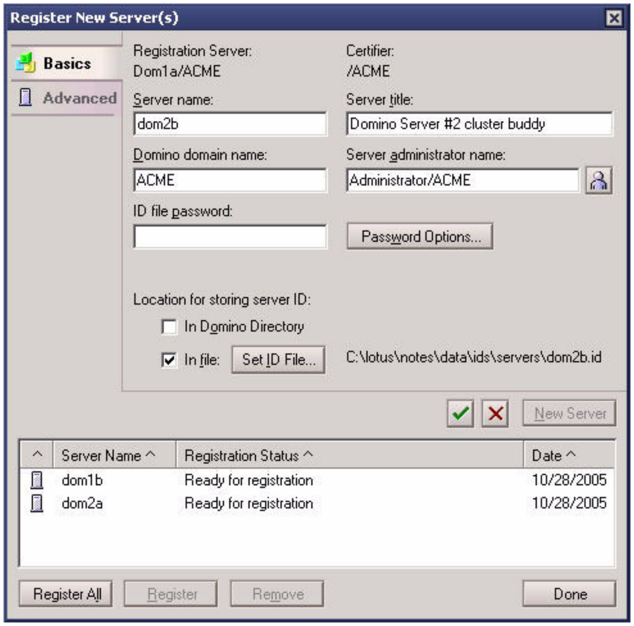
Location for storing server ID:

☐ In Domino Directory

☑ In file: C:\lotus\notes\data\ids\servers\dom2a.id

Server Name	Registration Status	Date
dom1b	Ready for registration	10/28/2005

Figure 5-83 Second additional server ready to stage in Registration work queue



Registration Server: Dom1a/ACME

Certifier: /ACME

Server name: dom2b

Server title: Domino Server #2 cluster buddy

Domino domain name: ACME

Server administrator name: Administrator/ACME

ID file password:

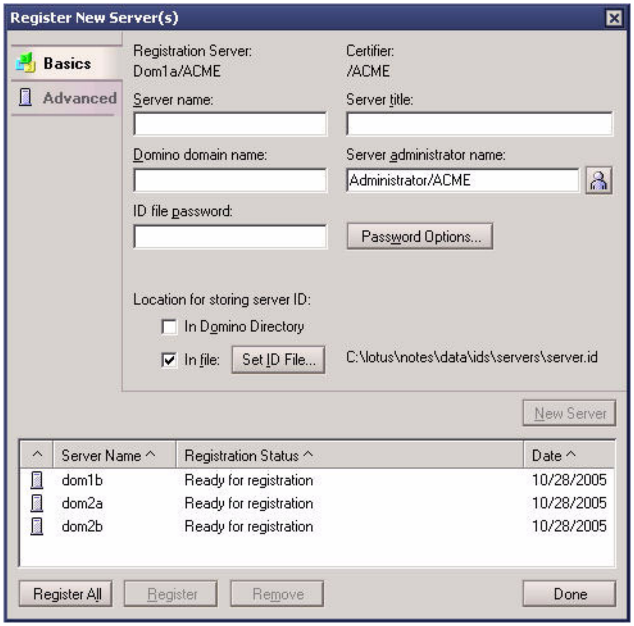
Location for storing server ID:

☐ In Domino Directory

☑ In file: C:\lotus\notes\data\ids\servers\dom2b.id

Server Name	Registration Status	Date
dom1b	Ready for registration	10/28/2005
dom2a	Ready for registration	10/28/2005

Figure 5-84 Second additional server moved to Registration work queue



Registration Server: Dom1a/ACME

Certifier: /ACME

Server name:

Server title:

Domino domain name:

Server administrator name: Administrator/ACME

ID file password:

Location for storing server ID:

☐ In Domino Directory

☑ In file: C:\lotus\notes\data\ids\servers\server.id

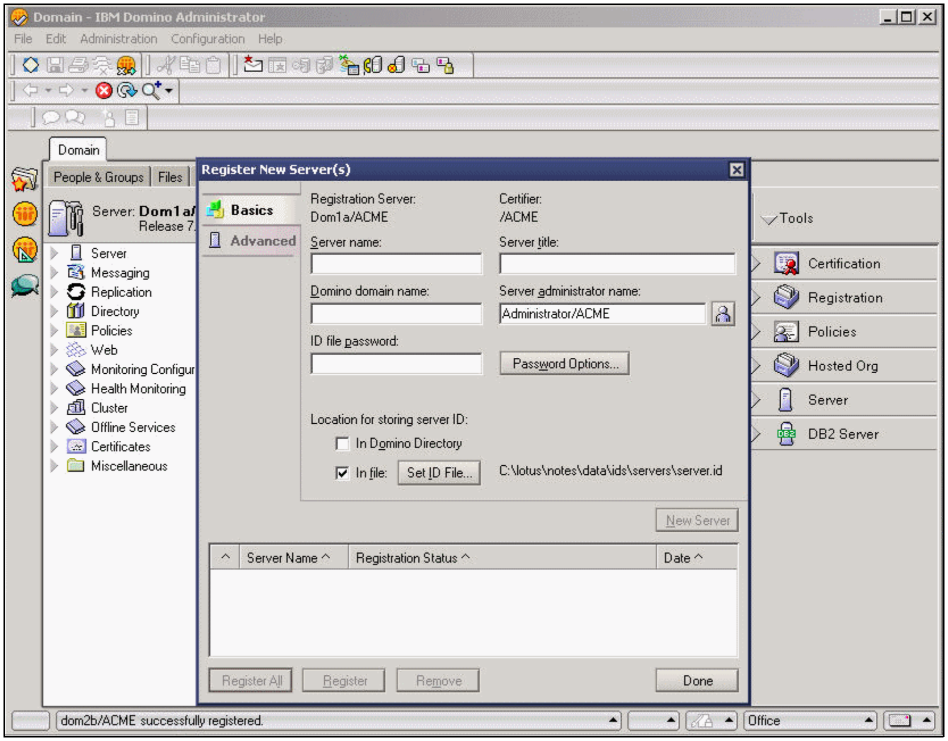
Server Name	Registration Status	Date
dom1b	Ready for registration	10/28/2005
dom2a	Ready for registration	10/28/2005
dom2b	Ready for registration	10/28/2005

Figure 5-85 Third additional server moved to Registration work queue

11. Figure 5-85 on page 145 shows that our Server Registration Queue contains all three of the additional servers in our example environment.

    If you detect errors here, make the necessary changes now. To make corrections, begin by highlighting the server to fix. This repopulates the field values you specified before placing the server in the Registration Queue. Change any erroneous field values and click the green check mark again to put the corrected server into the Registration Queue.

    When the information looks correct, click **Register All** to continue.



Registration Server: Dom1a/ACME

Certifier: /ACME

Server name:

Server title:

Domino domain name:

Server administrator name: Administrator/ACME

ID file password:

Password Options...

Location for storing server ID:

☐ In Domino Directory

☑ In file: Set ID File... C:\lotus\notes\data\ids\servers\server.id

dom2b/ACME successfully registered.

Figure 5-86 Registration completed

12. The servers in the Registration Queue will be processed, and when completed the Register New Servers window will be ready to process new entries again.

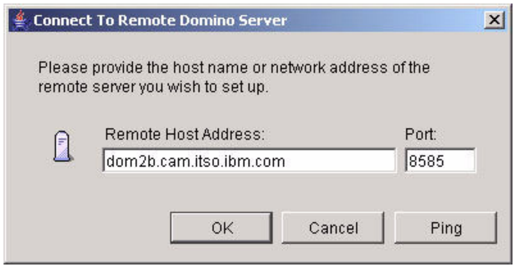
    Click **Done** to finish the Domino server registration process.

5.3.4 Setting up the second server

Make sure that the Domino server, from which you will replicate the Domino Directory, is running and that the network connection is up.

The following steps show how to set up an additional Domino server:

1. FTP any new server ID files that you have stored on another machine to the corresponding Domino partition's data directory in Solaris. In our example this is `notes/dom2b` and our owning Solaris account is `sol2b`.
2. Follow steps 1 on page 112 through 9 on page 114 to start the Remote Server Setup program, and advance to the point where we specify the remote host address (Figure 5-87) of our second Domino server (our first additional server).



Connect To Remote Domino Server

Please provide the host name or network address of the remote server you wish to set up.

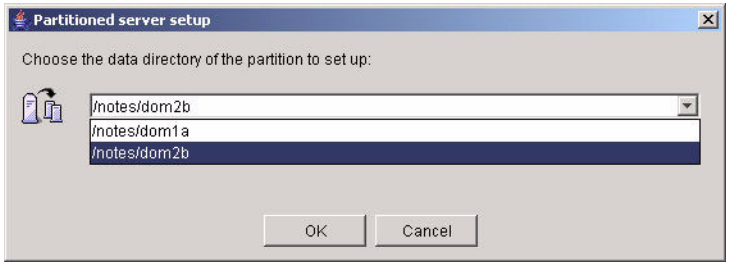
Remote Host Address: dom2b.cam.itso.ibm.com

Port: 8585

Figure 5-87 Beginning to set up the second Domino server

3. At this point, specify the host name of your additional server.

   In our example we choose the host name of the other Domino partition on the physical Solaris server that dom1a is on (Figure 5-88). This other partition is `dom2b`. Click **OK** to launch Remote Server Setup.



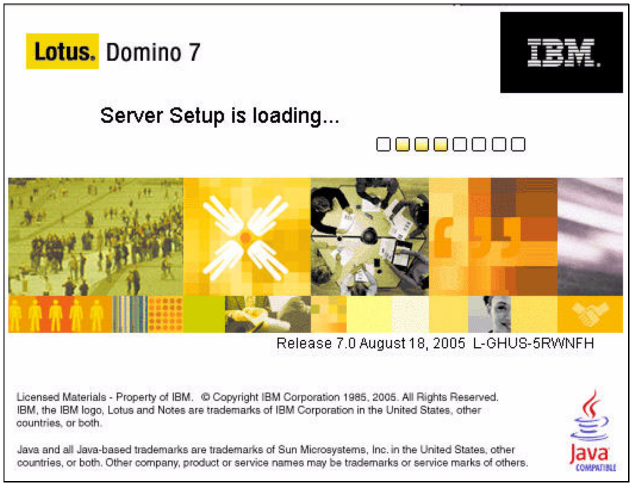
Partitioned server setup

Choose the data directory of the partition to set up: /notes/dom2b

/notes/dom1a
/notes/dom2b

Figure 5-88 Select the correct Domino partition

4. The Domino 7 Remote Server Setup splash screen displays briefly.

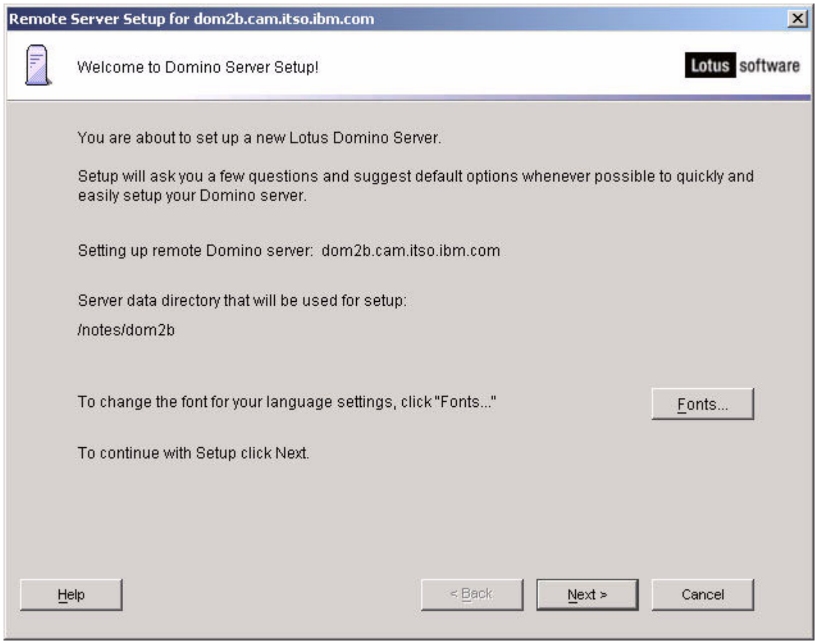

Lotus. Domino 7
IBM.
Server Setup is loading...
Release 7.0 August 18, 2005 L-GHUS-5RWNFH
Java COMPATIBLE

Licensed Materials - Property of IBM. © Copyright IBM Corporation 1985, 2005. All Rights Reserved. IBM, the IBM logo, Lotus and Notes are trademarks of IBM Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product or service names may be trademarks or service marks of others.

Figure 5-89 The Domino 7 Remote Server Setup utility

5. The Server Setup welcome window appears (Figure 5-90). If you changed the setup fonts last time, click **Fonts** to change them this time, too. When you are satisfied with the font selection, click **Next** to continue.



Welcome to Domino Server Setup!

You are about to set up a new Lotus Domino Server.

Setup will ask you a few questions and suggest default options whenever possible to quickly and easily setup your Domino server.

Setting up remote Domino server: dom2b.cam.itso.ibm.com

Server data directory that will be used for setup:

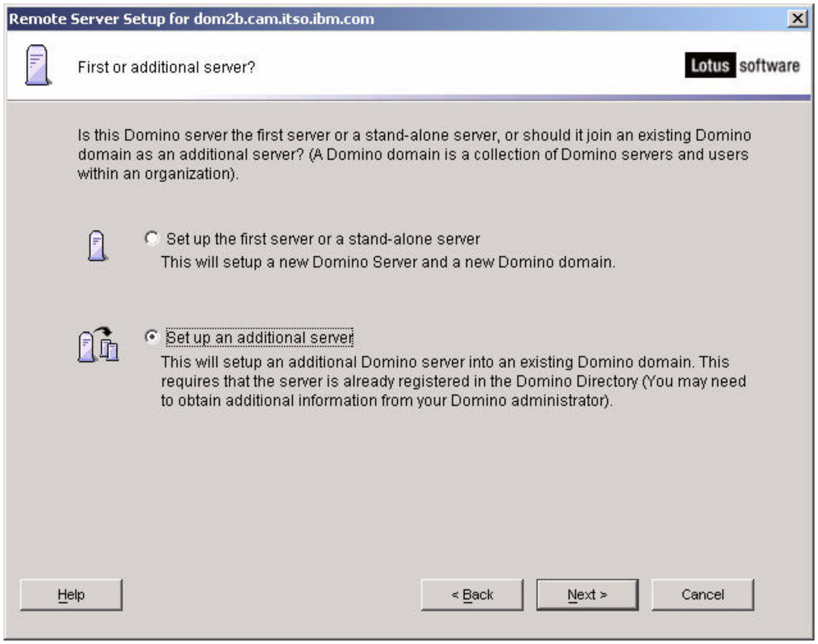
/notes/dom2b

To change the font for your language settings, click "Fonts..."

To continue with Setup click Next.

Figure 5-90 Preparing to specify details of the second server

6. Figure 5-91 prompts you to specify whether this is a first server or an additional server. Choose the option to **Set up an additional server** and click **Next** to continue.



Remote Server Setup for dom2b.cam.itso.ibm.com

First or additional server?

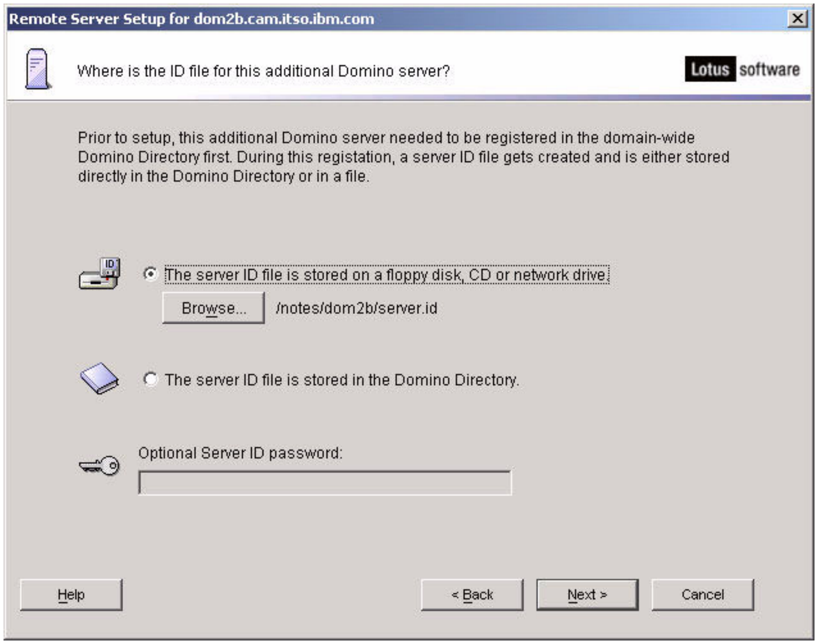
Is this Domino server the first server or a stand-alone server, or should it join an existing Domino domain as an additional server? (A Domino domain is a collection of Domino servers and users within an organization).

○ Set up the first server or a stand-alone server
This will setup a new Domino Server and a new Domino domain.

● Set up an additional server
This will setup an additional Domino server into an existing Domino domain. This requires that the server is already registered in the Domino Directory (You may need to obtain additional information from your Domino administrator).

Figure 5-91   Specifying setup of additional server

7. Remember that when we were preparing to set up additional servers, we recommended FTPing the ID files of our additional servers to their corresponding Domino data directory locations (after we registered the additional servers). Now we must find the ID file we created for this Domino server (Figure 5-92). Click **Browse** to find the server ID (in our example, `dom2b.id`) on Solaris.



Remote Server Setup for dom2b.cam.itso.ibm.com

Where is the ID file for this additional Domino server?

Prior to setup, this additional Domino server needed to be registered in the domain-wide Domino Directory first. During this registation, a server ID file gets created and is either stored directly in the Domino Directory or in a file.

● The server ID file is stored on a floppy disk, CD or network drive.

Browse... /notes/dom2b/server.id

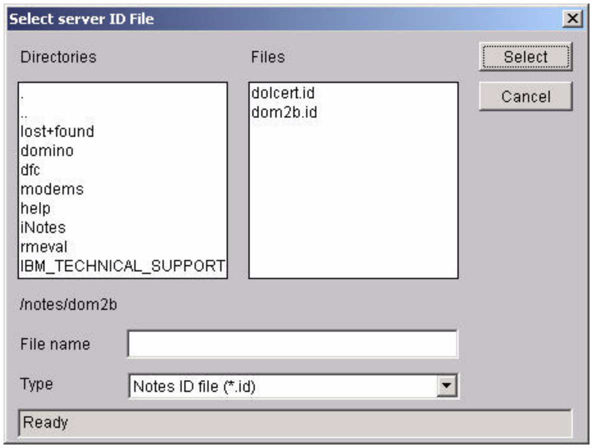
○ The server ID file is stored in the Domino Directory.

Optional Server ID password:

Figure 5-92 Prompt for Domino server ID file

8. Figure 5-93 on page 151 shows the Select server ID file dialog box. This displays a list of Solaris filesystem directories in the column on the left, and the files (type *.id) in the specified directory. Click the correct Server ID file name and **Select**.

> **Note:** You can also save the ID file to a floppy disk or CD after registering additional servers. Then, when you setup the Domino server, mount the removable media on Solaris to make the ID file accessible in this step.



/notes/dom2b

File name

Type Notes ID file (*.id)

Ready

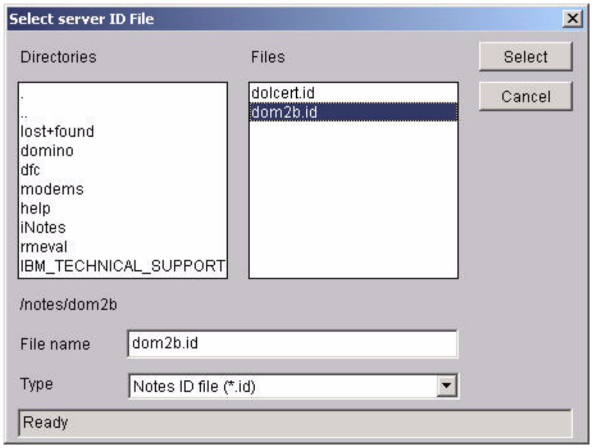
Figure 5-93 Select server ID file dialog

In our example, the Domino Data directory for this server, /notes/dom2b, has already been chosen. There are two ID files in the Domino Data directory:

dolcert.id This is specific to Domino Off-Line Services or DOLS, and is unrelated to our purposes here.

dom2b.id This is the Domino server ID we want.

In our example, we click **dom2b.id** and **Select** (Figure 5-94).



/notes/dom2b

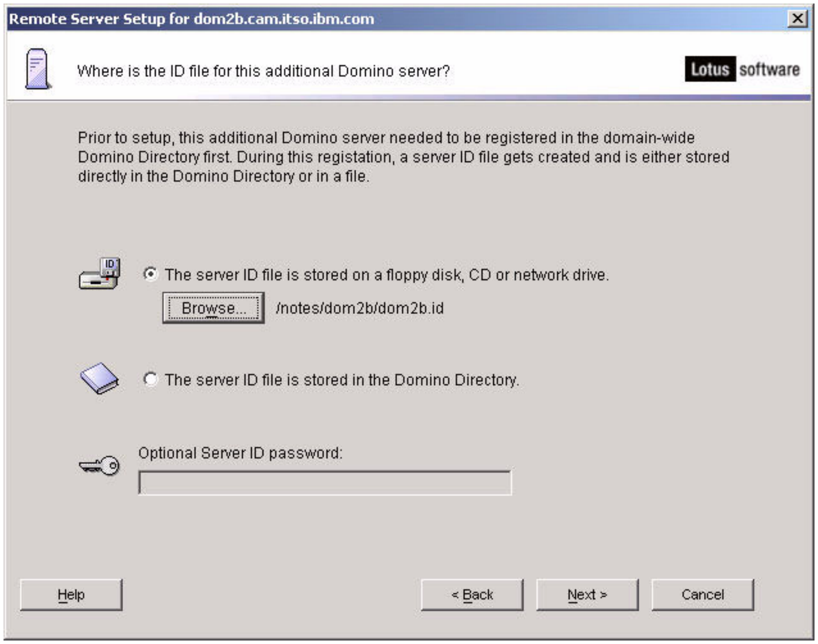
File name dom2b.id

Type Notes ID file (*.id)

Ready

Figure 5-94 Selecting our server ID file

9. Back at the initial ID file prompt screen, where the correct server ID file is identified now (Figure 5-95), click **Next** to continue.



Remote Server Setup for dom2b.cam.itso.ibm.com

Where is the ID file for this additional Domino server?

Prior to setup, this additional Domino server needed to be registered in the domain-wide Domino Directory first. During this registation, a server ID file gets created and is either stored directly in the Domino Directory or in a file.

● The server ID file is stored on a floppy disk, CD or network drive.

Browse... /notes/dom2b/dom2b.id

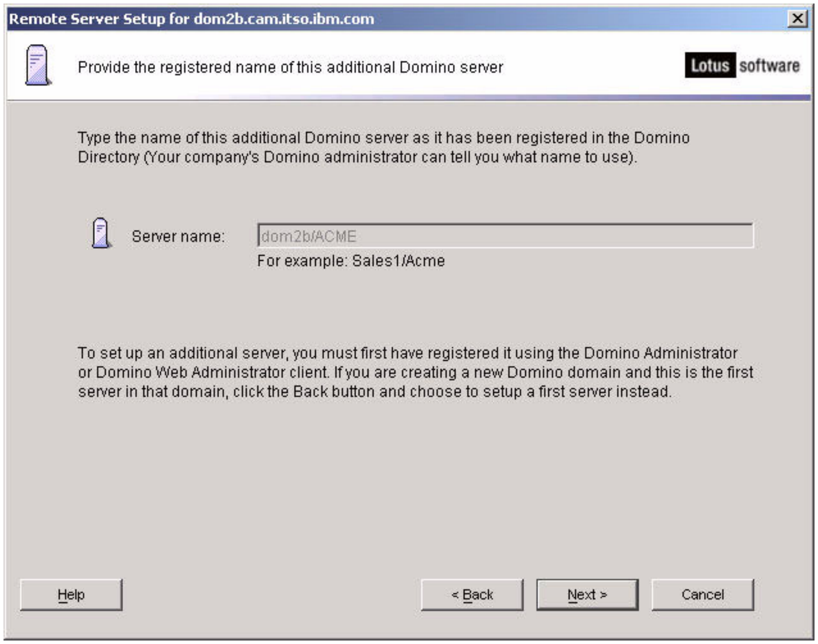
○ The server ID file is stored in the Domino Directory.

Optional Server ID password:

Figure 5-95 Server ID file chosen

10. Figure 5-96 prompts you to provide the registered name of this Domino server. The Server name field has been populated with information extracted from the server ID file, and you cannot change this field's contents manually.

    If there is a problem with the Domino server name, click **Back** to select a different Domino server ID. If this is the correct Domino server name, click **Next** to continue.



Remote Server Setup for dom2b.cam.itso.ibm.com

Provide the registered name of this additional Domino server

Type the name of this additional Domino server as it has been registered in the Domino Directory (Your company's Domino administrator can tell you what name to use).

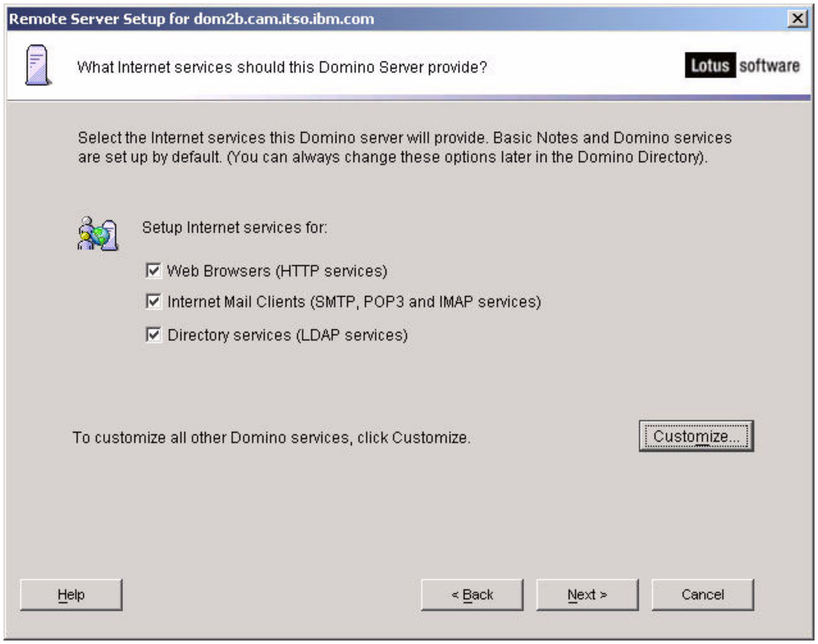
Server name: dom2b/ACME

For example: Sales1/Acme

To set up an additional server, you must first have registered it using the Domino Administrator or Domino Web Administrator client. If you are creating a new Domino domain and this is the first server in that domain, click the Back button and choose to setup a first server instead.

Figure 5-96 Providing the registered name of the additional server

11. As with the first Domino server, Figure 5-97 prompts you to select the Internet services and server tasks that you want to run on this additional server. Make the appropriate changes for your environment and click **Next**.



Remote Server Setup for dom2b.cam.itso.ibm.com

What Internet services should this Domino Server provide?

Select the Internet services this Domino server will provide. Basic Notes and Domino services are set up by default. (You can always change these options later in the Domino Directory).

Setup Internet services for:

☑ Web Browsers (HTTP services)

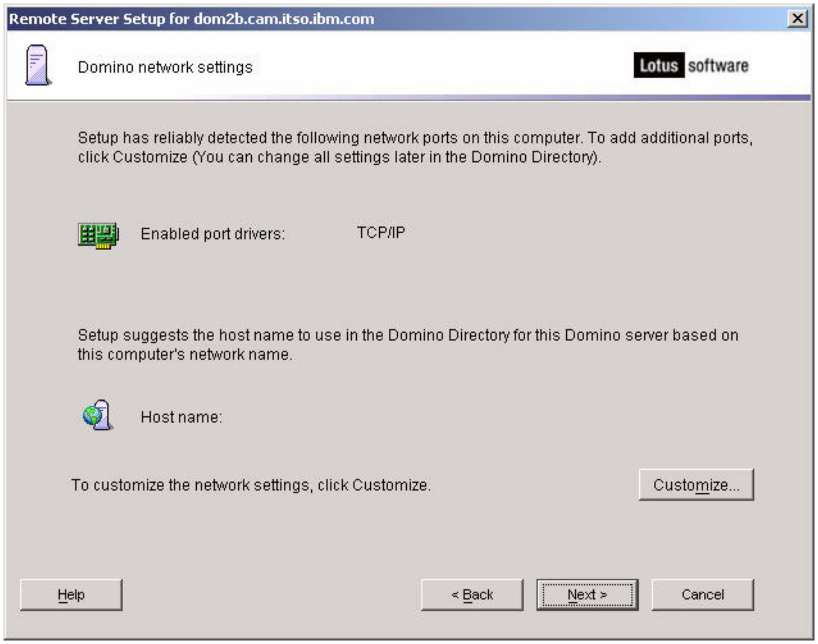
☑ Internet Mail Clients (SMTP, POP3 and IMAP services)

☑ Directory services (LDAP services)

To customize all other Domino services, click Customize.

Figure 5-97   Select Internet services

12. The window in Figure 5-98 prompts for this server's Domino network settings. Click **Customize** to configure this server's advanced network settings.



Remote Server Setup for dom2b.cam.itso.ibm.com

Domino network settings

Setup has reliably detected the following network ports on this computer. To add additional ports, click Customize (You can change all settings later in the Domino Directory).

Enabled port drivers: TCP/IP

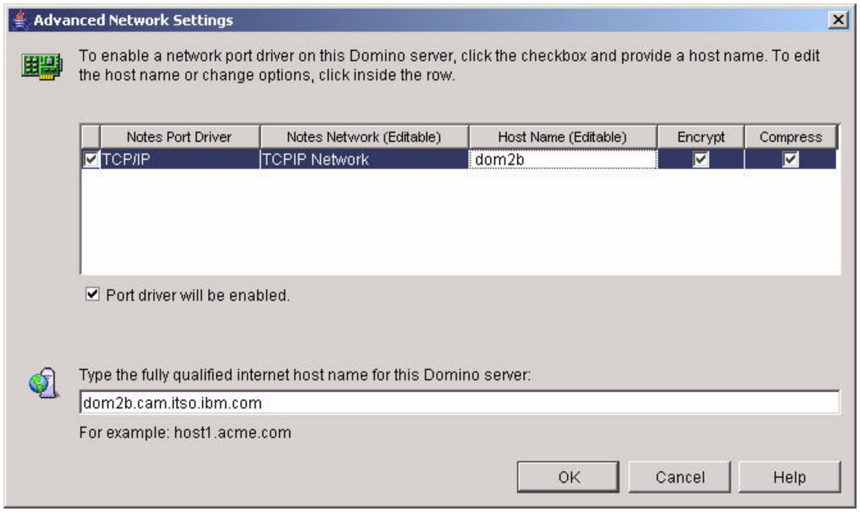
Setup suggests the host name to use in the Domino Directory for this Domino server based on this computer's network name.

Host name:

To customize the network settings, click Customize.

Figure 5-98 Prompt for Network Settings

13. Specify the network settings for this additional Domino server. Click **OK**.



Advanced Network Settings

To enable a network port driver on this Domino server, click the checkbox and provide a host name. To edit the host name or change options, click inside the row.

	Notes Port Driver	Notes Network (Editable)	Host Name (Editable)	Encrypt	Compress
☑	TCP/IP	TCPIP Network	dom2b	☑	☑

☑ Port driver will be enabled.

Type the fully qualified internet host name for this Domino server:

dom2b.cam.itso.ibm.com

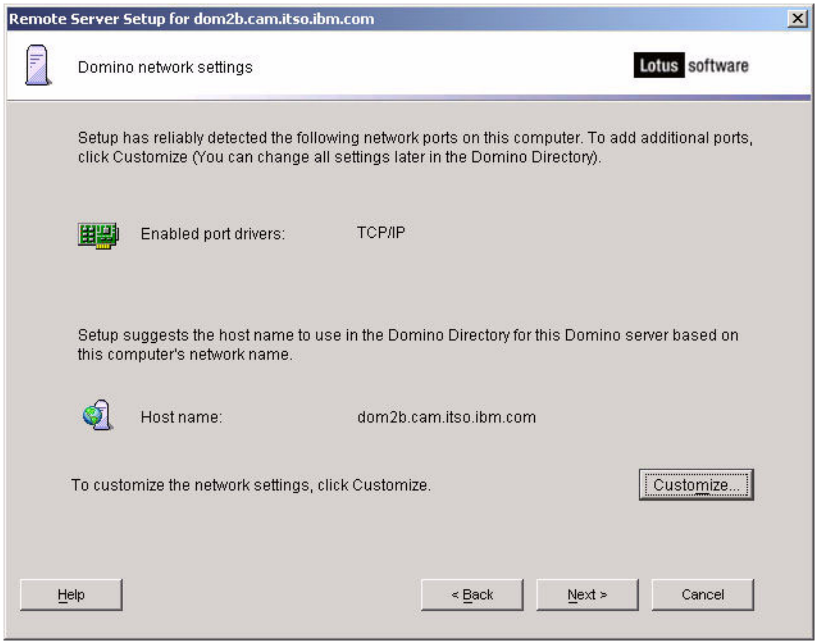
For example: host1.acme.com

Figure 5-99 Advanced Network Settings specified

14. You are returned to the initial network settings window, which is now populated with advanced network settings information, including the host name of your Domino server (Figure 5-100).

    To change any of the information displayed here, click **Customize**.

    When the information looks correct, click **Next** to continue.



Remote Server Setup for dom2b.cam.itso.ibm.com

Domino network settings

Setup has reliably detected the following network ports on this computer. To add additional ports, click Customize (You can change all settings later in the Domino Directory).

Enabled port drivers: TCP/IP

Setup suggests the host name to use in the Domino Directory for this Domino server based on this computer's network name.

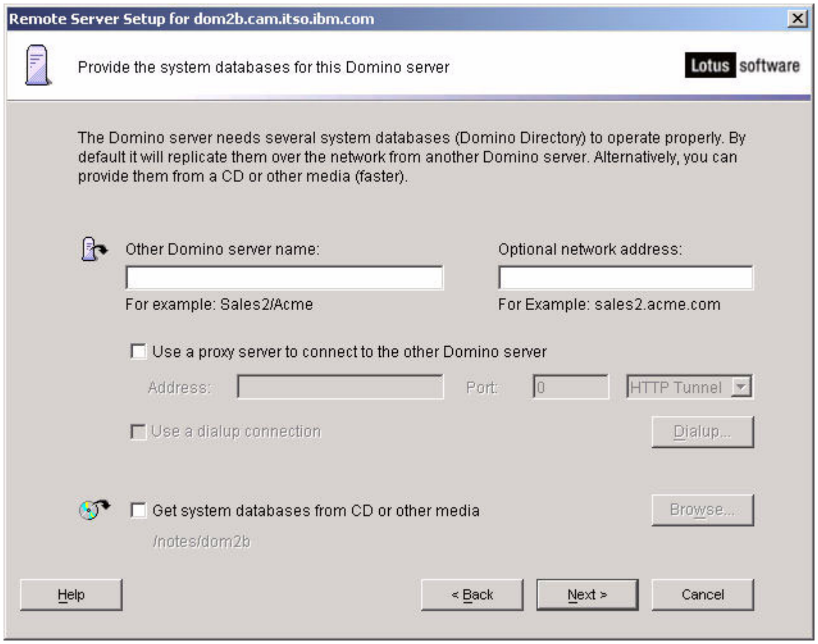
Host name: dom2b.cam.itso.ibm.com

To customize the network settings, click Customize.

Figure 5-100   Network settings completed

15. The window in Figure 5-101 prompts you for the location of the system databases for this Domino server.

When we set up the first Domino server, we created this Domino domain's Domino Directory (names.nsf) because there was no pre-existing server or Domino Directory to access. Now, for this additional server, we can specify the first Domino server as the Other Domino server name (as we did in Figure 5-102) and click **Next**.



Remote Server Setup for dom2b.cam.itso.ibm.com

Provide the system databases for this Domino server

The Domino server needs several system databases (Domino Directory) to operate properly. By default it will replicate them over the network from another Domino server. Alternatively, you can provide them from a CD or other media (faster).

Other Domino server name:
For example: Sales2/Acme

Optional network address:
For Example: sales2.acme.com

□ Use a proxy server to connect to the other Domino server

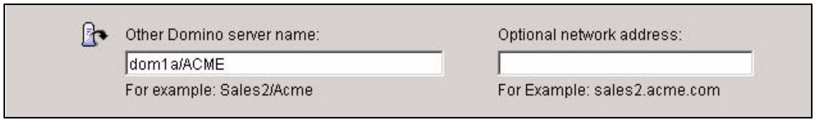
Address:
Port: 0
HTTP Tunnel

□ Use a dialup connection

□ Get system databases from CD or other media

/notes/dom2b

Figure 5-101 Prompt for (source) Domino system databases



Other Domino server name: dom1a/ACME
For example: Sales2/Acme

Optional network address:
For Example: sales2.acme.com

Figure 5-102 Other (source) Domino server specified

You also have the option of specifying your first Domino server's host name or IP address in the Optional network address field. This can be helpful if the first Domino server's name cannot be resolved as a network address. Other choices are presented here, too:

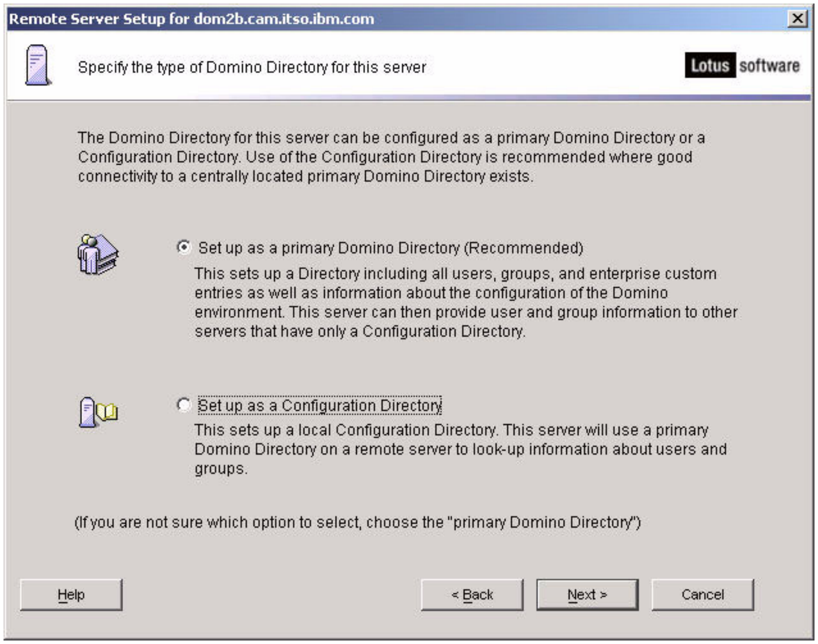
– Proxy Server connection specifics (if this is required in your environment).

– Dial-up information (if this how you will access the other Domino server).

– Copy system databases from the other Domino server onto other media and instruct the Setup utility to retrieve the required databases from this other media.

16. Select the Domino server directory type for this server (Figure 5-103) and click **Next**.

In our example, we used the recommended default.



Remote Server Setup for dom2b.cam.itso.ibm.com

Specify the type of Domino Directory for this server

The Domino Directory for this server can be configured as a primary Domino Directory or a Configuration Directory. Use of the Configuration Directory is recommended where good connectivity to a centrally located primary Domino Directory exists.

● Set up as a primary Domino Directory (Recommended)

This sets up a Directory including all users, groups, and enterprise custom entries as well as information about the configuration of the Domino environment. This server can then provide user and group information to other servers that have only a Configuration Directory.

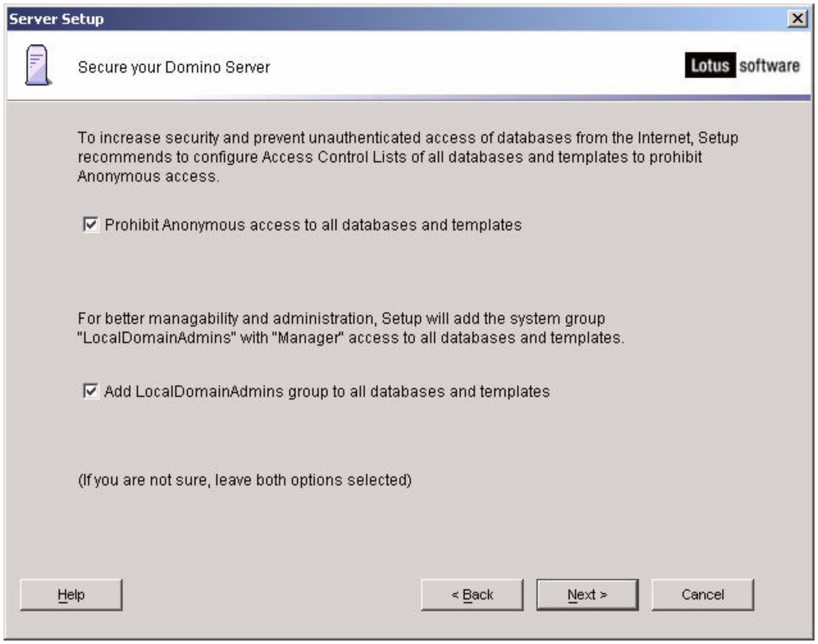
○ Set up as a Configuration Directory

This sets up a local Configuration Directory. This server will use a primary Domino Directory on a remote server to look-up information about users and groups.

(If you are not sure which option to select, choose the "primary Domino Directory")

Figure 5-103 Specify Domino Directory server type

17. Figure 5-104 shows that the setup process for this additional Domino server inherits the Security selection we specified when we set up the first Domino server. Review your security requirements for this Domino server and, when satisfied with your security settings, click **Next** to continue.



Server Setup

Secure your Domino Server

To increase security and prevent unauthenticated access of databases from the Internet, Setup recommends to configure Access Control Lists of all databases and templates to prohibit Anonymous access.

☑ Prohibit Anonymous access to all databases and templates

For better managability and administration, Setup will add the system group "LocalDomainAdmins" with "Manager" access to all databases and templates.

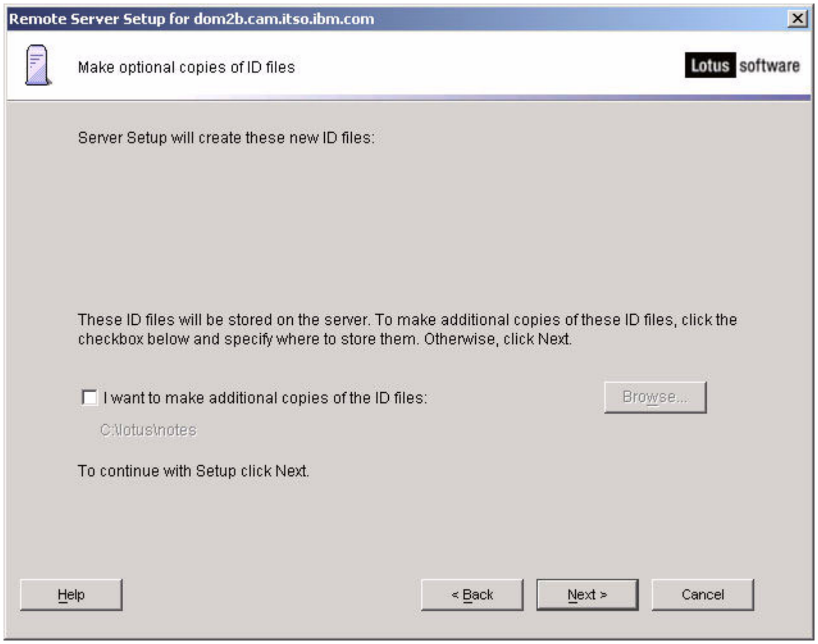
☑ Add LocalDomainAdmins group to all databases and templates

(If you are not sure, leave both options selected)

Figure 5-104 Securing the Domino server

18. The window in Figure 5-105 shows the option to make additional ID file copies. Specify the choice that pertains to your environment and click **Next**.

    In our example, we did not make optional copies of ID files.



Remote Server Setup for dom2b.cam.itso.ibm.com

Make optional copies of ID files

Server Setup will create these new ID files:

These ID files will be stored on the server. To make additional copies of these ID files, click the checkbox below and specify where to store them. Otherwise, click Next.

☐ I want to make additional copies of the ID files:

C:\lotus\notes

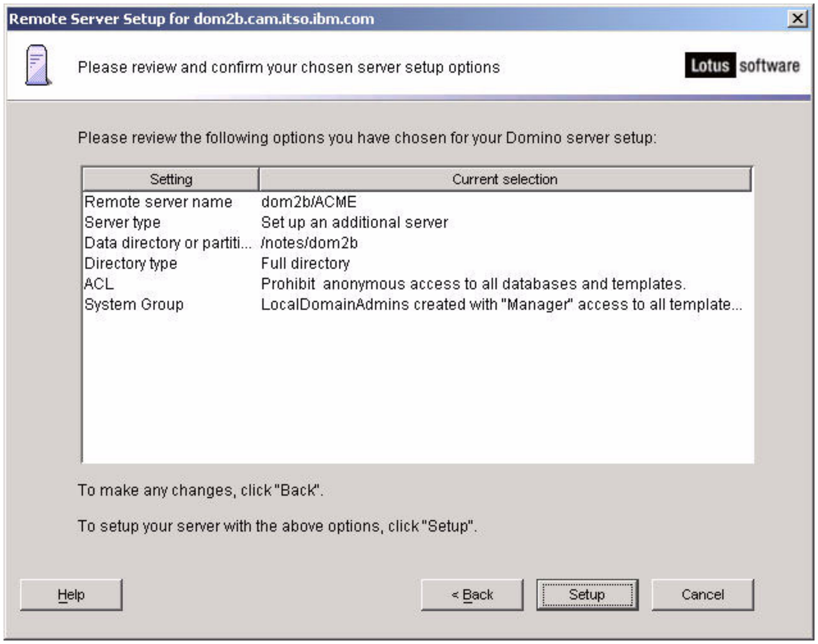
To continue with Setup click Next.

Figure 5-105 Make optional copies of ID files

19. Figure 5-106 shows the Server Setup window for reviewing and confirming your configuration settings.

    If you find errors with the settings shown in this display, click **Back** to step back through the Remote Server Setup windows until you reach the part you need to fix. Then click **Next** to advance through the Remote Server Setup windows until you return to this display to confirm your settings.

    When all appears correct, click **Setup** to launch the Domino Server Setup process.


Remote Server Setup for dom2b.cam.itso.ibm.com

Please review and confirm your chosen server setup options

Please review the following options you have chosen for your Domino server setup:

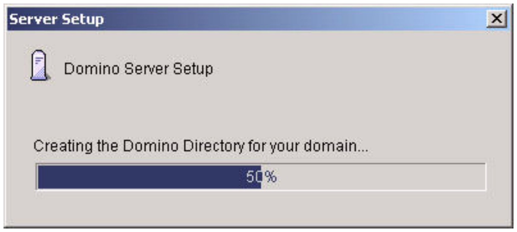
Setting	Current selection
Remote server name	dom2b/ACME
Server type	Set up an additional server
Data directory or partiti...	/notes/dom2b
Directory type	Full directory
ACL	Prohibit anonymous access to all databases and templates.
System Group	LocalDomainAdmins created with "Manager" access to all template...

To make any changes, click "Back".

To setup your server with the above options, click "Setup".

Figure 5-106 Review and confirm your Setup options

20. The Domino Server Setup progress bar appears (Figure 5-107) and should complete without stopping unless unexpected issues arise.


Server Setup

Domino Server Setup

Creating the Domino Directory for your domain...

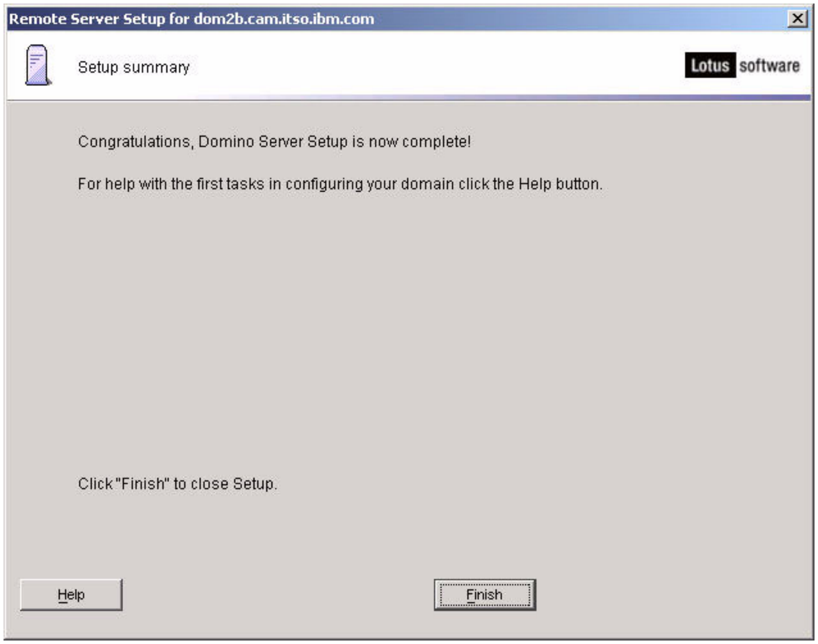
Figure 5-107 Progress bar, Setup running

Here are examples of errors that can occur, with suggestions about how to address them:

- If progress stops at *20%*: This normally happens only when setting up an additional server in the Domino domain. If this new Domino server cannot access the existing Domino server that has the Domino Directory, you can click **Back** to return to the Settings Review screen and check network and Access Control settings as a possible cause. When network access is restored, restart Remote Server Setup by clicking **Submit**.
- If progress stops at *50%*: This normally happens only when setting up an additional server in the Domino domain. If this new Domino server can access the existing Domino server that has the Domino Directory, but cannot read the Domino Directory, you can click **Back** to return to the Settings Review screen and check Access Control settings as a possible cause. When Domino Directory access is restored, restart Remote Server Setup by clicking **Submit**.
- If progress stops at *85%*: This normally happens only when setting up an additional server in the Domino domain. This can occur when there is already a Domino Directory (names.nsf) file in the Data directory of the Domino server being set up. This rogue Domino Directory might have gotten there if one was FTPed from an existing Domino server to the new server beforehand, and there might be UNIX ownership issues or other issues with this file. If this occurs, you can click **Back** to return to the Settings Review screen. Log onto your Solaris server, check for a names.nsf file already in the Data directory of the server you are setting up. If one exists, rename it for subsequent investigation. Restart Remote Server Setup by clicking **Submit**.

Tip: In case of a setup failure, you can find reasons for possible errors logged in the Domino server's notes.ini file. The notes.ini file is in the Server's Domino Data directory.

21. When Server Setup completes, you should see the window in Figure 5-108 on page 163. Click **Finish** to conclude the Remote Server Setup process.


Remote Server Setup for dom2b.cam.itso.ibm.com

Setup summary

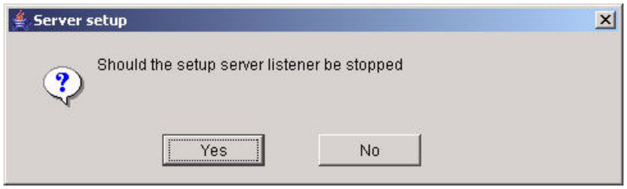
Congratulations, Domino Server Setup is now complete!

For help with the first tasks in configuring your domain click the Help button.

Click "Finish" to close Setup.

Figure 5-108 Successful completion

22. You will be asked about stopping the listener task on the server you just set up (Figure 5-109). Click **Yes** to stop the setup listener task.


Server setup

Should the setup server listener be stopped

Figure 5-109 Stop the Listener task on the remote Domino server

23. If you return to the Solaris terminal where the remote listener task was running (Figure 5-110 on page 164), you see that your Solaris user is returned to the UNIX command prompt. In our example this second Domino server is `dom2b`, owned by Solaris user `sol2b`.

    To make this Domino partition’s data directory current, type the following command as sol2b:

    ```
    cd /notes/dom2b
    ```

    To launch this Domino server, type:

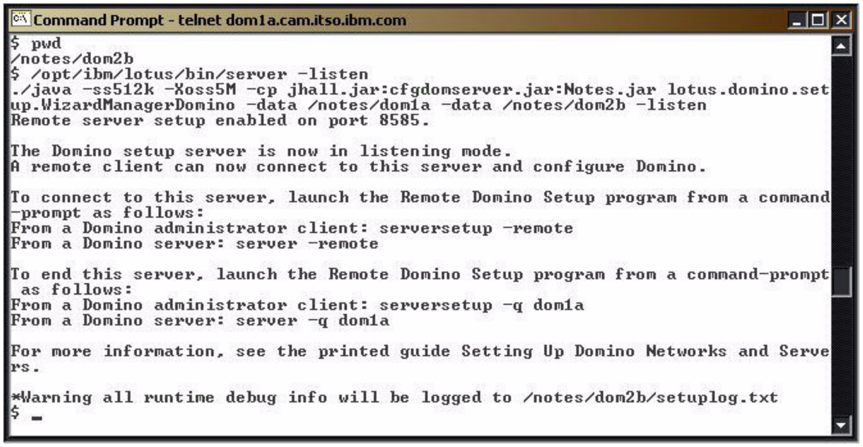
    ```
    /opt/ibm/lotus/bin/server &
    ```

This fully qualified command can be shortened to just **`server &`** when the PATH statement for the owning Solaris user (in our example, `sol2b`) already incorporates the path to the Domino program files.

You may leave this Domino server up and running.

Note: Because your *second* Domino server is starting for the first time, network and port-specific error messages might appear among the Domino Server Console information that begins to scroll by. This is common.

Such issues and errors are addressed in the Domino Administration steps in 5.4.1, “Partitioned server networking considerations” on page 181.



```
$ pwd
/notes/dom2b
$ /opt/ibm/lotus/bin/server -listen
./java -ss512k -Xoss5M -cp jhall.jar:cfgdomserver.jar:Notes.jar lotus.domino.set
up.WizardManagerDomino -data /notes/dom1a -data /notes/dom2b -listen
Remote server setup enabled on port 8585.

The Domino setup server is now in listening mode.
A remote client can now connect to this server and configure Domino.

To connect to this server, launch the Remote Domino Setup program from a command
-prompt as follows:
From a Domino administrator client: serversetup -remote
From a Domino server: server -remote

To end this server, launch the Remote Domino Setup program from a command-prompt
 as follows:
From a Domino administrator client: serversetup -q dom1a
From a Domino server: server -q dom1a

For more information, see the printed guide Setting Up Domino Networks and Serve
rs.

*Warning all runtime debug info will be logged to /notes/dom2b/setuplog.txt
$ _
```

Figure 5-110 Listener task finished on second Domino server

Important: There are many ways to start your Domino server, and we have shown you the most basic approach. We suggest that you refer to the following sections for additional information:

- 5.5, “Starting Domino and the server controller console” on page 194
- 9.4.1, “Domino Server Controller” on page 322
- 9.4.2, “Domino (Java) Console” on page 325

5.3.5 Re-running the Domino Server Setup

Occasionally the Domino Server Setup program will prompt you for information that either you do not have, or you have but is incorrect, and you might not have timely access to the correct information in order to continue setting up your Domino server. In this case:

1. Exit from the Server Setup program.
2. Get the required information.
3. Launch the Server Setup program.
4. Connect to the Domino server that is partially set up.
5. Advance to the point where you left off.
6. Enter the required information and continue through the Server Setup process to normal completion.

5.3.6 Local server setup

If you do not have the Domino Remote Server Setup utility, or you cannot remotely set up your Domino server via port 8585, you have the option of peforming the Domino Server Setup process locally.

The Local Server Setup utility runs in Solaris. This utility requires X.11 terminal access to the Solaris console of the Solaris user account that owns the Domino server partition you want to set up locally.

In anticipation of the potential need to establish an X.11 terminal session for Local Server Setup, we specified the inclusion of the corresponding Solaris system directories in the PATH for our Solaris user accounts in 4.7.3, "Configure the Solaris environment for the Solaris accounts" on page 69. We made sure to specify the necessary UNIX directories in our PATH statement, in advance, to support X.11 terminal access if required.

There are many free and commercially available X.11 terminal access solutions that you can use. In our example environment, we ran a VNC server on Solaris and used a VNC Viewer from a Windows workstation.

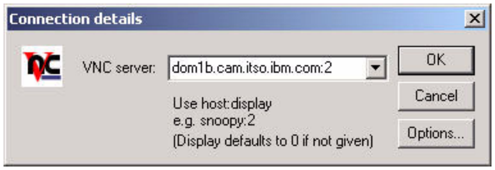
Use this procedure to perform a Local Server Setup:

1. From a Windows workstation, Telnet to the Solaris server and log on as the Solaris user account that owns the Domino partition you are about to setup Locally. In our example this will be Solaris user sol1b.
2. Change to the Domino Data directory for this Domino partition. In our example, this Domino partition is called `dom1b`, and our Data directory is `/notes/dom1b`.
3. To launch the VNC server process for this Solaris user, type this command:

   ```
   vncserver
   ```

You will be prompted for a VNC session password, which you will use when you connect from the VNC Viewer.

4. Launch the VNC Viewer on your Windows workstation by selecting **Programs** → **VNC** → **Run VNCViewer**.
5. The Connection details dialog opens (Figure 5-111). Specify the connection details (either host name or IP address) of the Domino partition to which you want to connect and click **OK**.

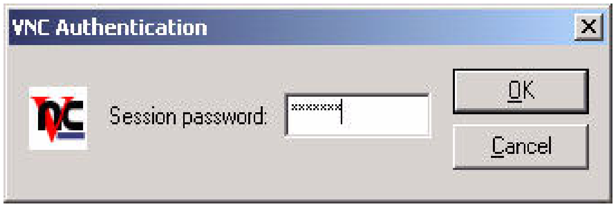


VNC server: dom1b.cam.itso.ibm.com:2

Use host:display
e.g. snoopy:2
(Display defaults to 0 if not given)

Figure 5-111 Establishing X.11 terminal access

6. When prompted for VMC authentication (Figure 5-112), enter the VNC session password you specified earlier in Solaris. Click **OK**.

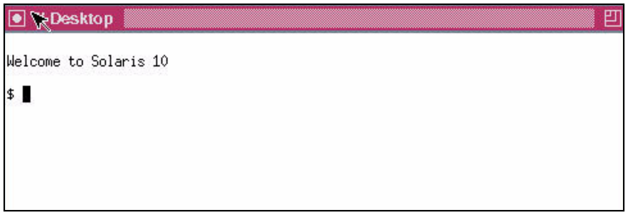


Session password: *******

Figure 5-112 Enter the X.11 session password

7. A new X.11 terminal window opens (Figure 5-113). Log on as the appropriate Solaris user account, make its corresponding Domino partition’s Data directory current, and invoke the Domino Server Setup program by typing:

```
/opt/ibm/lotus/bin/server
```



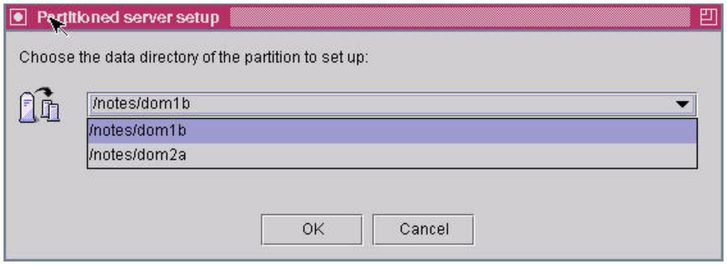
```
Welcome to Solaris 10
$ 
```

Figure 5-113 X.11 Terminal is ready

8. A *new* X.11 display appears for running the Local Domino Server Setup program (Figure 5-114 on page 167). From this point, the Local Domino

Server Setup appears nearly identical to the look and feel of the Remote Domino Server Setup that we described in 5.3.2, “Setting up the first Domino server” on page 111, and 5.3.4, “Setting up the second server” on page 147.

Choose the correct Domino partition and click **OK** to continue.


Partitioned server setup

Choose the data directory of the partition to set up:

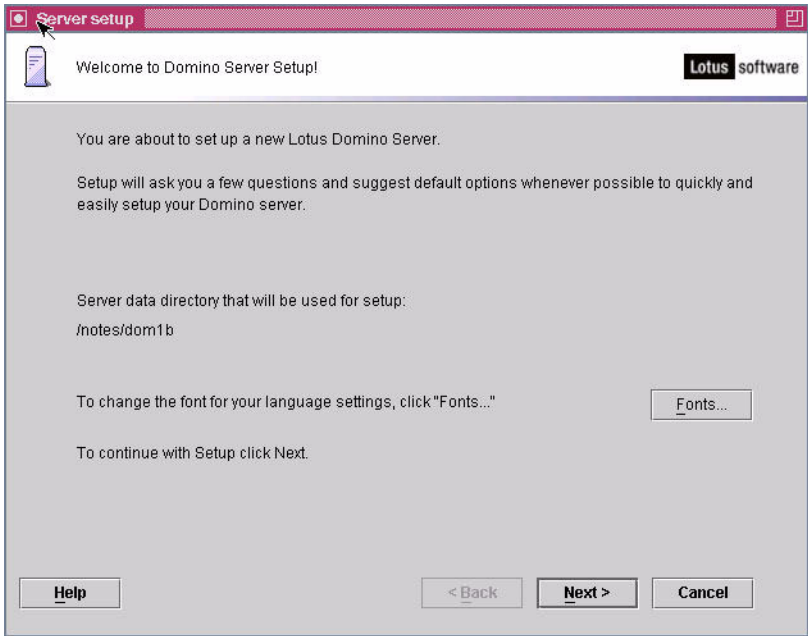
/notes/dom1b

/notes/dom1b

/notes/dom2a

Figure 5-114 Select the correct Data directory for the Domino partition

9. The Domino 7 Server Setup splash screen appears briefly, followed by the Welcome window (Figure 5-115). Confirm your Domino partition choice, change fonts if required, and click **Next** to continue.


Server setup

Welcome to Domino Server Setup!

You are about to set up a new Lotus Domino Server.

Setup will ask you a few questions and suggest default options whenever possible to quickly and easily setup your Domino server.

Server data directory that will be used for setup:

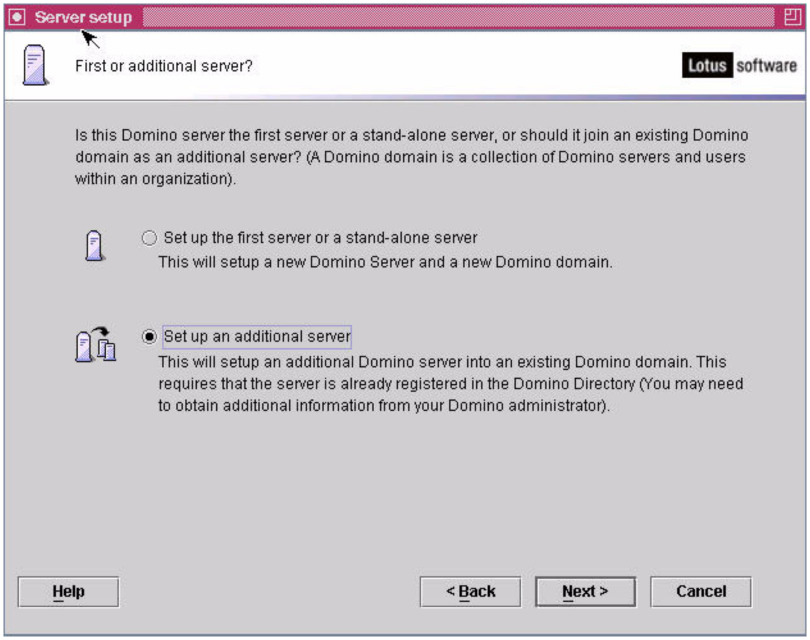
/notes/dom1b

To change the font for your language settings, click "Fonts..."

To continue with Setup click Next.

Figure 5-115 The Welcome window

10. By default, the first or standalone server option is selected (Figure 5-117 on page 169). Because this is an additional server in our example environment, the Set up an additional server option is selected. Click **Next** to continue.



First or additional server?

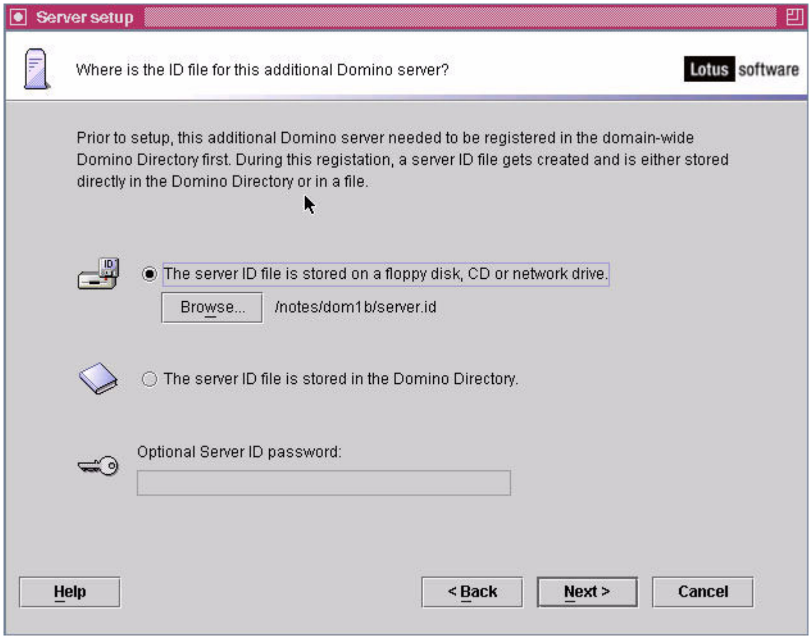
Is this Domino server the first server or a stand-alone server, or should it join an existing Domino domain as an additional server? (A Domino domain is a collection of Domino servers and users within an organization).

○ Set up the first server or a stand-alone server
This will setup a new Domino Server and a new Domino domain.

● Set up an additional server
This will setup an additional Domino server into an existing Domino domain. This requires that the server is already registered in the Domino Directory (You may need to obtain additional information from your Domino administrator).

Figure 5-116 Specifying an additional Domino server

11. Soon after we registered our additional servers, we FTPed the server ID files to their corresponding Domino Data directory locations on Solaris. Click **Browse** to locate the correct server ID (Figure 5-118 on page 170).



Where is the ID file for this additional Domino server?

Prior to setup, this additional Domino server needed to be registered in the domain-wide Domino Directory first. During this registation, a server ID file gets created and is either stored directly in the Domino Directory or in a file.

● The server ID file is stored on a floppy disk, CD or network drive.

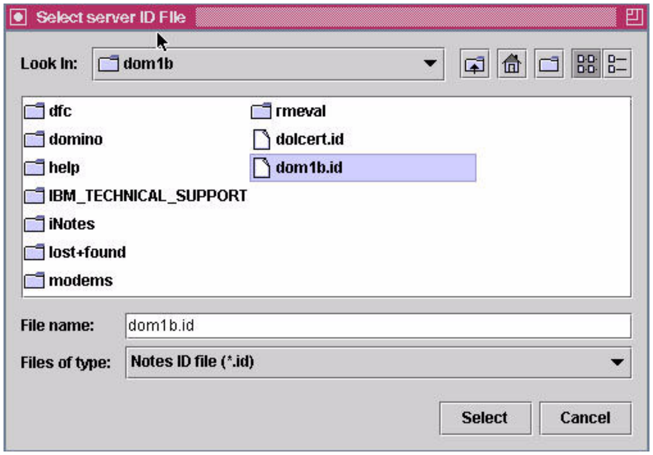
Browse... /notes/dom1b/server.id

○ The server ID file is stored in the Domino Directory.

Optional Server ID password:

Figure 5-117 Prompt for the Domino server ID file

12. Although slightly different from the corresponding display when using the Remote Server Setup utility, this is similar (Figure 5-118). Click the correct server ID file (in our example, it is **dom1b.id**), and click Select.



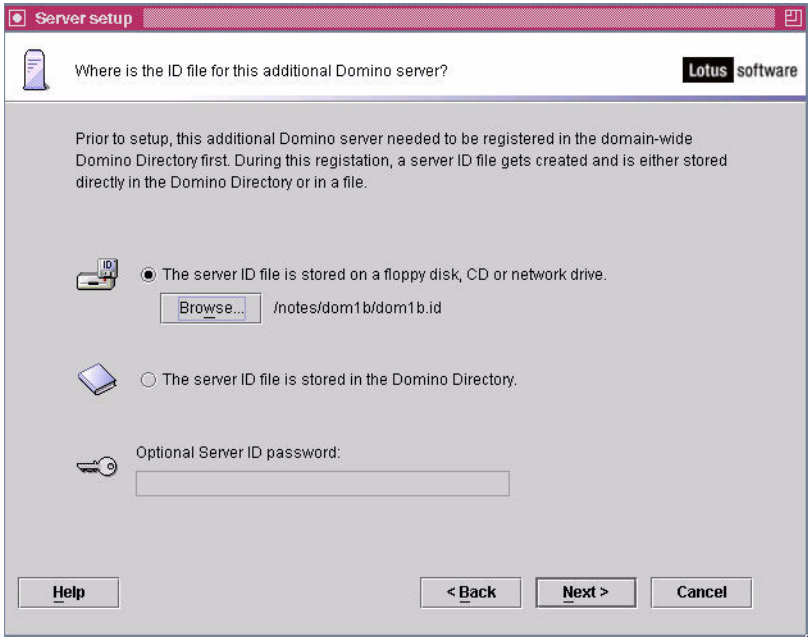
Look In: dom1b

File name: dom1b.id

Files of type: Notes ID file (*.id)

Figure 5-118 Locate and choose the server ID file

13. Review the updated display (Figure 5-119). You can click **Browse** again to change the Domino server ID file, or click **Next** to continue.



Where is the ID file for this additional Domino server?

Prior to setup, this additional Domino server needed to be registered in the domain-wide Domino Directory first. During this registation, a server ID file gets created and is either stored directly in the Domino Directory or in a file.

● The server ID file is stored on a floppy disk, CD or network drive.

/notes/dom1b/dom1b.id

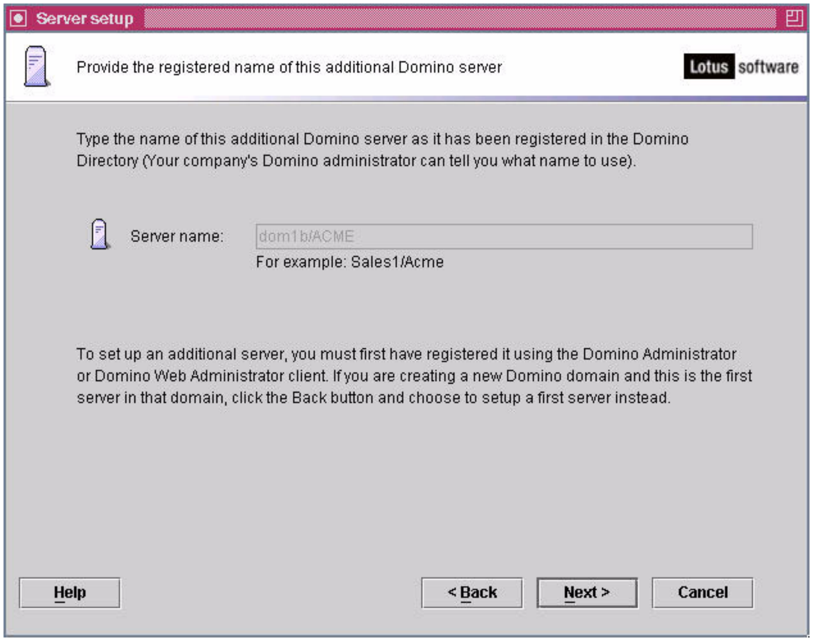
○ The server ID file is stored in the Domino Directory.

Optional Server ID password:

Figure 5-119 The correct server ID is specified

14. The Setup program extracts the server name from the ID file we just selected (Figure 5-120). The server name *cannot* be changed manually.

    If you detect a problem, click **Back** to correct the error; otherwise, click **Next**.



Server setup

Provide the registered name of this additional Domino server

Type the name of this additional Domino server as it has been registered in the Domino Directory (Your company's Domino administrator can tell you what name to use).

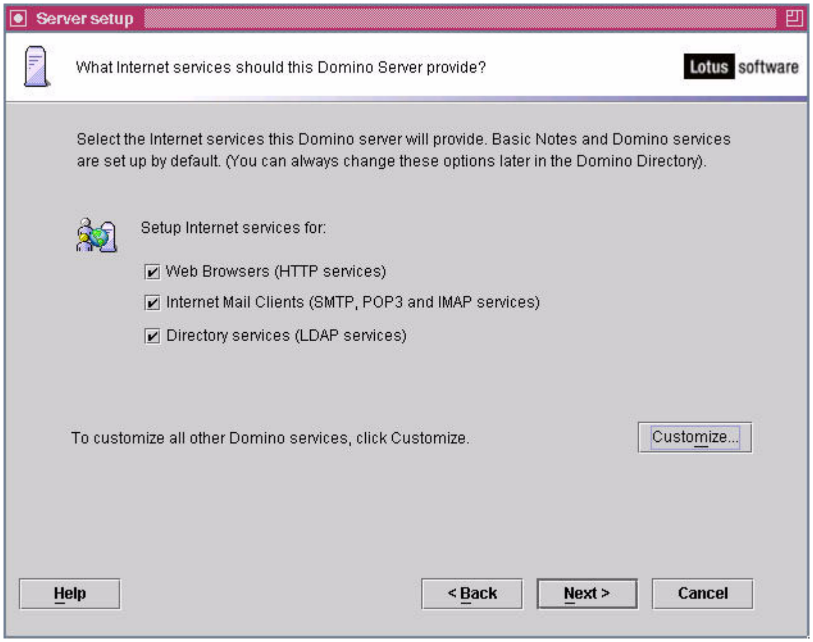
Server name: dom1b/ACME

For example: Sales1/Acme

To set up an additional server, you must first have registered it using the Domino Administrator or Domino Web Administrator client. If you are creating a new Domino domain and this is the first server in that domain, click the Back button and choose to setup a first server instead.

Figure 5-120 The registered Domino server name

15. Select the required Internet services you want to run on this Domino Server (Figure 5-121). Click **Customize** to review the available Domino Server tasks and refine your selections if necessary, or click **Next** to continue.



Server setup

What Internet services should this Domino Server provide?

Select the Internet services this Domino server will provide. Basic Notes and Domino services are set up by default. (You can always change these options later in the Domino Directory).

Setup Internet services for:

☑ Web Browsers (HTTP services)

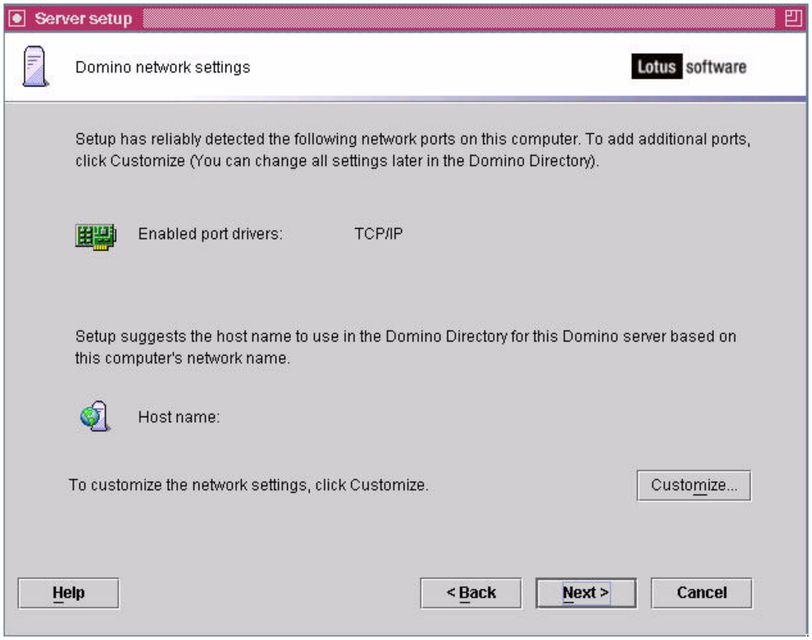
☑ Internet Mail Clients (SMTP, POP3 and IMAP services)

☑ Directory services (LDAP services)

To customize all other Domino services, click Customize.

Figure 5-121 Internet services and server tasks

16. Figure 5-122 shows the network settings. Click **Customize** to change the advanced network settings.



Server setup

Domino network settings

Setup has reliably detected the following network ports on this computer. To add additional ports, click Customize (You can change all settings later in the Domino Directory).

Enabled port drivers: TCP/IP

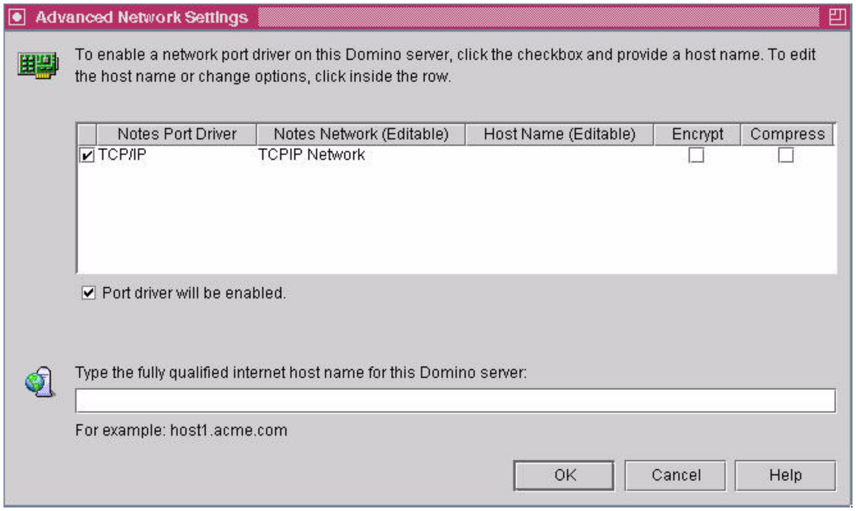
Setup suggests the host name to use in the Domino Directory for this Domino server based on this computer's network name.

Host name:

To customize the network settings, click Customize.

Figure 5-122 Review network settings

17. Enter the required network configuration settings (Figure 5-123). Click **OK** to accept these settings and return to the initial Network Settings window.



Advanced Network Settings

To enable a network port driver on this Domino server, click the checkbox and provide a host name. To edit the host name or change options, click inside the row.

Notes Port Driver	Notes Network (Editable)	Host Name (Editable)	Encrypt	Compress
☑ TCP/IP	TCPIP Network		□	□

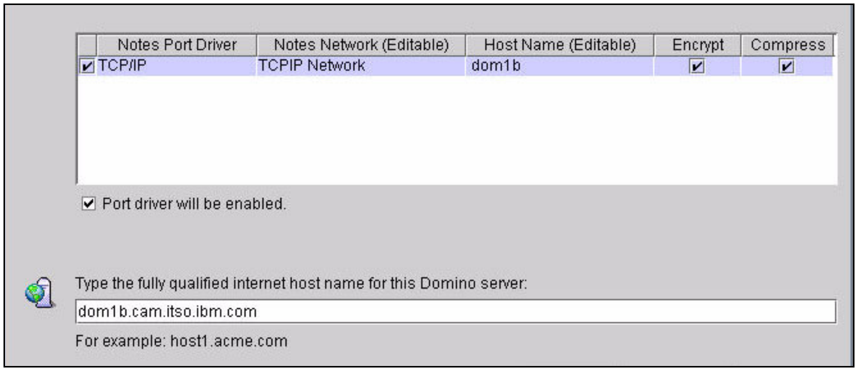
☑ Port driver will be enabled.

Type the fully qualified internet host name for this Domino server:

For example: host1.acme.com

Figure 5-123   Advanced Network Settings

Figure 5-124 shows our Advanced Network Settings.



Notes Port Driver	Notes Network (Editable)	Host Name (Editable)	Encrypt	Compress
☑ TCP/IP	TCPIP Network	dom1b	☑	☑

☑ Port driver will be enabled.

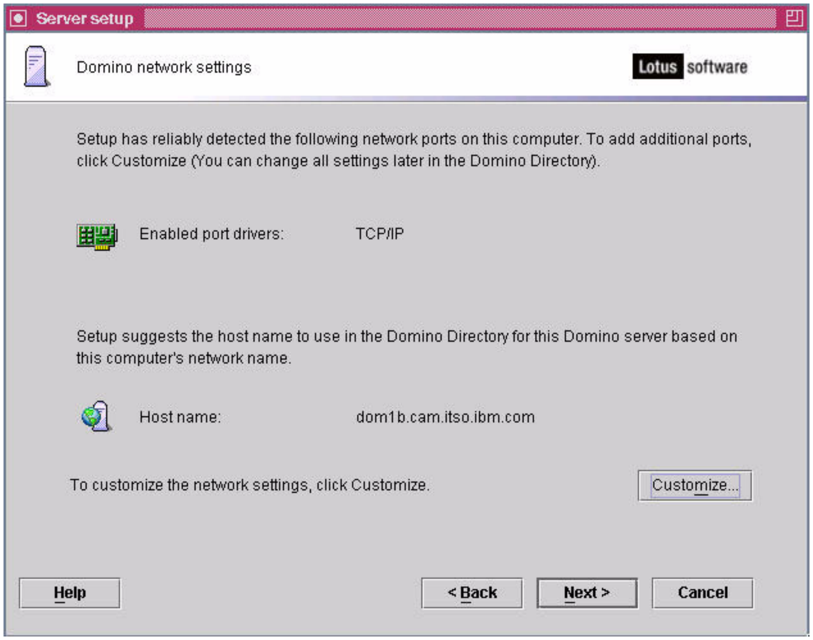
Type the fully qualified internet host name for this Domino server:

dom1b.cam.itso.ibm.com

For example: host1.acme.com

Figure 5-124   Advanced Network Settings specified

18. Your network settings now appear (Figure 5-126 on page 176). If you detect errors here, click **Customize** to correct them. Otherwise, click **Next** to continue.



Server setup

Domino network settings

Setup has reliably detected the following network ports on this computer. To add additional ports, click Customize (You can change all settings later in the Domino Directory).

Enabled port drivers: TCP/IP

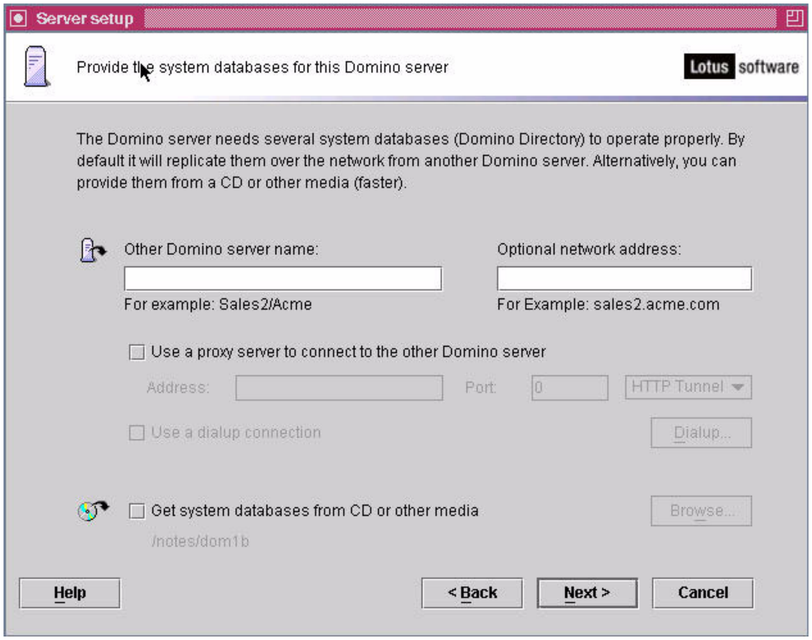
Setup suggests the host name to use in the Domino Directory for this Domino server based on this computer's network name.

Host name: dom1b.cam.itso.ibm.com

To customize the network settings, click Customize.

Figure 5-125 Network Settings completed

19. Enter the name of your other (source) Domino server and click **Next**.



Server setup

Provide the system databases for this Domino server

The Domino server needs several system databases (Domino Directory) to operate properly. By default it will replicate them over the network from another Domino server. Alternatively, you can provide them from a CD or other media (faster).

Other Domino server name:

For example: Sales2/Acme

Optional network address:

For Example: sales2.acme.com

□ Use a proxy server to connect to the other Domino server

Address: Port: 0 HTTP Tunnel

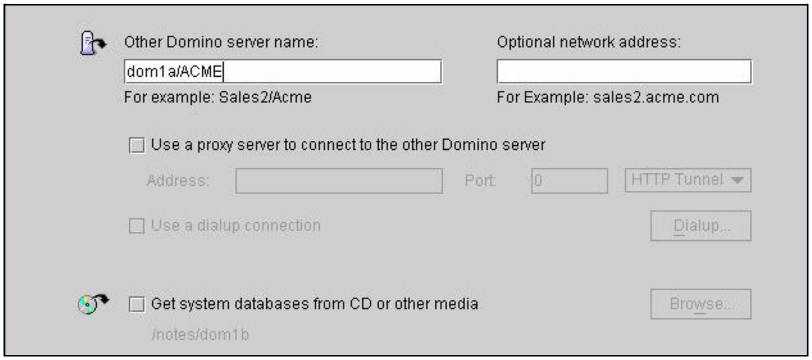
□ Use a dialup connection

□ Get system databases from CD or other media

/notes/dom1b

Figure 5-126 Prompt for other (source) Domino server

Figure 5-128 on page 177 shows the entries for our example.



Other Domino server name: dom1a/ACME

For example: Sales2/Acme

Optional network address:

For Example: sales2.acme.com

□ Use a proxy server to connect to the other Domino server

Address: Port: 0 HTTP Tunnel

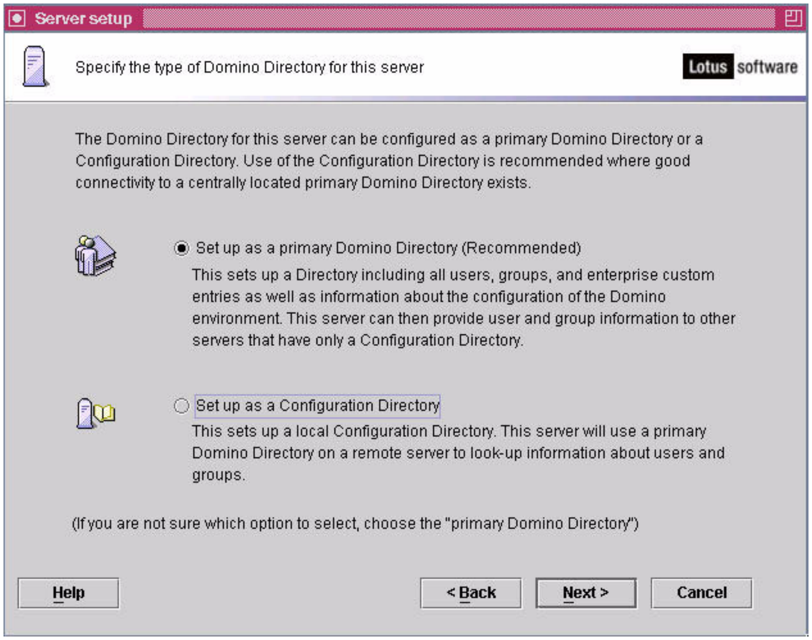
□ Use a dialup connection

□ Get system databases from CD or other media

/notes/dom1b

Figure 5-127 Other (source) Domino server specified

20. In our example, all of our servers use the default recommendation to be Domino Directory servers (Figure 5-128). Make the correct choice for your environment and click **Next**.



Specify the type of Domino Directory for this server

The Domino Directory for this server can be configured as a primary Domino Directory or a Configuration Directory. Use of the Configuration Directory is recommended where good connectivity to a centrally located primary Domino Directory exists.

● Set up as a primary Domino Directory (Recommended)

This sets up a Directory including all users, groups, and enterprise custom entries as well as information about the configuration of the Domino environment. This server can then provide user and group information to other servers that have only a Configuration Directory.

○ Set up as a Configuration Directory

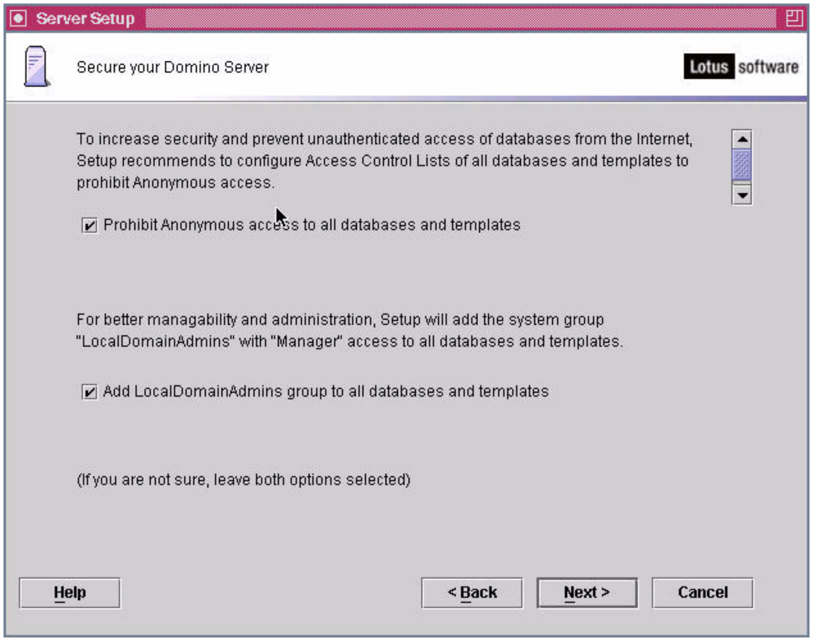
This sets up a local Configuration Directory. This server will use a primary Domino Directory on a remote server to look-up information about users and groups.

(If you are not sure which option to select, choose the "primary Domino Directory")

Figure 5-128 Specify the Domino Directory type for this server

21. The choices shown in Figure 5-129 reflect the choices we specified when we set up our First Domino server. Make the correct choice for your environment click **Next**.

    In our example, we applied these same settings to all of our Domino servers.



Server Setup

Secure your Domino Server

To increase security and prevent unauthenticated access of databases from the Internet, Setup recommends to configure Access Control Lists of all databases and templates to prohibit Anonymous access.

☑ Prohibit Anonymous access to all databases and templates

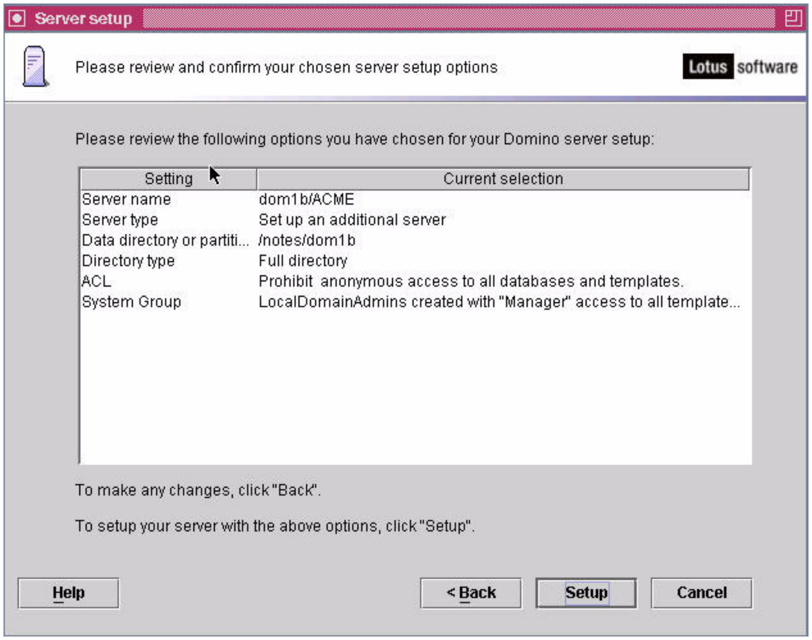
For better managability and administration, Setup will add the system group "LocalDomainAdmins" with "Manager" access to all databases and templates.

☑ Add LocalDomainAdmins group to all databases and templates

(If you are not sure, leave both options selected)

Figure 5-129 Securing your Domino server

22. Check your Server Setup configuration choices (Figure 5-131). If you detect errors, go back and fix them now. If the information looks correct, click **Setup** to continue.



Server setup

Please review and confirm your chosen server setup options

Please review the following options you have chosen for your Domino server setup:

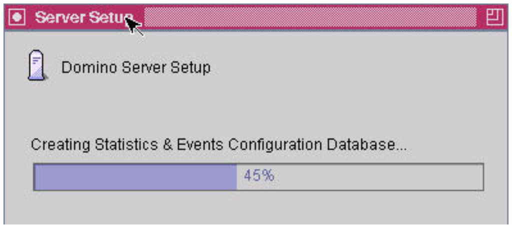
Setting	Current selection
Server name	dom1b/ACME
Server type	Set up an additional server
Data directory or partiti...	/notes/dom1b
Directory type	Full directory
ACL	Prohibit anonymous access to all databases and templates.
System Group	LocalDomainAdmins created with "Manager" access to all template...

To make any changes, click "Back".

To setup your server with the above options, click "Setup".

Figure 5-130 Review and confirm setup options

If there are no problems, the progress bar will soon reach 100% and disappear.



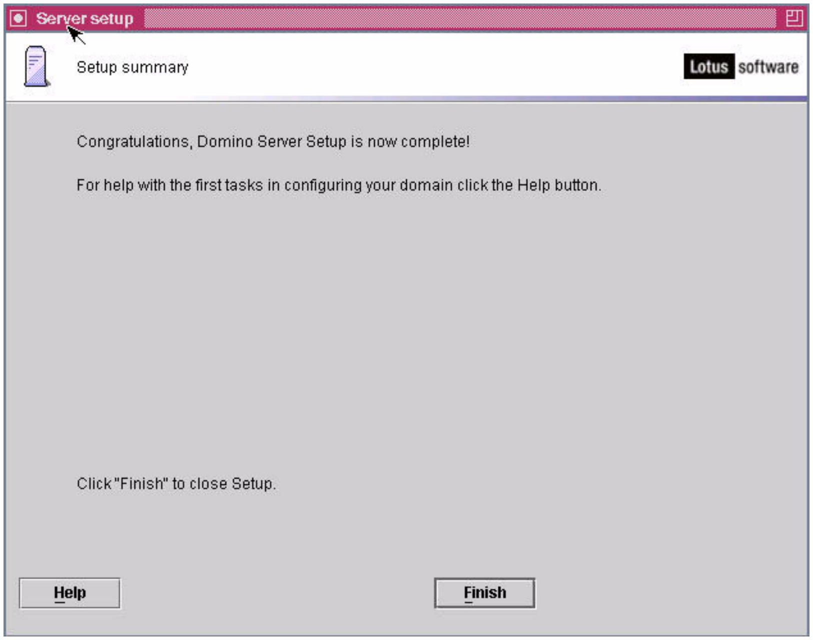
Server Setup

Domino Server Setup

Creating Statistics & Events Configuration Database...

Figure 5-131 Progress bar, Setup running

23. The summary window appears (Figure 5-132). Click Finish to end the Local Server Setup program.



Setup summary

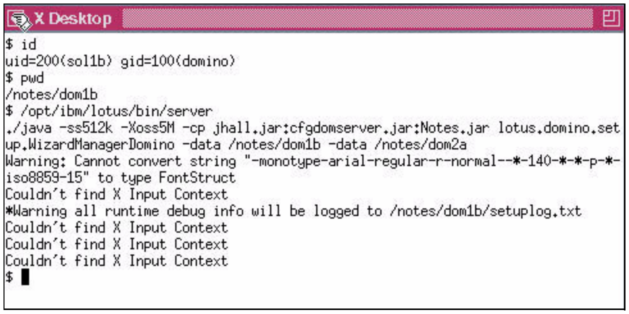
Congratulations, Domino Server Setup is now complete!

For help with the first tasks in configuring your domain click the Help button.

Click "Finish" to close Setup.

Figure 5-132 Successful completion

You can now shut down the X.11 terminal connection, because Local Domino Server Setup is completed, and start this Domino server.



```
$ id
uid=200(sol1b) gid=100(domino)
$ pwd
/notes/dom1b
$ /opt/ibm/lotus/bin/server
./java -ss512k -Xoss5M -cp jhall.jar:cfgdomserver.jar:Notes.jar lotus.domino.set
up.WizardManagerDomino -data /notes/dom1b -data /notes/dom2a
Warning: Cannot convert string "-monotype-arial-regular-r-normal--*-140-*-*-p-*-
iso8859-15" to type FontStruct
Couldn't find X Input Context
*Warning all runtime debug info will be logged to /notes/dom1b/setuplog.txt
Couldn't find X Input Context
Couldn't find X Input Context
Couldn't find X Input Context
$ █
```

Figure 5-133 X.11 Terminal stopped

Important: Because your third Domino server is starting for the first time, network and port-specific error messages might appear among the Domino Server Console information that begins to scroll by. This is common.

We address such issues and errors in the Domino Administration steps in 5.4.1, "Partitioned server networking considerations" on page 181.

Note: There are many ways to start your Domino server; we have shown you the most basic approach. Refer to these sections for additional information:

- 5.5, "Starting Domino and the server controller console" on page 194
- 9.4.1, "Domino Server Controller" on page 322
- 9.4.2, "Domino (Java) Console" on page 325

5.4 Last configuration steps

At this point you have accomplished the following:

- Set up and configured Solaris on your Sun server.
- Installed the Domino software.
- Set up your Domino partitions.

In this section we discuss the additional, manual steps that might be required to finish setting up your Domino partitions.

5.4.1 Partitioned server networking considerations

You might run across the following issues as you complete partition setup.

Port contention (or "My Domino server won't share!")

When you have multiple Domino partitions installed on a single physical server, these partitions might not cooperate with each other when it comes to binding ports and Internet services to an IP address.

For example, let's suppose you have a Solaris 10 server with two newly installed and configured Domino partitions.

After you start one of the two Domino server partitions, if you watch the server console display while the server launches, or examine the Domino server log file database (log.nsf) after the fact, you will likely observe that:

> *Everything looks fine!*

Next, and with great anticipation, you start the other Domino server partition on the same physical server. If you watch the server console display while the server launches, or you examine the Domino server log file database (log.nsf) after the fact, you will likely find that:

- This partitioned server cannot bind to port 80.
- This partitioned server cannot bind to port 25.
- Other potential network issues might exist.

This is because Domino assumes that it can bind to all available network ports on the physical host server, and this means that:

- The first Domino server partition to launch on the physical server binds to all ports it expects to use.
- The next, and subsequent, Domino server partitions to launch on the same physical server cannot bind to the required ports because those ports have already been taken by the first server.
- This means that the first Domino partition to start wins!

Because of this, Domino provides a method for the Domino Administrator to bind Transmission Control Protocol (TCP) ports and Internet services to specific IP addresses that correspond to a specific Domino server partition.

Default port for NRPC

By default, all NRPC connections use TCP port 1352. Because the Internet Assigned Number Authority (IANA) assigned this port number to Lotus Domino, non-Domino applications do not usually compete for this port.

Do not change the default NRPC port unless:

- You can use a NAT or PAT firewall system to redirect a remote system's connection attempt.
- You are using Domino port mapping.
- You create a connection document that contains the reassigned port number.

To change the default NRPC port number, use the notes.ini setting:

```
TCPIPportname_TCPIPAddress=
```

Enter an available value on the system that runs the Domino server. TCP ports with numbers less than 5000 are reserved for application vendors. You may use any number from 1024 through 5000, but be sure not to install a new application that requires that number.

Note: When setting the notes.ini variables for port mapping, do not include a zone in a port mapped address. The zone is only valid locally.

Default ports for Internet services

You might occasionally need to change the number of the TCP or SSL port assigned to an Internet service. Lotus Domino uses the default ports in Table 5-1 for Internet services.

Table 5-1 Default ports for Internet services

Service	Default TCP port	Default SSL port
POP3	110	995
IMAP	143	993
LDAP	389	636
SMTP Inbound	25	465
SMTP Outbound	25	465
HTTP	80	443
IIOP	63148	63149
Server Controller	N/A	2050

Binding a port to an IP address

By default, all TCP/IP-based services on a Domino server listen for network connections on all NICs and on all configured IP addresses on the server. If you have enabled more than one Notes network port for TCP/IP (TCP port for NRPC) on either a single Domino server or a Domino partitioned server, you must associate the NRPC ports and IP addresses by binding each port to an address:

1. For each IP address, make sure that you have added a Notes port for TCP/IP and that each port has a unique name.
2. In the notes.ini file, confirm that these lines appear for each port that you added (`TCPIPportname` is the port name you defined):

   ```
   Ports=TCPIPportname
   TCPIPportname=TCP, 0, 15, 0
   ```

3. For each port that you want to bind to an IP address, add this line to the notes.ini file (`IPaddress` is the IP address of the specific NIC):

   ```
   TCPIPportname_TCPIPAddress=0,IPaddress
   ```

For example:

```
TCPIP_TCPIPAddress=0,130.123.45.1
```

For IPv6, enclose the address in square brackets, as it contains colons. For example:

```
TCPIP_TCPIPAddress=0,[fe80::290:27ff:fe43:16ac]
```

Tip: To help you remember the function of each port, add the default TCP port number for NRPC to the end of the line you entered in Step 3, as follows:

```
:1352
```

Important: Do not change the assigned TCP port number unless you have a way to redirect the inbound connection with Domino port mapping or a firewall that has port address translation (PAT).

Binding an Internet service to an IP address

If the Domino server has multiple Notes network ports for TCP/IP and the server is also hosting the SMTP, POP3, IMAP, LDAP, or Internet Cluster Manager (ICM) service, you must specify the port that you want the service to use in the notes.ini file. If you do not specify a port for an Internet service, by default the service will use the port listed first in the Ports setting in the notes.ini file. You can specify the same port for multiple Internet services.

Important: For the Domino Web server (HTTP service), use the Server document to bind HTTP to a host name IP address.

Go to the server document for the Domino Web Server, click the **Internet Protocols** tab, then click the **HTTP** sub-tab. (See Figure 5-134 on page 185.)

The following example shows the lines (in bold) to add to the Ports section of the notes.ini file to bind two NRPC ports to their IP addresses and to specify the second NRPC port for the SMTP service:

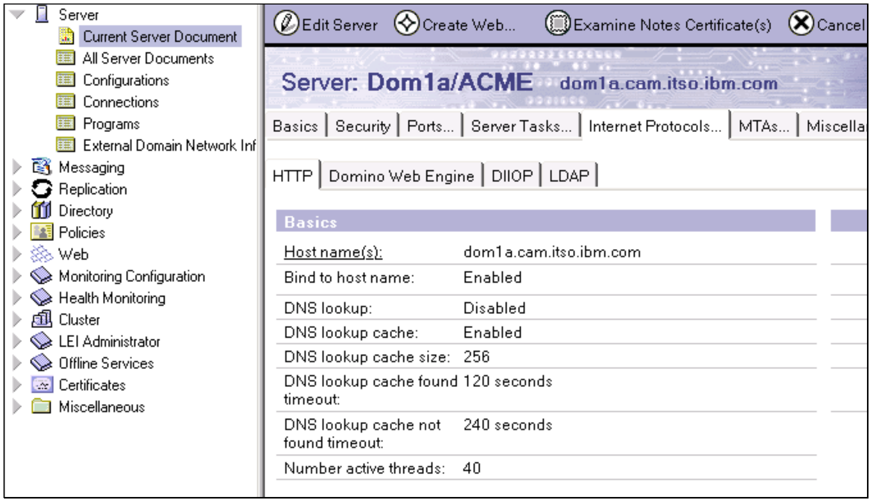
```
Ports=TCPIP, TCP1P2
TCPIP=TCP, 0, 15, 0
TCPIP_TCPIPAddress=0,10.33.52.1
TCPIP2=TCP, 0, 15, 0
TCPIP2_TCPIPAddress=0, 209.98.76.10
SMPTNotesPort=TCPIP2
```

Note: Domino adds the lines that are not bold when you use either the Domino Server Setup program or the Domino Administrator's Setup Ports dialog to enable a port.

To bind the HTTP service (Figure 5-134):

a. On the Internet Protocols - **HTTP** tab of the Server document, enter one or more IP addresses or FQDNs for the server in the Host name(s) field.

b. Select **Enabled** in the Bind to host name field.



Host name(s):	dom1a.cam.itso.ibm.com
Bind to host name:	Enabled
DNS lookup:	Disabled
DNS lookup cache:	Enabled
DNS lookup cache size:	256
DNS lookup cache found timeout:	120 seconds
DNS lookup cache not found timeout:	240 seconds
Number active threads:	40

Figure 5-134 Admin client - Bind HTTP port to host name of Domino partition

Note: If the server is a partitioned server and has Web sites configured with separate IP addresses, or has virtual servers (Domino 5) configured for one or more partitions, enter the partition's IP address, and each Web site or virtual server's IP address in the Host name(s) field, separated by semicolons. Alternatively, you can use FQDNs in this field. Do not list additional Web sites and virtual hosts that have IP addresses that are already listed in this field.

Binding the Domino Server Controller port

If you are using the Domino Server Controller / Java Console and you have multiple Domino partitions, you must bind the Server Controller port 2050 to the partition's TCP/IP address; as with the HTTP procedure above, this is also done via the Domino Administrator client.

To bind the server controller port:

a. Start the Domino Administrator client.

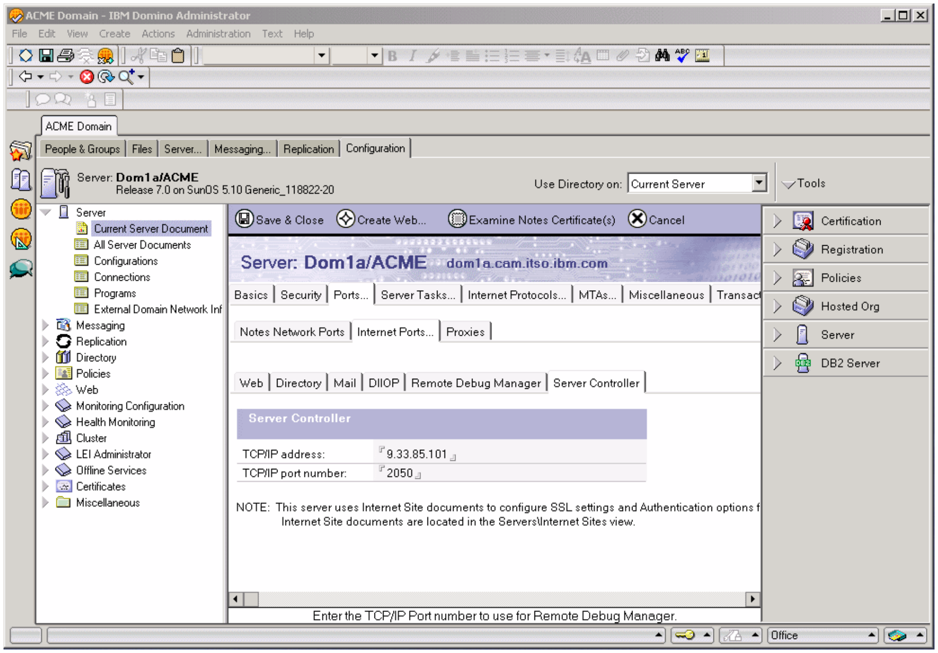
b. Click the **Configuration** tab → **Server** → **Server Document for the server you are modifying** → **Internet Ports** tab → **Server Controller** tab.

c. Click **Edit Server**.

d. Enter the IP address in the IP address field.

e. Click **Save and Close**.

See Figure 5-135 for an example.


ACME Domain - IBM Domino Administrator
File Edit View Create Actions Administration Text Help
ACME Domain
People & Groups | Files | Server... | Messaging... | Replication | Configuration
Server: Dom1a/ACME
Release 7.0 on SunOS 5.10 Generic_118822-20
Use Directory on: Current Server
Tools
Server
Current Server Document
All Server Documents
Configurations
Connections
Programs
External Domain Network Inf
Messaging
Replication
Directory
Policies
Web
Monitoring Configuration
Health Monitoring
Cluster
LEI Administrator
Offline Services
Certificates
Miscellaneous
Save & Close
Create Web...
Examine Notes Certificate(s)
Cancel
Server: Dom1a/ACME dom1a.cam.itso.ibm.com
Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transact
Notes Network Ports | Internet Ports... | Proxies
Web | Directory | Mail | DIIOP | Remote Debug Manager | Server Controller
Server Controller
Certification
Registration
Policies
Hosted Org
Server
DB2 Server
Office

TCP/IP address: 9.33.85.101

TCP/IP port number: 2050

NOTE: This server uses Internet Site documents to configure SSL settings and Authentication options f
Internet Site documents are located in the Servers\Internet Sites view.

Enter the TCP/IP Port number to use for Remote Debug Manager.

Figure 5-135 Binding Server Controller port

What we did in our Redbook Lab environment

In our lab environment, each of our servers has a Public External IP address for external network traffic *and* a Private Internal IP address for internal Cluster network traffic. For our Domino server partition called dom1a, our external IP address was 9.33.85.101, our internal IP address was 192.168.1.101, our TCP port was called TCPIP, and out Cluster port was called CLUSTER.

Based on this we entered the following information into dom1a's notes.ini file to implement our NRPC port binding:

```
Ports=CLUSTER,TCPIP
TCPIP=TCP, 0, 15, 0,,32800
TCPIP_TCPIPADDRESS=0,9.33.85.101:1352
CLUSTER=TCP,0,15,0,,12288,
CLUSTER_TCPIPADDRESS=0,192.168.1.101:1352
Server_Default_Cluster_Port=CLUSTER
```

The display in Figure 5-134 on page 185 shows where we bound HTTP port 80 to our Domino server partition's SMTP host name: `dom1a.cam.itso.ibm.com`.

Important: For additional information about configuring Domino networking for partitioned servers, refer to the following sources:

- 8.3, "Configuring network resources for partitioning" on page 255
- Domino Administrator Help sections. Look for:
  - Binding an NRPC port to an IP address
  - Binding an Internet service to an IP address
  - Changing an TCP or SSL port number
  - TCP/IPportname_PortMappingNN
  - TCP/IPportname_TCPIPAddress
  - Advanced Domino TCP/IP configurations

5.4.2 Installing start/stop scripts

When you boot a Solaris system, use the **`init`** command to change run levels, or shut down the Solaris system. Solaris 10 uses two methods to automate the starting and stopping of Solaris services and applications.

1. Traditional Run Control (RC) scripts, which we describe in this section
2. The Service Management Facility (SMF), which we describe in 5.4.3, "Running servers via the Service Management Facility (SMF)" on page 192

Explanation of Run Control (RC) scripts

One automated method to start a service on Solaris is to use Run Control (RC) startup scripts. On Solaris, the RC scripts are organized into several subdirectories. The /etc/init.d directory contains the Run Control scripts. These scripts are written to accept a **`start`** argument to start a service and a **`stop`** argument to stop a service.

In /etc, there are also Run Control directories named rc*x*.d where the *x* is a run level. For example, rc3.d represents Run Level 3, and rcS.d is for Single User. To automatically run a script for a particular run level, links to the script are created in these rcx.d directories.

Link names that begin with S cause the script to be called with the start argument. Link names that begin with K are called with the stop argument. After the S or K is a two-digit number indicating the order in which the scripts will be executed. There is no harm in applying the same sequence number to multiple scripts. In this case, the order of execution is deterministic but unspecified. When entering a run level, the K scripts are executed first, followed by the S scripts.

This is the general procedure to use RC scripts to automate a service:

1. Create a script that accepts the start and stop arguments and has the commands required to start and stop the service.
2. Place the script in /etc/init.d and make it “executable” by setting the *x* permission.
3. Create a link that starts with S in the rc directory for the run level you wish to start the service. Often this is done in /etc/rc3.d for services such as Domino.
4. Create links that start with K in the run-level directories where you want to stop your service. For services such as Domino, this is usually /etc/rc0.d and /etc/rc1.d.

For more information about run levels and Run Control scripts, see the man pages for init and init.d.

Our example RC scripts

The provided Run Control (RC) script in this book is an example of how you can automate the start and stop procedure of your Domino servers during startup, shutdown, and run level changes of your Solaris system.

We also include an installation script that will assist you if you decide to use the examples included in the book.

The complete example install and start/stop scripts can be found in Appendix C, “Domino Server starting and shutting-down scripts” on page 527, and can also be downloaded from the ITSO Web site. (See Appendix H, “Additional material” on page 571.)

The example script that we provide has the following features:

- Support for multiple Domino partitions.
- Allows for different versions of Domino; the program directories for each Domino partition are specified separately.
- Creates a console input file that accepts Domino Console commands.
- Creates a console output file that will store Domino Console output
- Can be run manually to start or stop for all or just one of your Domino partitions.
- Cleans up after an abnormal Domino termination or hang by running **`nsd -kill`**.
- Has an install script that simplifies installing the example script.

Note: Our example script assumes that the Solaris accounts are set up to use the Bourne shell (/bin/sh). To use another shell, modify the sections of the install script that set the Solaris account's profile information to match the syntax for the shell you are using.

Note: Our example script does not start the Domino partitions with the server controller. (It does not use the **-**jc option.) Should you decide to start the server controller and have more than one Domino partition, bind the server controller port, 2050, to each partition's TCP/IP address. See 5.4.1, "Partitioned server networking considerations" on page 181.

Our install script performs all of the steps described in the previous section to install an RC script. Here is the install procedure:

1. Download the script zip file, SG247162.zip, from the ITSO Web site. See Appendix H, "Additional material" on page 571.
2. Log on as `root`.
3. Copy the file to a temporary directory (for example, /tmp).
4. Make the temporary directory your working directory:

   ```
   cd /tmp
   ```

5. Unzip the file:

   ```
   unzip SG247162.zip
   ```

6. You should find three files now:
   - lotusdomino
   - install
   - postinstall

   Make them executable:

   ```
   chmod 755 *
   ```

7. Run the install script:

   ```
   ./install
   ```

Note: For all questions presented by the install script, you have four options:

- Press Enter to accept the default (displayed as `default`).
- Enter the setting you want and press Enter.
- Enter `?` and press Enter for a brief help message.
- Enter `q` to quit the install script.

8. The first screen appears:

   ```
   You will be asked a few questions regarding the configuration

   The following are the recommended settings:

   o One Solaris account per Domino partition
   o Solaris account names are domino1, domino2, ...
   o All Solaris accounts belong to the notes group

   2 partitions were found on this system


   Enter number of Domino partitions [2]:  [?,q]
   ```

9. If the number of partitions is correct, press Enter; otherwise type the number of partitions.

10. The script displays the default options:

    ```
    User                      = domino1
    Group                     = notes
    Home                      = /lotus/domino1
    Data directory            = /lotus/domino1/notesdata
    NSD log directory         =
    /lotus/domino1/notesdata/IBM_TECHNICAL_SUPPORT
    Lotus binaries directory  = /opt/ibm/lotus/bin


    User                      = domino2
    Group                     = notes
    Home                      = /lotus/domino2
    Data directory            = /lotus/domino2/notesdata
    NSD log directory         =
    /lotus/domino2/notesdata/IBM_TECHNICAL_SUPPORT
    Lotus binaries directory  = /opt/ibm/lotus/bin


    Use defaults [n] ?  [y,n,?,q]
    ```

    Usually you will answer this prompt with `n` and enter the information for each Domino partition.

11. You are prompted for the following information for each Domino partition:

    – Solaris account name
    – Group name for the Solaris account
    – Home directory for the Solaris account
    – Data directory
    – nsd-log directory
    – Lotus binaries directory

The install script validates the information, then:

a. Stores the configuration information in /opt/lotus/domsun.cfg or /opt/ibm/lotus/bin, depending what the install script finds when searching for installed partitions.

b. Creates a .profile_Dom_Sun for each partition's Solaris account's home directory adding lines that set the user's parameters.

c. Changes the Solaris account's .profile to execute .profile_Dom_Sun.

d. Copies the lotusdomino start/stop script to /etc/init.d.

e. Creates links in the appropriate rc directories to automate the startup and shutdown:

```
/etc/rc0.d/K00lotusdomino to stop partitions
/etc/rc1.d/K00lotusdomino to stop partitions
/etc/rc3.d/S99lotusdomino to start partitions
```

In our example script, the Domino Console input file is called `cinput` and the Domino Console output file is called `coutput`. Both of these files are in the Domino partition's data directory.

In our example, /opt/ibm/lotus/domsun.cfg looks like this for our second server, which has the dom2a and dom1b partitions:

```
# more domsun.cfg
NUM_DOMINO_PARTITIONS=2

# Configuration Settings for partition 1

NOTES_USER_1_NAME=sol2a
NOTES_USER_1_GROUP=domino
NOTES_USER_1_HOME=/export/home/sol2a
NOTES_USER_1_NOTES_DATA=/notes/dom2a
NOTES_USER_1_LOTUSBIN_DIR=/opt/ibm/lotus/bin
NOTES_USER_1_NSDLOG_DIR=/notes/dom2a/IBM_TECHNICAL_SUPPORT

# Configuration Settings for partition 2

NOTES_USER_2_NAME=sol1b
NOTES_USER_2_GROUP=domino
NOTES_USER_2_HOME=/export/home/sol1b
NOTES_USER_2_NOTES_DATA=/notes/dom1b
NOTES_USER_2_LOTUSBIN_DIR=/opt/ibm/lotus/bin
NOTES_USER_2_NSDLOG_DIR=/notes/dom1b/IBM_TECHNICAL_SUPPORT
#
```

5.4.3 Running servers via the Service Management Facility (SMF)

UNIX operating systems, including Solaris, have traditionally included a set of *services*: software programs not associated with any interactive user login that listen for and respond to requests to perform certain tasks, such as delivering e-mail, responding to FTP requests, or permitting remote command execution. These traditional services were usually individual applications that executed as a single process that started at boot time and executed continuously while a system was up and running, servicing any requests that were received.

Today, administrators must contend with a collection of services that has grown to such a point that it has exceeded the utility of this original model. Sun has created the *Service Management Facility (SMF)* to simplify management of these system services. SMF, a new feature of the Solaris Operating System that creates a supported, unified model for services and service management on each Solaris system, is a core part of the Predictive Self-Healing technology available in Solaris 10, which provides automatic recovery from software and hardware failures as well as administrative errors.

Features

The Service Management Facility has improved several aspects of the Solaris administrative model. Some of the most notable updates are:

- Services are represented as first-class objects that can be viewed (using the new **`svcs(1)`** command) and managed (using **`svcadm(1M)`** and **`svccfg(1M`**)).
- Failed services are automatically restarted in dependency order, whether they failed as the result of administrator error, software bug, or uncorrectable hardware error.
- More information is available about misconfigured or misbehaving services, including an explanation of why a service is not running (using **`svcs -x`**), as well as individual, persistent log files for each service.
- Problems during the boot process are easier to debug, as boot verbosity can be controlled, service startup messages are logged, and console access is provided more reliably during startup failures.
- Snapshots of service configurations are taken automatically, making it easier to back up, restore, and undo changes to services.
- Services can be enabled and disabled using a supported tool (**`svcadm(1M)`**), enabling the changes to persist across upgrades and patches.
- Administrators can securely delegate tasks to non-root users more easily, including the ability to configure, start, stop, or restart services (as described in the smf_security(5) man page).
- Large systems boot faster by starting services in parallel according to their dependencies.

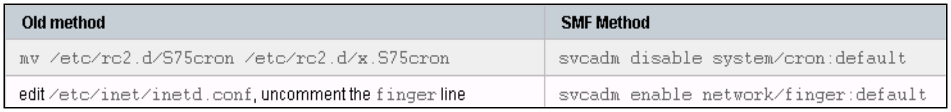
Despite these changes, compatibility with existing administrative practices has been preserved wherever possible. For example, most site-local and ISV-supplied RC scripts will still work as usual.

Common Tasks

SMF is a particularly notable change in Solaris because it affects the administrative model. We encourage you to read more about the features of SMF (see “References” on page 194), but you might want to start by learning how to do some common system administration tasks.

Enabling and disabling services

Prior to Solaris 10, there was no good way to permanently disable a service in Solaris. The typical method was to rename the relevant RC script to a name that would not be executed, but that change would be overlooked the next time the system is upgraded. Furthermore, inetd-based services were enabled and disabled by a totally different method: editing a configuration file. Under SMF, both types of services can be configured using the **svcadm(1M)** command, and the changes will persist if the machine is upgraded. The following figure shows a comparison of how to enable and disable some services.



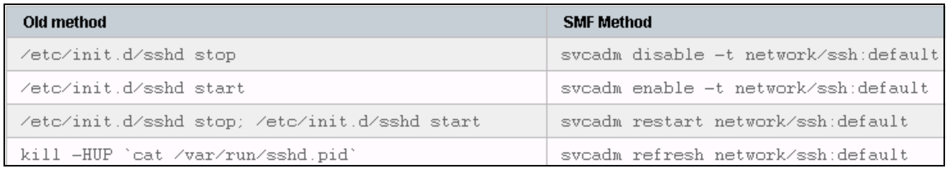
Old method	SMF Method
`mv /etc/rc2.d/S75cron /etc/rc2.d/x.S75cron`	`svcadm disable system/cron:default`
edit `/etc/inet/inetd.conf`, uncomment the `finger` line	`svcadm enable network/finger:default`

The last argument to **svcadm** in these examples is the FMRI of the service.

svcadm should be used only for SMF services; legacy RC script–controlled services work the same as in past releases.

Stopping, starting, and restarting services

Traditionally, services have been started by an RC script that is run at boot with the start argument. Some RC scripts provide a stop option, and a few also allow restart. In SMF, these tasks are all accomplished with the **svcadm(1M)** command.



Old method	SMF Method
`/etc/init.d/sshd stop`	`svcadm disable -t network/ssh:default`
`/etc/init.d/sshd start`	`svcadm enable -t network/ssh:default`
`/etc/init.d/sshd stop; /etc/init.d/sshd start`	`svcadm restart network/ssh:default`
``kill -HUP `cat /var/run/sshd.pid` ``	`svcadm refresh network/ssh:default`

The -t option to **svcadm enable** and **svcadm disable** indicates that the requested action should be temporary — it will not affect whether the service is started the next time the system boots. As with the enabling and disabling of services,

svcadm should not be used to control RC script-controlled services; they continue to work the same as in past releases.

Follow these steps:

1. Create a service manifest file.

   ```
   /var/svc/manifest/application/domino.xml
   ```

2. Fix the permissions for the two files created.

   ```
   chown root:sys /var/svc/manifest/application/domino.xml
   chmod 444 /var/svc/manifest/application/domino.xml
   ```

3. Import the service into the service repository.

   ```
   svccfg import /var/svc/manifest/application/domino.xml
   ```

4. Enable the service.

   ```
   svcadm -v enable domino
   ```

Detailed XML examples can be downloaded from the Sun Web site:

http://www.sun.com

References

For further information, see the following Sun documentation:

- *Solaris 10 System Administrator Collection* — search at:

  http://www.sun.com/docs

- *Solaris Service Management Facility - Quickstart Guide*

  http://www.sun.com/bigadmin/content/selfheal/smf-quickstart.html

- *Solaris Service Management Facility - Service Developer Introduction*

  http://www.sun.com/bigadmin/content/selfheal/sdev_intro.html

5.5 Starting Domino and the server controller console

There are many ways to start your Domino server. This section describes some of the more common methods.

5.5.1 Domino Server Controller

Domino can be started with or without the Domino Server Controller. The Server Controller is a Java-based program that controls a Domino server. Starting the Server Controller starts the Domino server it controls. When a server runs under a Server Controller, you can send operating system commands (shell commands), Controller commands, and Domino server commands to the Server

Controller. For example, from a remote console, you can use Controller commands to kill Domino processes on a server that is hung or to start a Domino server that is down.

You can use the Domino Java Console to communicate with a Server Controller. You can run the Java Console on any platform except Apple Macintosh. Using the Java Console, you can send commands to multiple servers. The Java Console does not require a Notes ID, only a Domino Internet name and password, so you can connect to servers certified by different certifiers without having multiple Notes IDs or cross-certificates.

The Domino Console functions strictly as a server console. Consequently, the Domino Console does not include the full set of Domino administration features that are available through the Domino Administrator and the Web Administrator, and you cannot use it to open and manage Notes databases.

Start the server controller by using the -jc option when you start the Domino partition.

If your Solaris server has graphics, keyboard, mouse, and the X11 Windows software installed, or you have remotely logged in and your DISPLAY environment variable is pointed to a workstation running X11, then the Java console will start on what your DISPLAY environment variable is pointing to. A DISPLAY set to :0.0 indicates the main local display; *hostname*:0.0 indicates the main display on the workstation called *hostname*. If you are using X11, you may connect to the server controller using the command jconsole**,** which is included in the Domino program directory.

If you are not using X11, the -jc option still starts the Domino server controller, and you can connect to this controller with the Domino Console client from a Windows workstation.

Additional information about the server controller can be found in 9.4, “The Domino Server Controller and Domino Console” on page 322.

5.5.2 Solaris command line to start Domino in the foreground

The following steps show a standard way to start the Domino server from a command line which will run your Domino server in the foreground. The Domino Console will use the Solaris command line's keyboard for input and display for output.

1. Make sure you are logged on with the Solaris account you created for running the Domino server.
2. Change to your Domino data directory; for example:

   ```
   cd /notes/dom1b
   ```

3. Start the server:
   - With the server controller:

     ```
     /opt/ibm/lotus/bin/server -jc
     ```

   - Without the server controller:

     ```
     /opt/ibm/lotus/bin/server
     ```

4. You will see the console output as Domino starts, as shown in Example 5-1, and eventually the console prompt (>). You can enter Domino Console commands at this prompt.

Example 5-1 Startup console output

```
Lotus Domino (r) Server, Release 7.0, August 18, 2005
Copyright (c) IBM Corporation 1987, 2005. All Rights Reserved.

11/04/2005 11:44:34   Event Monitor started
11/04/2005 11:44:35   Server started on physical node dom1b
11/04/2005 11:44:35   NOTES.INI contains more than one definition for
TCPIP_TCPI
PADDRESS
11/04/2005 11:44:35   The Console file is
/notes/dom1b/IBM_TECHNICAL_SUPPORT/con
sole.log
11/04/2005 11:44:35   Console Logging is ENABLED
11/04/2005 11:44:35   Adding server to cluster CLUSTER1
11/04/2005 11:44:35   Index update process started
11/04/2005 11:44:35   Database Replicator started
11/04/2005 11:44:35   Replicator is set to Ignore Database Quotas
11/04/2005 11:44:35   Admin Process: Dom1a/ACME is the Administration Server of
the Domino Directory.
11/04/2005 11:44:35   Calendar Connector started
11/04/2005 11:44:35   Administration Process started
11/04/2005 11:44:35   Mail Router started for domain ACME
11/04/2005 11:44:35   Router: Internet SMTP host dom1b in domain
cam.itso.ibm.com
```

```
11/04/2005 11:44:35   Agent Manager started
11/04/2005 11:44:36   AMgr: Executive '1' started. Process id '13674'
11/04/2005 11:44:36   Schedule Manager started
11/04/2005 11:44:36   Rooms and Resources Manager started
11/04/2005 11:44:36   HTTP Server: Using Web Configuration View
111/04/2005 11:44:43   HTTP Server: Started
11/04/2005 11:44:45   Cluster Database Directory started
11/04/2005 11:44:45   Finished initialization of Cluster Database Directory
.
.
.
>
```

5.5.3 Solaris command line to start Domino in the background

From an operational standpoint, running the Domino server in the background is often desirable. The server is started without taking control of the command line's input (keyboard) and output (display).

The following steps show a standard way to start Domino in the background:

1. Log on with the Solaris account you created for running the Domino server (for example, sol1b).
2. Change to your Domino data directory; for example:

   ```
   cd /notes/dom1b
   ```

3. Start the server:
   - With the server controller:

     ```
     /opt/ibm/lotus/bin/server -jc &
     ```

   - Without the server controller:

     ```
     /opt/ibm/lotus/bin/server &
     ```

5.5.4 Starting the Domino server using a startup script

In 5.4.2, "Installing start/stop scripts" on page 187, we described how to install the example start/stop scripts. As noted in that section, these scripts are run automatically when the Solaris system is started or shut down, or changes run levels (via the **init** command).

You can run your script manually to start your Domino partitions by performing the following steps:

1. Log on as root.

2. To start all of your Domino partitions:

   ```
   /etc/init.d/lotusdomino start
   ```

   To start a single Domino partition (for example, the dom1b partition, which uses the sola1b Solaris account):

   ```
   /etc/init.d/lotusdomino start sol1b
   ```

5.6 Sending commands to the Domino Console

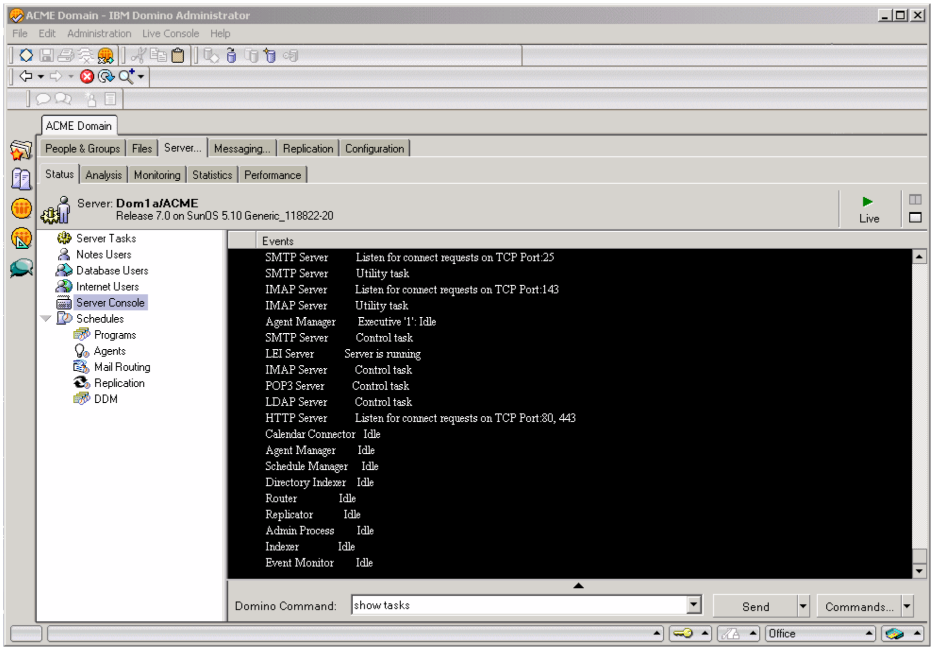
After the Domino partition is started, you can send Domino commands to the Domino Console in a number of ways. Your options vary depending on how you started the partition.

5.6.1 Console commands: Domino Administrator client

One of the most common ways to send Domino Console commands to a partition is with the Live Console feature of the Domino Administrator client. Use the following steps to start the Domino Administrator client and the Live Console. For more information about using the Domino Administrator client, refer to Chapter 9, “IBM Lotus Domino administration” on page 265

1. Open the Domino Administrator client.
2. Click the **Status** tab on the Server panel.
3. Choose the server you want.
4. Click **Server Console**.

5. In the Domino Command field, you may enter Domino Console commands, which will be sent to the Domino Console when you press Enter (Example 5-136).



Server: Dom1a/ACME
Release 7.0 on SunOS 5.10 Generic_118822-20

```
SMTP Server        Listen for connect requests on TCP Port:25
SMTP Server        Utility task
IMAP Server        Listen for connect requests on TCP Port:143
IMAP Server        Utility task
Agent Manager      Executive '1': Idle
SMTP Server        Control task
LEI Server         Server is running
IMAP Server        Control task
POP3 Server        Control task
LDAP Server        Control task
HTTP Server        Listen for connect requests on TCP Port:80, 443
Calendar Connector Idle
Agent Manager      Idle
Schedule Manager   Idle
Directory Indexer  Idle
Router             Idle
Replicator         Idle
Admin Process      Idle
Indexer            Idle
Event Monitor      Idle
```

Domino Command: show tasks

Figure 5-136 Admin Client - Live Console

5.6.2 Console commands: the cconsole command

To send a command to the console of a Domino server running in the background, you can use the remote console feature in a Notes, Domino Administrator, or Web Administrator client. You can also use the Character Console (cconsole) program (Example 5-2 on page 200):

1. Log on as the Solaris account you created for running the server (for example, sola1a).
2. Change to your Domino data directory:

   ```
   cd /notes/dom1a
   ```

3. Enter on the command line:

   ```
   /opt/ibm/lotus/bin/cconsole
   ```

4. Enter the path to the administrator's ID file; for example:

   ```
   /notes/dom1a/admin.id
   ```

5. Enter the password.

6. The Domino Console prompt (>) appears, indicating that console commands may now be entered. For example, type the Domino command `show tasks` and the output from the show tasks command displays.
7. To end a console session, type `done` at the console prompt.

Example 5-2 cconsole command

```
$ /opt/ibm/lotus/bin/cconsole
Domino Character Console v0.0
Warning:  You are remotely connected to host dom1a.
If you have not taken precautions to secure this connection,
passwords will be exposed over the network.
Do you want to end this cconsole session? [y/n] n

Enter the full path to your ID file: /notes/dom1a/admin.id

Enter your password:
12/02/2005 09:00:28   Initiating cconsole on dom1a
>
```

Attention: Entering `quit` or `q` shuts down the Domino server (after a confirmation prompt).

See 9.3, “The Domino Character Console” on page 321 for additional information about using the Domino character console program.

5.6.3 Console commands: the jconsole command

In addition to the cconsole command (Introduced with Domino R5) you can also use the Domino (Java) Console (jconsole) program.

See 9.4, “The Domino Server Controller and Domino Console” on page 322 for more information about the Domino Server controller and the Java console.

Note: To use jconsole you must have started your Domino partition with the server controller by using the -jc option.

Note: Your Solaris system must run the X Window System for the Domino (Java) Console to work directly on your Solaris system. You can display the Java Console output over the network to a workstation running the X Window System or an X Window emulator. You may access the server controller with the Domino Console program on a Windows workstation.

To run the Java Console on Solaris, follow these steps:

1. In an X-Terminal session, log on as the Solaris user you created for running the server.
2. Change to your Domino data directory (for example, `cd` to your notesdata directory) and enter on the Solaris command line:

   ```
   /opt/ibm/lotus/bin/jconsole
   ```

3. A new X-Window opens. Specify the Domino server you want to access.
4. Enter your Notes user name and HTTP password.
5. The Domino (Java) Console display appears, indicating that console commands may now be entered.

See 9.4, “The Domino Server Controller and Domino Console” on page 322 for additional information about using the Domino (Java) console.

5.6.4 Console commands via the example start script cinput file

As noted in 5.4.2, “Installing start/stop scripts” on page 187, the example start/stop script creates two files in the Domino partition’s data directory:

- cinput (input to the Domino Console)
- coutput (output from the Domino Console)

You can send Domino Console commands to cinput, and the output will be placed in coutput. In this example we use our Solaris account `sol1a` and host `dom1a`:

1. Make sure you are logged on with the Solaris account you created for running the Domino server.
2. Change to your Domino data directory, for example:

   ```
   cd /notes/dom1a
   ```

3. To send a command to cinput use the shell’s echo command and redirect the output to cinput:

   ```
   $ echo show tasks >> cinput
   ```

4. The output is written to coutput. You can use the `cat` or `more` commands to display coutput, as shown in Example 5-3.

Example 5-3 Using the more command

```
more coutput
Copyright (c) IBM Corporation 1987, 2005. All Rights Reserved.

Performing consistency check on log.nsf...
Completed consistency check on log.nsf
```

```
12/01/2005 17:04:05   Event Monitor started
12/01/2005 17:04:05   Begin scan of databases to be consistency checked
12/01/2005 17:04:05   End scan of databases: 2 found
.
.
.
show tasks

      Task                  Description

 Database Server      Consistency check will start in 78 seconds
 Database Server      Consistency check will start in 10 seconds
 Database Server      Perform console commands
 Database Server      Listen for connect requests on TCPIP
 Database Server      Listen for connect requests on CLUSTER
 Database Server      Load Monitor is idle
 Database Server      Database Directory Manager Cache Refresher is idle
 Database Server      Organization Name Cache Refresher is idle
 Database Server      Cluster Replication Cleanup Thread
 Database Server      Idle task
 Database Server      Idle task
 Database Server      Perform Database Cache maintenance
 Database Server      Idle task
 Database Server      Idle task
.
.
.
```

5.7 Shutting down the Domino server

There are many ways to shut down your Domino server. This section describes some of the more common methods.

5.7.1 Shutdown from Solaris command line; Domino in foreground

If your Domino server was started from a Solaris command line prompt, the Domino Console is running in the foreground, so you can perform the following steps to shut down the server:

1. At the Domino Console prompt, type `exit` or `quit`.
2. Press Enter. It might take a few seconds or more for the server to shut down.

Example 5-4 on page 203 shows the console output of a Domino server after `quit` was entered.

Example 5-4 Shutting down from the Solaris command line

```
11/04/2005 14:14:01   LDAP Server: Waiting for all tasks to complete
11/04/2005 14:14:01   Cluster Database Directory Terminating
11/04/2005 14:14:01   Cluster Database Directory shutdown
11/04/2005 14:14:01   DOMWS Convert AddIn Terminating
11/04/2005 14:14:01   Calendar Connector shutdown
11/04/2005 14:14:02   Administration Process shutdown
11/04/2005 14:14:02   Database Replicator shutdown
11/04/2005 14:14:02   Router: Shutdown is in progress
11/04/2005 14:14:02   Mail Router shutdown
11/04/2005 14:14:02   Cluster Replicator shutdown
11/04/2005 14:14:02   Schedule Manager shutdown complete
11/04/2005 14:14:02   Rooms and Resources Manager shutdown complete
11/04/2005 14:14:02   AMgr: Executive '1' shutting down. Process id '16188'
11/04/2005 14:14:02   Agent Manager shutdown complete
11/04/2005 14:14:02   DOMWS Convert AddIn Termination Complete
11/04/2005 14:14:03   SMTP Server: Waiting for all tasks to complete
11/04/2005 14:14:03   IMAP Server: Waiting for all tasks to complete
11/04/2005 14:14:03   POP3 Server: Waiting for all tasks to complete
11/04/2005 14:14:03   Index update process shutdown
11/04/2005 14:14:04   Event Monitor shutdown
11/04/2005 14:14:04   Domino Off-Line Services HTTP extension unloaded.
11/04/2005 14:14:05   HTTP Server: Shutdown
11/04/2005 14:14:07   This server is currently a member of a cluster
11/04/2005 14:14:08   IMAP Server: All tasks have completed
11/04/2005 14:14:08   IMAP Server: Shutdown
11/04/2005 14:14:09   POP3 Server: All tasks have completed
11/04/2005 14:14:09   POP3 Server: Shutdown
11/04/2005 14:14:09   LDAP Server: All tasks have completed
11/04/2005 14:14:09   LDAP Server: Shutdown
11/04/2005 14:14:29   SMTP Server: All tasks have completed
11/04/2005 14:14:29   SMTP Server: Shutdown
11/04/2005 14:14:29   Server shutdown complete
```

5.7.2 Shutdown from Solaris command line; Domino in background

For a command-line shutdown of a Domino server running in the background, there are two options to shut down the Domino partition.

- The **server** command:

  a. Log on with the Solaris account you created to run the Domino server.

  b. Make the Domino data directory your current directory; for example:

  ```
  cd /notes/dom1a
  ```

  c. Type:

  ```
  /opt/ibm/lotus/bin/server -q
  ```

- Using cconsole (Example 5-5):
  a. Log on as the Solaris account you created for running the server.
  b. Change to your Domino data directory:

     `cd /notes/dom1a`

  c. Enter the following command:

     `/opt/ibm/lotus/bin/cconsole`

  d. Enter the path to the administrator’s ID file; for example:

     `/notes/dom1b/admin.id`

  e. Enter the password.
  f. The Domino Console prompt (>) appears, indicating that console commands may now be entered.
  g. To shut down the server, type `quit` at the console prompt.

Example 5-5 cconsole quit

```
$ /opt/ibm/lotus/bin/cconsole
Domino Character Console v0.0
Warning:  You are remotely connected to host dom1a.
If you have not taken precautions to secure this connection,
passwords will be exposed over the network.
Do you want to end this cconsole session? [y/n] n

Enter the full path to your ID file: /notes/dom1a/admin.id

Enter your password:
12/02/2005 09:00:28   Initiating cconsole on dom1a
>quit
Warning:  You entered the command to shutdown the Domino server.
(Use the "done" command to stop the console without server shutdown.)
Do you really want to shutdown the Domino server? [y/n] y
broadcast "Domino server exiting" >/notes/dom1a/23940271.TMP
12/02/2005 09:11:36   BROADCAST from Dom1a/ACME: Domino server exiting
> Command has been executed on remote server. Use 'Live' console option, in
futu
re, to view response from server.> quit
12/02/2005 09:11:42   Ending cconsole on dom1a.
$ 12/02/2005 09:11:43   AMgr: Executive '1' shutting down. Process id '7772'
12/02/2005 09:11:43   Router: Shutdown is in progress
12/02/2005 09:11:43   Mail Router shutdown
12/02/2005 09:11:43   Administration Process shutdown
12/02/2005 09:11:44   Calendar Connector shutdown
12/02/2005 09:11:44   Schedule Manager shutdown complete
.(more output from shutdown here)
.
```

```
.
.
12/02/2005 09:11:50   LDAP Server: All tasks have completed
12/02/2005 09:11:50   LDAP Server: Shutdown
12/02/2005 09:11:58   IMAP Server: All tasks have completed
12/02/2005 09:11:58   IMAP Server: Shutdown
12/02/2005 09:11:59   POP3 Server: All tasks have completed
12/02/2005 09:11:59   POP3 Server: Shutdown
12/02/2005 09:11:59   SMTP Server: All tasks have completed
12/02/2005 09:11:59   SMTP Server: Shutdown
12/02/2005 09:12:37   Server shutdown complete

$
```

5.7.3 Shutting down the server from a script

In 5.4.2, “Installing start/stop scripts” on page 187, we described how to install the example start/stop scripts. As noted in that section, these scripts are run automatically when the Solaris system is started or shut down, or changes in run levels (via the `init` command).

You can run your script manually to shut down your Domino partitions by performing the following steps:

a. Log on as root.

b. Shut down all of your Domino partitions by entering:

```
/etc/init.d/lotusdomino stop
```

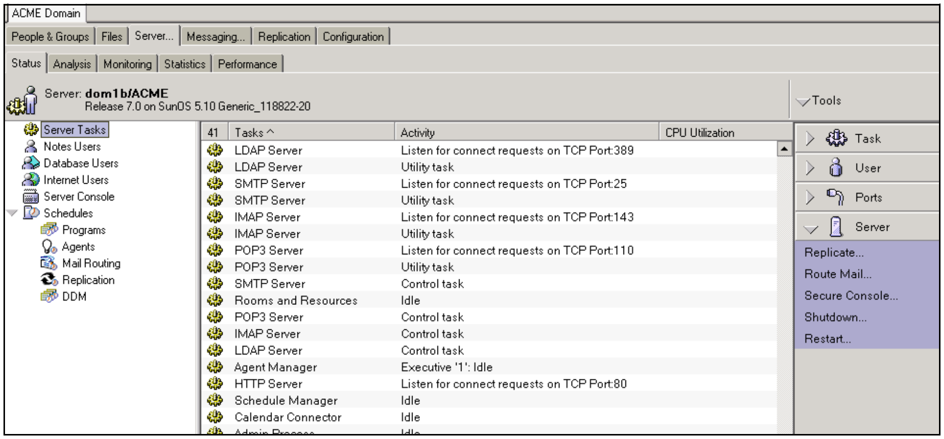
Or shut down a single Domino partition (for example, the partition that uses the sol1b Solaris account):

```
/etc/init.d/lotusdomino stop sol1b
```

5.7.4 Shutting down from the Domino Administrator

You can also shut down the server using the Domino Administrator client. Follow these steps to start the Domino Administrator client and shut down the server. (For more information about using the Domino Administrator client, refer to Chapter 9, “IBM Lotus Domino administration” on page 265.)

1. Open the Domino Administrator client.
2. Click the **Status** tab in the Server panel.
3. Choose the server you want to shut down and select **Tools** → **Server** → **Shutdown** or, from the menu bar, **Server** → **Server** → **Shutdown** (Figure 5-137).



Server: **dom1b/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

41	Tasks ^	Activity	CPU Utilization
	LDAP Server	Listen for connect requests on TCP Port:389	
	LDAP Server	Utility task	
	SMTP Server	Listen for connect requests on TCP Port:25	
	SMTP Server	Utility task	
	IMAP Server	Listen for connect requests on TCP Port:143	
	IMAP Server	Utility task	
	POP3 Server	Listen for connect requests on TCP Port:110	
	POP3 Server	Utility task	
	SMTP Server	Control task	
	Rooms and Resources	Idle	
	POP3 Server	Control task	
	IMAP Server	Control task	
	LDAP Server	Control task	
	Agent Manager	Executive '1': Idle	
	HTTP Server	Listen for connect requests on TCP Port:80	
	Schedule Manager	Idle	
	Calendar Connector	Idle	
	Admin Process	Idle	

Figure 5-137 Admin client - server shutdown in Tools pane

4. Click **Yes** to confirm the shutdown.
5. The Domino Administrator indicates that the server no longer responds.

> **Tip:** You can shut down and restart your Domino server by using the `restart server` command from the console. However, this does not work if the server is in a hung state.

5.8 Summary

In this chapter, we gave a short checklist of preparations prior to installation of the Domino server. We showed step-by-step instructions for installing the Domino server code and for setting up the Domino server using a browser and the Web Setup database. Finally, we showed different methods for starting and stopping your Domino server.

6

Tuning and monitoring Domino servers on Solaris

This chapter discusses how to tune Solaris and IBM Lotus Domino for best performance, and how to monitor the system for warning signs of worsening performance.

© Copyright IBM Corp. 2006. All rights reserved.

6.1 Essential tuning

Both Solaris 10 and Domino 7 are more self-adjusting than earlier versions; also, many of their default settings have been upgraded to better match modern servers' demands and resources. You need adjust only a few parameters to get Domino 7 to run well on Solaris 10. We recommend that you adjust *only* these few parameters until you have had the chance to observe Domino's performance for a while; the time to apply the finer adjustments discussed in *Domino on Solaris: Common Tuning Tips* is after you have established a baseline, not before.

In particular, if you have upgraded to Solaris 10 and Domino 7 from earlier versions, it is likely that several adjustments have already been made in /etc/system, notes.ini, and elsewhere. We recommend that you comment out or otherwise rescind such adjustments and begin with a clean slate.

Some tuning information is volatile, constantly being refined as new machines become available and as both Domino and Solaris are upgraded and improved. Therefore, this chapter covers only the essentials. For a more comprehensive and up-to-date treatment, visit http://www.sun.com/lotus/ and look for the latest edition of *Domino on Solaris: Common Tuning Tips* in the Technical Documentation section. Also, be sure to consult the release notes for Domino 7 updates as they appear.

6.1.1 Essential Solaris tuning

As the `root` user, edit the /etc/system file and add this line at the bottom:

```
set segmap_percent=40
```

This adjustment makes it easier for Solaris' file system buffer cache to handle Domino's file access patterns. We suggest the value 40 as a starting point for most systems; systems with small amounts of memory might need to use values as low as 25, and memory-rich systems might benefit from values as high as 60. We encourage you to experiment with different values to find your own system's optimal setting. The general guideline is to make segmap_percent as large as you can, but not so large as to cause page scanning. See 6.2.1, "The vmstat utility" on page 213 for information about monitoring the page scanner.

Believe it or not, this is the *only* /etc/system adjustment required. Adjustments to rlim_fd_max and msgsys:msginfo_msgtql, which previously were mandatory, are now unnecessary. Adjusting autoup and tune_t_fsflushr might still be useful but are not essential, so we suggest you run for a while with the default settings and tune them only if you find evidence of a problem. Broadly speaking, "less is more" when adjusting /etc/system parameters: Have a reason for each adjustment you make, and do not simply inherit adjustments from previous Solaris versions.

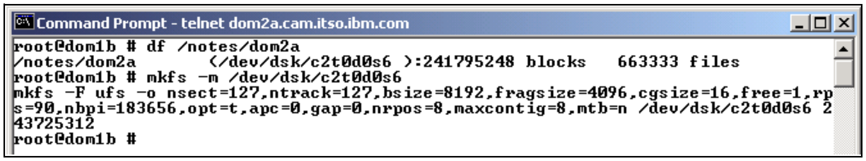
After saving your changes to /etc/system, you must reboot Solaris for the new settings to take effect.

6.1.2 File system tuning

If Domino's files reside on dedicated UNIX File System (UFS) volumes, you should make sure that the file systems' settings are optimal and that extraneous I/O activity is suppressed. This section describes how to do both.

File system settings

See 4.6, "File system layout" on page 53, which describes how to create Domino file systems and recommends values for the file system parameters. If your file systems were not originally created for use with Domino they might have been built with different settings, and you might need to change them. To inspect the parameters of an existing file system, use the **df** command to determine the name of the device where the file system resides and then use the **mkfs** command to list the parameters, as shown in Figure 6-1 for the file system mounted at /notes/dom2a.



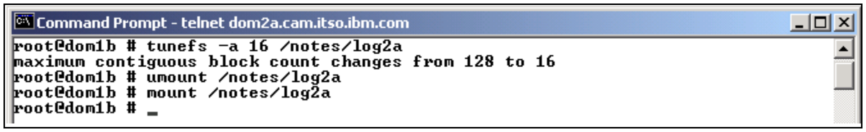
```
root@dom1b # df /notes/dom2a
/notes/dom2a       (/dev/dsk/c2t0d0s6 ):241795248 blocks   663333 files
root@dom1b # mkfs -m /dev/dsk/c2t0d0s6
mkfs -F ufs -o nsect=127,ntrack=127,bsize=8192,fragsize=4096,cgsize=16,free=1,rp
s=90,nbpi=183656,opt=t,apc=0,gap=0,nrpos=8,maxcontig=8,mtb=n /dev/dsk/c2t0d0s6 2
43725312
root@dom1b #
```

Figure 6-1 Inspecting file system settings

Unfortunately, the parameter names that **mkfs** displays do not match the option letters **newfs** uses to specify the values in the first place. Here is a brief explanation of the important settings:

- The `maxcontig` value corresponds to the **newfs** option -C (upper case). We recommend a value of 8 for Domino's server directories and databases, or 16 for Domino's transactional logs.
- The `free` value corresponds to the **newfs** option -m. For Domino file systems, we suggest the value 1.
- The `cgsize` value corresponds to **newfs** option -c (lower case). We suggest 256 for Domino, but this setting is less important than the others.

If the values are not as you expect, the best course is to unmount and re-create the file system as described in 4.6, "File system layout" on page 53. This destroys any data already stored in the file system, so you should only re-create the file system if it is empty or if you can later restore its contents from backup. If it is not practical to re-create the file system, you can still use **tunefs** to adjust the -C (maxcontig) and -m (free) values. (Confusingly enough, **tunefs** uses the -a option to specify the maxcontig value that **newfs** specifies with -C.) After changing the settings, unmount and remount the file system to have the new values take effect. Figure 6-2 shows how to change maxcontig to 16 for a transactional log's file system.



```
root@dom1b # tunefs -a 16 /notes/log2a
maximum contiguous block count changes from 128 to 16
root@dom1b # umount /notes/log2a
root@dom1b # mount /notes/log2a
root@dom1b # _
```

Figure 6-2 Changing file system settings

Suppressing needless I/O

You should also arrange to eliminate some extraneous I/O activity. Ordinarily, UFS keeps track of the time when each file was last accessed. Domino does not need or use this information, so recording it creates unnecessary extra disk I/O. You can suppress this activity by mounting the file systems with the *noatime* option. Edit the /etc/vfstab file and add noatime to the mount options for each Domino file system; the result will resemble this:

```
/dev/dsk/... /dev/rdsk/... /notes/data ufs 2 yes noatime
/dev/dsk/... /dev/rdsk/... /notes/logs ufs 2 yes noatime
```

Save the file, then unmount and remount each of the affected file systems for the noatime option to take effect.

Alternative file systems

If you use a file system other than UFS, consult that file system's documentation to learn about the adjustments and controls it offers. Here are some points to consider when tuning other file systems:

- File systems for Domino server home directories should be optimized for a random I/O load. Most individual I/O operations transfer a fairly small amount of data, in the range of 16 to 24 KB, but some occasional, much larger transfers will occur. Service times should not exceed 15 milliseconds or so. There will be (roughly) twice as many reads as writes.
- File systems for mail databases face a similar load but can afford to be somewhat slower, up to 20 ms or even 30 ms.
- It is important to prevent excessive read-ahead on these two kinds of file systems. Domino often reads several contiguous areas of a file, and this might fool the file system into believing that the access pattern is sequential.

However, the overall pattern is definitely random, and aggressive read-ahead usually just increases the load on the disks to little purpose.

- File systems for transactional logs should be optimized for a load consisting almost entirely of sequential writes. Transfer sizes can be as small as 4 KB, but can grow much larger on busy systems. Service times should be no worse than 5 milliseconds.

6.1.3 Domino tuning

Domino 7 has better out-of-the-box performance than its predecessors, and requires relatively little initial tuning. We recommend that you make only the essential adjustments at first, and establish a baseline before tinkering with finer tunings.

Limiting resource consumption

If you intend to run multiple Domino partitions on a single Solaris server (see 8.1, “Domino partitioning” on page 252) you must prevent any one partition from trying to monopolize the server’s resources. Edit each partition’s notes.ini file and add a line such as:

```
PercentAvailSysResources=33
```

This instructs the partition to use only one-third of the server’s memory and other resources, leaving two-thirds for other Domino partitions or for other applications. It is possible to use different values for different partitions if their loads are dissimilar. For example, a lightly loaded administrative partition might be granted a small percentage of the system resources, with larger shares going to more heavily loaded mail partitions. In any case, the total of all partitions’ settings must not exceed 100.

The notes.ini parameter NSF_Buffer_Pool_Size_MB is another way to control Domino’s memory usage by limiting the size of its single largest consumer of memory. Values of between 800 MB and 1800 MB are reasonable, depending on the load a partition serves. The total for all partitions should not exceed about one-third of the system’s physical memory.

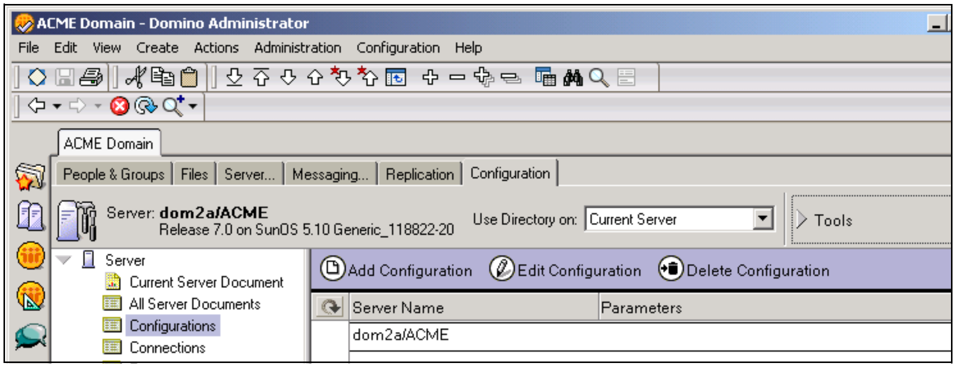
Important: Use PercentAvailSysResources or NSF_Buffer_Pool_Size_MB, but not both unless specifically directed by Lotus Support.

If you choose to use System V shared memory instead of Domino’s default mechanism, different tunings apply. See Appendix B, “Using System V shared memory” on page 521 for more information.

Multiple mailboxes

Most mail partitions, especially those with high traffic levels, benefit from having more than one mail.box file. Two such files are much better than one, and three are a little better still, but there is virtually no improvement beyond four.

To configure additional mailboxes, start the Administrator client, go to the **Configuration** tab, expand the **Server** view, and open the **Configurations** item (see Figure 6-3).



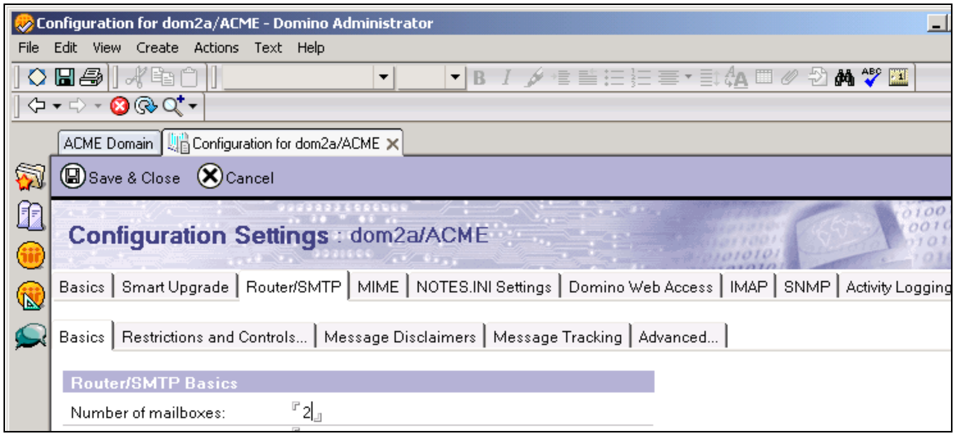
Server: **dom2a/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

Use Directory on: Current Server

Server Name	Parameters
dom2a/ACME	

Figure 6-3 Finding the server's Configuration document

If no Configuration document exists for the partition, create one as described in Domino Administrator Help. (You may create a Configuration document for a single server, for a group of servers, or for all servers, as appropriate.) Otherwise, select the appropriate Configuration document, click **Edit Configuration**, and when the document opens click the **Router/SMTP** tab and the **Basics** sub-tab (Figure 6-4 on page 213). Enter the desired mailbox count in the Number of mailboxes field, and click **Save & Close**. Next time Domino starts, it will create the additional mailboxes and start using them.



Number of mailboxes: 2

Figure 6-4 Configuring more mailboxes

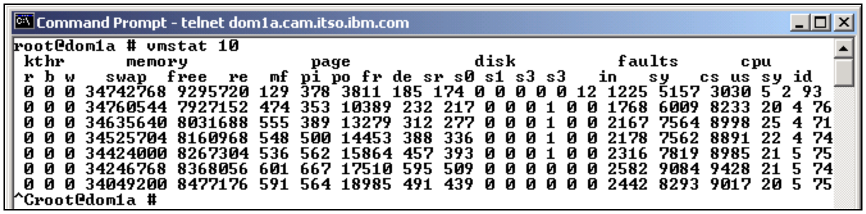
6.2 Monitoring Solaris performance

Tuning your system is not enough. You must also measure the system's performance before and after each adjustment to see whether it made things better or worse. Sustained monitoring over longer time spans helps you forecast changing demands on the system and can help in troubleshooting by enabling you to compare measurements from a misbehaving system with those from an earlier time when it was behaving well. This section describes tools for observing the performance of an entire Solaris system, both ad hoc and long term.

6.2.1 The vmstat utility

The purpose of **`vmstat`** is to report statistics about Solaris' virtual memory performance; it also reports useful data about CPU utilization and contention. Type `vmstat 10` in a terminal window to get a report every 10 seconds (you can specify shorter or longer intervals if desired); the utility will continue reporting until you use CTRL+C to stop it. The very first line of numbers reports average values for the entire time since Solaris was booted, and it usually should be ignored. Thereafter, each line reports the average values for the period since the preceding line was output.

Figure 6-5 on page 214 shows a sample of **`vmstat`** output. Although the values are arranged in columns, large numbers near the left tend to disrupt the columns farther to the right, and they make the output difficult to read. Fortunately, most of the values of interest for Domino are near the extreme left or right and are not too hard to locate; the **`sr`** value, though, is near the middle. The only recourse is to count the column headings when they appear and then count off groups of numbers to find the matching values. The heading for the **sr** column is twelfth from the left, so the twelfth number in each row is the **sr** value.



```
root@dom1a # vmstat 10
 kthr      memory            page            disk          faults      cpu
 r b w   swap  free  re  mf pi po fr de sr s0 s1 s3 s3   in   sy   cs us sy id
 0 0 0 34742768 9295720 129 378 3811 185 174 0 0 0 0 0 12 1225 5157 3030 5 2 93
 0 0 0 34760544 7927152 474 353 10389 232 217 0 0 0 1 0 0 1768 6009 8233 20 4 76
 0 0 0 34635640 8031688 555 389 13279 312 277 0 0 0 1 0 0 2167 7564 8998 25 4 71
 0 0 0 34525704 8160968 548 500 14453 388 336 0 0 0 1 0 0 2178 7562 8891 22 4 74
 0 0 0 34424000 8267304 536 562 15864 457 393 0 0 0 1 0 0 2316 7819 8985 21 5 75
 0 0 0 34246768 8368056 601 667 17510 595 509 0 0 0 0 0 0 2582 9084 9428 21 5 74
 0 0 0 34049200 8477176 591 564 18985 491 439 0 0 0 0 0 0 2442 8293 9017 20 5 75
^Croot@dom1a #
```

Figure 6-5 Running vmstat

We have just learned how to locate **sr**, so now we examine what it is, what it means, and what you might need to do about it. Solaris is a virtual memory operating system, meaning that it uses disk space to give running programs the illusion that the system has more memory than is actually installed. To maintain the illusion, Solaris must be able to evict parts of one program's memory and write them to disk so that the physical memory they occupied can be used by another program. The **sr** statistic is the *scan rate*, the number of memory pages per second Solaris considers for possible eviction.

On a properly configured and tuned system dedicated to Domino, the scan rate should almost always be zero because all of Domino's data should be able to fit in physical memory. An occasional spike in **sr** is nothing to worry about, especially if it coincides with the startup of a program. For example, a short burst of page scanning is perfectly normal when the full-text indexer starts. But persistent page scanning, even at a low level, is a sign that the system might be short of memory. If **sr** is non-zero for lengthy periods, try one or more of the following remedies:

- If you have been experimenting with high values of segmap_percent (see 6.1.1, "Essential Solaris tuning" on page 208), retreat to smaller values.
- If you are running several Domino partitions, try reducing some of their PercentAvailSysResources values (or NSF_Buffer_Pool_Size_MB, whichever you are using). See 6.1.3, "Domino tuning" on page 211.
- If you have configured Domino to use System V shared memory, consider reducing the amount of memory allocated. See Appendix B, "Using System V shared memory" on page 521.
- If you are running many Domino partitions, move one or more of them to other physical machines.
- Install more physical memory.

The leftmost column of **vmstat** output is *r*, the number of runnable processing threads. Runnable threads are not actually running on one of the system's CPUs, but are ready to run as soon as they can get a CPU's attention. Thus, the r statistic is an indicator of the system's computational backlog.

On a well-configured system, the r value should not usually exceed about four times the number of "processing cores" in the system. (An UltraSPARC-T1 CPU has four, six, or eight cores; an UltraSPARC-IV or UltraSPARC-IV+ CPU has two processing cores; and earlier UltraSPARC designs have one core.) If r hovers above four times the core count for extended periods, the computational load on the system is approaching the danger level. Try moving some CPU-intensive activities to off-peak hours, or try shifting some users to partitions on other machines.

The three farthest-right columns of **vmstat** output are *us*, *sy*, and *id*, reporting the percent of time the system's CPUs are executing user code, executing system code, or sitting idle. Usually, the us value ranges between three times sy (for systems serving mostly Lotus Notes clients) to eight times sy (if Domino Web Access clients predominate). Ratios outside this range *might* suggest a configuration problem or perhaps a runaway process. However, an unusual user-to-system ratio might be benign; it is a cause for investigation but not necessarily for alarm. If the system behaves well and gives good service to the users, it is probably just serving an atypical demand. Keep track of the ratio and be alert for sudden changes, but do not panic.

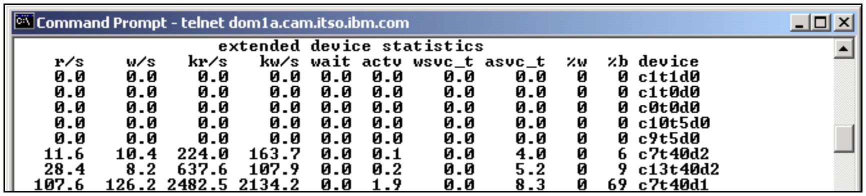
The id value at the extreme right indicates how much computational capacity the system has in reserve to deal with sudden surges in demand. It is difficult to say how much spare capacity a system requires, because different user populations have different hour-by-hour demand profiles. A very rough guideline is that if id drops below fifteen percent at times of extreme load, it is time to get more CPU power or redistribute what you already have.

Although there is no specific threshold value for idle time, it is worthwhile to keep track of the lowest id value observed each day. For example, if the lowest id values are around 40% in May, 35% in June, and 30% in July, it suggests that the demands on your system are growing and might reach the 15% threshold in about four or five more months. An early warning of this kind can let you start planning how to redistribute the load or acquire more computing power.

Finally, id can contribute a useful piece of negative information. If you are experiencing performance problems but there is still plenty of idle time, the problems must be caused by something other than a lack of CPU power. Knowing this, you can better focus your investigation on other possible trouble sources such as disk I/O, memory shortage, semaphore timeouts, and the like.

6.2.2 The iostat utility

The **iostat** utility reports performance data for disks, tapes, and NFS mount points. Many command-line options cause **iostat** to generate different kinds of output, which you can learn more about with **man iostat**. For basic monitoring, we suggest **iostat -xn 10** to report I/O statistics every 10 seconds until you stop it with CTRL+C; change the number to specify longer or shorter intervals if desired. Figure 6-6 illustrates the output from this command.



```
                   extended device statistics
    r/s    w/s   kr/s   kw/s wait actv wsvc_t asvc_t  %w  %b device
    0.0    0.0    0.0    0.0  0.0  0.0    0.0    0.0   0   0 c1t1d0
    0.0    0.0    0.0    0.0  0.0  0.0    0.0    0.0   0   0 c1t0d0
    0.0    0.0    0.0    0.0  0.0  0.0    0.0    0.0   0   0 c0t0d0
    0.0    0.0    0.0    0.0  0.0  0.0    0.0    0.0   0   0 c10t5d0
    0.0    0.0    0.0    0.0  0.0  0.0    0.0    0.0   0   0 c9t5d0
   11.6   10.4  224.0  163.7  0.0  0.1    0.0    4.0   0   6 c7t40d2
   28.4    8.2  637.6  107.9  0.0  0.2    0.0    5.2   0   9 c13t40d2
  107.6  126.2 2482.5 2134.2  0.0  1.9    0.0    8.3   0  69 c7t40d1
```

Figure 6-6 Output of iostat -xn 10 (partial)

The first group of lines reports average values for the entire time since Solaris was last booted, and usually should be ignored. Each of the later groups reports the activity statistics for the period since the preceding group, using one line to report the values for each I/O device.

The *r/s* and *w/s* columns report the number of read and write operations issued to the device each second, and the *kr/s* and *kw/s* columns give the actual data transfer rate in kilobytes per second. There are no good or bad absolute values for these quantities, as disk systems vary widely in their capabilities. However, it is a good idea to compare the input and output transfer rates. On a disk holding Domino server directories and databases, kr/s should account for one-half to two-thirds the total KBps; that is, the kr/s value should be somewhere between kw/s and twice kw/s. For a disk holding transactional logs, the input rate should be very low; kr/s should be much smaller than kw/s most of the time. If you observe a different relationship, the file systems might be improperly tuned (see 6.1.2, “File system tuning” on page 209) or Domino might be misconfigured.

When a program initiates I/O to a disk, Solaris starts the operation immediately if the disk is not too busy. If the disk is already servicing all the I/O operations it can handle, Solaris places the request in a wait queue to be dispatched when the disk has worked its way through some of the backlog. The *wait* column reports the average number of I/O requests deferred in this way, the `wsvc_t` value is the average number of milliseconds a deferred request spent waiting on the queue before being dispatched to the disk, and the *%w* value is the percentage of requests that were deferred. All three values should be zero practically all the time; if they are not, it means the disk is overloaded and has become a performance bottleneck. Try moving heavily used databases from overloaded disks to less heavily stressed devices.

However, before moving databases around, you should determine whether the real bottleneck is the disk itself or the controller that communicates with it. If many devices are attached to the same controller, perhaps the disks are lightly loaded but the controller's capacity has been exceeded. The *actv* column reports the average number of I/O operations being worked on by the disk; if this is substantially lower than the disk's rated ability but the deferral values are non-zero, suspicion should fall on the controller, especially if other disks attached to the same controller show a similar pattern. You might have to migrate active files to other disks or even to disks on different controllers.

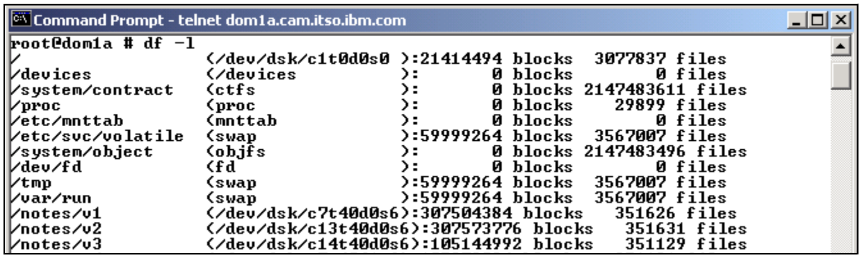
The *asvc_t* column reports the average number of milliseconds that are required to complete an I/O request when it is actually dispatched to the disk. If disk service is slow, Domino's performance can suffer badly. The definition of "slow" depends on the kind of data the disk holds and how frequently Domino needs to access that data:

- Disks that hold Domino's transactional logs must be very fast indeed, because they are on the critical path for any transaction that modifies a database. Service times of five milliseconds or less are good; times up to about seven milliseconds are marginal but acceptable.
- Disks that hold Domino's server directories and view rebuild directories must be moderately fast, because Domino uses them frequently. Service times of 10 milliseconds or less are excellent; 15-millisecond service is still acceptable. Slower times will be detrimental to Domino's performance.
- Disks that hold only mail databases are less critical to Domino's overall performance. Service times of up to 30 milliseconds are usually acceptable.

However, high asvc_t values are not a problem on a disk that is very lightly loaded. The *%b* column reports the percentage of time when the disk was servicing I/O requests; if this is less than about 15% or 20%, it is safe to ignore high service times.

The right-most column names the I/O device in "controller, target, device" form. There are two ways to translate these device names to file system mount points:

- Try using the -p and -m options, so the command becomes **`iostat -xnpm 10`**. With these options, **`iostat`** attempts to translate the names for you. However, **`iostat`** cannot make the translation for all disk models.
- If **`iostat`** cannot translate the names itself, use the **`df -l`** command to list all locally mounted file systems, as shown in Figure 6-7 on page 218. The left-most column shows the mount points, and the second shows the corresponding device names; for example, the figure shows that the device `c7t40d0` holds the `/notes/v1` file system on its `s6` partition or *slice*. (A single disk can contain different file systems on different partitions.)



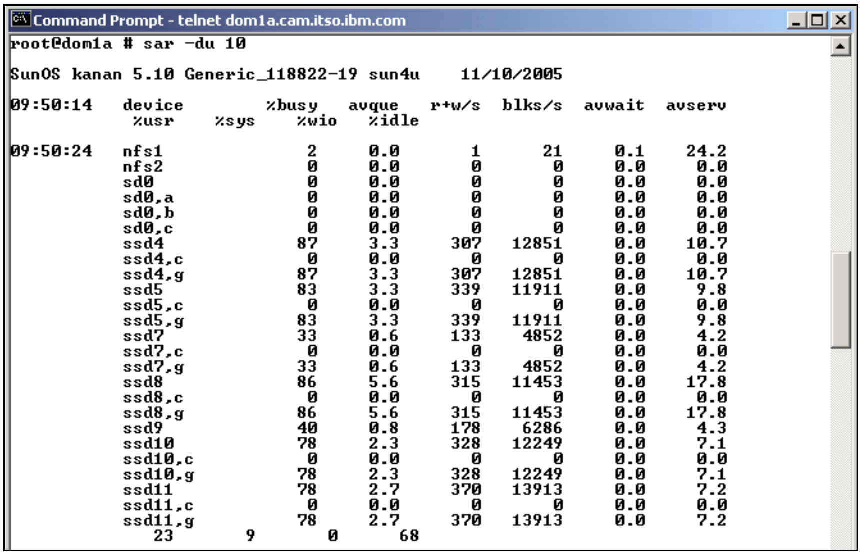
```
root@dom1a # df -l
/                  (/dev/dsk/c1t0d0s0 ):21414494 blocks  3077837 files
/devices           (/devices          ):       0 blocks        0 files
/system/contract   (ctfs              ):       0 blocks 2147483611 files
/proc              (proc              ):       0 blocks    29899 files
/etc/mnttab        (mnttab            ):       0 blocks        0 files
/etc/svc/volatile  (swap              ):59999264 blocks  3567007 files
/system/object     (objfs             ):       0 blocks 2147483496 files
/dev/fd            (fd                ):       0 blocks        0 files
/tmp               (swap              ):59999264 blocks  3567007 files
/var/run           (swap              ):59999264 blocks  3567007 files
/notes/v1          (/dev/dsk/c7t40d0s6):307504384 blocks   351626 files
/notes/v2          (/dev/dsk/c13t40d0s6):307573776 blocks   351631 files
/notes/v3          (/dev/dsk/c14t40d0s6):105144992 blocks   351129 files
```

Figure 6-7 Identifying disks for file systems

6.2.3 The sar utility

The **sar** program can display most of the performance statistics Solaris collects, including those displayed by **vmstat** and **iostat** and many others as well. A bewildering variety of option flags (use **man sar** to learn about them) controls which statistics are displayed. An advantage of **sar** is that it can display (for example) I/O and CPU statistics at the same time; a disadvantage is that the output can be hard to read if too many values are displayed simultaneously.

Figure 6-8 on page 219 shows the output of **sar -du 10**, which records disk statistics (-d) and CPU utilization statistics (-u) for 10 seconds and then displays them. The first few lines describe the system and give headers for the columns of data that follow. (The headers vary depending on which statistics you have chosen to display.). The actual data lines follow; **sar** output can sometimes be hard to read because the data lines up with the column headings, but there is no indication of which set of headings corresponds to which data lines so you simply have to apply common sense. In this figure, most of the lines describe disk statistics and correspond to the first line of headers, and the very last line gives the CPU performance figures and matches the second header row.



```
root@dom1a # sar -du 10

SunOS kanan 5.10 Generic_118822-19 sun4u    11/10/2005

09:50:14   device        %busy   avque   r+w/s   blks/s   avwait   avserv
            %usr    %sys    %wio   %idle

09:50:24   nfs1              2     0.0       1       21      0.1     24.2
           nfs2              0     0.0       0        0      0.0      0.0
           sd0               0     0.0       0        0      0.0      0.0
           sd0,a             0     0.0       0        0      0.0      0.0
           sd0,b             0     0.0       0        0      0.0      0.0
           sd0,c             0     0.0       0        0      0.0      0.0
           ssd4             87     3.3     307    12851      0.0     10.7
           ssd4,c            0     0.0       0        0      0.0      0.0
           ssd4,g           87     3.3     307    12851      0.0     10.7
           ssd5             83     3.3     339    11911      0.0      9.8
           ssd5,c            0     0.0       0        0      0.0      0.0
           ssd5,g           83     3.3     339    11911      0.0      9.8
           ssd7             33     0.6     133     4852      0.0      4.2
           ssd7,c            0     0.0       0        0      0.0      0.0
           ssd7,g           33     0.6     133     4852      0.0      4.2
           ssd8             86     5.6     315    11453      0.0     17.8
           ssd8,c            0     0.0       0        0      0.0      0.0
           ssd8,g           86     5.6     315    11453      0.0     17.8
           ssd9             40     0.8     178     6286      0.0      4.3
           ssd10            78     2.3     328    12249      0.0      7.1
           ssd10,c           0     0.0       0        0      0.0      0.0
           ssd10,g          78     2.3     328    12249      0.0      7.1
           ssd11            78     2.7     370    13913      0.0      7.2
           ssd11,c           0     0.0       0        0      0.0      0.0
           ssd11,g          78     2.7     370    13913      0.0      7.2
              23       9       0      68
```

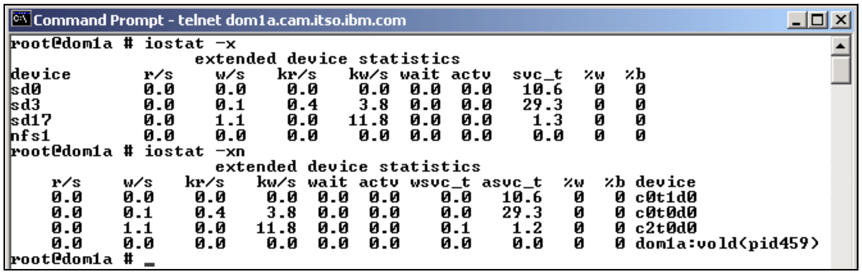
Figure 6-8 Output of the sar utility

You can specify a repetition count to monitor many intervals in succession; for example, **`sar -du 15 8`** records and outputs the same statistics for eight successive 15-second intervals, followed by a report of the averages over the entire two-minute period. It is also common to use a command such as **`sar -du 10 1000`** and cancel it with CTRL+C after a while.

Although **`sar`** reports many of the same statistics as **`vmstat`** and **`iostat`**, it does not always display them in quite the same way or in the same units. For example, **`iostat`** reports the kilobytes per second read from and written to a device, but **`sar`** displays the combined input and output rate, and expresses it in 512-byte blocks per second instead of kilobytes per second. Be alert for such differences.

The figure also shows that **`sar`** uses yet another scheme for identifying I/O devices. The rest of this section describes how to translate **`sar`**'s device names to the `c1t2d3s4` form used elsewhere, so you can then use **`df`** as shown in previous sections to determine which file system the statistics pertain to.

The simplest way to translate between the two forms of device names is to run both **`iostat -x`** and **`iostat -xn`**, as shown in Figure 6-9 on page 220. The first command displays the device names in the form **`sar`** uses, and the second rearranges the output a bit and displays the familiar `c1t2d3s4` form. The important point is that both commands display the devices in the same order. Reading from top to bottom in each set of output, we see that on this system `sd0` is `c0t1d0`, `sd3` is `c0t0d0`, and `sd17` is `c2t0d0`.



```
root@dom1a # iostat -x
                  extended device statistics
device        r/s    w/s   kr/s    kw/s wait actv  svc_t  %w  %b
sd0           0.0    0.0    0.0     0.0  0.0  0.0   10.6   0   0
sd3           0.0    0.1    0.4     3.8  0.0  0.0   29.3   0   0
sd17          0.0    1.1    0.0    11.8  0.0  0.0    1.3   0   0
nfs1          0.0    0.0    0.0     0.0  0.0  0.0    0.0   0   0
root@dom1a # iostat -xn
                    extended device statistics
    r/s    w/s   kr/s   kw/s wait actv wsvc_t asvc_t  %w  %b device
    0.0    0.0    0.0    0.0  0.0  0.0    0.0   10.6   0   0 c0t1d0
    0.0    0.1    0.4    3.8  0.0  0.0    0.0   29.3   0   0 c0t0d0
    0.0    1.1    0.0   11.8  0.0  0.0    0.1    1.2   0   0 c2t0d0
    0.0    0.0    0.0    0.0  0.0  0.0    0.0    0.0   0   0 dom1a:vold(pid459)
root@dom1a # _
```

Figure 6-9 Translating device names

The remainder of the translation is straightforward. **sar** designates each disk partition with a comma and a single letter from a to h; these correspond to the “slice numbers” s0 through s7 of the familiar names. Putting it all together, we see that sd3,b is c0t0d0s1. (You could also have found this by using **iostat -xp** and **iostat -xpn** and matching the output lines as described above, but on systems with many disks each **iostat** will produce a lot of output, making it hard to match up things without a misstep.)

After you have established the correspondence between the two forms of device names and the file systems mounted on the devices, it is a good idea to make a simple translation table such as Table 6-1. (The device names might change if you add or remove devices and perform a reconfiguration boot by using **boot -r** at the system console prompt or by using **touch /reconfigure** before any Solaris reboot.)

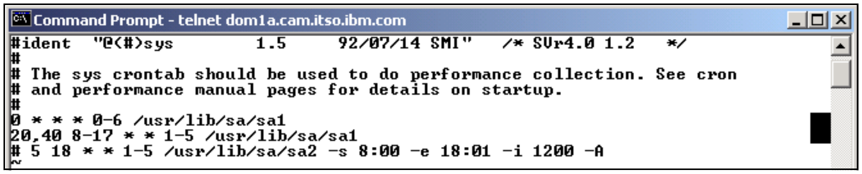
Table 6-1 Translation table example

c0t1d0s7	sd0,h	/export/home	Solaris user accounts
c0t0d0s0	sd3,a	/	Solaris boot partition
c0t0d0s1	sd3,b		Solaris swap partition
c2t0d0s3	sd17,d	/notes/log1a	dom1a transactional logs
c2t0d0s4	sd17,e	/notes/log2b	dom2b transactional logs
c2t0d0s5	sd17,f	/notes/dom1a	dom1a server home
c2t0d0s6	sd17,g	/notes/dom2b	dom2b server home

6.2.4 Long-term monitoring with sar

The real benefit of becoming familiar with **sar** is that you can arrange for it to capture system statistics on a regular basis and record them for later display. If a system that was once performing well starts behaving poorly, it can be useful to examine statistics from the good and bad times to see what has changed. You can also mine the collected data to monitor trends in the system's performance.

To enable automatic recording of system statistics, use the **`crontab -e sys`** command to edit the **`cron`** table of the fictitious user `sys`. In a freshly installed Solaris, all table entries are commented out; remove the comment characters from the two lines just before the last, as shown in Figure 6-10, then save the edited file. This causes **`sar`** to record performance statistics once an hour every day, and once every 20 minutes between 8 AM and 5 PM Monday through Friday. If you choose to uncomment the final line, too, it will also generate a summary report for each weekday. For more information about editing **`cron`** tables, use **`man crontab`**.

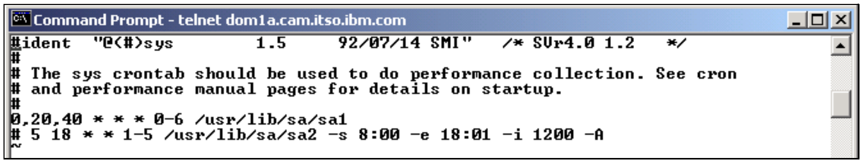


```
#ident  "@(#)sys        1.5     92/07/14 SMI"   /* SVr4.0 1.2   */
#
# The sys crontab should be used to do performance collection. See cron
# and performance manual pages for details on startup.
#
0 * * * 0-6 /usr/lib/sa/sa1
20,40 8-17 * * 1-5 /usr/lib/sa/sa1
# 5 18 * * 1-5 /usr/lib/sa/sa2 -s 8:00 -e 18:01 -i 1200 -A
~
```

Figure 6-10 Enabling automatic statistics collection

Each day's collected data is recorded in /var/adm/sa/sa*dd*, where *dd* represents the day of the month, 01 through 31. Thus, the collected data remains available for a month before it is replaced with data from the following month. Use a command such as **`sar -f /var/adm/sa/sa19 -s 11:00 -e 13:00`** to examine the archived data; this example displays the statistics recorded on the nineteenth of the month between 11 AM and 1 PM, All of the usual **`sar`** options are available for choosing the statistics to be displayed; use **`man sar`** and **`man -s1m sar`** for more information.

The collection schedule that ships with Solaris dates from an era of small disks and nine-to-five workdays. In today's networked world in which users may access your server from any time zone, it is advisable to capture performance data around the clock and on every day. Fortunately, today's vastly larger disks have plenty of storage to spare. The exact amount of space required for the recorded data depends on how many disk devices are present, but will usually come to less than a megabyte a day, less than 25 megabytes per month. To enable a more comprehensive recording schedule, use **`crontab -e sys`** and edit the table as shown in Figure 6-11 on page 222. This schedule records performance statistics every 20 minutes, around the clock, every day of the week.



```
#ident  "@(#)sys        1.5     92/07/14 SMI"   /* SVr4.0 1.2   */
#
# The sys crontab should be used to do performance collection. See cron
# and performance manual pages for details on startup.
#
0,20,40 * * * 0-6 /usr/lib/sa/sa1
# 5 18 * * 1-5 /usr/lib/sa/sa2 -s 8:00 -e 18:01 -i 1200 -A
~
```

Figure 6-11 Customizing statistics collection

For further information about customizing the collection schedules, use **`man -s1m sar`** and **`man crontab`**.

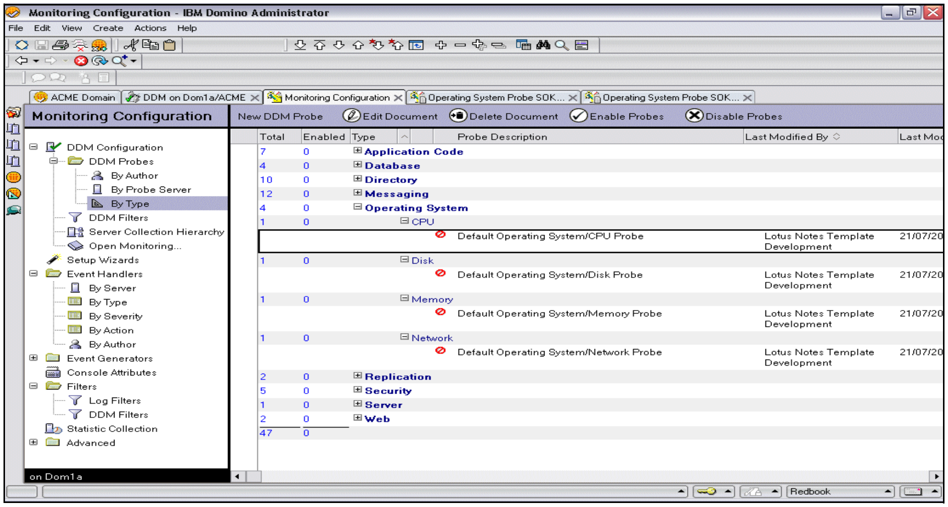
6.3 Monitoring Domino

A new tool was introduced in Domino 7 named *Domino Domain Monitoring* (DDM). This tool enables you to monitor a whole Domino environment and consolidate the monitoring data in one place. Also it introduces new autonomic computing features to the Domino server.

> **Tip:** Domino 7 is capable of reporting Domino Domain Monitoring operating system events to Tivoli Enterprise™ Console. This capability is possible because the new OS probes were implemented using the Tivoli Autonomic Management Engine. As of Domino 7.0, all other Domino domain monitoring probes do not use Tivoli Autonomic Management Engine, which is why other events do not get forwarded to Tivoli Enterprise Console®.

Out of the box probes

Basically there are four O/S probes out of the box (Figure 6-12).



Total	Enabled	Type	Probe Description	Last Modified By	Last Mod
7	0	⊞ **Application Code**			
4	0	⊞ **Database**			
10	0	⊞ **Directory**			
12	0	⊞ **Messaging**			
4	0	⊟ **Operating System**			
1	0	⊟ CPU			
		⊘	Default Operating System/CPU Probe	Lotus Notes Template Development	21/07/20
1	0	⊟ Disk			
		⊘	Default Operating System/Disk Probe	Lotus Notes Template Development	21/07/20
1	0	⊟ Memory			
		⊘	Default Operating System/Memory Probe	Lotus Notes Template Development	21/07/20
1	0	⊟ Network			
		⊘	Default Operating System/Network Probe	Lotus Notes Template Development	21/07/20
2	0	⊞ **Replication**			
5	0	⊞ **Security**			
1	0	⊞ **Server**			
2	0	⊞ **Web**			
47	0				

Figure 6-12 O/S probes

- CPU: The default thresholds for Solaris are a reasonable starting point, if a bit conservative. We suggest you run for a while with the thresholds at their default settings, and then raise them a bit if you get too many false alarms. See the discussion of CPU indicators in 6.2.1, “The vmstat utility” on page 213.
- Disk: The built-in disk probe applies the same threshold values to all disks on the system, which we feel is not flexible enough for effective monitoring. As described in 6.2.2, “The iostat utility” on page 216, we feel that disk performance requirements depend on the disk’s duty. If you wish to monitor a particular disk, consider setting the thresholds appropriately for that disk’s use and filtering out the alerts for other disks.
- Memory: We believe that the default thresholds are too high, and should be lowered. See the discussion of the sr statistic in 6.2.1, “The vmstat utility” on page 213.
- Network: Proper threshold settings depend on the nature of the server’s network connections. The default values are appropriate for old-style CSMA shared Ethernet. For the switched networks that are all but universal today, the utilization thresholds can be raised significantly but the collision rate thresholds should be lowered drastically: A switched network should have no collisions at all, and if any occur it is a sign of possible hardware failure.

For further information about DDM and how to model and set up a monitoring environment, refer to the Domino Domain Monitoring Redpaper at:

http://www.redbooks.ibm.com/redpieces/abstracts/redp4089.html

Also, the Activity Trend feature introduced in Domino 6 is helpful to analyze trend loads and resource utilization patterns, and to predict environment growth.

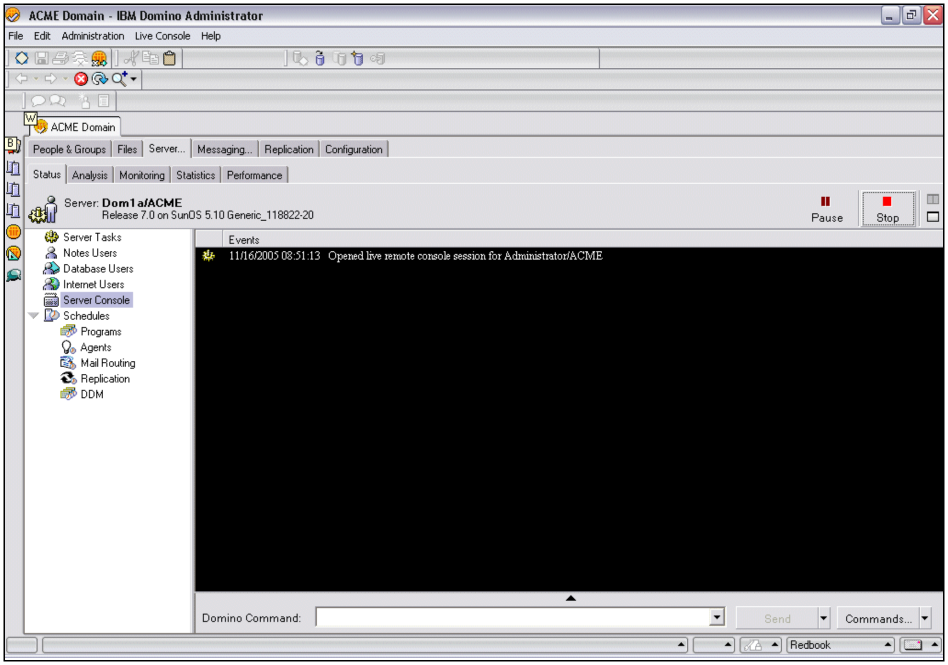
6.3.1 Monitoring operational system resources

Although we do not recommend relying *only* on the Domino statistics flags when you monitor the operational system resources, using statistics collected by Domino can be helpful to alert administrators of emergency issues that are critical for the server operation and are usually a good approach to address issues proactively.

Most of the Solaris statistics are preset to be used in the event4.nsf database, but some have to be manually configured.

Manually configuring OS statistics

1. Open the Administrator client and connect to the Domino server. Start the server console.

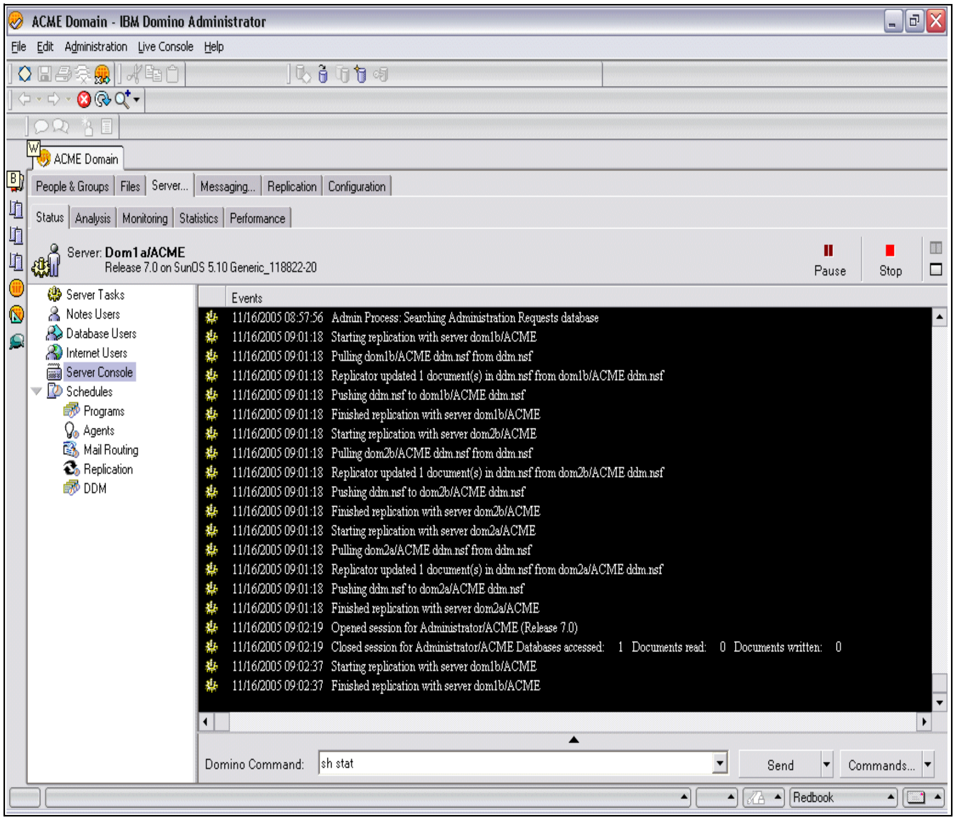


Server: Dom1a/ACME
Release 7.0 on SunOS 5.10 Generic_118822-20

```
11/16/2005 08:51:13   Opened live remote console session for Administrator/ACME
```

Figure 6-13 Opening the administrator client

2. In the console, issue the command **`show stat`**, which presents all available system stats.



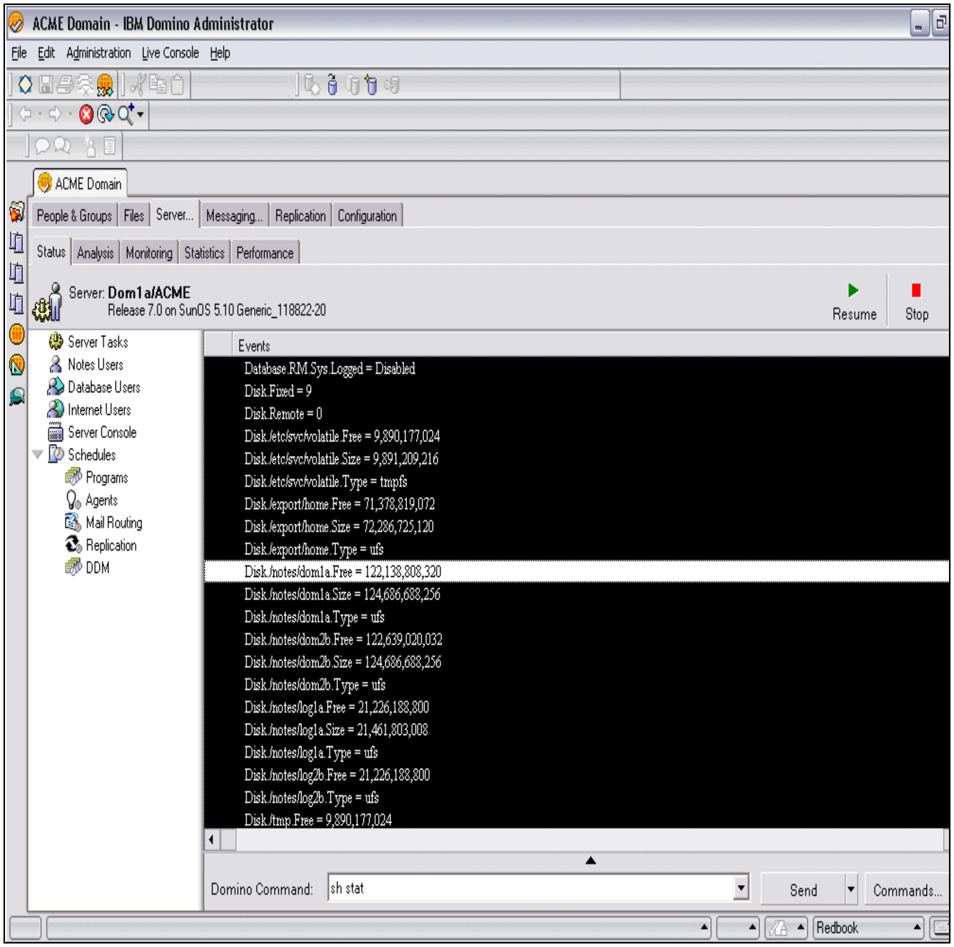
Server: Dom1a/ACME
Release 7.0 on SunOS 5.10 Generic_118822-20

```
11/16/2005 08:57:56 Admin Process: Searching Administration Requests database
11/16/2005 09:01:18 Starting replication with server dom1b/ACME
11/16/2005 09:01:18 Pulling dom1b/ACME ddm.nsf from ddm.nsf
11/16/2005 09:01:18 Replicator updated 1 document(s) in ddm.nsf from dom1b/ACME ddm.nsf
11/16/2005 09:01:18 Pushing ddm.nsf to dom1b/ACME ddm.nsf
11/16/2005 09:01:18 Finished replication with server dom1b/ACME
11/16/2005 09:01:18 Starting replication with server dom2b/ACME
11/16/2005 09:01:18 Pulling dom2b/ACME ddm.nsf from ddm.nsf
11/16/2005 09:01:18 Replicator updated 1 document(s) in ddm.nsf from dom2b/ACME ddm.nsf
11/16/2005 09:01:18 Pushing ddm.nsf to dom2b/ACME ddm.nsf
11/16/2005 09:01:18 Finished replication with server dom2b/ACME
11/16/2005 09:01:18 Starting replication with server dom2a/ACME
11/16/2005 09:01:18 Pulling dom2a/ACME ddm.nsf from ddm.nsf
11/16/2005 09:01:18 Replicator updated 1 document(s) in ddm.nsf from dom2a/ACME ddm.nsf
11/16/2005 09:01:18 Pushing ddm.nsf to dom2a/ACME ddm.nsf
11/16/2005 09:01:18 Finished replication with server dom2a/ACME
11/16/2005 09:02:19 Opened session for Administrator/ACME (Release 7.0)
11/16/2005 09:02:19 Closed session for Administrator/ACME Databases accessed:    1  Documents read:    0  Documents written:    0
11/16/2005 09:02:37 Starting replication with server dom1b/ACME
11/16/2005 09:02:37 Finished replication with server dom1b/ACME
```

Domino Command: sh stat

Figure 6-14 Issuing the show stat command

3. Pause the server console and locate the stat you want to monitor. In our example, we configure Domino partition free disk space. Usually these stats are preconfigured to Windows servers, but not for UNIX systems. If it is a Domino partitioned installation, you have to locate the mounted partition that your Domino is running on.



Server: Dom1a/ACME
Release 7.0 on SunOS 5.10 Generic_118822-20

```
Database.RM.Sys.Logged = Disabled
Disk.Fixed = 9
Disk.Remote = 0
Disk./etc/svc/volatile.Free = 9,890,177,024
Disk./etc/svc/volatile.Size = 9,891,209,216
Disk./etc/svc/volatile.Type = tmpfs
Disk./export/home.Free = 71,378,819,072
Disk./export/home.Size = 72,286,725,120
Disk./export/home.Type = ufs
Disk./notes/dom1a.Free = 122,138,808,320
Disk./notes/dom1a.Size = 124,686,688,256
Disk./notes/dom1a.Type = ufs
Disk./notes/dom2b.Free = 122,639,020,032
Disk./notes/dom2b.Size = 124,686,688,256
Disk./notes/dom2b.Type = ufs
Disk./notes/log1a.Free = 21,226,188,800
Disk./notes/log1a.Size = 21,461,803,008
Disk./notes/log1a.Type = ufs
Disk./notes/log2b.Free = 21,226,188,800
Disk./notes/log2b.Type = ufs
Disk./tmp.Free = 9,890,177,024
```

Domino Command: sh stat

Figure 6-15 Locating stat that will be configured

7

Clustering

A Domino cluster links multiple Domino servers together so that they appear as one resource from the client perspective. The cluster functions as a “single” provider of resources, enabling client requests to be processed in a timely manner.

If any given server is unavailable or too busy when the request arrives, the cluster transparently passes the request to a server that is capable of handling the work.

The cluster members can be on a mixture of the supported Domino platforms, including Windows NT®, various UNIX systems, IBM AS/400®, and OS/2. The clusters support Notes clients only.

Domino clustering is accomplished entirely at the application level. No special hardware is needed, but be aware that you have to add resources to your system (CPU and RAM). Clustering has to be considered in the sizing of a system.

Domino clusters replicate database changes to all replica copies of the database as the changes occur. This synchronization of cluster components is key to Domino’s high availability. This style of replication is referred to as event-driven (immediate) replication, in contrast to standard replication that occurs on a schedule. Event-driven replication is a function of the cluster replicator.

© Copyright IBM Corp. 2006. All rights reserved.

7.1 Domino cluster components

These are the components of a Domino cluster.

Cluster Manager

The Cluster Manager resides on each cluster member and is responsible for exchanging messages with other cluster members (probes) to determine who is available in the cluster and their current capacity. The Cluster Manager decides where to send a connection request based on this data and reports server status to other cluster members.

Cluster Administration

Cluster Administration creates the database cldbdir.nsf, which defines the databases contained within the cluster. The other components of clustering use this database to perform their functions. Cluster Replicator uses this database to decide which databases to replicate.

Cluster Replicator

Cluster Replicator handles the replication of the databases within the cluster. Replication in clustering is event-driven: When a change is made to a database, the Cluster Replicator immediately propagates the change to the other cluster members.

Internet Cluster Manager

The Internet Cluster Manager (ICM) enables you to use Domino clusters to provide failover and workload balancing to HTTP clients (Internet browsers) when they access Domino Web servers. This makes your Web servers and databases highly available to clients. You can run the ICM on a Lotus Domino 7 Enterprise server, a Lotus Domino 7 Utility server, a Lotus Domino 6 or 6.5 Enterprise server, a Lotus Domino 6 or 6.5 Utility server, or a Domino Release 5 Enterprise Server. Install and configure Domino clusters as you normally would, then configure the ICM. The ICM supports the HTTP and HTTPS protocols.

The ICM acts as an intermediary between HTTP clients and the Domino Web servers in a cluster. When Domino Web servers are running in a cluster, they generate URLs that direct HTTP client requests to the ICM. The ICM maintains information about the availability of servers and databases in the cluster. When the ICM receives a client request, it redirects the client to the most available server that contains a replica of the requested database.

The ICM sends periodic probes to the Web servers in the cluster to determine their status and availability. When the ICM receives a client request, it looks at the information in the Cluster Database Directory to find a server that contains the requested database. The ICM determines the most available server that contains the requested database and then redirects the client to that server. This results in the client closing the session with the ICM and opening a new session with the selected server. The user might see this as a change in the host name in the URL. The user might also see the path to the database change in the URL because the database might have a different path on the target server.

Note: Network dispatchers and load balance software can be used to cluster Internet protocols, but the Domino Cluster is the only tool to cluster NRPC.

7.2 Workload balancing

With clustering, multiple copies of databases on multiple servers provide high availability. In addition, Domino distributes the workload between the cluster members (this is called workload balancing), allowing for lower overall response times and more consistency in response times during peak intervals.

Domino clusters provide workload balancing by redistributing user requests to an overloaded server to other servers in the cluster that have available capacity. To optimize workload balancing, you can modify the following settings:

- Database distribution
- Server availability index limit (parameter `SERVER_AVAILABILITY_THRESHOLD`)
- Location document of the clients (specify different home servers)
- Maximum number of concurrent users in a server (parameter `SERVER_MAXUSERS`)

Database distribution

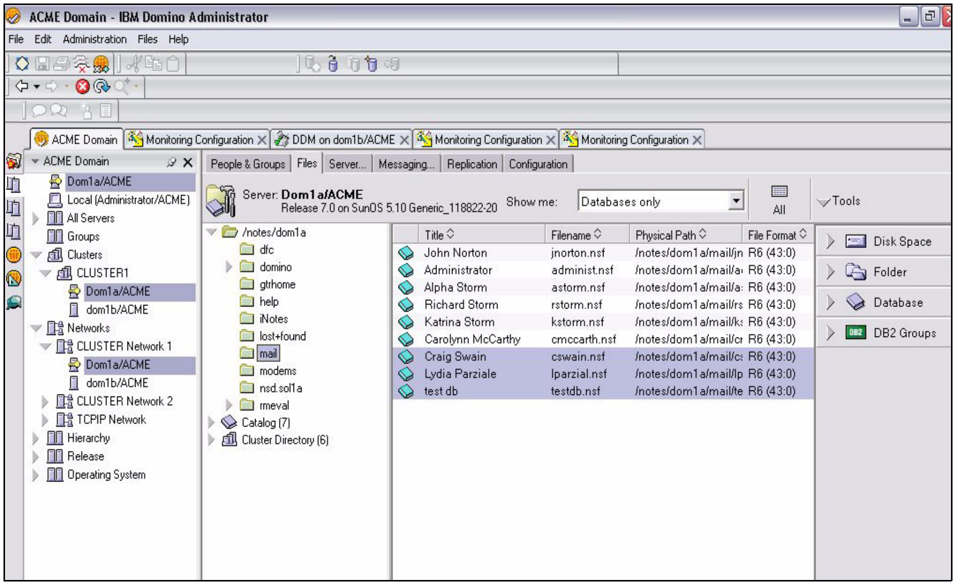
Make sure that you distribute databases evenly in the cluster. When a server in the cluster fails or becomes overloaded, user requests automatically redirect to other servers in the cluster.

Ideally, this load should be spread equally across all other servers in the cluster. However, this can happen only when replicas of the databases on the failed server are spread roughly equally across the other servers in the cluster.

Note that if you distribute the databases evenly across the servers, you are assuming that the databases have about the same activity. If you have power users or particularly active databases, you might need to fine tune the distribution of those databases to make the activity on each server approximately equal.

You can use the Administration Process to make database distribution easier:

1. Open the administrator client. Select the source server, open the tab for your current domain, and click on the pushpin icon.
2. Hold down the CTRL key while you select as many databases as you want to create new replicas for. Drag them over the server you want to be the destination of the new replicas.



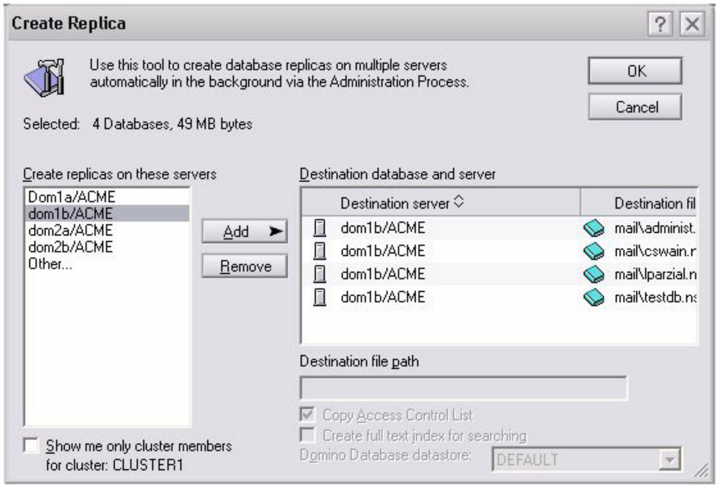
Server: **Dom1a/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

Show me: Databases only

Title	Filename	Physical Path	File Format
John Norton	jnorton.nsf	/notes/dom1a/mail/jn	R6 (43:0)
Administrator	administ.nsf	/notes/dom1a/mail/a	R6 (43:0)
Alpha Storm	astorm.nsf	/notes/dom1a/mail/a	R6 (43:0)
Richard Storm	rstorm.nsf	/notes/dom1a/mail/rs	R6 (43:0)
Katrina Storm	kstorm.nsf	/notes/dom1a/mail/k	R6 (43:0)
Carolynn McCarthy	cmccarth.nsf	/notes/dom1a/mail/c	R6 (43:0)
Craig Swain	cswain.nsf	/notes/dom1a/mail/c	R6 (43:0)
Lydia Parziale	lparzial.nsf	/notes/dom1a/mail/lp	R6 (43:0)
test db	testdb.nsf	/notes/dom1a/mail/te	R6 (43:0)

Figure 7-1 Domino administrator files tab

3. The databases are replicated by the Administration Process. Check for possible errors in the admin4.nsf database from the administration server in the Domino Directory.



Use this tool to create database replicas on multiple servers automatically in the background via the Administration Process.

Selected: 4 Databases, 49 MB bytes

Create replicas on these servers

- Dom1a/ACME
- dom1b/ACME
- dom2a/ACME
- dom2b/ACME
- Other...

Destination database and server

Destination server	Destination fil
dom1b/ACME	mail\administ.
dom1b/ACME	mail\cswain.r
dom1b/ACME	mail\lparzial.n
dom1b/ACME	mail\testdb.ns

Destination file path

☑ Copy Access Control List

□ Create full text index for searching

Domino Database datastore: DEFAULT

□ Show me only cluster members for cluster: CLUSTER1

Figure 7-2 Distributing a database in the Domino cluster

7.2.1 Clustering over a WAN

A cluster over a wide area network (WAN) works the same way as a cluster on a LAN. However, if you have a low-speed WAN, you should consider disabling cluster replication. Instead, use scheduled replication more frequently than usual, such as every hour. This reduces WAN traffic, bottlenecks, and the cost of continual transmission.

Also keep in mind that Domino fails over to the most available server in the cluster, not the closest server. For example, if you have three servers — one in Boston, one in New York, and one in Hong Kong — the Boston server would fail over to the Hong Kong server if it is more available than the New York server. You can control this behavior to some extent by changing the server availability thresholds on the cluster servers.

Using a cluster over a WAN is a good idea for disaster planning. Having emergency backup servers at different locations is a good way to ensure that necessary data is always available when you need it.

7.3 Server availability index

Each server in a cluster periodically determines its own workload based on the response time of the requests the server has processed recently. The workload is expressed as a number from 0 to 100, where 0 indicates a heavily loaded server and 100 indicates a lightly loaded server. This number is called the server availability index. As response times increase, the server availability index decreases.

The server availability index is based on the expansion factor, which indicates the current workload on a server. The expansion factor is determined by comparing recent response times for specific types of transactions to the minimum time in which the server has ever completed the same types of transactions. For example, if the server is currently averaging 12 microseconds to perform Database Open transactions, but the minimum time the server has ever performed a Database Open transaction is 3 microseconds, the expansion factor for Database Open transactions would be 4 (the current time of 12 microseconds divided by the fastest time of 3 microseconds). In other words, the expansion factor determines how many times longer it takes for a transaction to complete currently than it takes under optimal conditions.

> **Note:** It was brought to our attention that the Administrator Help file documentation indicates that the SAI calculation is a linear indication of the amount of resources being used. After further investigation it was noticed that this information is not completely true and in fact SAI is not a linear number. It represents a calculation based in a resource average estimate. For example, if SAI is equal to 65, that means you have less then 35% of free resources, and not 35% free as the Help files indicates.

Domino stores the minimum time for each type of transaction in memory and in the loadmon.ncf file, which the server reads each time it starts. When the server shuts down, Domino updates the loadmon.ncf file with the latest information.

> **Important:** Remember to delete loadmon.ncf in case of a version upgrade. The cluster service will create a new one and this will prevent version conflicts.

To determine the current expansion factor, Domino tracks the most commonly used types of Domino transactions for specified periods of time. By default, Domino tracks these transactions for five periods of 15 seconds each. Domino then determines the average time it took to complete each type of transaction and divides that time by the minimum time it ever took to complete that same type of transaction. This determines an expansion factor for each type of transaction. To determine the expansion factor for the entire server, Domino averages the expansion factors for all the types of transactions, giving a heavier weighting to the most frequently used types of transactions.

As the server gets busier, adding more load has an increasingly greater effect on performance and availability. Thus, adding more load to a busy server increases the expansion factor faster than adding more load to a less busy server.

Because servers differ in speed, capacity, and power, servers also differ in the workload they can handle. Therefore, the same expansion factor on two different servers does not necessarily indicate the same workload relative to the ability of the servers. For example, on a small server that takes a long time to perform transactions when the server is otherwise idle, an expansion factor of 40 might indicate that users are waiting many seconds for responses. On a very large, fast server, however, an expansion factor of 400 might indicate that users are waiting less than a second for responses.

7.3.1 How the availability index compares to the expansion factor

To determine the availability index, Domino uses a formula that converts the expansion factor into an approximation of the percentage of the total server capacity that is still available. Table 7-1 shows a few examples of expansion factors converted to availability indexes.

Note: The values in the table are based an expansion factor of 64 indicating a fully loaded server.

Table 7-1 Expansion factors converted to availability indexes

Expansion factor	Availability index
1	100
2	83
4	67
8	50
16	33
32	17
64	0

Note: The expansion factor and the availability index measure only the response time of the server, which is usually only a small portion of the response time clients experience. For example, the network response time between a client and a server often accounts for a significant portion of the response time the client experiences.

7.3.2 Changing the value of the expansion factor that indicates a fully loaded server

To use Domino workload balancing effectively, you must adjust the relationship between the expansion factor and the availability index so that servers fail over when they reach the workload at which you want them to fail over. You do this by specifying the expansion factor value that you want to represent a fully loaded server. The default value in Domino is 64. When the expansion factor reaches that value, the server is considered to be fully loaded, and the availability index drops to 0 (zero).

Note: You can use the **`Show AI`** server command to view a suggested availability index setting.

If your server is particularly powerful and fast, you might want to increase the value of the expansion factor that is considered fully loaded. On some very fast servers, you might want to make this value several hundred or higher. If your server is particularly slow, you might want to decrease this value.

To change the expansion factor value that indicates a fully loaded server, add the following setting to your notes.ini file, and then restart the server.

```
SERVER_TRANSINFO_RANGE=n
```

For the value of *n*, choose a number such that 2 raised to the power of *n* equals the expansion factor value that you want to indicate a fully loaded server. The default value for *n* is 6, which leads to an expansion factor value of 64 because 2 raised to the 6^{th} power is 64. If you set SERVER_TRANSINFO_RANGE to 7, then the expansion factor value that indicates a fully loaded server becomes 128. If you set SERVER_TRANSINFO_RANGE to 8, the value becomes 256.

To determine the optimal value for SERVER_TRANSINFO_RANGE:

1. During a period of heavy usage, monitor the expansion factor on your server. You can use the console command **`show stat server.expansionfactor`** to do this. You can also monitor performance statistics during these periods. Record enough values for the expansion factor during heavy usage so that

you can determine the expansion factor value you want to indicate a fully loaded server.

2. Determine a value for SERVER_TRANSINFO_RANGE so that 2 raised to the power of that value results in the expansion factor value you chose in step 1.

When you change the expansion factor value that indicates a fully loaded server, the relationship between the expansion factor and the availability index changes. Table 7-2 shows a few examples of expansion factors converted to availability indexes when the value of SERVER_TRANSINFO_RANGE is 8. The maximum expansion factor in this example is 256 because 2 raised to the power of 8 is 256.

Table 7-2 SERVER_TRANSINFO_RANGE = 8

Expansion factor	Availability index
1	100
2	85
4	75
8	63
16	50
32	38
64	25
128	13
256	0

The server console command **`Show AI`** is used to obtain an appropriate value for this variable. Type the command after running the server under load for a while, and it will display the history of the expansion factor and availability index for the server.

7.3.3 Changing the amount of data to compute the expansion factor

Although it is not usually necessary, you can use the following notes.ini settings to change the amount of data that Domino collects in order to figure the expansion factor.

To change the number of data collection periods that Domino uses, use the notes.ini setting `Server_Transinfo_Max=`*`x`* where *`x`* is the number of collection periods you want Domino to use.

To change the length of each data collection period, use the notes.ini setting `Server_Transinfo_Update_Interval=x` where *x* is the length of each period in seconds.

Note: Improvements in the SAI calculation algorithms were made in Domino versions 6 and above that improve the accuracy and, therefore, reliability of the SAI number. This is useful when the load balance feature is used. Based on the SAI, the load balance feature can direct client connection requests to the cluster member with more free resources.

7.4 Failover

In a Domino cluster, if one member of the cluster fails, another member of the cluster transparently assumes the failing member's workload.

This action is called *failover*. Failover is client-driven, and when a client cannot connect to a server it checks in its cluster cache for other servers in the cluster, thus redirecting requests to another server in the cluster that has a replica of the database needed to service the request.

Tip: To quickly test a failover, use the SERVER_RESTRICTED=1 variable from the server console **`set config SERVER_RESTRICTED=1`**. A server in restricted state does not accept any connection. Remember to disable the server restriction by resetting the variable to 0.

7.5 Creating the cluster

The cluster configuration consists of two parts: the configuration of the port that will be used by the server within the cluster and the cluster itself. The correct configuration of the cluster ports ensures more reliability and good performance of the cluster, and well as the rest of the factors mentioned before.

7.5.1 Configuring the cluster ports

We recommend that users create the cluster port from the Administrator client. This helps the system configure the best parameters for your ports settings, such as port compression.

1. Make sure you have administrative rights on the server (at least server administrator access). Open the administrator client to start the configuration.

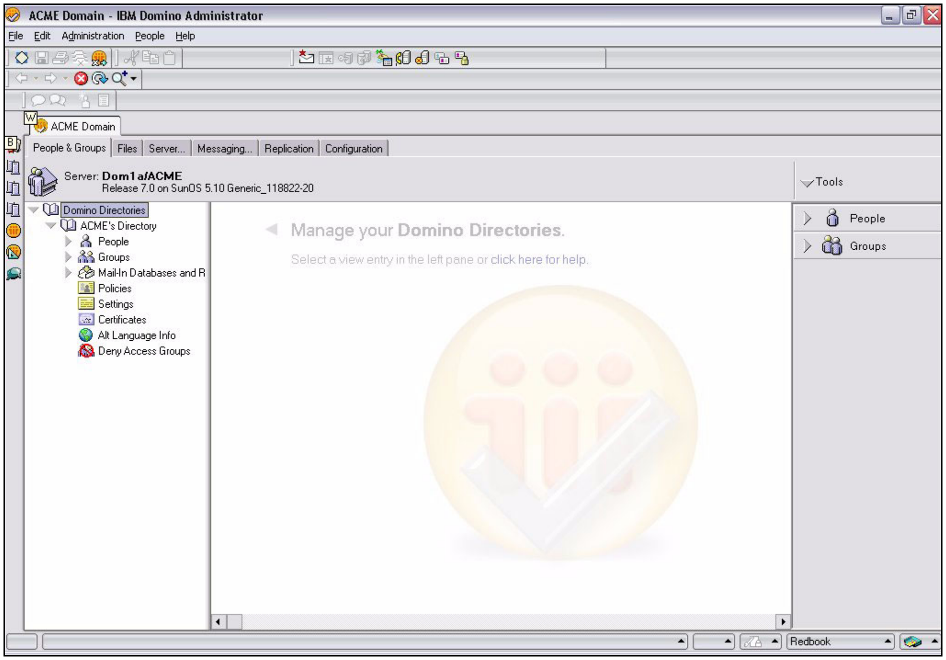


Figure 7-3 Administrator client initial screen

2. Select the server within your Domain to configure the cluster port. You can use the Domain server list on the left pane of the administrator client, or from the menu, select **File** → **Open** server.

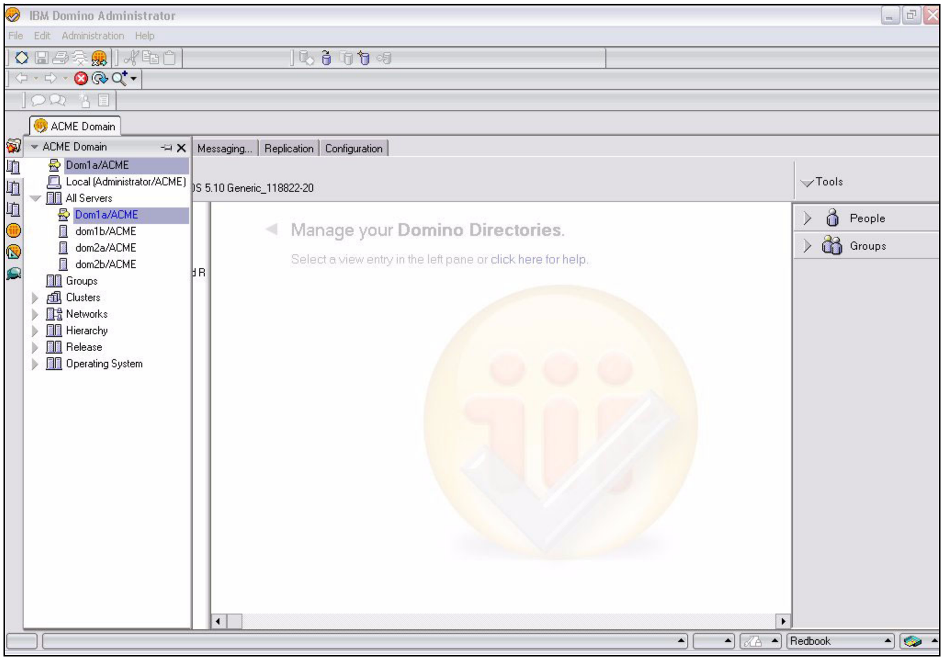
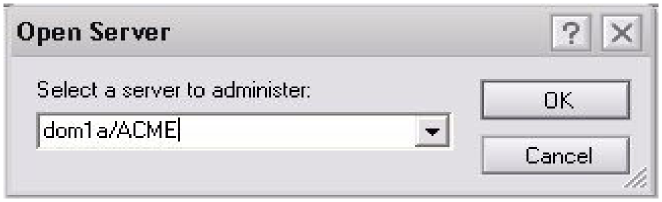

IBM Domino Administrator
File Edit Administration Help
ACME Domain
ACME Domain
Dom1a/ACME
Local (Administrator/ACME)
All Servers
Dom1a/ACME
dom1b/ACME
dom2a/ACME
dom2b/ACME
Groups
Clusters
Networks
Hierarchy
Release
Operating System
Messaging... Replication Configuration
OS 5.10 Generic_118822-20
Manage your Domino Directories.
Select a view entry in the left pane or click here for help.
Tools
People
Groups
Redbook

Figure 7-4 Selecting the server

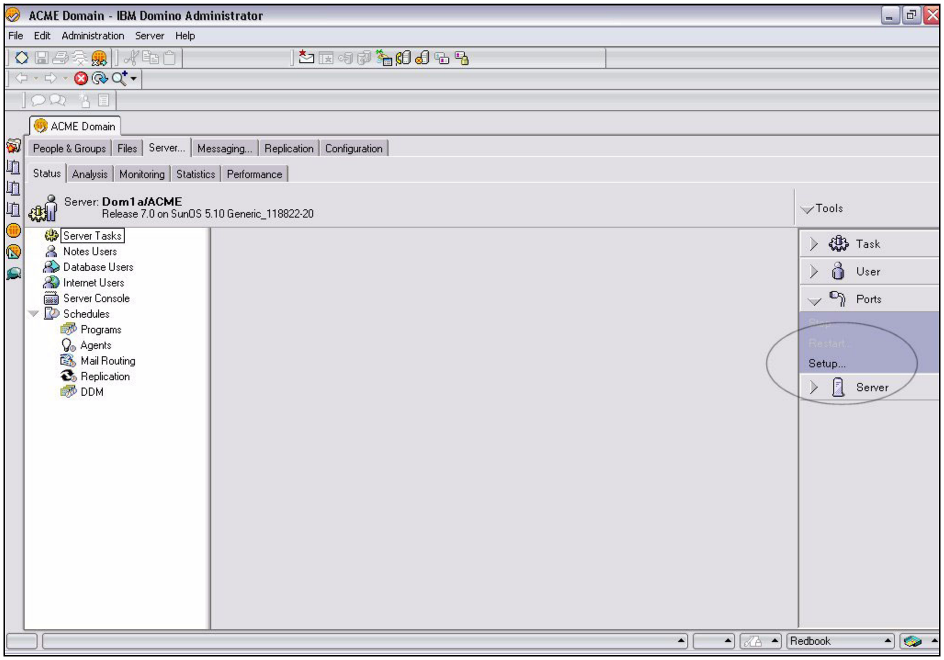
3. You might need to type in the server DNS hostname or IP address, or create a connection document if this is the first time you connect to the server.


Open Server

Select a server to administer: dom1a/ACME

Figure 7-5 Directly selecting the server within the Domino domain

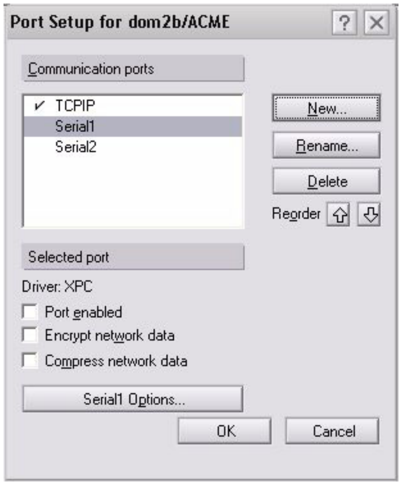
4. Click the **Server** tab. Under the ports configuration, click **Setup** (circled in Figure 7-6) to configure and start the cluster ports.



Server: Dom1a/ACME
Release 7.0 on SunOS 5.10 Generic_118822-20

Figure 7-6   Selecting the port configuration in the Server tab

5. There should be a existing port that the server is using to communicate with the other servers in the environment and the clients. In the Port Setup window, click **New** to set up the new cluster port.



Port Setup for dom2b/ACME

Communication ports

✓ TCPIP
Serial1
Serial2

Selected port

Driver: XPC

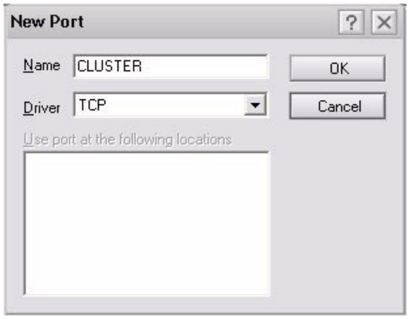
□ Port enabled

□ Encrypt network data

□ Compress network data

Figure 7-7 New port creation

> **Note:** This new port might want to represent a different NIC dedicated only to cluster traffic. This is highly recommended for best results. Also, 1.1 KBps/user is a good start to measure cluster replication traffic load between the cluster members. Although this number is not an absolute reference, you might want to use it as a base and include more users if the environment behaves efficiently.



New Port

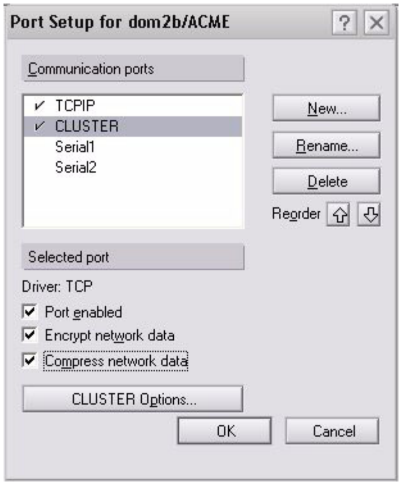
Name: CLUSTER

Driver: TCP

Use port at the following locations

Figure 7-8 Naming the cluster port

Attention: The new cluster port is created, but to ensure that all cluster communication uses only the cluster port, the new port must be reorganized as the first port listed in the Communication ports box list.



Driver: TCP

☑ Port enabled

☑ Encrypt network data

☑ Compress network data

Figure 7-9 New port settings

Depending on your network topology, it might be interesting to enable/disable port compression. If the servers are using a dedicated and fast network segment, it is best to disable network compression to prevent the additional workload required by the compression algorithm.

The port configuration changes will be available after the server is restarted.

The port configuration in notes.ini should look similar to Example 7-1.

Example 7-1 notes.ini port configuration example

```
Ports=CLUSTER,TCPIP
TCPIP=TCP, 0, 15, 0,,32800
TCPIP_TCPIPADDRESS=0,9.33.85.102:1352
CLUSTER=TCP,0,15,0,,45056,
CLUSTER_TCPIPADDRESS=0,192.168.1.102:1352
```

You may also include the Server_Default_Cluster_Port parameter to force the cluster to communicate using the desired cluster port:

```
Server_Default_Cluster_Port=CLUSTER
```

There is a disadvantage to using the Server_Cluster_Default_Port setting to assign a port to the private LAN for cluster traffic. If a cluster server encounters a problem connecting over this port, it will not try another port. Therefore, the server will not be able to communicate or replicate with other cluster servers. You will have to resolve the network problem or remove this setting from the notes.ini file before the server will be able to communicate with the cluster again.

> **Note:** The port configuration must be performed on each server that will belong to the Domino Cluster. Make sure you configure all servers' ports before moving on to the next step.

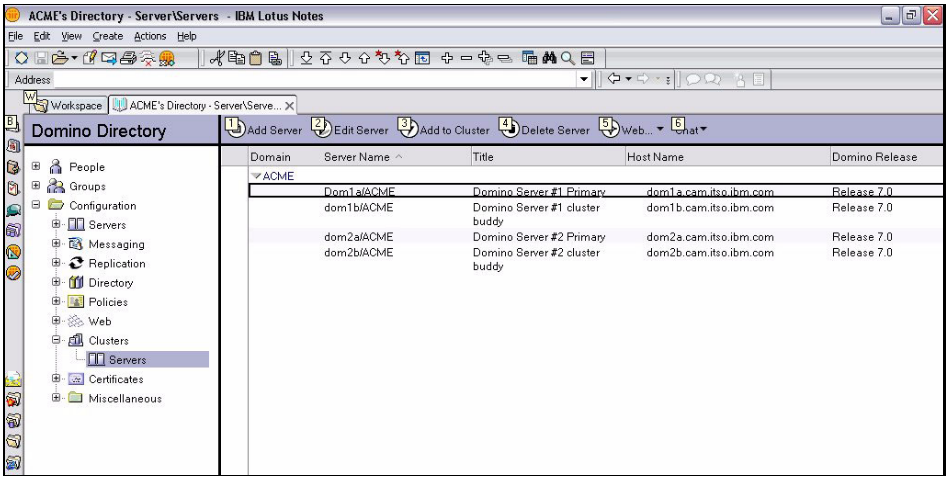
7.5.2 Setting up the Domino Cluster

After port configuration, we move through the steps of the cluster configuration procedure:

1. Open the Domino Directory database (names.nsf) in the administration server.

   > **Note:** Make sure you open the Domino Directory database located at administration server in order to have the administration taking care of the final cluster configurations

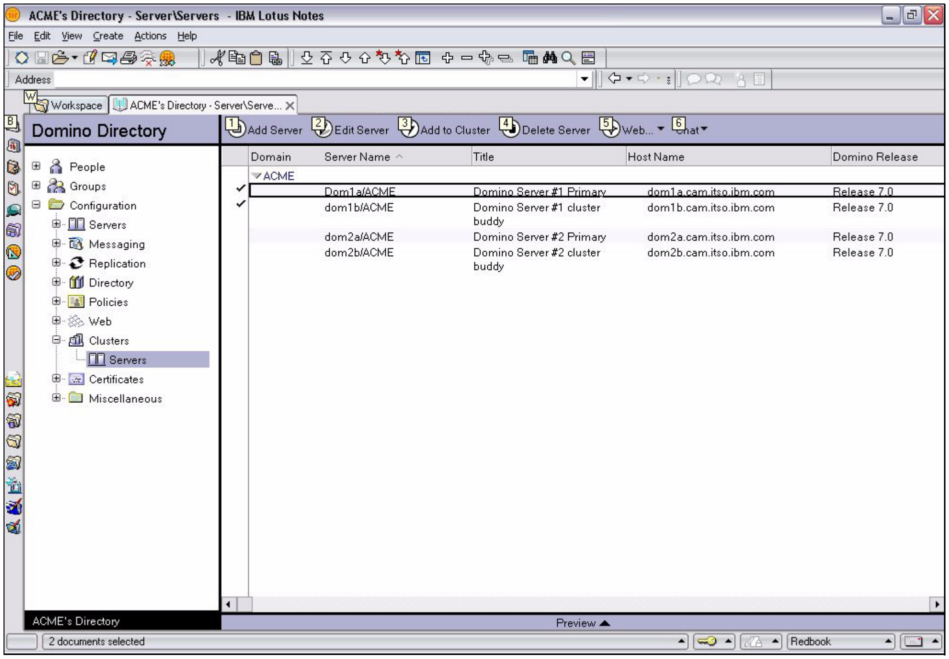
2. Select the view **All Servers Documents** under **Server** → **Configurations** view as in Figure 7-10.



Domain	Server Name	Title	Host Name	Domino Release
ACME				
	Dom1a/ACME	Domino Server #1 Primary	dom1a.cam.itso.ibm.com	Release 7.0
	dom1b/ACME	Domino Server #1 cluster buddy	dom1b.cam.itso.ibm.com	Release 7.0
	dom2a/ACME	Domino Server #2 Primary	dom2a.cam.itso.ibm.com	Release 7.0
	dom2b/ACME	Domino Server #2 cluster buddy	dom2b.cam.itso.ibm.com	Release 7.0

Figure 7-10 Domino Directory database

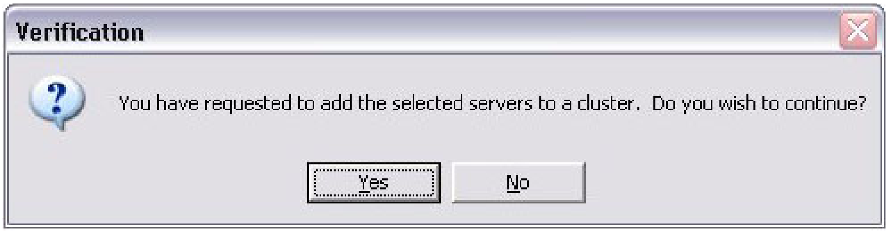
3. Mark the servers that will be clustered and click **Add to Cluster**.



	Domain	Server Name	Title	Host Name	Domino Release
	ACME				
✓		Dom1a/ACME	Domino Server #1 Primary	dom1a.cam.itso.ibm.com	Release 7.0
✓		dom1b/ACME	Domino Server #1 cluster buddy	dom1b.cam.itso.ibm.com	Release 7.0
		dom2a/ACME	Domino Server #2 Primary	dom2a.cam.itso.ibm.com	Release 7.0
		dom2b/ACME	Domino Server #2 cluster buddy	dom2b.cam.itso.ibm.com	Release 7.0

Figure 7-11 Selecting server to be clustered

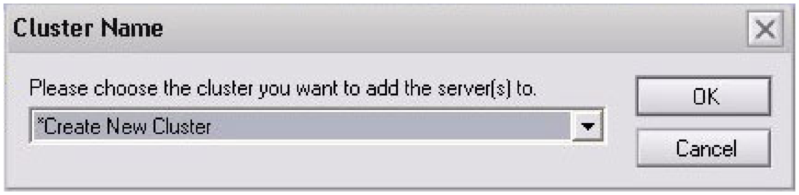
4. If you are sure you marked the right servers, click **Yes**; otherwise click No and reselect the desired servers.



You have requested to add the selected servers to a cluster. Do you wish to continue?

Figure 7-12 Confirming the setup of the selected servers

5. A combo box appears for you to create a new cluster or include another server in a existing Domino Cluster. If this is a new cluster, select ***Create New Cluster** in the pull-down menu**.** If this is a existing server, select the Domino Cluster in which the server or servers will be included.



Cluster Name

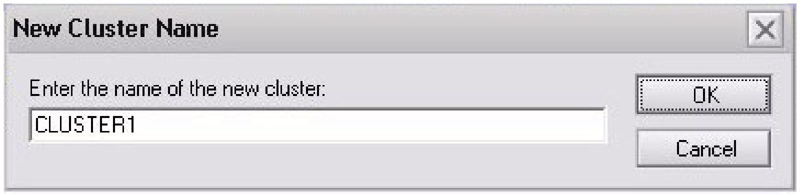
Please choose the cluster you want to add the server(s) to.

*Create New Cluster

Figure 7-13 Setting up the Cluster Name

6. Type the new cluster name and click **OK**.

Attention: Make sure that this cluster name is unique in the Domino Directory.



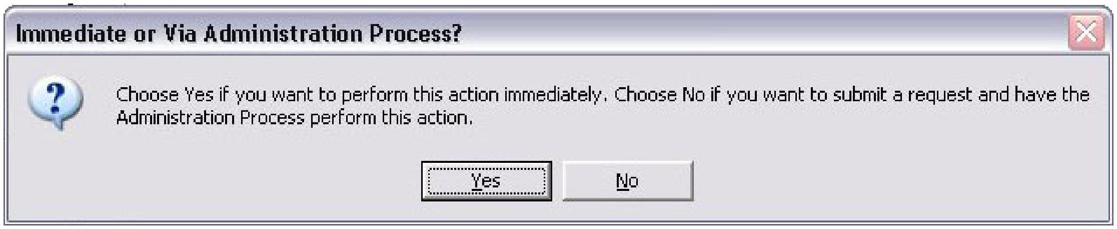
New Cluster Name

Enter the name of the new cluster:

CLUSTER1

Figure 7-14 Naming the cluster

7. The system asks whether you want to create the cluster immediately (click Yes) or let the Administration Process create it for you (click No).



Immediate or Via Administration Process?

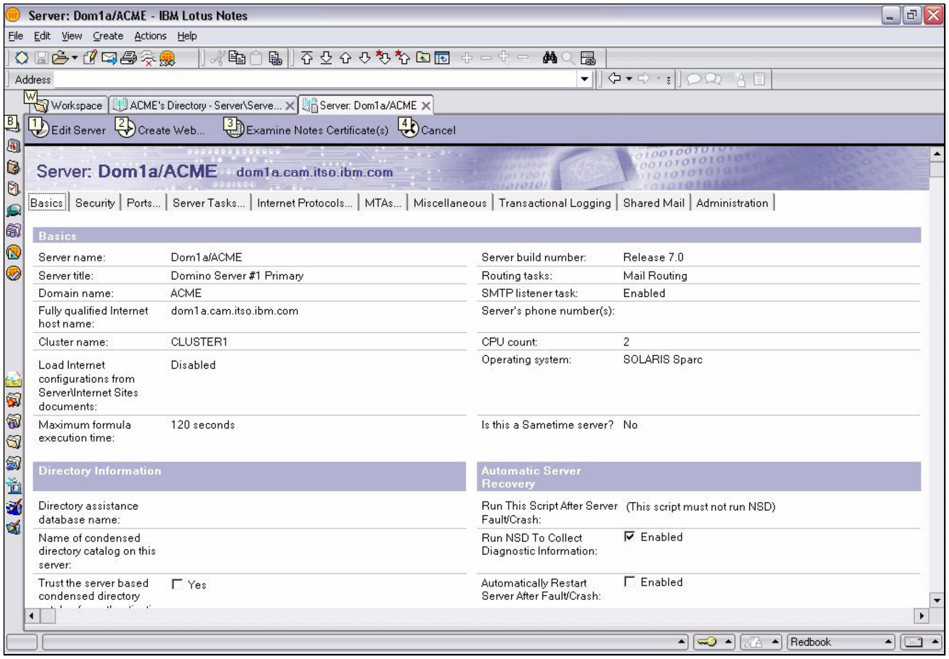
Choose Yes if you want to perform this action immediately. Choose No if you want to submit a request and have the Administration Process perform this action.

Figure 7-15 Creating the cluster using the Administration process

Attention: Use the Administration Process whenever is possible. This automates the rest of the cluster creation and ensures the proper cluster setup across all servers within the Domino Cluster.

7.5.3 Checking the cluster creation and correct replication flow

To check cluster creation, determine whether it was logically created and whether the cluster traffic is being addressed by the right port. This prevents the cluster traffic from creating unnecessary broadcasts in the public segment and helps it to concur with user access.



Server: Dom1a/ACME dom1a.cam.itso.ibm.com

Basics

Server name:	Dom1a/ACME	Server build number:	Release 7.0
Server title:	Domino Server #1 Primary	Routing tasks:	Mail Routing
Domain name:	ACME	SMTP listener task:	Enabled
Fully qualified Internet host name:	dom1a.cam.itso.ibm.com	Server's phone number(s):	
Cluster name:	CLUSTER1	CPU count:	2
Load Internet configurations from Server\Internet Sites documents:	Disabled	Operating system:	SOLARIS Sparc
Maximum formula execution time:	120 seconds	Is this a Sametime server?	No

Directory Information		Automatic Server Recovery	
Directory assistance database name:		Run This Script After Server Fault/Crash:	(This script must not run NSD)
Name of condensed directory catalog on this server:		Run NSD To Collect Diagnostic Information:	☑ Enabled
Trust the server based condensed directory	□ Yes	Automatically Restart Server After Fault/Crash:	□ Enabled

Figure 7-16 Server document of a cluster member

The Administration Process updates the Cluster name field with the name of the newly created Domino Cluster. If the configuration is not updated, confirm that the Administration Process already ran by opening the admin4.nsf database. If it ran, refer to the 7.8, “Troubleshooting” on page 248.

If the process has not run yet, you can manually force processing of the pending requests by issuing the following command in the administration server Domino Console:

```
tell adminp process all
```

Then you can replicate admin4.nsf to all the members of the Domino Cluster.

7.6 Cluster directory database

A replica of the Cluster Database Directory (CLDBDIR.NSF) resides on every server in a cluster. The Cluster Database Directory contains a document about each database and replica in the cluster, as well as such information as the database name, server name, path, and replica ID, and other replication and access information. The cluster components use this information to perform their functions, such as determining failover paths, controlling access to databases, and determining which events to replicate and where to replicate them to.

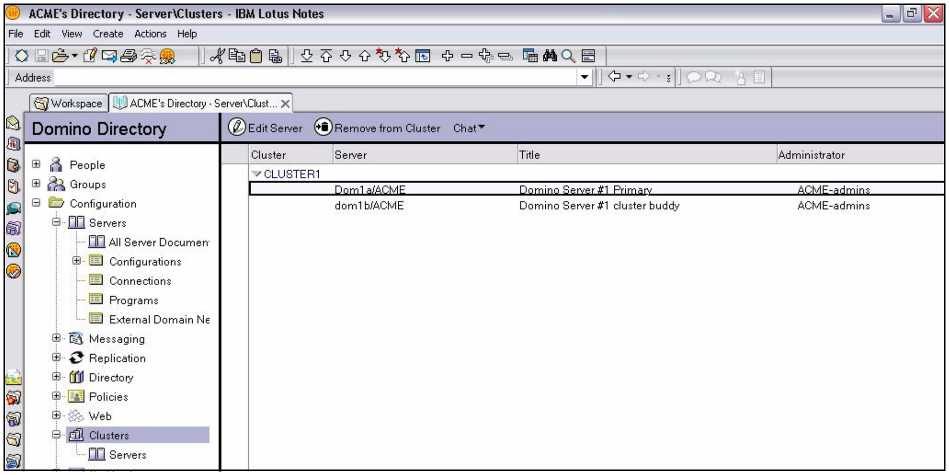
> **Note:** Be sure to disable replication between system databases, unless you know exactly what you are doing. Most of the system databases can be replicated in a normal replication fashion and do not have to be synchronized as regularly as the cluster replication provides.

7.7 Removing a server from a cluster

Use these steps to remove a server from the Domino Cluster.

> **Note:** Do this procedure in the Administration server in the Domino domain.

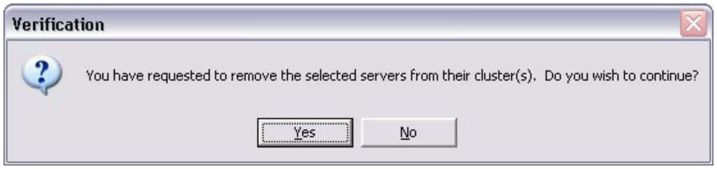
1. Click **Configuration** → **Clusters** in the Domino Directory database (names.nsf) for the Clusters view.
2. Select the servers to be removed from the Cluster, and click **Remove from Cluster**.



Cluster	Server	Title	Administrator
CLUSTER1			
	Dom1a/ACME	Domino Server #1 Primary	ACME-admins
	dom1b/ACME	Domino Server #1 cluster buddy	ACME-admins

Figure 7-17 Cluster view in Domino Directory

3. Click **Yes** to confirm.

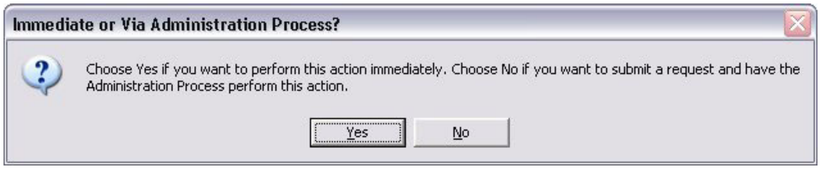


Verification

You have requested to remove the selected servers from their cluster(s). Do you wish to continue?

Figure 7-18 Delete from cluster confirmation screen

4. Choose whether to delete the server from the cluster immediately or use the Administration Process. We recommend using the Administration Process whenever possible.



Immediate or Via Administration Process?

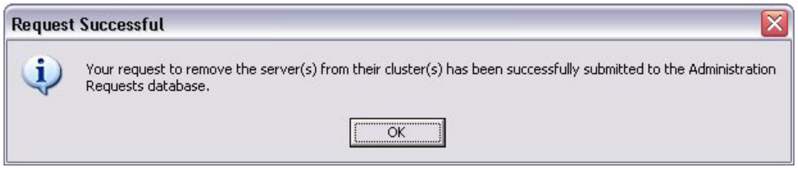
Choose Yes if you want to perform this action immediately. Choose No if you want to submit a request and have the Administration Process perform this action.

Figure 7-19 Delete immediately or using adminp

The cluster processes clrepl and cldbdir are stopped on the server, and the entries are removed from the ServerTasks line in notes.ini.

The database entries in the Cluster Directory database (cldbdir.nsf), for databases on the server being removed, are purged from the replica copy on the least busy of the remaining cluster servers.

The local Cluster Directory database is deleted from the server that is being removed from the cluster.



Request Successful

Your request to remove the server(s) from their cluster(s) has been successfully submitted to the Administration Requests database.

Figure 7-20 Deletion request process success notice

7.8 Troubleshooting

Troubleshooting a cluster can be an exhaustive task because many variables are involved in a cluster setup. Basically we recommended trying to isolate the problem as best as possible, then working with the issue.

7.8.1 Cluster creation/deletion issues

Letting the Administration Process create the cluster for you is the best way to make sure that all cluster setup steps are performed correctly; however, because it relies on the Administration process, every time a problem is noticed, we recommend checking how the Administration Process is behaving across the domain. Be sure the admin4.nsf database is being replicated properly across all of the cluster members and that the Administration Process is running as well. You might need to run updall and compact tasks against the admin4.nsf database at least weekly, because this database is being updated constantly.

7.8.2 Connectivity

Confirm that the members of the cluster can communicate issuing **trace** commands in the problematic server console to the other members in the cluster. Be sure to use the full Domino server names, and issue the same commands using the fully qualified name. Being able to connect through FQN is not required, but could indicate DNS issues.

```
trace DOM1B/ACME
```

Make sure the servers are using the desired NIC selected as the dedicated cluster traffic handler.

7.8.3 Ensuring that cluster replication is using the private LAN

It is also a good idea to check the cluster to be sure that cluster replication is using the private LAN. To do this, you can look at some of the cluster statistics:

1. From the Domino Administrator or the Web Administrator, click the **Statistics** tab under the Server tab.
2. In the list of statistics, expand **NET** and the port name you gave to the cluster.
3. Look for the BytesReceived/BytesSent statistics for the private LAN port.
4. Expand **Replica** and **Cluster**.
5. Expand **SessionBytes**, and look for the In/Out replication statistics for the cluster.

6. Compare the NET.portname.BytesReceived value with the Replica.Cluster.SessionBytes.In value. These values should be fairly close to each other, although they will not be the same.
7. Compare the NET.portname.BytesSent value with the Replica.Cluster.SessionBytes.Out value. These values should also be close to each other. They will not match exactly because the private network is used for more than just cluster replication.

You can fine cluster troubleshooting tips in Administrator Help under **Troubleshooting** → **Troubleshooting the Domino system** → **Clusters - Troubleshooting**.

8

Partitioning

Partitioning is a method of running multiple instances of the IBM Lotus Domino 7 server on a single physical system. The chapter covers how to run multiple instances of Domino with multiple versions of the Domino software. The chapter also covers basic recommendations for sharing resources between the Domino instances.

© Copyright IBM Corp. 2006. All rights reserved.

8.1 Domino partitioning

As with previous releases of Domino, a partitioned Domino server allows multiple instances of Domino on the same physical system. The following releases of Domino support the partitioned server technology:

An additional benefit of the Domino server on UNIX is the ability to run multiple versions of the Domino software on the same physical system. Starting in Domino 6, UNIX servers can support multiple versions of Domino, allowing for the administrator to specify which version of Domino a server instance is running.

Domino 7 server has support for IPv6. A partitioned server's IP address can make use of the IPv6 IP addresses. For more information about this new feature, see "IPv6 and Lotus Domino" in Lotus Domino Administrator 7 Help. The Lotus Domino Administrator 7 Help is available in developerWorks® at:

`http://www.ibm.com/developerworks`

Go to **developerWorks** → **Lotus** → **Technical Library** → **Lotus Documentation**.

Partitioned servers enable the administrator to configure independent data directories to allow for customization of multiple server instances on a single physical system.

Using the example server instances provided in this book, the single physical Server 1 with two Domino instances (dom1a and dom2b) can run two different versions of Domino software. For example, the Domino server instance for dom1a could be configured to run from /opt/ibm7/lotus/bin containing the program files for Domino 7. The second instance of the Domino server could be configured to run /opt/lotus/bin containing the program files for Domino 6.5.4.

As in the past, there are several reasons for implementing partitioned server instances:

- Reduction of operating system and hardware limiting factors. Multiple Domino partition instances make more efficient use of server resources than a single server instance, as certain processes can be run in parallel.
- Segregation of server tasks between server instances. For example, a mail instance server and application instance server can be individually tuned to maximize the performance of required tasks while being run on the same physical hardware.
- Segregation of independent user communities. For example, partitioning enables the hosting of multiple Domino domains or Domino-hosted Web sites on a single physical system.

- Independent operation of services and resources. Partitions operate independently and do not have any effect on each other, enabling the independent administration of each server instance.
- Reduction in administration effort of the platform. There are fewer physical systems to administer for your Solaris administrator.
- The ability to have multiple versions of Domino extends this concept to allow multiple Domino binaries, executables, on the same physical system.
- Multiple versions of Domino on a single physical system enables control over migration from D6 to D7, enabling the administrator to upgrade server instances all at once or as part of a multi-phased deployment.
- Multiple versions of Domino also allow for verification of point releases of Domino without the commitment of upgrading the entire physical system.
- Multiple versions of Domino allow for great flexibility and specialization of Domino server instances within the wider context of a corporate infrastructure.

8.2 Installation

The following example of installing a second server assumes that a Lotus Domino 6.5.4 Enterprise server is installed with a working Domino server instance. This section demonstrates installation of a second server that will use the Lotus Domino 7 Enterprise server program and data files.

Review the “Installation” section of the Lotus Domino Administrator 7 Help and the “Domino Server” → “Installation, migration, upgrade, and configuration” section of the Domino 7 Release Notes. After reading the documentation, gather the following information to install the files for the partitioned server:

- The new location for the Domino 7 program directory, in this example: /opt/ibm7/lotus
- The new location for the Domino 7 data directory, in this example: /notes/dom1a
- The Solaris account and Solaris group that will be used to run the new Domino 7 server instance, in this example: account: sol1a, group: domino.

The Solaris account (or user name) must be an account recognized by Solaris. This account will be made the owner of the files in the data directory, as well as the owner of the processes that are run by that Domino partition.

Note: Using a different user for each Domino partitioned server is recommended to facilitate the administration of the different servers.

1. Make sure the Domino server kit is available from your network or CD-ROM.
2. Log on to the root account for Domino Server installation.
3. Change to the directory containing the install script.
4. Enter this at the root command prompt to run the script:

```
./install
```

Option	Action
Add data directories only	Choose one: Yes to change a single Domino server into a partitioned server or add data directories to an existing partitioned server. No to install Domino Software and create Domino partitions.
Domino Server installation type	Choose the server type in this example Domino Enterprise Server.
Install template files	Choose one: Yes to install new templates.
Configure this server with ASP functionality	Choose one: No if this is not an ASP server.
Program directory	Specify the directory in which Domino will store program files, in this example /opt/ibm7/lotus.
Create /opt/ibm/lotus soft link	Choose one: No if this system will have multiple Domino installations (multiple program directories).
Data directory	Specify the directory in which Domino will store data files. If you are installing a partitioned server, indicate that and specify multiple data directories. Enter /notes/dom1a in this example. Only one data directory is necessary because the first Domino server instance has already been installed.
UNIX user name	Specify the Solaris account that will be responsible for the server configuration data. Because we are installing a partitioned server instance in this example, specify a single Solaris account for the new data directory, such as sol1a.
UNIX group name	Specify the group to which the Solaris account belongs. In this example, specify `domino` for the new data directory.

Refer to Chapter 5, “Installing Lotus Domino 7 on Sun Solaris 10” on page 77 for examples with screen shots.

8.3 Configuring network resources for partitioning

There are three methods of configuring network resources for partitioning:

- Multiple IP address on a single NIC
- Single IP address, single dedicated NIC
- Port mapping (multiple server instances, single IP address on a single NIC)

We believe that the best configuration for setting up a Domino partitioned server has multiple IP addresses on single network interface card (NIC). With 100 Mb connections being widely available since the last Solaris/Domino redbook, it is now better to let a single NIC manage multiple IP addresses.

All three configurations can make use of the new network support of IPv6 available in Domino 7.

8.3.1 Multiple IP addresses on a single NIC

Assign a unique IP address to each partitioned server instance using a single NIC for *all* server instances. In addition, if your servers are clustered, we recommend a second NIC for the private cluster network.

See 4.5.2, “Our Redbooks Lab topology” on page 49, for detailed examples from our Redbooks Lab of setting up multiple IP addresses on a single NIC.

To summarize the procedure:

1. Add one entry in the local host name’s /etc/hosts file for each server partition. The entry for the computer host name should already exist.
2. For each partition, create a file named `/etc/hostname.`*`device`*`:`*`n`* where *device* is the device name of the NIC, and *n* is a number that increments for each logical interface.
3. Start your new network configuration by either rebooting the server or using a series of **`ifconfig`** commands.
4. Test the configuration. From another computer, use the **`ping`** command with the server names. To show the network status, use the **`netstat`** command.

The host name / IP address can then be used in as it would be for any other server setup. See “The Domino Server Setup program” of the Lotus Domino Administrator 7 Help.

8.3.2 Single IP address, single dedicated NIC

Assigning a separate unique IP address to each partitioned server instance using a separate NIC or a separate port on a multiport NIC for each Domino partition is an optional approach when setting up partitioned servers.

Configuring, installing, and enabling NIC cards is described in A.2, "Installing additional network interfaces" on page 518.

The hostnames / IP address can then be used as it would be for any other server setup. See "The Domino Server Setup program" of Lotus Domino Administrator 7 Help.

8.3.3 Bind Domino's ports

After assigning unique host names and IP addresses to a Domino partition either with multiple IP addresses on a single NIC or dedicated NICs per IP address, it is recommend that you bind Domino's NRPC to a specific port and the Internet services to unique ports.

Lotus Domino is designed to listen for TCP/IP connections on all NICs in a computer system. If more than one partition is hosting the same service (NRPC, SMTP, POP3, IMAP, LDAP, or HTTP), fine-tune which partitions listen for which connections by associating each service's TCP port with a specific IP address.

Binding Domino NRPC to specific port for a given IP address

When setting the notes.ini variables for port mapping, do not include a zone in a port mapped address. The zone is only valid locally.

1. For each IP address, make sure you have added a Notes port for TCP/IP. Also make sure that each port has a unique name.
2. In the notes.ini file, confirm that these lines appear for each port that you added, replacing *TCPIPportname* with the port name you defined:

   ```
   Ports=TCPIPportname
   TCPIPportname=TCP, 0, 15, 0
   ```

3. For each port that you want to bind to an IP address, add this line to the notes.ini file, replacing *IPaddress* with the IP address of the specific NIC:

   ```
   TCPIPportname_TCPIPAddress=0,IPaddress
   ```

   For example:

   ```
   TCPIP_TCPIPAddress=0,130.123.45.1
   ```

Note: For IPv6, enclose the address in square brackets, as it contains colons. For example:

```
TCPIP_TCPIPAddress=0,[fe80::290:27ff:fe43:16ac]
```

4. (Optional) To help remember the function of each port, add the default TCP port number for NRPC to the end of the line you entered in step 3 on page 256, as follows:

```
TCPIP_TCPIPAddress=0,130.123.45.1:1352
```

To bind the SMTP, POP3, IMAP, LDAP, or ICM service

After binding NRPC to specific port outlined above, the Internet ports can be assigned.

1. In the notes.ini file, specify the appropriate port for each Internet service, as listed in Table 8-1.

Table 8-1 Internet service and corresponding action

Service	Action
POP3	Enter POP3NotesPort=*port name*[a]
IMAP	Enter IMAPNotesPort=*port name*
SMTP	Enter SMTPNotesPort=*port name*
LDAP	Enter LDAPNotesPort=*port name*
ICM	Enter ICMNotesPort=*port name*

a. *port name* is the name of the port that you want to link the service to.

The following example shows the lines (in bold) to add to the Ports section of the notes.ini file to bind two ports to their IP addresses and to specify the second port for the SMTP service:

```
Ports=TCPIP, TCP1P2
TCPIP=TCP, 0, 15, 0
TCPIP_TCPIPAddress=0,10.33.52.1
TCPIP2=TCP, 0, 15, 0
TCPIP2_TCPIPAddress=0, 209.98.76.10
SMPTNotesPort=TCPIP2
```

8.3.4 Port mapping

Port mapping uses a single IP address for all partitioned server instances, assigning a unique port to each partitioned server instance. The port mapping configuration enables the use of a single network interface card.

To configure for one IP address and port mapping

When you set up port mapping, the port-mapping partition automatically routes NRPC communication requests to the other server partitions.

> **Note:** When setting the notes.ini variables for port mapping, do not include a zone in a port-mapped address. The zone is only valid locally.

1. Decide which server partition will perform port mapping.
2. Choose a unique TCP/IP port number for each server partition on the computer. The port-mapping partition uses the assigned port 1352. It is best to use port numbers 13520, 13521, 13522, 13523, or 13524 for the additional server partitions.
3. In the notes.ini file of the port-mapping partition, include one line for the port-mapping partition and one line for each of the other partitions. For the port-mapping partition, enter:

   ```
   TCPIP_TcpIpAddress=0,IPAddress:1352
   ```

   (*TCPIP* is the port name, and *IPAddress* is the IP address of the port-mapping partition.)

   For each of the other partitions, enter:

   ```
   TCPIP_PortMappingNN=CN=server_name/O=org,IPaddress:TCP/IP port number
   ```

   Here, *TCPIP* is the port name, *NN* is a number between 00 and 04 assigned in ascending sequence, *server_name* is the server name of the partition, *org* is the organization name, *IPAddress* is the shared IP address, and *TCP/IP port number* is the unique port number you chose for the partition.

   > **Note:** You must assign the numbers for *NN* in ascending order beginning with 00 and ending with a maximum of 04. If there is a break in the sequence, Domino ignores the subsequent entries.

4. In the notes.ini file of each of the other partitions, include this line:

   ```
   TCPIP_TcpIpAddress=0, IPAddress:IPport_number
   ```

   Here, *TCPIP* is the port name, *IPAddress* is the shared IP address, and *IPport_number* is the unique port number you chose for the partitioned server.

5. In the Net Address field on the Ports - Notes Network Ports tab in the Server document for each partition, enter the fully qualified domain name (for example, sales.acme.com) or the common server name (for example, Sales).
6. Create an IP address entry for the port-mapping partition in the DNS, NIS, or the local hosts file.
7. Include each partition name as a separate CNAME entry in the DNS, NIS, or the local hosts file.
8. If you also plan to set up the partitions for IMAP, LDAP, and POP3 services and Web server communication, assign to each protocol a unique port number in the TCP/IP port number field on the appropriate sub-tabs (Web, Directory, and Mail) on the Ports - Internet Ports tab of the Server document.

> **Note:** You must make these port numbers available to users when they try to connect to these servers. For example, if you assign port 12080 to the Web server acme.com, users must include acme.com:12080 in the URL in order to connect to the server, unless they have a means to redirect the connection to this port assignment.

This example shows the lines you add to the notes.ini files of the server partitions to set up port mapping for six partitions.

- Partition 1 (the port-mapping partition)

```
TCPIP_TcpIpAddress=0,192.94.222.169:1352
TCPIP_PortMapping00=CN=Server2/O=Org2,192.94.222.169:13520
TCPIP_PortMapping01=CN=Server3/O=Org3,192.94.222.169:13521
TCPIP_PortMapping02=CN=Server4/O=Org4,192.94.222.169:13522
TCPIP_PortMapping03=CN=Server5/O=Org5,192.94.222.169:13523
TCPIP_PortMapping04=CN=Server6/O=Org6,192.94.222.169:13524
```

- Partition 2

```
TCPIP_TcpIpAddress=0,192.94.222.169:13520
```

- Partition 3

```
TCPIP_TcpIpAddress=0,192.94.222.169:13521
```

- Partition 4

```
TCPIP_TcpIpAddress=0,192.94.222.169:13522
```

- Partition 5

```
TCPIP_TcpIpAddress=0,192.94.222.169:13523
```

- Partition 6

```
TCPIP_TcpIpAddress=0,192.94.222.169:13524
```

8.4 Configuring memory resources for partitioning

When running multiple Domino partitions on a single machine, you must divide the system's memory among the partitions in accordance with their load. Domino uses memory for many purposes and in many ways, and supports several approaches to manage its memory use. This section describes the two most frequently used memory-management techniques, and touches on a few more advanced techniques for special circumstances. A full treatment of all Domino memory-related tunable parameters is beyond the scope of this book; see "Domino memory pre-allocation configuration" in the IBM Lotus Notes/Domino 7 Release Notes for additional information.

8.4.1 Managing memory: typical cases

The two memory management techniques described in this section suffice for the great majority of Domino installations.

> **Important:** Use one or the other of these approaches, but do not try to combine them without assistance from Lotus Support.

PercentAvailSysResources

PercentAvailSysResources is the simplest method for dividing resources among Domino server instances and therefore is the one we recommend using before trying the alternative methods. In each partition's notes.ini file, add a line such as:

```
PercentAvailSysResources=nn
```

(*nn* is the percentage of system memory this partition should use.) The total of all partitions' values should not exceed 100%.

If the partitions are fairly equally loaded, divide 100 by the number of partitions and use the same value in all notes.ini files: 33 if running three partitions, 20 if running five, and so on.

If different partitions serve different loads and thus have different appetites for memory, you can adjust the more heavily loaded partitions' values higher and reduce the other partitions' values accordingly. For example, if you are running a lightly loaded application server, a moderately busy Web server, and two heavily loaded mail partitions, you might set PercentAvailSysResources to 15 for the application server, 25 for the Web server, and 30 for each mail server, for a grand total of 100.

It might seem paradoxical, but large values of PercentAvailSysResources usually do not increase the amount of memory that is available to Domino. As a 32-bit application, Domino is limited to a total address space of 4 GB, which must contain the shared and local working memory, stack space, executable code, and everything else. If the actual system memory multiplied by the stated percentage exceeds 4 GB, Domino limits itself to subdividing the 4 GB, not the possibly larger percentage share. On an 8 GB system, for example, all PercentAvailSysResources values greater than 50% are effectively the same because of the 4 GB maximum. The upshot is that on systems with large amounts of memory, only very small values of PercentAvailSysResources are effective, and the adjustment is fairly coarse: a 1% change on a system with 64 GB corresponds to an increase or decrease of 640 MB, a fairly large increment. If your system is memory-rich, you should consider using the technique described next instead of trying to adjust PercentAvailSysResources.

Controlling the NSF buffer pool share of memory resources

The single largest region of memory in Domino is the NSF buffer pool, an area of shared memory dedicated to buffering I/O transfers between the NIF (Notes Index Facility) indexing functions and disk storage. If PercentAvailSysResources is not suitable for your partitions, you can control Domino's memory usage by direct adjustment of the size of this single largest component. In each partition's notes.ini file, add a line such as:

```
NSF_Buffer_Pool_Size_MB=nnn
```

(*nnn* is the maximum amount of memory the buffer pool should be allowed to use, in megabytes.) The rest of this subsection describes how to choose a good value for nnn and how to monitor its effects on a partition's performance.

Overall performance will suffer if the buffer pool is too large for physical memory because Solaris will be forced to do swapping for buffer I/O. If the buffer pool is too small, then NIF will be less likely to find the data it needs in the pool and will be forced to wait for much slower disk I/O. An approximate method for gauging the correct size for the NSF buffer pool is to review the PerCentReadsInBuffer listed from the output of "show stat database." The setting can also be referred to as the *hit rate*. In the example provided the value is 98.92:

```
show stat database
...
  Database.DAFailoverCount = 0
  Database.DARefreshServerInfoCount = 0
  Database.DAReloadCount = 0
  Database.Database.BufferPool.Maximum.Megabytes = 1515
  Database.Database.BufferPool.MM.Reads = 0
  Database.Database.BufferPool.MM.Writes = 0
  Database.Database.BufferPool.Peak.Megabytes = 11
  Database.Database.BufferPool.PerCentReadsInBuffer = 98.92
...
```

98.92 is good value for the hit rate. Any value above 92% is considered an acceptable rate. If a Domino server instance has a low value for the hit rate, increasing to the NSF buffer pool can improve performance. Any modifications must be monitored to ensure that additional shared memory that is allocated for the NSF buffer pool is not harmful for other consumers of shared memory.

The NSF buffer pool should always be larger than 500 MB on a system running multiple Domino instances. In most cases, the total size of all of the partitions' buffer pools should not exceed one-third of the system's total memory.

Monitor the Database.Database.BufferPool.PerCentReadsInBuffer statistic on all partitions to detect imbalances. For example, if most partitions have hit rates of about 99% but one has a rate of only 90%, you can probably improve overall performance by stealing a little memory from the buffer pools of the high-rate partitions and giving it to the low-rate partition. When making adjustments of this kind it is important not to change things too frequently: Be sure to track the performance through at least one period of peak load, if not more, before adjusting yet again.

8.4.2 Managing memory: special circumstances

This subsection considers some advanced techniques for memory management that might be appropriate for partitions that serve atypical loads.

Expanding local memory

In typical Domino servers, most of the memory is shared by all of the cooperating processes that make up a partition, and a smaller amount consists of local memory that is private to each process. In some situations you might need to reduce the amount of shared memory to allow the local memory to grow larger than it would normally.

An example: The http server task manages communication with Web clients, and uses a fairly large amount of local memory. If you have deployed a specialized Web application that raises the demand for local memory — a full text searching capability, for instance — the http task might exhaust its local memory and be unable to continue. By reducing the amount of memory that http shares with the other server tasks, you can allow it to have the greater amounts of local memory that the application requires.

In this example, you could reduce the shared memory by adding two lines to the partition's `notes.ini` file:

```
ConstrainedSHMSizeMB=2048
NSF_Buffer_Pool_Size_MB=500
```

The first line causes Domino to limit its total shared memory to no more than 2 GB, which is half of its maximum address space of 4 GB. Most of the remaining 2 GB would then be available for local memory.

The second line amounts to a sort of correction: Because of the memory limit imposed by the first line, left to its own devices Domino would calculate a sharply lower size for the NSF buffer pool and this size might be inadequate. As shown, the second line re-establishes the recommended minimum size for the buffer pool, ensuring that the server's NIF activities have sufficient buffering for good performance.

MEM_EnablePreAlloc

Ordinarily, Domino begins with a modest amount of shared memory and adds more as its needs grow. In order for this to work, all of the processes belonging to a partition must be informed that shared memory has been added and must attach to the new shared memory area. If a process is unable to access the new memory area, you will see an error message such as "Error attaching to shared memory," "Error on mapping memory," or "PANIC: Cannot attach to shared memory." This condition is always fatal, and is particularly likely to happen if a process' local memory has grown so large that it has no address space left over for the new shared memory.

Instead, Domino 7 can preallocate all of its shared memory before starting any subordinate processes. This prevents the server panic because there is no incremental growth of shared memory after the server starts: the situation of one process being unable to access shared memory created by another simply does not arise. To enable preallocation, add this line to the partition's notes.ini file:

```
MEM_EnablePreAlloc=1
```

The downside of this is that Domino will always use up its maximum amount of virtual memory for shared memory, whether it actually needs it or not. This might "starve" other parts of Domino (local memory, for example) or of Solaris (the file system in particular) by seizing memory they need for good performance. If you decide to use preallocation, you must be willing to monitor the server closely to ensure that the amount of shared memory is neither too large nor too small.

Enabling System V shared memory

Domino ordinarily uses mmapped files to share memory between its processes, but it can be configured to use System V shared memory instead. System V memory offers some performance advantages but requires more attention than the default mechanism. See Appendix B, "Using System V shared memory" on page 521 for further information.

9

IBM Lotus Domino administration

In this chapter we describe the different ways you can access your Domino server for administration. Because there is no Notes client for the Solaris platform, you must administer your Domino servers with one of the administration tools described in this chapter.

We provide an overview of:

- The Domino Administrator client, which provides you with tools for graphical monitoring of servers, services, replication, and routing. You can use the Domino Administrator client to perform most administration tasks.
- The Domino Web Administrator, which enables you to manage and view settings for a Domino server with a browser. It helps you to keep your Domino server up and running, even if you do not have access to a Domino Administrator client.
- The Domino Server Controller and Domino (Java) Console, which provides real-time interaction with the Domino server and is a fast way to see what is happening with the server.
- The Domino Character Console (the cconsole program), which provides a way to access the server console from the Solaris command line. This feature is supported only for UNIX platforms.

© Copyright IBM Corp. 2006. All rights reserved.

9.1 The Domino Administrator client

Prior to Lotus Domino R5, only the single, all-purpose Lotus Notes client was available for users, administrators, and application developers alike. Then, with R5, the Notes client was subdivided into three functionally specialized clients:

- Lotus Notes - the user's client
- Lotus Domino Administrator - the Administrator's client
- Lotus Domino Designer - the Developer's client

Since R5, and through ND6, these three clients have continued to evolve in feature and functional capability. With ND7 they are now:

- Lotus Notes 7
- Lotus Domino Administrator 7
- Lotus Domino Designer 7

In this chapter, we look at the Domino Administrator client and some of its features. If you want to learn about the Domino Administrator in more detail, refer to Domino 7 Administrator Help and the Notes and Domino 7 Release Notes.

Note: The Lotus Domino Administrator client is available only for Win32.

We also look at the Domino 7 Web Administrator, which enables you to administer Domino from a Web browser. Finally we will look at the Character Console (first introduced in R5), the Domino Server Controller, and Domino (Java) Console.

9.1.1 Overview

The Domino Administrator is the administration client for Notes and Domino. You can use the Domino Administrator to perform most administration tasks. You can administer the Domino environment using the native Domino Administrator client or the browser-based Web Administrator.

With the Domino Administrator client you can administer all Domino servers in your enterprise from the same workstation, even if they are in multiple Domino domains.

The Domino Administrator client implements common features such as:

- Drag and drop
- Multiple selections using the Shift and Ctrl keys
- Right-click context-sensitive menus

You can configure, manage, and enforce user desktop settings centrally.

New with Domino 7, the Domino Administrator client now offers Domino Domain Monitoring (DDM) which you can use to view the overall status of multiple servers across one or more Domino domains, and then use the information provided by DDM to resolve problems proactively.

Note: For more information about Domino Domain Monitoring and other new Domino features, see 1.5, “New Notes Domino features” on page 5.

9.1.2 Starting the Domino Administrator client

There are at least four ways you can start the Domino Administrator client:

- Double-click the Domino Administrator icon on your desktop.
- In Windows. click **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
- In the Notes client, click the Domino Administrator bookmark button.
- In the Notes client, choose **File** → **Tools** → **Server Administration**.

Note: Refer to the Domino 7 Administration Help for detailed instructions on administering the Domino server.

After launching the Domino Administrator, the Administrator Welcome window opens (Figure 9-1).

Click **All New Features in Release 7** to display the content of “What’s new in IBM Lotus Domino 7” in Domino Administrator Help.

To suppress displaying the Welcome screen in the future, select the **Don’t show this again** check box.

Click the tab with your domain name. (In our example, it is **ACME Domain**.)

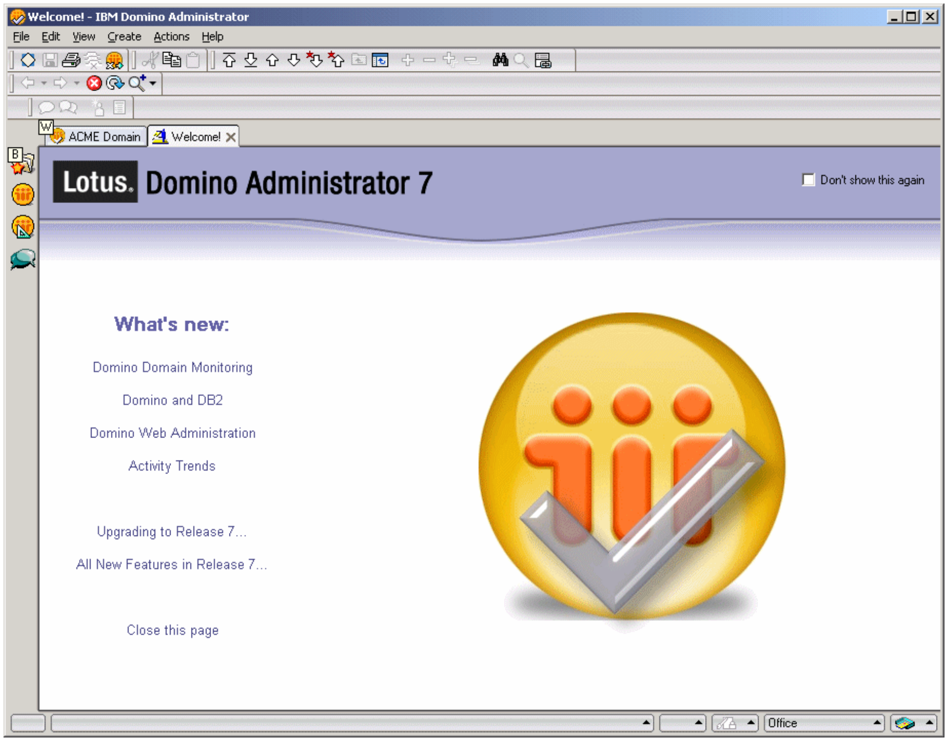

Welcome! - IBM Domino Administrator
File Edit View Create Actions Help
ACME Domain
Welcome!
Lotus. Domino Administrator 7
□ Don't show this again
What's new:
Domino Domain Monitoring
Domino and DB2
Domino Web Administration
Activity Trends
Upgrading to Release 7...
All New Features in Release 7...
Close this page
Office

Figure 9-1 Domino Administrator - Welcome window

An Administration window appears. This window has three main areas:

- Server list
- Tabs
- Tools

Next we highlight several important Domino Administrator features.

9.1.3 Using server lists

The first time you start the Domino Administrator client, the system automatically creates a server list, which is accessible from the Domain servers icon on the bookmark bar, similar to the one shown in Figure 9-2.

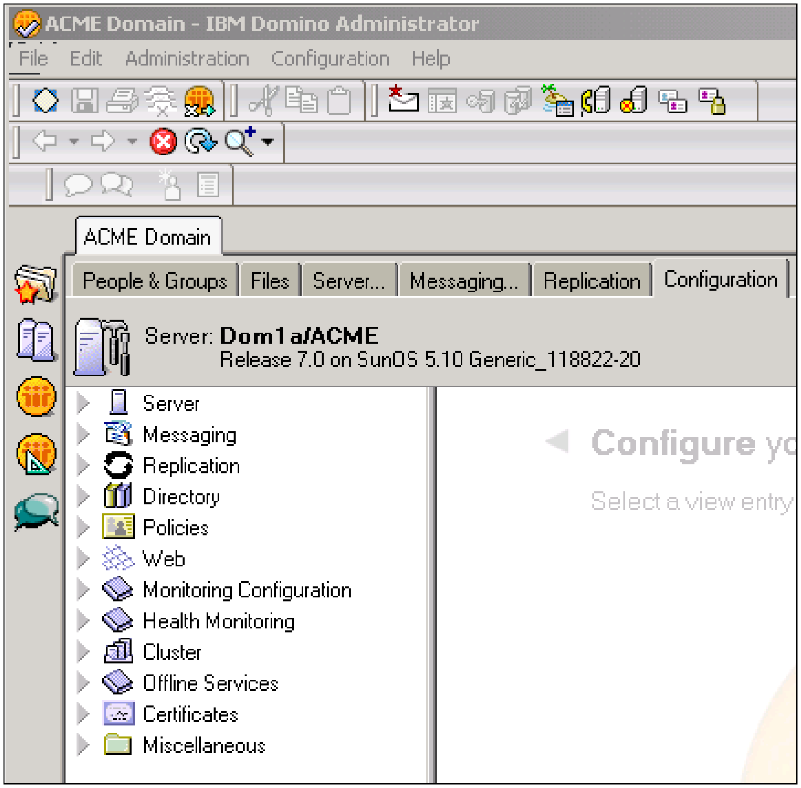


Figure 9-2 Admin client - Server list for the specified Domino domain

Tip: Choose **Administration** → **Refresh Server List** to update the server list if yours is not already created. (See example in Figure 9-3 on page 270.)

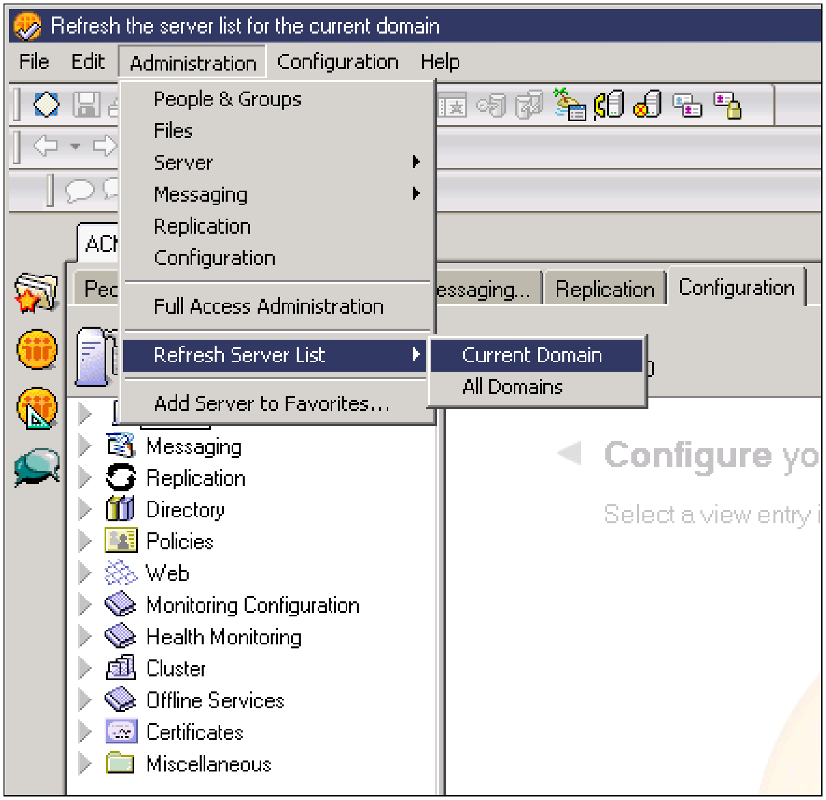
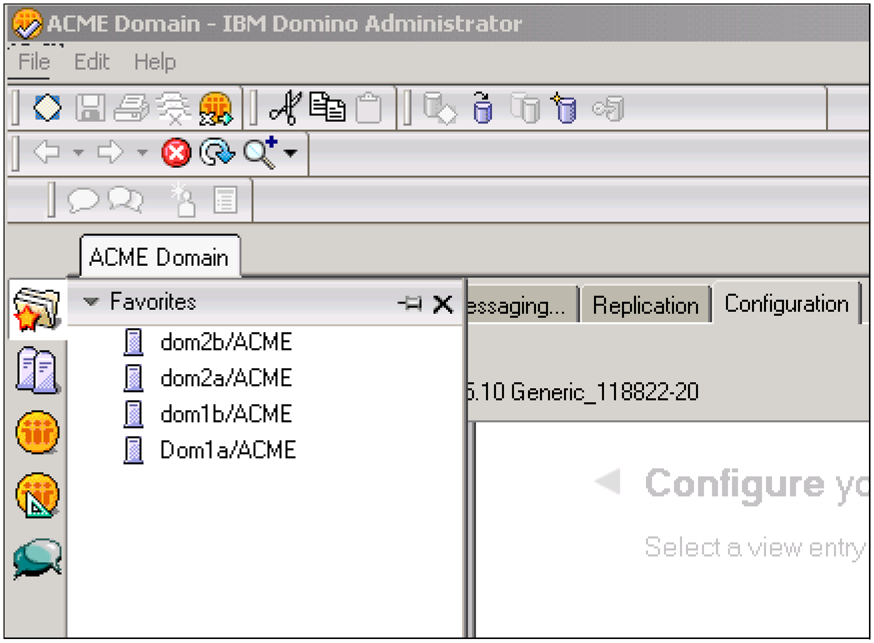


Figure 9-3 Admin client - Refreshing the Domino Server list

The bookmark bar along the left border features two bookmark buttons (the upper two icons) from which you can access the server list. You can add the servers you administer most often to the first bookmark icon, which is your "Favorites" icon (Figure 9-4).



ACME Domain - IBM Domino Administrator

dom2b/ACME
dom2a/ACME
dom1b/ACME
Dom1a/ACME

5.10 Generic_118822-20

Configure yo

Select a view entry

Figure 9-4 Admin client - Favorites icon

The second bookmark is the Domino domain icon, which displays all servers in the specified domain (Figure 9-5).

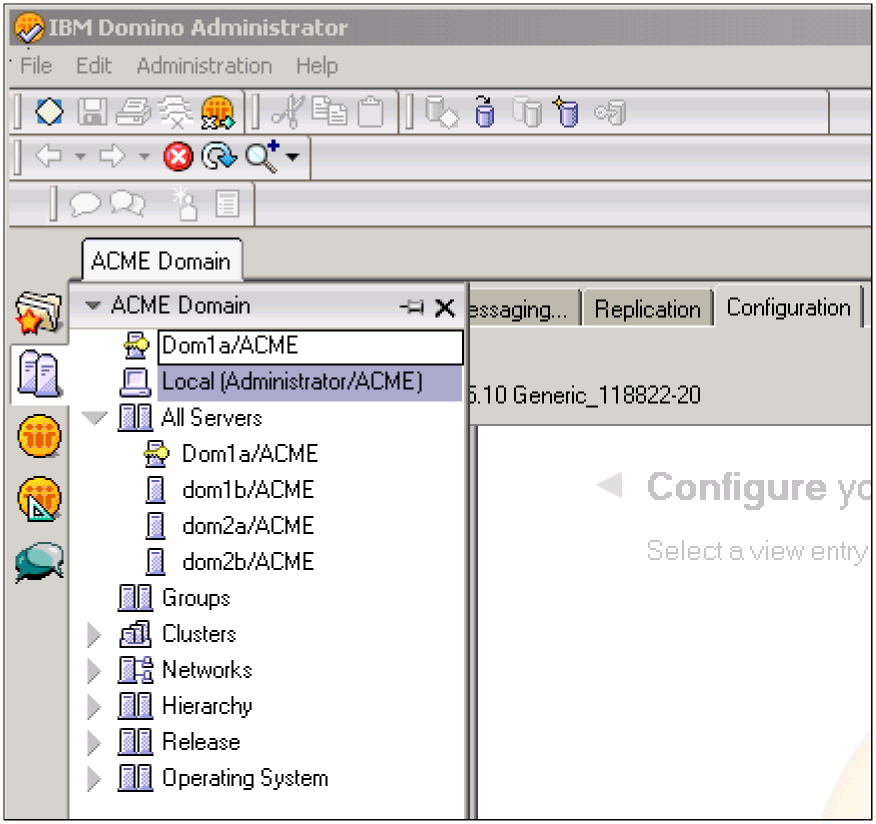


Figure 9-5 Admin client - Domino domain icon

All servers are grouped by category, which makes it easy for you to select the server you want to administer.

Note: If you administer more than one Domino domain from the Administrator client, there will be a separate Domino domain icon for each domain.

9.1.4 Setting administration preferences

Setting administration preferences for the Domino Administrator makes it easier for you to administer your Domino servers. Administration Preferences are separate from the standard User Preferences.

Accessing Administration Preferences

Choose **File** → **Preferences** → **Administration Preferences** (Figure 9-6).

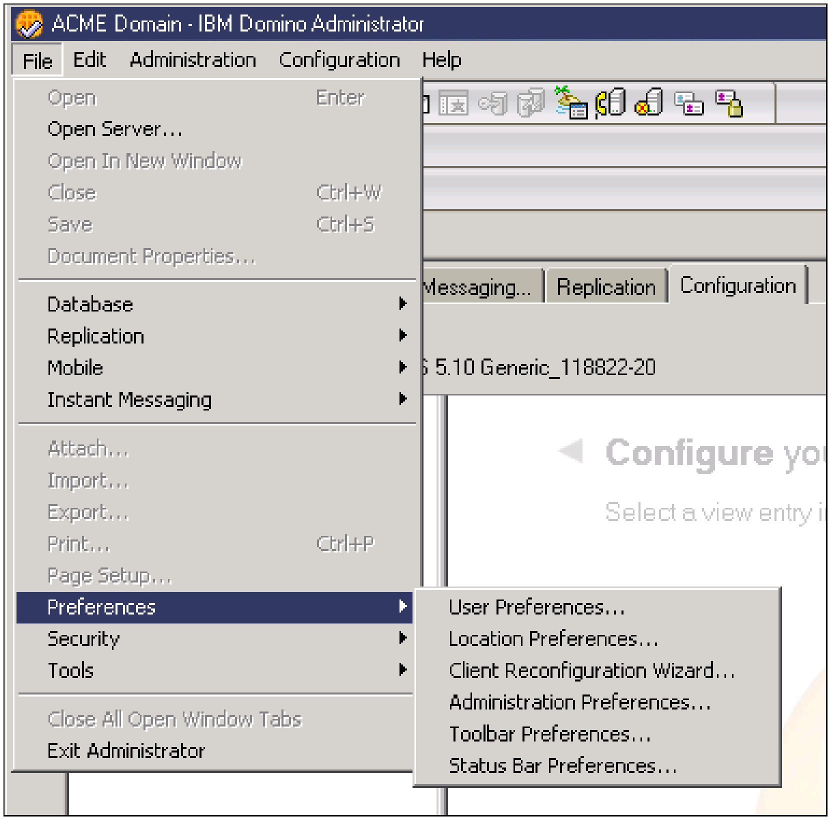
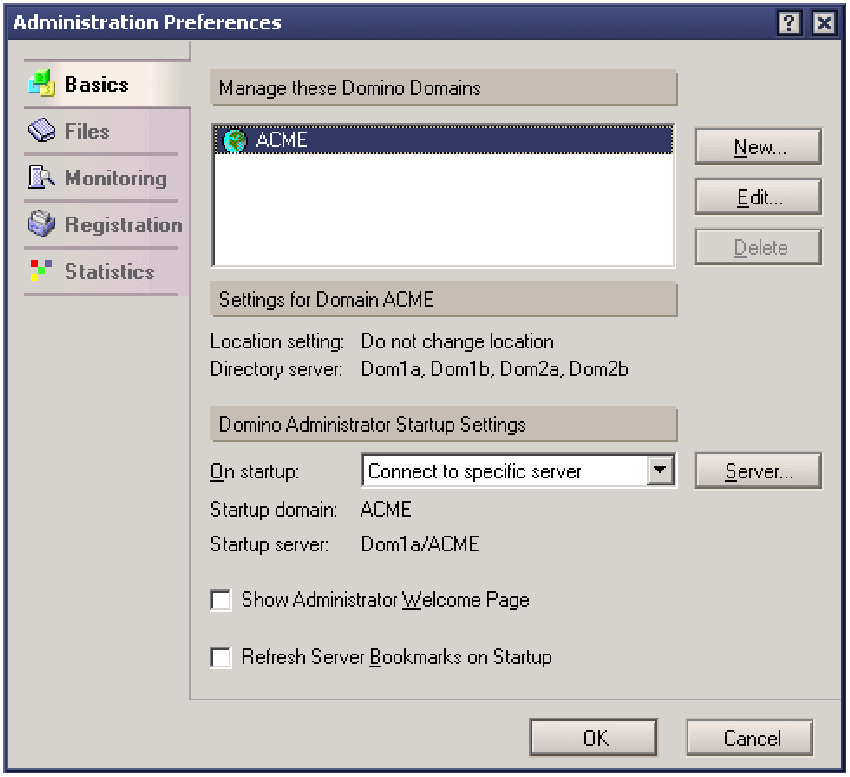


Figure 9-6 Admin client - Accessing Administration Preferences

The Administration Preferences dialog box appears, similar to the one shown in Figure 9-7.



Manage these Domino Domains

ACME

Settings for Domain ACME

Location setting: Do not change location
Directory server: Dom1a, Dom1b, Dom2a, Dom2b

Domino Administrator Startup Settings

On startup: Connect to specific server
Startup domain: ACME
Startup server: Dom1a/ACME

□ Show Administrator Welcome Page

□ Refresh Server Bookmarks on Startup

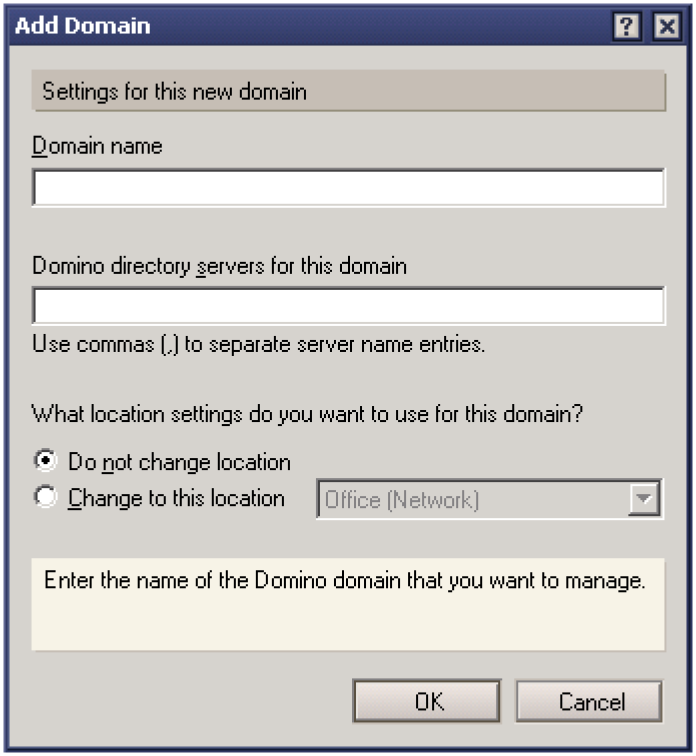
Figure 9-7 Admin client - Administration Preferences - Basics tab

The Administration Preferences dialog has five sub-tabs with specific purposes:

- Basics: Define which Domino domains you want to manage from the Domino Administrator client. You can choose to switch locations when you switch Domino domains.
- Files: Select the columns to be displayed in the Files tab of the Domino Administrator client.
- Monitoring: Configure the collection of monitoring data from the servers you administer, including how often and from which server to collect the data.
- Registration: Set the defaults for the registration process. You can specify a default certification server and certification ID, several mail options, and the locations for ID files for users and servers.
- Statistics: Select global settings for statistic reporting and charting, and enable alarms while monitoring statistics.

Adding domains to your Bookmark bar

1. Choose **File** → **Preferences** → **Administration Preferences**.
2. Click **Basics** and then click **New** to add a domain. The Add Domain dialog box displays, as shown in Figure 9-8.



Add Domain

Settings for this new domain

Domain name

Domino directory servers for this domain

Use commas (,) to separate server name entries.

What location settings do you want to use for this domain?

● Do not change location

○ Change to this location   Office (Network)

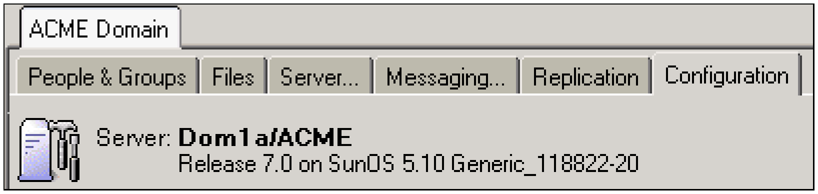
Enter the name of the Domino domain that you want to manage.

Figure 9-8 Admin client - Add Domain dialog box

3. In the Domain name field, enter the name of the Domino domain you are adding.
4. In the Domino directory servers for this domain field, enter one or more directory servers, separated by commas.
5. If you want to switch to a location automatically when you choose the domain, select **Change to this location**, then select the desired location.
6. Click **OK**.

9.1.5 Using tabbed pages

The middle pane in the Domino Administrator client contains tabbed pages (Figure 9-9). Each tab represents a general administration task to perform.

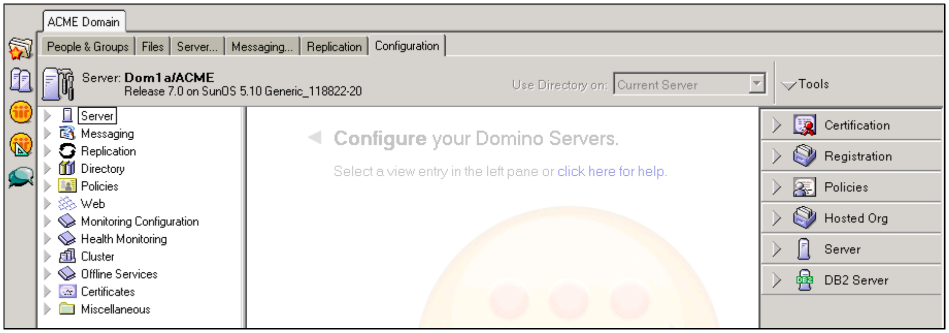


Server: **Dom1a/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

Figure 9-9 Admin client - tabbed pages

Click a tab to display its contents or use the Administration menu to navigate among the tabs. For example, to move to the Replication tab, you can choose **Administration** → **Replication**. The Domino Administrator client provides more than one way to navigate to most of its functions.

The Administrator tabs also provide context-specific tools that appear on the right side of the Administrator client display. Figure 9-10 shows an example of the tools associated with the Configuration tab.



Server: **Dom1a/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

Use Directory on: Current Server

Configure your Domino Servers.

Select a view entry in the left pane or click here for help.

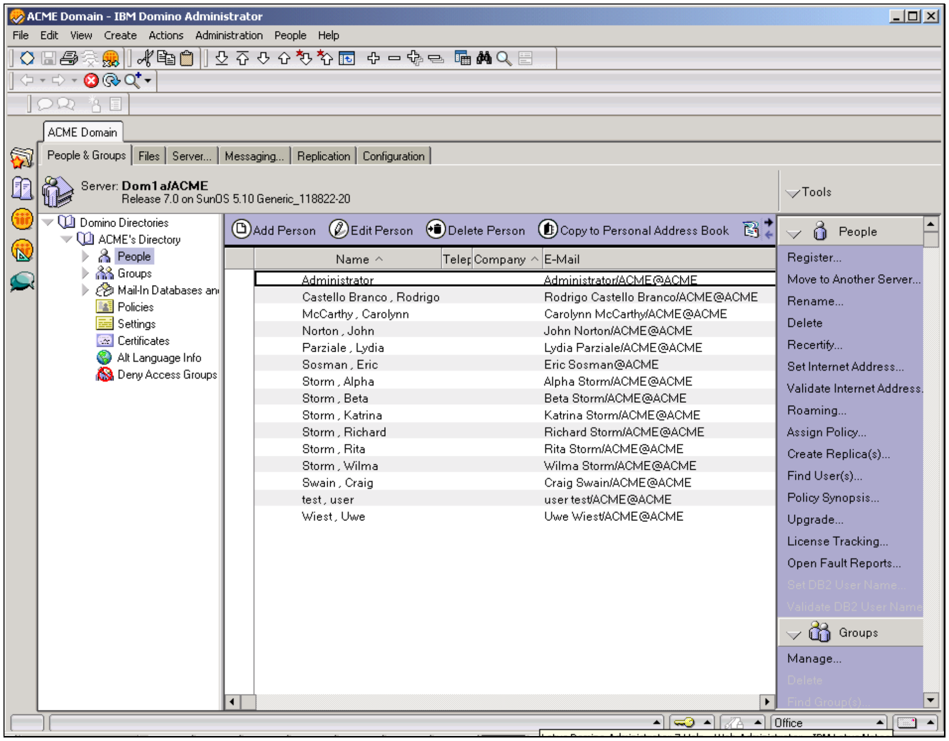
Figure 9-10 Admin client - Configuration tab with companion Tools

The available tools change based on tab you select. For example, if you click the Files tab, the following tools appear: Disk Information, Directory, and Database.

> **Tip:** You can also right-click on certain objects to access tools that are relevant to those objects. For example, right-click a Person document to access People tools.

People & Groups tab

Figure 9-11 shows the People & Groups tab. You can use the tools associated with this tab to register new users, rename or recertify users, move or delete users, and set or validate the Internet address.



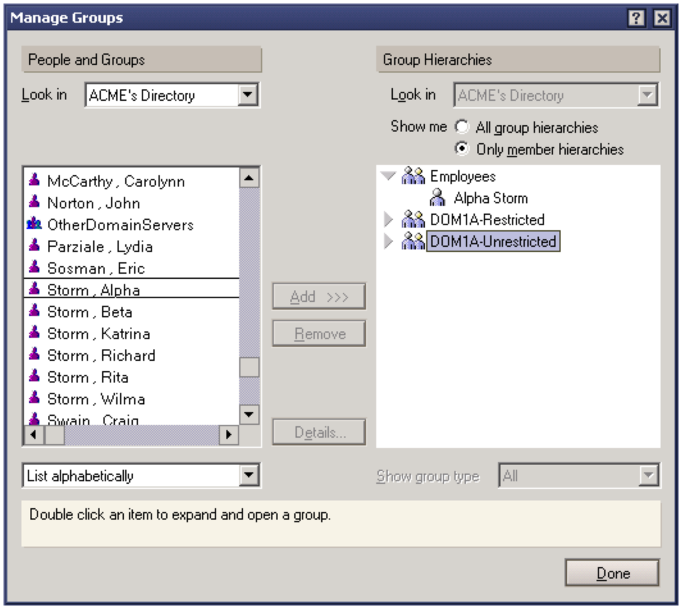
Server: **Dom1a/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

Name	Telep	Company	E-Mail
Administrator			Administrator/ACME@ACME
Castello Branco , Rodrigo			Rodrigo Castello Branco/ACME@ACME
McCarthy , Carolynn			Carolynn McCarthy/ACME@ACME
Norton , John			John Norton/ACME@ACME
Parziale , Lydia			Lydia Parziale/ACME@ACME
Sosman , Eric			Eric Sosman@ACME
Storm , Alpha			Alpha Storm/ACME@ACME
Storm , Beta			Beta Storm/ACME@ACME
Storm , Katrina			Katrina Storm/ACME@ACME
Storm , Richard			Richard Storm/ACME@ACME
Storm , Rita			Rita Storm/ACME@ACME
Storm , Wilma			Wilma Storm/ACME@ACME
Swain , Craig			Craig Swain/ACME@ACME
test , user			user test/ACME@ACME
Wiest , Uwe			Uwe Wiest/ACME@ACME

Figure 9-11 Admin client - People & Groups tab

In addition, you can access the tools for managing groups, as shown in Figure 9-12. From this window you can:

- View the membership of multiple groups while adding and removing users.
- Sort the groups by their purpose.
- Select a user and display only the groups to which the selected user belongs.



Manage Groups

People and Groups

Look in: ACME's Directory

- McCarthy , Carolynn
- Norton , John
- OtherDomainServers
- Parziale , Lydia
- Sosman , Eric
- Storm , Alpha
- Storm , Beta
- Storm , Katrina
- Storm , Richard
- Storm , Rita
- Storm , Wilma
- Swain , Craig

List alphabetically

Group Hierarchies

Look in: ACME's Directory

Show me: ○ All group hierarchies ● Only member hierarchies

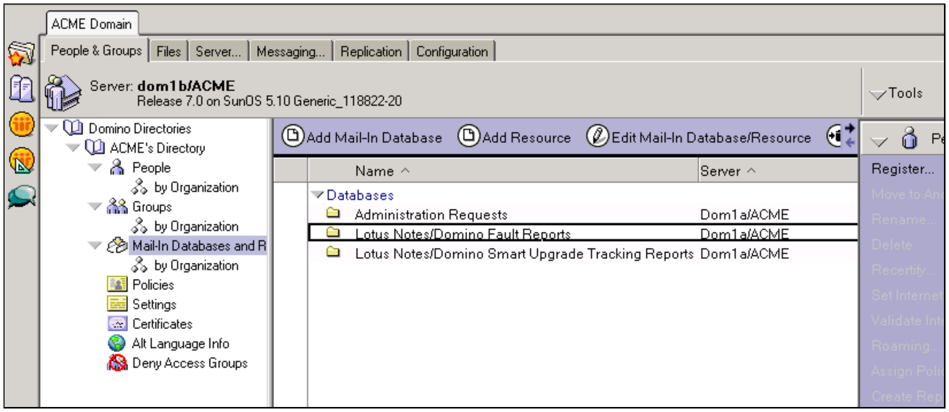
- Employees
  - Alpha Storm
- DOM1A-Restricted
- DOM1A-Unrestricted

Show group type: All

Double click an item to expand and open a group.

Figure 9-12 Admin client - Manage Groups

You can also manage mail-in databases and resources (Figure 9-13).



Server: **dom1b/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

- Domino Directories
  - ACME's Directory
    - People
      - by Organization
    - Groups
      - by Organization
    - Mail-In Databases and R
      - by Organization
    - Policies
    - Settings
    - Certificates
    - Alt Language Info
    - Deny Access Groups

Name	Server
Databases	
Administration Requests	Dom1a/ACME
Lotus Notes/Domino Fault Reports	Dom1a/ACME
Lotus Notes/Domino Smart Upgrade Tracking Reports	Dom1a/ACME

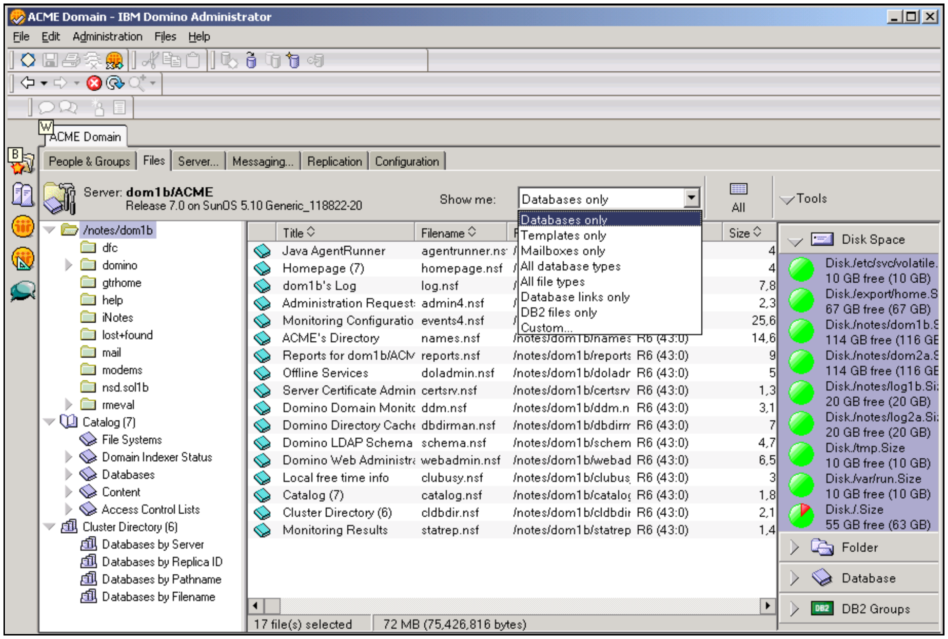
Figure 9-13 Admin client - Managing Mail-in Databases and Resources

Files tab

You can use the Files tab to access:

- Databases
- Templates
- Flat files

The Files tab provides a simple way to get an overall picture of your data directory structure, including database and directory links. You can check the hard disk space to see how much free disk space is available. This information is shown on the right side of the window in Figure 9-14.



Server: **dom1b/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

Show me: Databases only

- Databases only
- Templates only
- Mailboxes only
- All database types
- All file types
- Database links only
- DB2 files only
- Custom...

Title	Filename	F		Size
Java AgentRunner	agentrunner.ns	/		4
Homepage (7)	homepage.nsf	/		4
dom1b's Log	log.nsf	/		7,8
Administration Request	admin4.nsf	/		2,3
Monitoring Configuratio	events4.nsf	/		25,6
ACME's Directory	names.nsf	/notes/dom1b/names	R6 (43:0)	14,6
Reports for dom1b/ACM	reports.nsf	/notes/dom1b/reports	R6 (43:0)	9
Offline Services	doladmin.nsf	/notes/dom1b/doladr	R6 (43:0)	5
Server Certificate Admin	certsrv.nsf	/notes/dom1b/certsrv	R6 (43:0)	1,3
Domino Domain Monitc	ddm.nsf	/notes/dom1b/ddm.n	R6 (43:0)	3,1
Domino Directory Cache	dbdirman.nsf	/notes/dom1b/dbdirm	R6 (43:0)	7
Domino LDAP Schema	schema.nsf	/notes/dom1b/schem	R6 (43:0)	4,7
Domino Web Administra	webadmin.nsf	/notes/dom1b/webad	R6 (43:0)	6,5
Local free time info	clubusy.nsf	/notes/dom1b/clubus	R6 (43:0)	3
Catalog (7)	catalog.nsf	/notes/dom1b/catalo	R6 (43:0)	1,8
Cluster Directory (6)	cldbdir.nsf	/notes/dom1b/cldbdir	R6 (43:0)	2,1
Monitoring Results	statrep.nsf	/notes/dom1b/statrep	R6 (43:0)	1,4

17 file(s) selected 72 MB (75,426,816 bytes)

Disk./etc/svc/volatile.
10 GB free (10 GB)
Disk./export/home.S
67 GB free (67 GB)
Disk./notes/dom1b.S
114 GB free (116 GB
Disk./notes/dom2a.S
114 GB free (116 GB
Disk./notes/log1b.Si
20 GB free (20 GB)
Disk./notes/log2a.Si
20 GB free (20 GB)
Disk./tmp.Size
10 GB free (10 GB)
Disk./var/run.Size
10 GB free (10 GB)
Disk./.Size
55 GB free (63 GB)

Figure 9-14 Admin client - Files tab

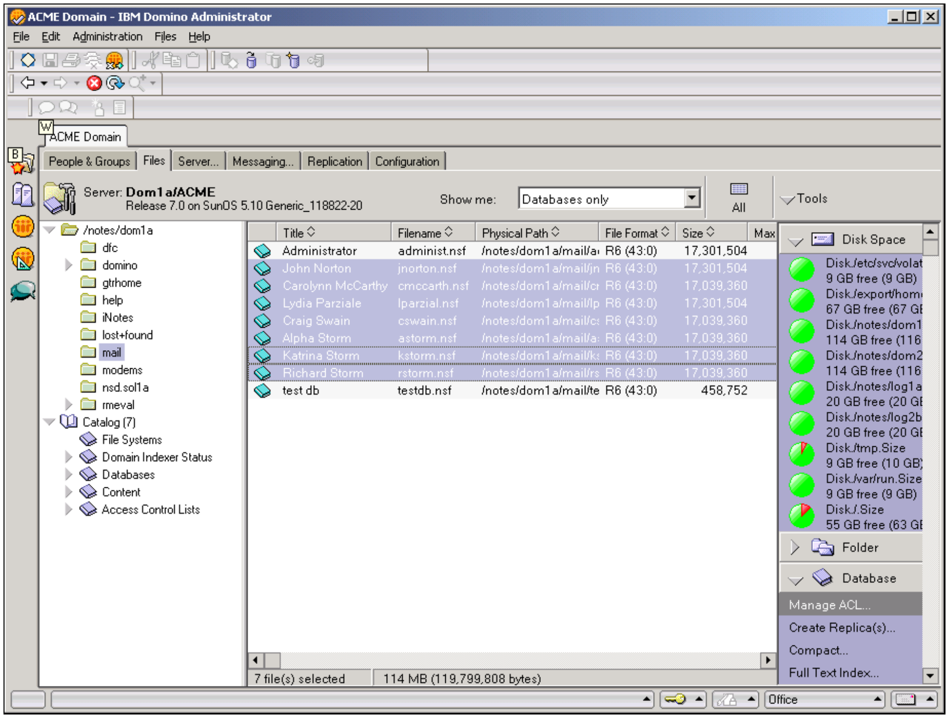
Use the Folder tools to create new folders and directory links, or to delete folders.

The Database tools assist you in performing day-to-day administrative tasks, such as:

- Managing ACLs (access control lists)
- Creating replicas
- Compacting, moving, fixing, analyzing, or signing databases
- Managing full-text indexes
- Setting advanced properties or quotas
- Finding a specified document in a database
- Enabling or disabling databases for cluster replication

You can work with the ACLs of multiple selected databases:

1. Select the databases whose ACLs are to be managed (Figure 9-15).
2. In the Tools pane, select **Database** → **Manage ACL**.



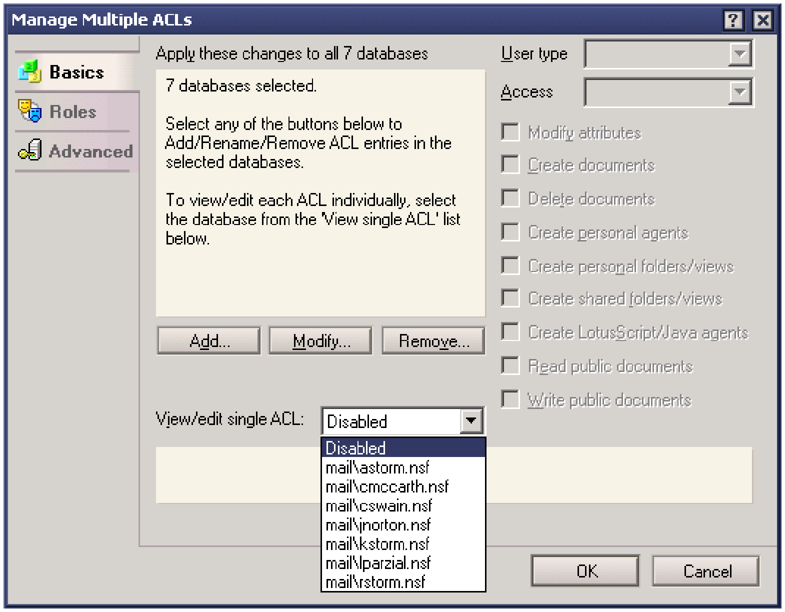
Title	Filename	Physical Path	File Format	Size	Max
Administrator	administ.nsf	/notes/dom1a/mail/a	R6 (43:0)	17,301,504	
John Norton	jnorton.nsf	/notes/dom1a/mail/jn	R6 (43:0)	17,301,504	
Carolynn McCarthy	cmccarth.nsf	/notes/dom1a/mail/cr	R6 (43:0)	17,039,360	
Lydia Parziale	lparzial.nsf	/notes/dom1a/mail/lp	R6 (43:0)	17,301,504	
Craig Swain	cswain.nsf	/notes/dom1a/mail/c:	R6 (43:0)	17,039,360	
Alpha Storm	astorm.nsf	/notes/dom1a/mail/a:	R6 (43:0)	17,039,360	
Katrina Storm	kstorm.nsf	/notes/dom1a/mail/k:	R6 (43:0)	17,039,360	
Richard Storm	rstorm.nsf	/notes/dom1a/mail/rs	R6 (43:0)	17,039,360	
test db	testdb.nsf	/notes/dom1a/mail/te	R6 (43:0)	458,752	

7 file(s) selected 114 MB (119,799,808 bytes)

Figure 9-15 Admin client - Select databases for ACL management

Tip: You can copy the ACL of a selected database by right-clicking it to display its context menu options.

You can modify the ACL of multiple databases simultaneously by using the Manage ACL tool. Be aware that you can only add, remove, or rename users in the ACLs this way.



Apply these changes to all 7 databases

7 databases selected.

Select any of the buttons below to Add/Rename/Remove ACL entries in the selected databases.

To view/edit each ACL individually, select the database from the 'View single ACL' list below.

View/edit single ACL: Disabled

Figure 9-16 Admin client - Managing ACLs of multiple databases

You can use the Compact tool both for compaction of selected databases and to start the Archiving process. Before using this tool for archiving, you must configure the database for archiving. Use the Archive Settings button in the Database Properties box to configure archiving.

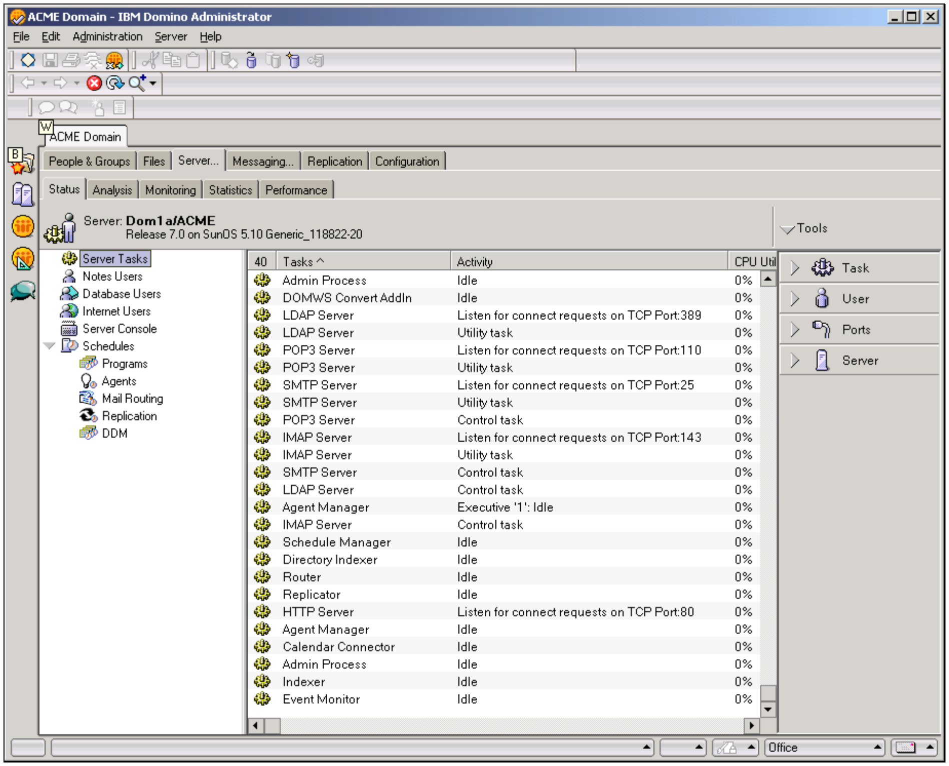
To open a Database or Template just double-click it; it opens directly from the Domino Administrator.

Server tab

Use the Server tab to administer current server activity and tasks. The Server tab has five sub-tabs:

- Status
- Analysis
- Monitoring
- Statistics
- Performance

The Status sub-tab gives an overview of the current task and user activity (Figure 9-17).



Server: **Dom1a/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

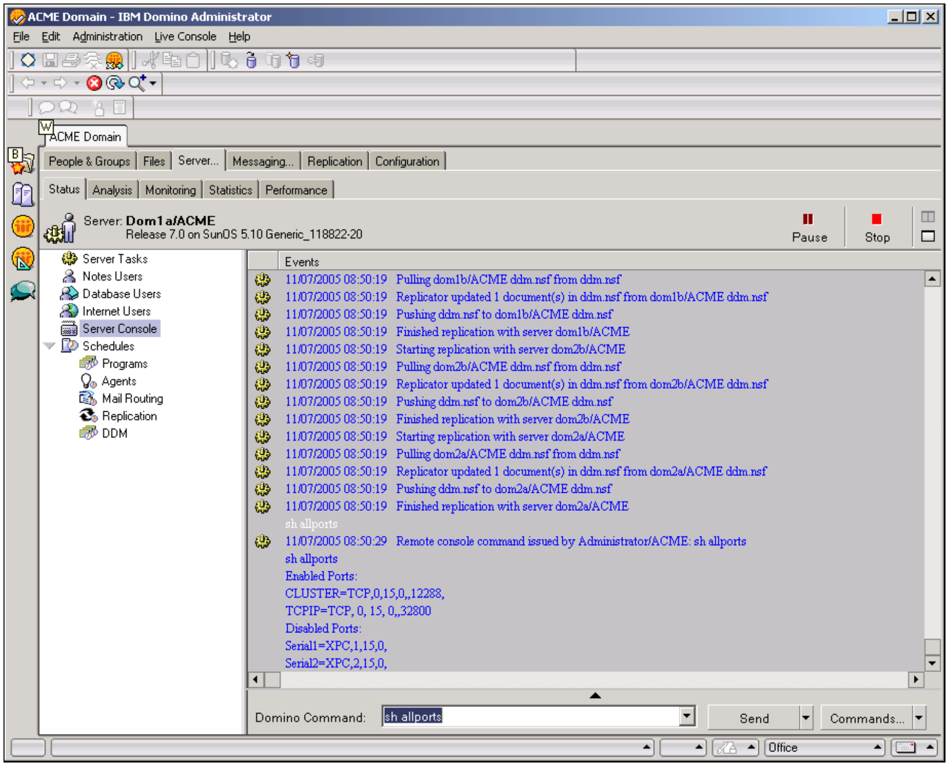
40	Tasks ^	Activity	CPU Util
	Admin Process	Idle	0%
	DOMWS Convert AddIn	Idle	0%
	LDAP Server	Listen for connect requests on TCP Port:389	0%
	LDAP Server	Utility task	0%
	POP3 Server	Listen for connect requests on TCP Port:110	0%
	POP3 Server	Utility task	0%
	SMTP Server	Listen for connect requests on TCP Port:25	0%
	SMTP Server	Utility task	0%
	POP3 Server	Control task	0%
	IMAP Server	Listen for connect requests on TCP Port:143	0%
	IMAP Server	Utility task	0%
	SMTP Server	Control task	0%
	LDAP Server	Control task	0%
	Agent Manager	Executive '1': Idle	0%
	IMAP Server	Control task	0%
	Schedule Manager	Idle	0%
	Directory Indexer	Idle	0%
	Router	Idle	0%
	Replicator	Idle	0%
	HTTP Server	Listen for connect requests on TCP Port:80	0%
	Agent Manager	Idle	0%
	Calendar Connector	Idle	0%
	Admin Process	Idle	0%
	Indexer	Idle	0%
	Event Monitor	Idle	0%

Figure 9-17 Admin client - Server tab - Server Tasks

You can run a remote Domino server console by clicking **Server Console** in the left navigation pane. Click **Live** (above the right side of the console window) to enable the server console.

Note: After clicking **Live**, it is immediately replaced with Pause and Stop console control buttons.

This provides another way to start and stop Domino server tasks, to issue `Tell` commands, and to remotely perform Domino Console commands (Figure 9-18).



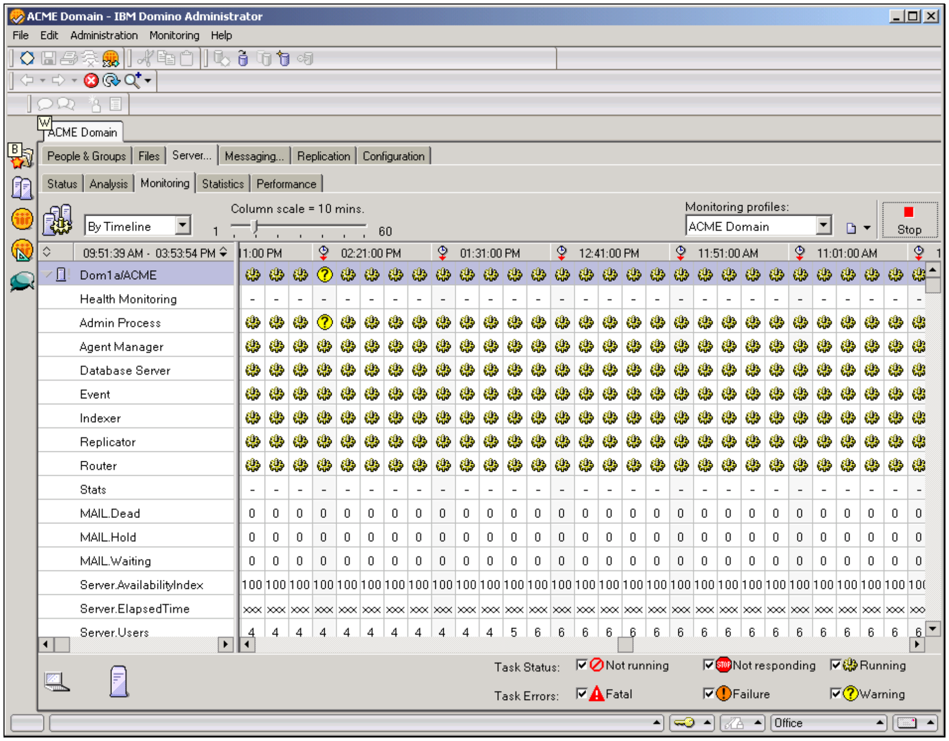
```
11/07/2005 08:50:19   Pulling dom1b/ACME ddm.nsf from ddm.nsf
11/07/2005 08:50:19   Replicator updated 1 document(s) in ddm.nsf from dom1b/ACME ddm.nsf
11/07/2005 08:50:19   Pushing ddm.nsf to dom1b/ACME ddm.nsf
11/07/2005 08:50:19   Finished replication with server dom1b/ACME
11/07/2005 08:50:19   Starting replication with server dom2b/ACME
11/07/2005 08:50:19   Pulling dom2b/ACME ddm.nsf from ddm.nsf
11/07/2005 08:50:19   Replicator updated 1 document(s) in ddm.nsf from dom2b/ACME ddm.nsf
11/07/2005 08:50:19   Pushing ddm.nsf to dom2b/ACME ddm.nsf
11/07/2005 08:50:19   Finished replication with server dom2b/ACME
11/07/2005 08:50:19   Starting replication with server dom2a/ACME
11/07/2005 08:50:19   Pulling dom2a/ACME ddm.nsf from ddm.nsf
11/07/2005 08:50:19   Replicator updated 1 document(s) in ddm.nsf from dom2a/ACME ddm.nsf
11/07/2005 08:50:19   Pushing ddm.nsf to dom2a/ACME ddm.nsf
11/07/2005 08:50:19   Finished replication with server dom2a/ACME
sh allports
11/07/2005 08:50:29   Remote console command issued by Administrator/ACME: sh allports
sh allports
Enabled Ports:
CLUSTER=TCP,0,15,0,,12288,
TCPIP=TCP, 0, 15, 0,,32800
Disabled Ports:
Serial1=XPC,1,15,0,
Serial2=XPC,2,15,0,
```

Domino Command: sh allports

Figure 9-18 Admin client - Server Console

From the Analysis sub-tab you can perform tasks such as analyzing your server log files or cluster, or start a tool to assist you in planning the decommissioning of a server.

You can easily monitor server tasks and real-time system statistics by using the Monitor sub-tab. Status indicators show the current status of each task that you monitor (Figure 9-19).



Dom1a/ACME	●	●	●	?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Health Monitoring	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Admin Process	●	●	●	?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Agent Manager	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Database Server	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Event	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Indexer	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Replicator	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Router	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Stats	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
MAIL.Dead	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MAIL.Hold	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MAIL.Waiting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Server.AvailabilityIndex	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	10(
Server.ElapsedTime	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx
Server.Users	4	4	4	4	4	4	4	4	4	4	4	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6

Task Status: ☑ Not running ☑ Not responding ☑ Running

Task Errors: ☑ Fatal ☑ Failure ☑ Warning

Figure 9-19 Admin client - Server tab - Monitoring

The Statistics sub-tab shows a list of available statistics and their most current values for the current Domino server.

The Performance sub-tab lets you configure and display Realtime and Historical statistics charts and graphical Activity Trend displays.

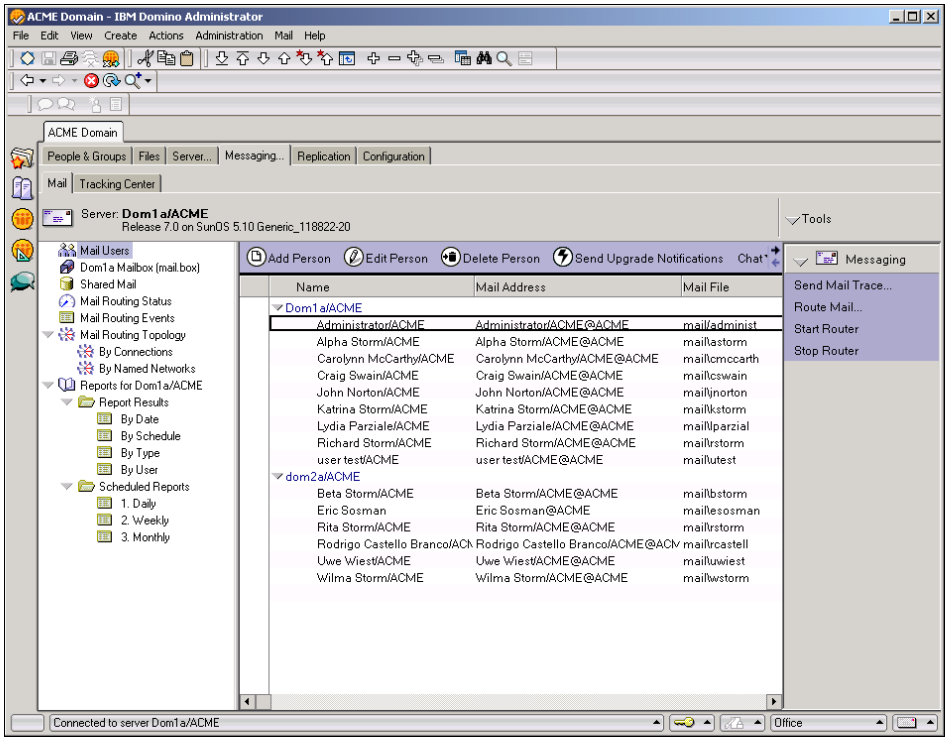
Messaging tab

You can get mail-related information from the Messaging tab, as shown in Figure 9-20 on page 285. The Messaging tab has two sub-tabs:

- Mail
- Tracking Center

The Mail sub-tab enables you to view and maintain your Domino messaging infrastructure.

You can use the Mailbox view to manage dead or stopped mail messages. In the Mail Users view, you can manage the Person documents of mail users, which are organized by Domino server (Figure 9-20).



Server: **Dom1a/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

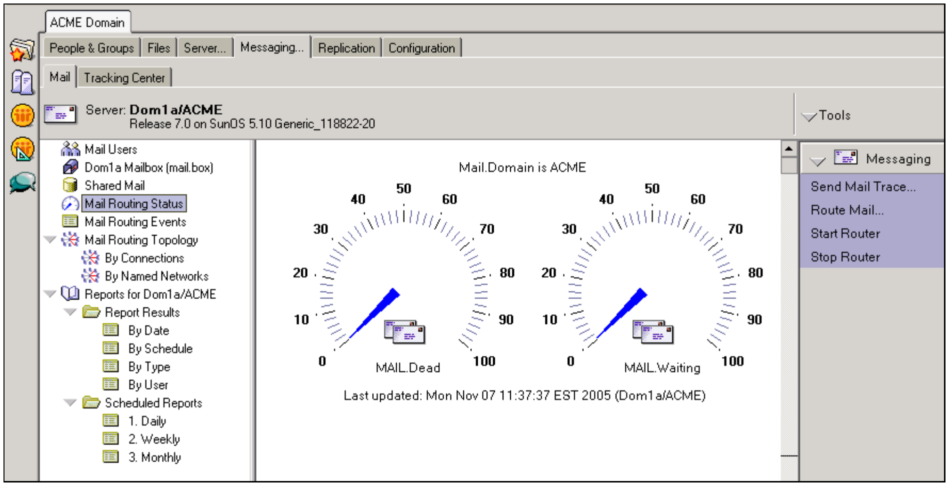
Name	Mail Address	Mail File
Dom1a/ACME		
Administrator/ACME	Administrator/ACME@ACME	mail/administ
Alpha Storm/ACME	Alpha Storm/ACME@ACME	mail\astorm
Carolynn McCarthy/ACME	Carolynn McCarthy/ACME@ACME	mail\cmccarth
Craig Swain/ACME	Craig Swain/ACME@ACME	mail\cswain
John Norton/ACME	John Norton/ACME@ACME	mail\jnorton
Katrina Storm/ACME	Katrina Storm/ACME@ACME	mail\kstorm
Lydia Parziale/ACME	Lydia Parziale/ACME@ACME	mail\lparzial
Richard Storm/ACME	Richard Storm/ACME@ACME	mail\rstorm
user test/ACME	user test/ACME@ACME	mail\utest
dom2a/ACME		
Beta Storm/ACME	Beta Storm/ACME@ACME	mail\bstorm
Eric Sosman	Eric Sosman@ACME	mail\esosman
Rita Storm/ACME	Rita Storm/ACME@ACME	mail\rstorm
Rodrigo Castello Branco/ACN	Rodrigo Castello Branco/ACME@ACM	mail\rcastell
Uwe Wiest/ACME	Uwe Wiest/ACME@ACME	mail\uwiest
Wilma Storm/ACME	Wilma Storm/ACME@ACME	mail\wstorm

Connected to server Dom1a/ACME

Figure 9-20 Admin client - Messaging tab - Mail Users

For a graphical representation of dead and waiting mail in your Domino server's Mailbox, choose the Mail Routing Status view (Figure 9-21).

> **Note:** To see the graphical representations of Mail Routing Topology, and other Topology views, you must load the Maps Extractor (MAPS) Domino server task.



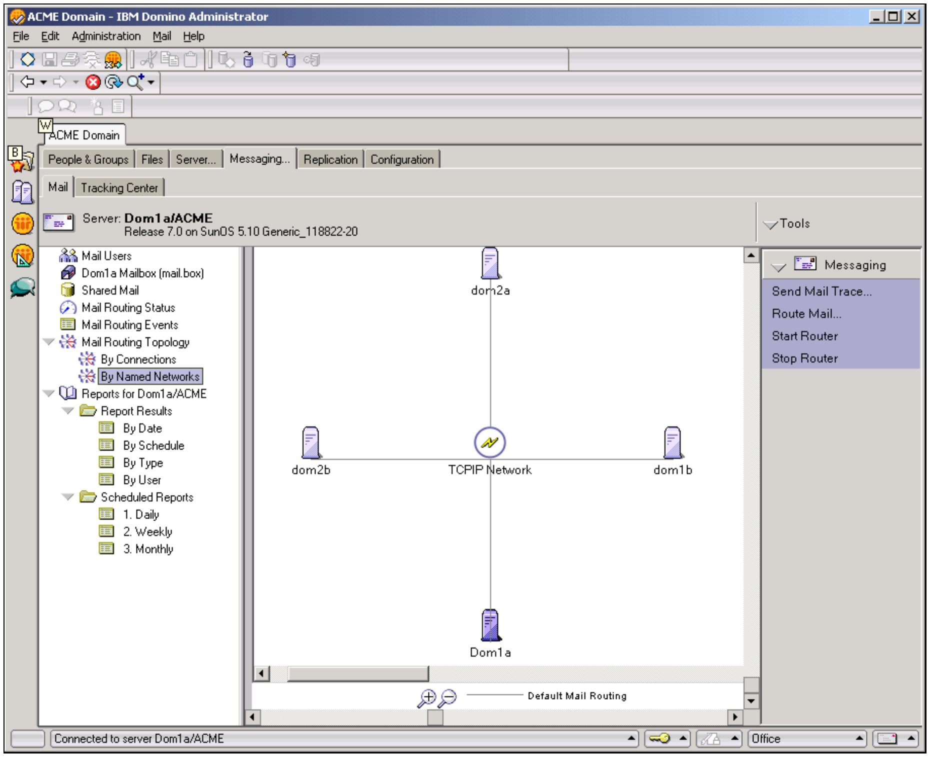
Server: **Dom1a/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

Mail.Domain is ACME

Last updated: Mon Nov 07 11:37:37 EST 2005 (Dom1a/ACME)

Figure 9-21   Admin client - Messaging tab - Mail Routing Status

Choose the Mail Routing Topology view to get a graphical depiction of your Mail Routing topology (Figure 9-22).



Server: Dom1a/ACME
Release 7.0 on SunOS 5.10 Generic_118822-20

Connected to server Dom1a/ACME

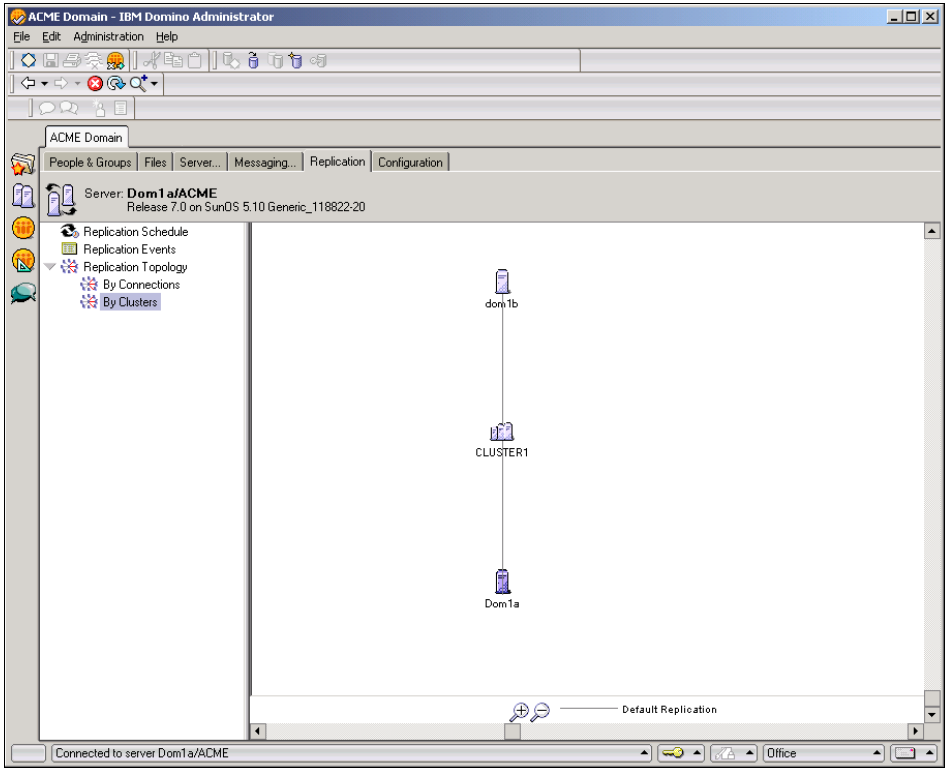
Figure 9-22 Admin client - Messaging tab - Mail Routing Topology

The Tracking Center sub-tab enables you to track the status of individual e-mail messages and determine whether the intended recipient received the message. The Message Tracking service must be enabled (individually, by server) first.

Replication tab

The Replication tab provides you with replication-related information. It is the only tab that has no context-specific tools associated with it. As shown in Figure 9-22 on page 287, you can view:

- A graphical representation of the current server's replication schedule
- The Replication events view from the log file
- A graphical representation of your Replication topology



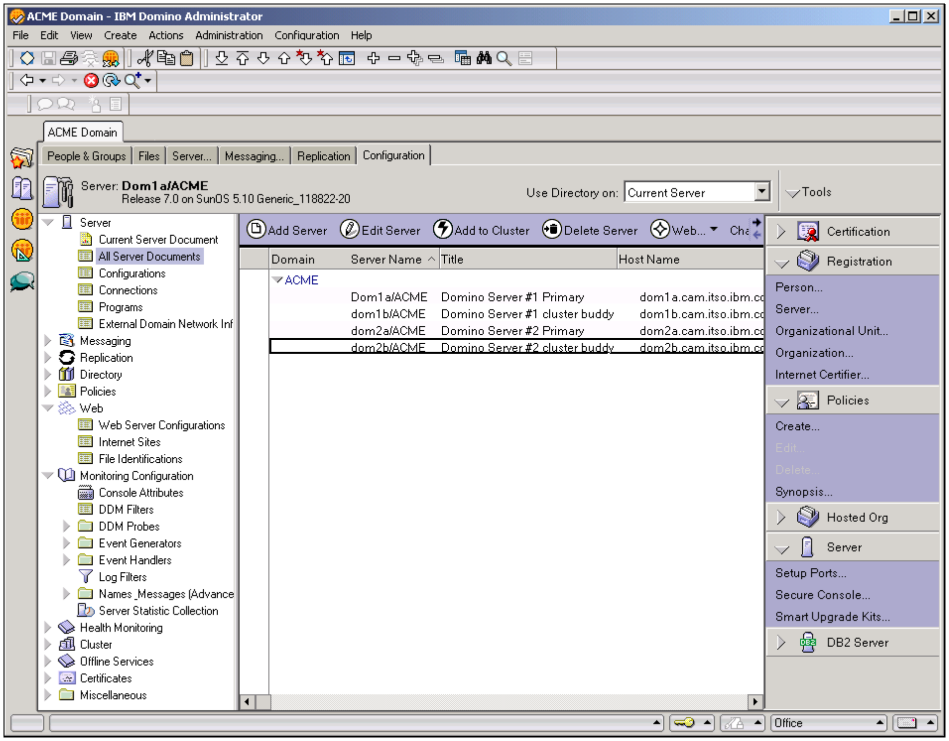
Server: Dom1a/ACME
Release 7.0 on SunOS 5.10 Generic_118822-20

Connected to server Dom1a/ACME

Figure 9-23 Admin client - Replication tab - Replication Topology

Configuration tab

The Configuration tab, shown in Figure 9-24, gives you access to all server configuration documents. You can access Server, Connection, Configuration, Program, and External Domain Documents under the Server category. You can also find documents related to Messaging, Replication, Web, Clustering, Statistics, and Events, and the Directory itself under the appropriate categories.



Server: **Dom1a/ACME**
Release 7.0 on SunOS 5.10 Generic_118822-20

Use Directory on: Current Server

Domain	Server Name	Title	Host Name
ACME			
	Dom1a/ACME	Domino Server #1 Primary	dom1a.cam.itso.ibm.cc
	dom1b/ACME	Domino Server #1 cluster buddy	dom1b.cam.itso.ibm.cc
	dom2a/ACME	Domino Server #2 Primary	dom2a.cam.itso.ibm.cc
	dom2b/ACME	Domino Server #2 cluster buddy	dom2b.cam.itso.ibm.cc

Figure 9-24 Admin client - Configuration tab

Use the Certification tools to certify, cross-certify, edit multiple passwords, and edit and extract recovery information. In addition, you can open the Certification Log file and view the properties of an ID file.

With the Registration tools you can register people, servers, organizations, organizational units, and Internet certifiers.

9.2 The Web Administrator

The Web Administrator enables you to manage and view settings for a Domino server from a browser. You can use it to keep your Domino server up and running, even when you do not have access to a Domino Administrator client.

In this section we present an overview of the things you can and cannot do with the Web Administrator, as well as how you can work with it.

9.2.1 Web Administrator functionality

Here is a list of some of the things you can do with the Web Administrator:

- Monitor mail, server memory, server disk space, and Web server statistics
- View server information and add and edit Server documents
- Manage database access control lists (ACLs)
- Create and delete databases
- Compact databases
- Create, update, and delete full-text indexes for databases
- Replicate databases
- Create new copies of databases
- Create new replicas of databases
- View database sizes and usage
- Manage users and groups
- View server log information and monitor messages in the log
- View database catalog information
- View events and statistics reports in the Statistics database
- Use the remote server console
- View Administration Process requests in the Administration Requests database
- Track messages
- Edit text files (for example, notes.ini)

9.2.2 Web Administrator limitations

Keep the following limitations in mind before using the Web Administrator:

- The Server you administer must be set up as a Web server, running the HTTP task.
- You can only administer the server on which the Web Administrator runs.
- You cannot use pass thru to access another server using the Web Administrator.

9.2.3 Working with the Web Administrator

In this section we describe how to work with the Web Administrator.

> **Note:** Refer to the Domino 7 Administration Help for detailed instructions on administering the Domino server.

Setting up the Web Administrator

With the Web Administrator, all you need to administer your server is a network connection to the server and a Web browser.

The Web Administrator uses the Web Administrator database (WEBADMIN.NSF). The first time the HTTP task starts on a Web server, Domino automatically creates this database in the Domino data directory. However, you need to make sure that the Web browser meets the following requirement for the Web Administrator to run.

Web browser requirement

You must use one of these browsers with the Web Administrator:

- Microsoft Internet Explorer 6.0 on Windows 2000 or Windows XP
- Mozilla 1.7.6 on Microsoft Windows XP Professional, Microsoft Windows 2000, IBM AIX, Solaris, Linux REL 3.0 and Novell Linux Desktop 9
- Mozilla on Windows 2000 and Linux 7.x
- The Mozilla Foundation Firefox 1.0.x browser on Microsoft Windows 2000, Windows XP, and Linux.

For current information about supported browsers, see the Release Notes.

Note: We experienced identical, minor display-formatting issues in the Domino 7 Web Administrator using the following browsers:

- Mozilla Navigator 1.7.12 on Windows 2000
- Internet Explorer 6.0 on Windows 2000
- Mozilla Firefox 1.0.7 (unsupported) on Windows 2000

Domino server tasks required

You must have the following Domino 7 server tasks running:

- The Administration Process (AdminP) server task must be running on the Web Administrator server.
- The Certificate Authority (CA) process must be running on the Domino 7 server that has the Issued Certificate List database on it in order to register users or servers.
- The HTTP task must be running on the Web server so that you can use a browser to access it. For information about setting up a Domino Web server, see Chapter 14, “IBM Lotus Domino 7 as a Web server” on page 431.

Notes user requirement

Your Lotus Notes user name and Internet (HTTP) password are required to authenticate with the server and log on as a Web Administrator. Set the Internet password in your Person document in the Domino Directory. You can find it on the Basics tab when in Edit mode.

Your Notes user name must be in the corresponding Notes group that is granted the privileges and permissions required to access the Web Administrator.

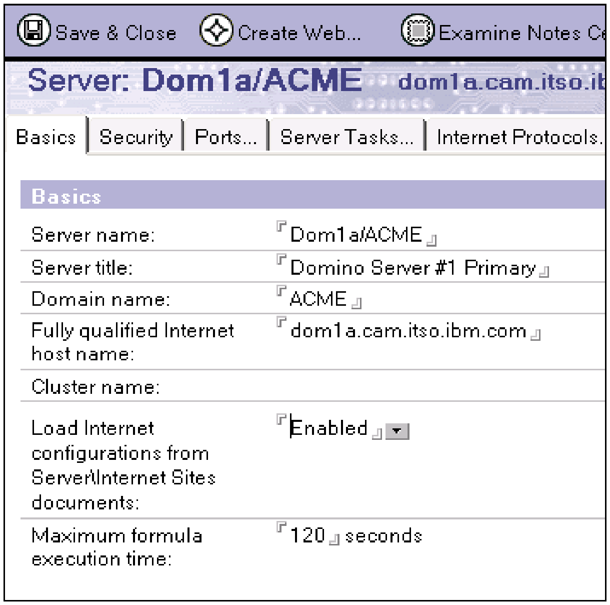
You can specify that you want to run the HTTP task on a Domino server. The Domino server then acts as a Web server so that browser clients can access databases on the server.

1. Set up the Domino server.
   - Make sure you understand TCP/IP concepts, including DNS host names and IP addressing.
   - Set up the Domino server. (See 5.3, “Setting up Domino servers” on page 109.)
   - Set up security for the server. (See Chapter 10, “Security” on page 331.)
2. Decide on an Internet connection strategy.
   - To enable users to connect to the server over the Internet, connect the server to an Internet Service Provider (ISP) and register the server’s

domain name and IP address on the ISP's DNS server. For more information, contact your ISP.

  - To enable users to connect to the server internally without connecting to the Internet, register the server's domain name and IP address in your organization's DNS.

3. Start the Domino server.
4. From the Domino Administrator, select the **Files** tab, open the Server document for the Domino server you want to administer via the Web, and enable **Load internet configurations from Server\Internet Sites documents** (Figure 9-25).



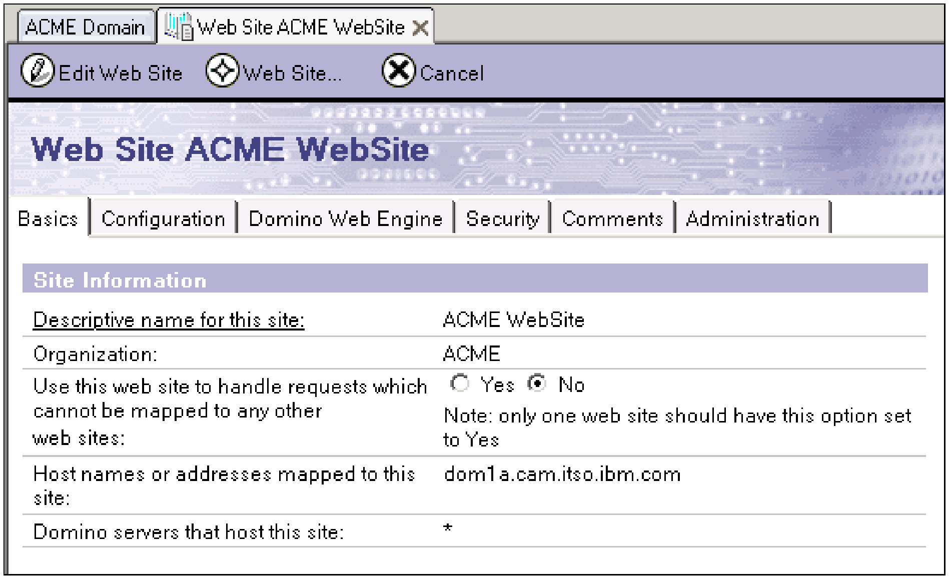
Basics

Server name:	Dom1a/ACME
Server title:	Domino Server #1 Primary
Domain name:	ACME
Fully qualified Internet host name:	dom1a.cam.itso.ibm.com
Cluster name:	
Load Internet configurations from Server\Internet Sites documents:	Enabled
Maximum formula execution time:	120 seconds

Figure 9-25 Admin client - Load Internet Configuration

> **Note:** This is new in Domino 7. In Domino 6 you would edit the Server document for the Domino Web server in the Domino Directory, then add the user or group name to the "Administer the server from a browser" field on the server's Security tab.

5. Create at least one Web site (Domino Web Site document). Select the **Configuration** tab and click **Web** → **Internet Sites** → **Add Internet Site** to create a new one if you do not already have one defined. Figure 9-26 shows an example.



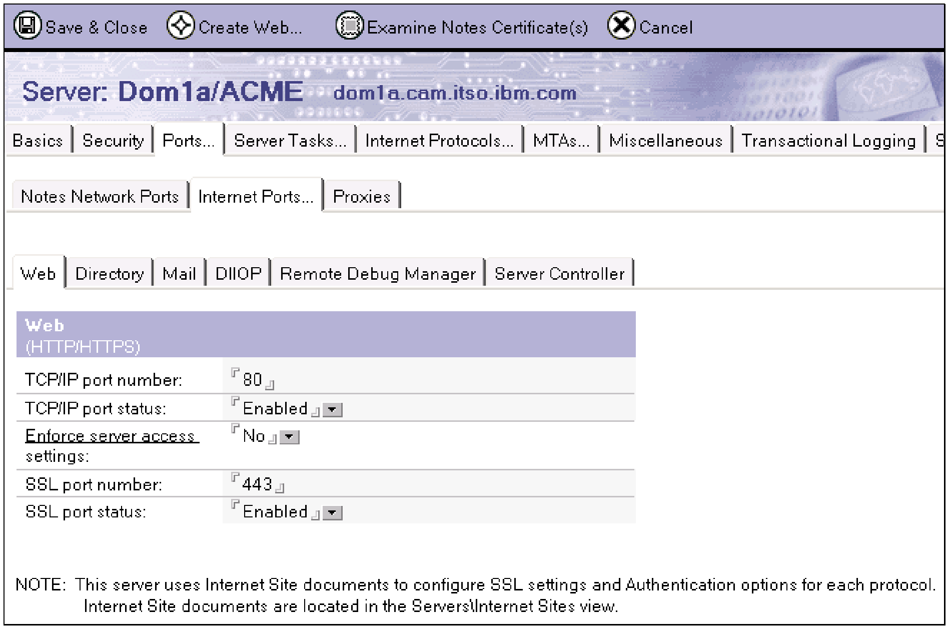
Web Site ACME WebSite

Site Information

Descriptive name for this site:	ACME WebSite
Organization:	ACME
Use this web site to handle requests which cannot be mapped to any other web sites:	○ Yes ● No Note: only one web site should have this option set to Yes
Host names or addresses mapped to this site:	dom1a.cam.itso.ibm.com
Domino servers that host this site:	*

Figure 9-26 Admin client - Sample Web Site Document

6. Decide on an HTTP port strategy. You can enable ports for TCP/IP, SSL, or both. Edit the desired Server document (Figure 9-27), click **Ports** → **Internet Ports** → **Web**, and enable **TCP/IP port status**, **SSL port status**, or both.



TCP/IP port number:	80
TCP/IP port status:	Enabled
Enforce server access settings:	No
SSL port number:	443
SSL port status:	Enabled

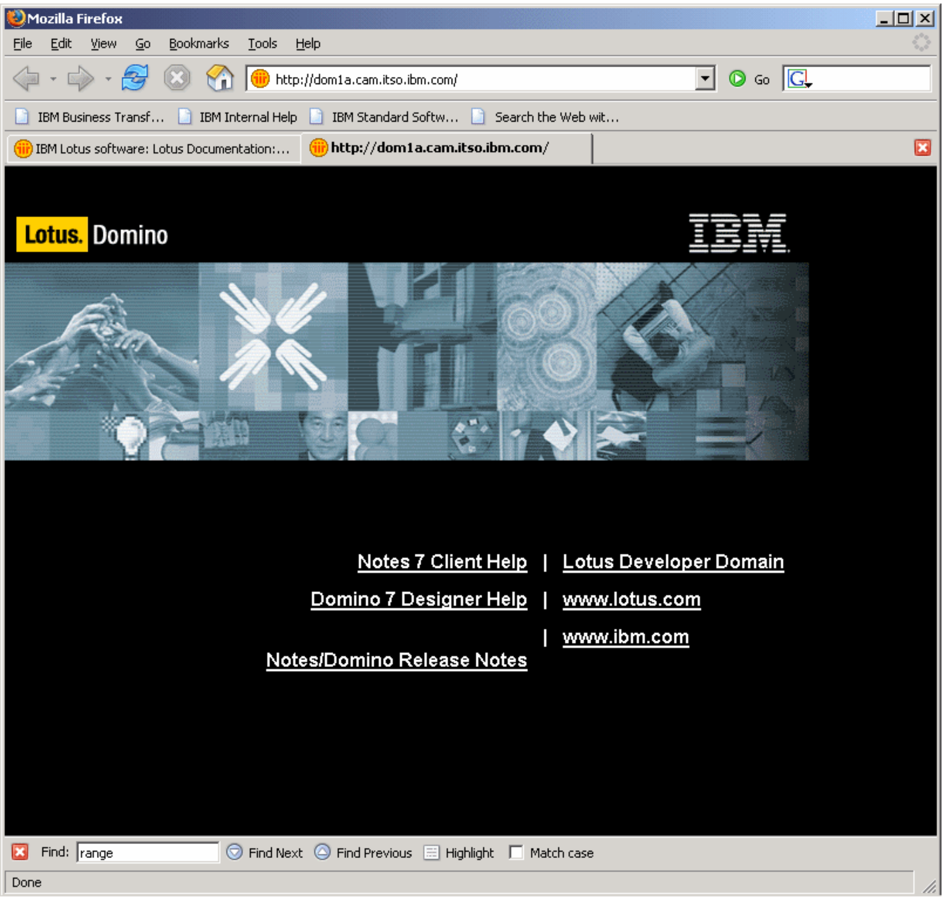
NOTE: This server uses Internet Site documents to configure SSL settings and Authentication options for each protocol. Internet Site documents are located in the Servers\Internet Sites view.

Figure 9-27 Admin client - HTTP/SSL Port config

7. (Optional) Enable the Domino Web server log. You can log your server activity and Web server requests to the Domino Web server log (DOMLOG.NSF) database. This option might be preferable if you want to create views and view data in different ways. Refer to Domino Administrator Help for configuration details.

8. Start the HTTP task on the Domino server.

To check the basic Web server setup, launch your browser and enter the DNS name or IP address for the Domino Web server. If the configuration is correct, you will see a display that resembles Figure 9-28.



http://dom1a.cam.itso.ibm.com/

Find: range

Figure 9-28 Domino 7 Web Administrator - Validate web server configuration

> **Note:** Each Web Administrator database has a unique replica ID. Therefore, it cannot replicate between servers.

Recall that in order to run the Web Administrator, you require access to the Webadmin.nsf database. This is our next step.

Setting up access to the Web Administrator database

Domino automatically sets up default database security when the Web Administrator database (WEBADMIN.NSF) is created for the first time. At that time, all names listed in either the Full Access Administrators or Administrators fields of the Server document are given Manager access with all roles to the Web Administrator database. In addition, the HTTP server task periodically (about every 20 minutes) updates the Web Administrator database ACL with names that have been added to the Server document in either the Full Access Administrators or Administrators fields, but only if the names are not already on the ACL list.

To allow additional administrators to use the Web Administrator, you must give them the appropriate access.

Perform the following steps to set up access for another server administrator (individual person) or a group of server administrators:

1. Add the new server administrator's name or the new group name to the ACL of Webadmin.nsf and give the user or group Manager access.

   Tip: We strongly advise giving the required Web Admin access to specialized groups that are designed for this purpose. Then, when changing Web Administrator personnel, you can change the membership of the group without having to change the ACL. This is a generally advised practice with Domino ACL management.

2. Refine access by assigning the appropriate Web Administrator database roles for your environment.

   Restriction: Web Administrators cannot Register new users unless they have the [UserCreator] Role assigned to them in the ACL. Similarly, Web Administrators cannot register new servers unless they have the [ServerCreator] Role assigned to them.

3. Make sure that all Web server administrators have an Internet password set in their Person document.

   Note: If you are using Secure Sockets Layer (SSL) for authentication, you have to set up the browser for SSL. For more information, see "Setting up Notes and Internet clients for SSL authentication" in Domino 7 Administrator Help.

Controlling access to the Web Administrator files

File Protection documents control access to non-database files that users can access via Web browsers. Like database file (.NSF) access control lists (ACLs), which specify the names of the users who can access them and the level of access they have, you can enforce file protection for files that browser users can access — for example, HTML, JPEG, and GIF — also by specifying the level of access for these types of files and the names of the users who can access them.

> **Important:** You do not need to use a File Protection document to protect a database (.NSF) file; instead, you use a database ACL.

The Web Administrator files are stored in the subdirectory domino/adm-bin of the Domino data directory. You should protect access to this directory so that unauthorized users cannot access the Web Administrator.

A File Protection document is created in the Domino Directory during initial server startup. This document provides administrators with Write, Read, and Execute access to the Domino Directory. Other users are assigned No Access. The File Protection document is a security feature that protects the files on a server's hard drive by controlling the Web clients' access to files. You can enforce file system security for files that browser users can access, including levels of access and the names of users who may access the files.

You can create a File Protection document for a directory or for an individual file.

Creating file protection for Web Site documents

In Domino 7, you create a File Protection document for a specific Web site. This document then only applies to that specific Web site.

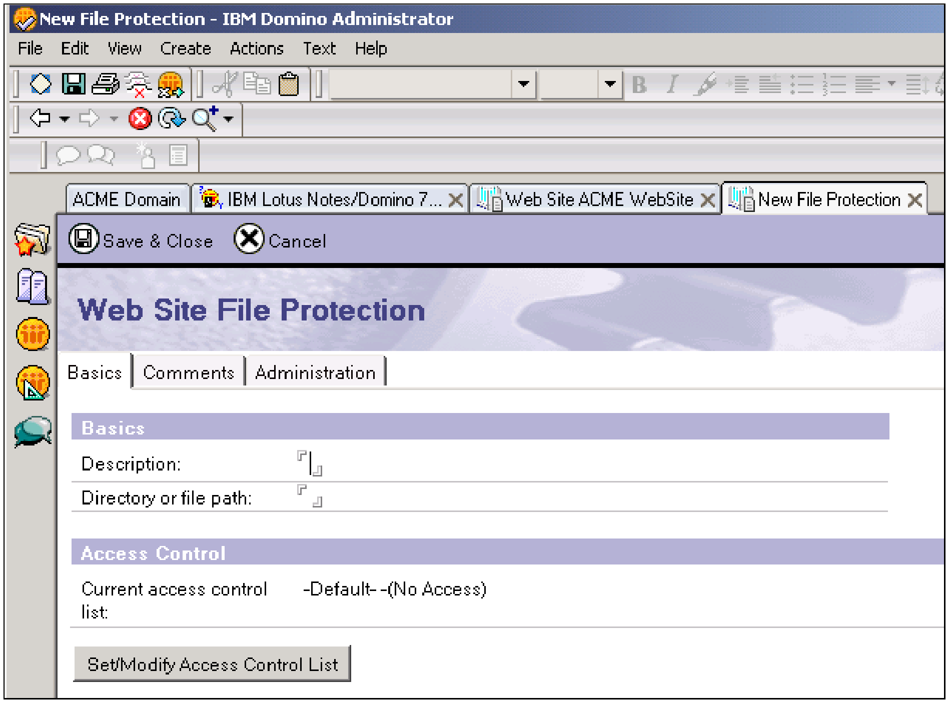
File Protection documents provide limited security. Use Domino security features, such as database ACLs, to protect sensitive information.

To create file protection for a Web Site document:

1. From the Domino Administrator, choose **Configuration** → **Web** → **Internet Sites**.
2. Open the Web Site document for which you want to create file protection.
3. Click **Web Site** and choose **Create File Protection**. (See Figure 9-29 on page 299.)
   - Click the **Basics** tab and complete the fields.
   - Click the **Administration** tab and complete the fields.
4. Save the document.

5. Enter this Domino Console command to refresh the HTTP settings:

```
tell http refresh
```



Web Site File Protection

Basics

Description:

Directory or file path:

Access Control

Current access control list: -Default- -(No Access)

Figure 9-29 Domino 7 Web Administrator - Create File Protection document

Note: Refer to Domino 7 Administrator Help for more information about how to configure File Protection documents for your environment.

Launching the Web Administrator

Use the following steps to start the Web Administrator:

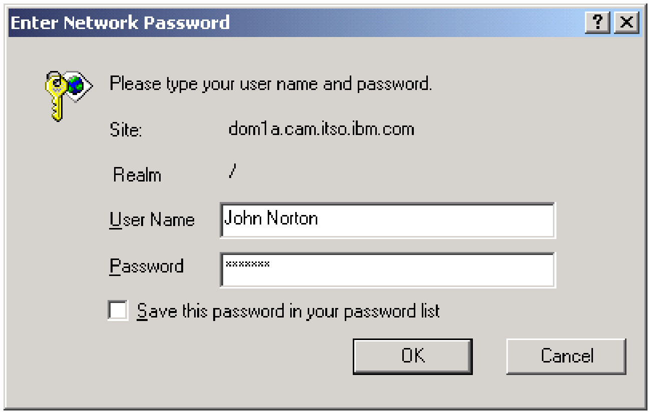
1. Start the HTTP task on the server if it is not already running.
2. From the browser, enter the URL for the Web Administrator database on the server you want to administer. For example, enter:

   ```
   http://yourserver.domain.com/webadmin.nsf
   ```

   Or for SSL, enter:

   ```
   https://yourserver.domain.com/webadmin.nsf
   ```

3. Enter your user name and Internet password (Figure 9-30); user name is your Notes hierarchical name or common name (John Doe/Company or John Doe).



Please type your user name and password.

Site: dom1a.cam.itso.ibm.com

Realm /

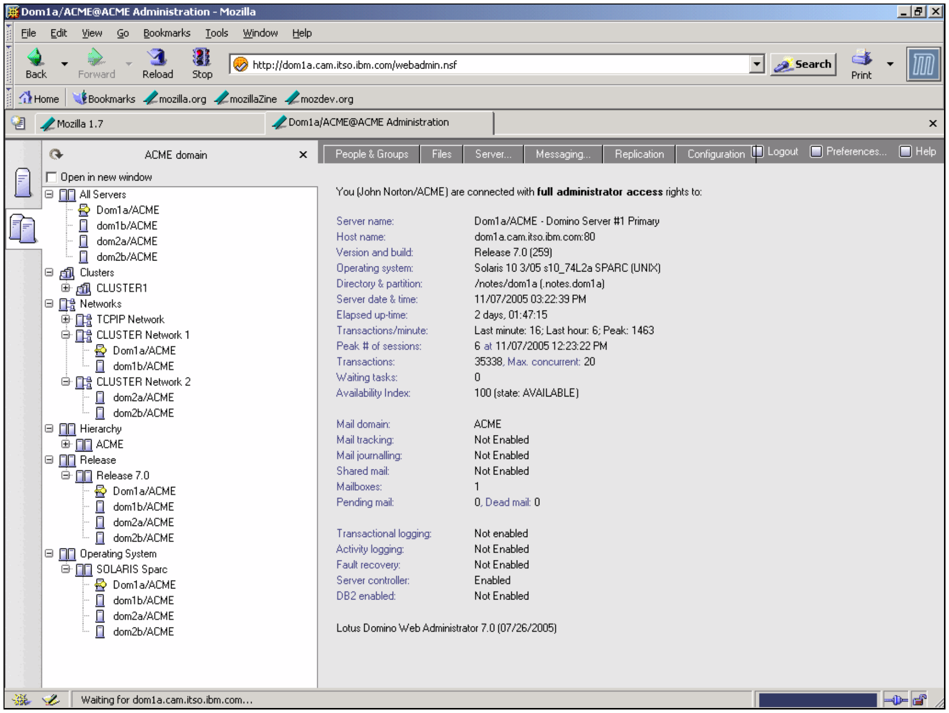
User Name John Norton

Password *******

□ Save this password in your password list

Figure 9-30 Domino 7 Web Administrator - User Authentication

After you have authenticated successfully, a window appears similar to Figure 9-31.



You (John Norton/ACME) are connected with **full administrator access** rights to:

Server name: Dom1a/ACME - Domino Server #1 Primary
Host name: dom1a.cam.itso.ibm.com:80
Version and build: Release 7.0 (259)
Operating system: Solaris 10 3/05 s10_74L2a SPARC (UNIX)
Directory & partition: /notes/dom1a (.notes.dom1a)
Server date & time: 11/07/2005 03:22:39 PM
Elapsed up-time: 2 days, 01:47:15
Transactions/minute: Last minute: 16; Last hour: 6; Peak: 1463
Peak # of sessions: 6 at 11/07/2005 12:23:22 PM
Transactions: 35338, Max. concurrent: 20
Waiting tasks: 0
Availability Index: 100 (state: AVAILABLE)

Mail domain: ACME
Mail tracking: Not Enabled
Mail journalling: Not Enabled
Shared mail: Not Enabled
Mailboxes: 1
Pending mail: 0, Dead mail: 0

Transactional logging: Not enabled
Activity logging: Not Enabled
Fault recovery: Not Enabled
Server controller: Enabled
DB2 enabled: Not Enabled

Lotus Domino Web Administrator 7.0 (07/26/2005)

Figure 9-31 Domino 7 Web Administrator - Initial screen (expanded)

Tip: You can use multiple instances of the Web Administrator at the same time by starting another copy of the browser. Then you can arrange the windows so both copies are displayed onscreen.

Main administrator tasks

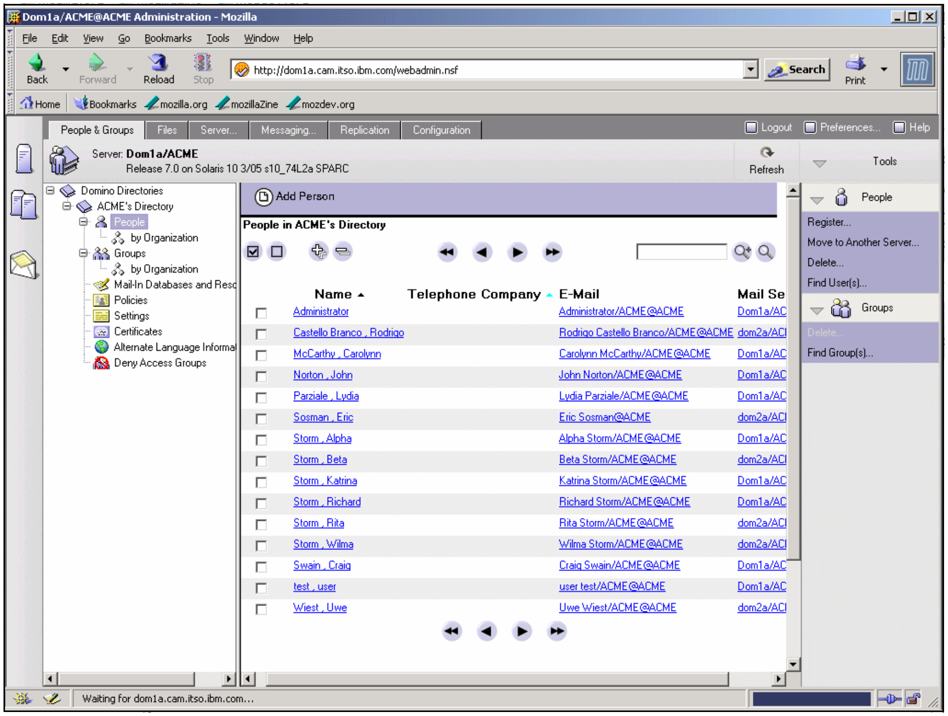
The Web Administrator offers a variety of tools which help you to administer your Domino servers. The look and feel of the Web Administrator closely mirrors the look and feel of the Lotus Domino Administrator client for Win32.

Note: The Web Administrator does not provide any of the rich graphical representations available in the Domino Administrator client.

Just like when you click on a tab in the Domino Administrator client, clicking on Web Administrator tabs such as *People & Groups* or *Messaging* produces context-specific Tool options. The Web Administrator interface will look familiar if you are already accustomed to the Domino Administrator client. This section describes a few of the main Web Administrator tasks.

People & Groups tab

Figure 9-32 shows the administration functions available to the Domino 7 Web Administrator, including the Tools drop-down list for user registration and group creation.


Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search
Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Refresh
Tools
Domino Directories
ACME's Directory
People
by Organization
Groups
by Organization
Mail-In Databases and Reso
Policies
Settings
Certificates
Alternate Language Informa
Deny Access Groups
Add Person
People
Register...
Move to Another Server...
Delete...
Find User(s)...
Groups
Delete...
Find Group(s)...

Server: **Dom1a/ACME**
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC

People in ACME's Directory

	Name ▲	Telephone Company ▲	E-Mail	Mail Se
□	Administrator		Administrator/ACME@ACME	Dom1a/AC
□	Castello Branco , Rodrigo		Rodrigo Castello Branco/ACME@ACME	dom2a/ACI
□	McCarthy , Carolynn		Carolynn McCarthy/ACME@ACME	Dom1a/AC
□	Norton , John		John Norton/ACME@ACME	Dom1a/AC
□	Parziale , Lydia		Lydia Parziale/ACME@ACME	Dom1a/AC
□	Sosman , Eric		Eric Sosman@ACME	dom2a/ACI
□	Storm , Alpha		Alpha Storm/ACME@ACME	Dom1a/AC
□	Storm , Beta		Beta Storm/ACME@ACME	dom2a/ACI
□	Storm , Katrina		Katrina Storm/ACME@ACME	Dom1a/AC
□	Storm , Richard		Richard Storm/ACME@ACME	Dom1a/AC
□	Storm , Rita		Rita Storm/ACME@ACME	dom2a/ACI
□	Storm , Wilma		Wilma Storm/ACME@ACME	dom2a/ACI
□	Swain , Craig		Craig Swain/ACME@ACME	Dom1a/AC
□	test , user		user test/ACME@ACME	Dom1a/AC
□	Wiest , Uwe		Uwe Wiest/ACME@ACME	dom2a/ACI

Waiting for dom1a.cam.itso.ibm.com...

Figure 9-32 Domino 7 Web Administrator - People

In the People view of the People & Groups tab, you can see the registered users of your Domino domain. You can register, move, and delete users using the links in the Tools pane located on the right side of the window.

To use the Web Administrator to register new Notes users, you must use the Domino server-based certification authority. Any request or task that requires a certifier ID file (for example, to migrate or modify ID) is not available.

You cannot set registration preferences in the Web Administrator. You must use the registration settings in the CA and in the Registration policy settings document.

Note: You must have at least Editor access, or Author access and the [UserCreator] role in the Domino Directory, to create new Person documents. You must have at least Editor access, or Author access and the [GroupCreator] role in the Domino Directory, to create new group documents.

In the People view of the People & Groups tab, you can see the registered users of your Domino domain. You can register, move, and delete users using the links in the Tools pane located on the right side of the window.

Important: To use the Web Administrator to register new Notes users, you must use the Domino server–based certification authority. Any request or task that requires a certifier ID file—for example, migrate or modify ID—is not available.

To use the Web Administrator to register users or servers, you must have Registration Authority (RA) access in the server-based certification authority (CA). The server that is running the Web Administrator should also be listed as an RA but that role is not required for the server. If, however, the server is not listed as an RA, the administrator that is an RA must open the Administration Requests database and approve the administration request to register the user. You must assign the RA role in the Domino Administrator, not in the Web Administrator. To assign the RA role, use the Modify Certifier tool on the Configuration panel.

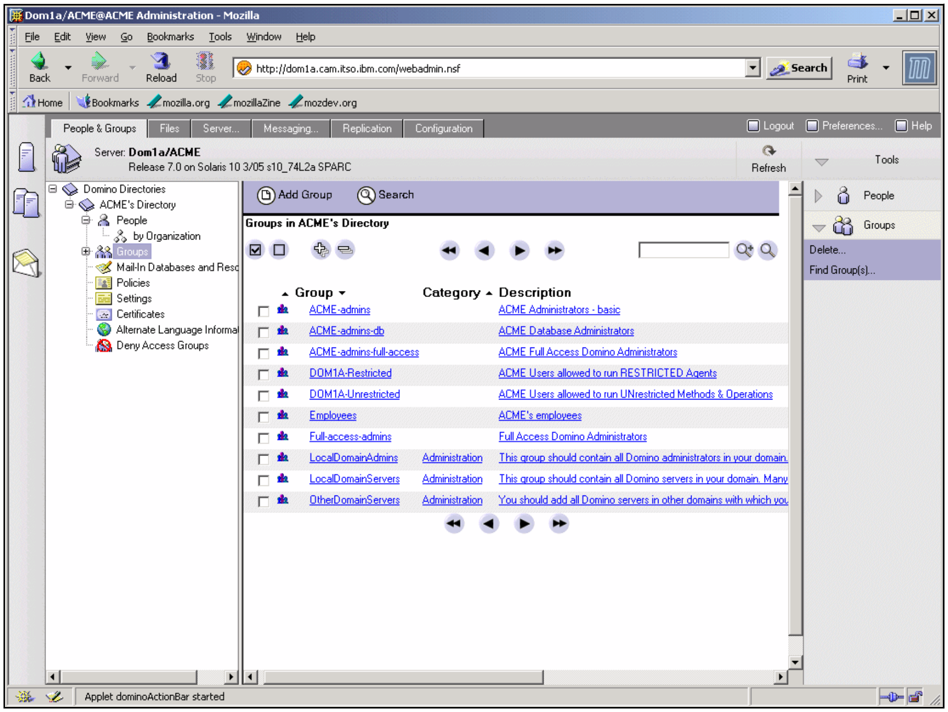
You cannot set registration preferences in the Web Administrator. You must use the registration settings in the CA and in the Registration policy settings document.

In the Web Administrator, you cannot configure a server for SSL during the server registration process.

In the Groups view of the People & Groups tab (Figure 9-33), you can see all of the groups in your Domino Directory. Each group has a *type*, and the available types are:

- Access Control only
- Deny List only
- Mail only
- Server only
- Multi-purpose

You can administer groups using the view buttons and the links in the Tools pane.



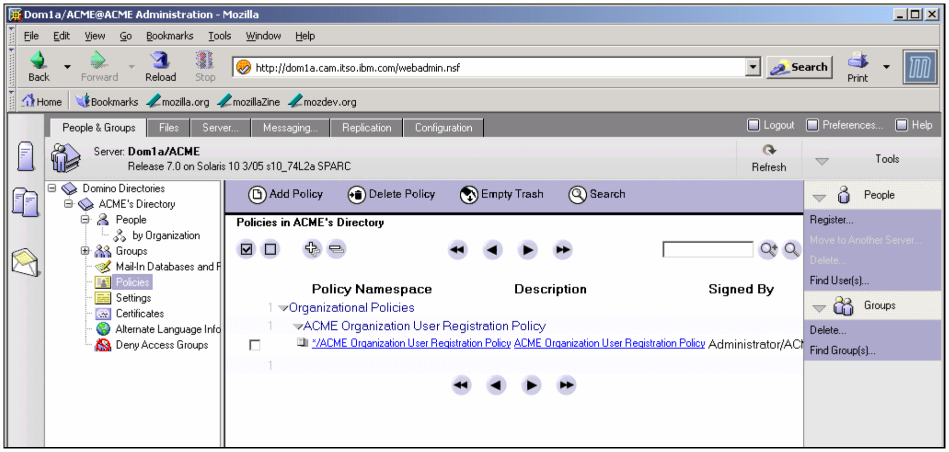
Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Server: Dom1a/ACME
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC
Refresh
Tools
Domino Directories
ACME's Directory
People
by Organization
Groups
Mail-In Databases and Reso
Policies
Settings
Certificates
Alternate Language Informa
Deny Access Groups
Add Group
Search
People
Groups
Delete...
Find Group(s)...
Applet dominoActionBar started

Groups in ACME's Directory

Group	Category	Description
ACME-admins		ACME Administrators - basic
ACME-admins-db		ACME Database Administrators
ACME-admins-full-access		ACME Full Access Domino Administrators
DOM1A-Restricted		ACME Users allowed to run RESTRICTED Agents
DOM1A-Unrestricted		ACME Users allowed to run UNrestricted Methods & Operations
Employees		ACME's employees
Full-access-admins		Full Access Domino Administrators
LocalDomainAdmins	Administration	This group should contain all Domino administrators in your domain.
LocalDomainServers	Administration	This group should contain all Domino servers in your domain. Many
OtherDomainServers	Administration	You should add all Domino servers in other domains with which you

Figure 9-33 Domino 7 Web Administrator - groups

The Domino 7 Web Administrator enables a Domino administrator to work with Mail-In Databases, Policies (both explicit and organizational), Settings, and Certificates (Figure 9-34).


Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Server: Dom1a/ACME
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC
Refresh Tools
Domino Directories
ACME's Directory
People
by Organization
Groups
Mail-In Databases and F
Policies
Settings
Certificates
Alternate Language Info
Deny Access Groups
Add Policy Delete Policy Empty Trash Search
People
Register...
Move to Another Server...
Delete...
Find User(s)...
Groups
Delete...
Find Group(s)...

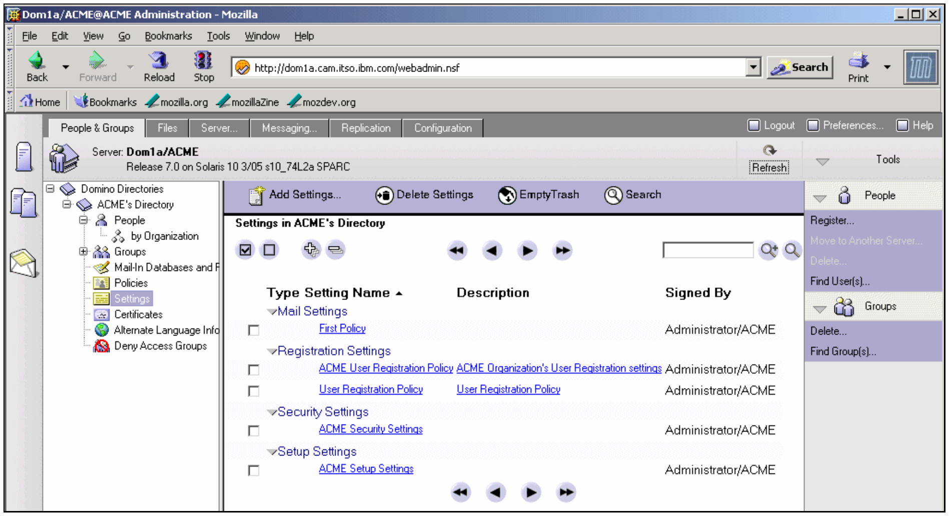
Policies in ACME's Directory

	Policy Namespace	Description	Signed By
1	Organizational Policies		
1	ACME Organization User Registration Policy		
□	*/ACME Organization User Registration Policy	ACME Organization User Registration Policy	Administrator/ACI
1			

Figure 9-34 Domino 7 Web Administrator - Policies

Domino Administrators can create policies and, using an established hierarchy, automatically distribute those policies across a group, a department, or an entire organization. The use of policies makes it easy for administrators to establish and maintain standard settings and configurations; it also automates redundant administrative tasks.

Policy Settings documents (Figure 9-35) organize settings by administrative function. The settings in these documents determine defaults, configuration, and rules that are applied to users or groups using Policy documents. Although policy setting documents define the default settings for users, there is no vehicle for assigning policy settings, except by using a Policy document. Policy setting documents are also where you control inheritance or enforcement of parent settings.



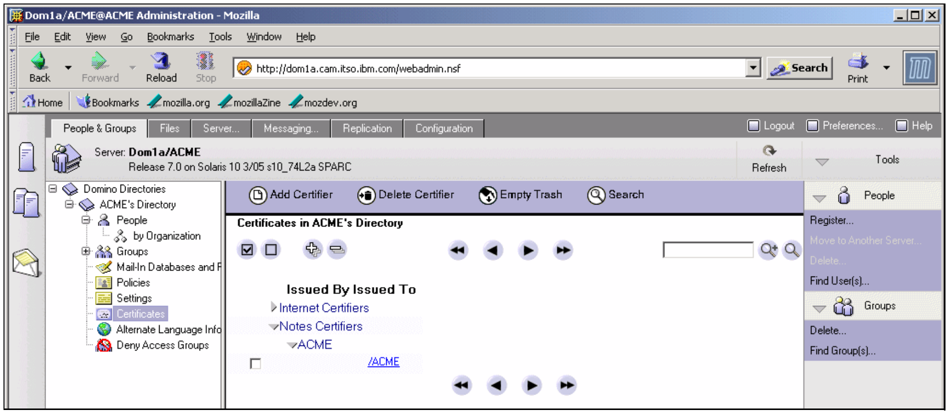
Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Server: Dom1a/ACME
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC
Refresh
Tools
Domino Directories
ACME's Directory
People
by Organization
Groups
Mail-In Databases and F
Policies
Settings
Certificates
Alternate Language Info
Deny Access Groups
Add Settings... Delete Settings EmptyTrash Search
People
Register...
Move to Another Server...
Delete...
Find User(s)...
Groups
Delete...
Find Group(s)...

Settings in ACME's Directory

Type	Setting Name ▲	Description	Signed By
Mail Settings			
□	First Policy		Administrator/ACME
Registration Settings			
□	ACME User Registration Policy	ACME Organization's User Registration settings	Administrator/ACME
□	User Registration Policy	User Registration Policy	Administrator/ACME
Security Settings			
□	ACME Security Settings		Administrator/ACME
Setup Settings			
□	ACME Setup Settings		Administrator/ACME

Figure 9-35 Domino 7 Web Administrator - Settings

The Certificates view (Figure 9-36) enables you to view and administer the certificates that authenticate users.



Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Server: Dom1a/ACME
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC
Refresh
Tools
Domino Directories
ACME's Directory
People
by Organization
Groups
Mail-In Databases and F
Policies
Settings
Certificates
Alternate Language Info
Deny Access Groups
Add Certifier Delete Certifier Empty Trash Search
People
Register...
Move to Another Server...
Delete...
Find User(s)...
Groups
Delete...
Find Group(s)...

Certificates in ACME's Directory

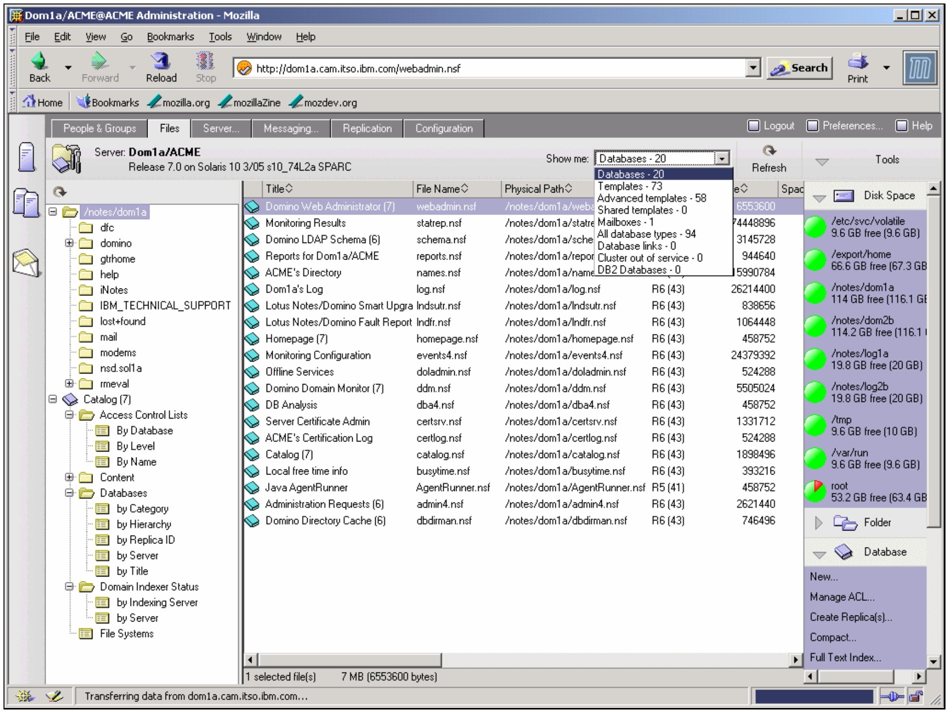
Issued By	Issued To
Internet Certifiers	
Notes Certifiers	
ACME	
□	/ACME

Figure 9-36 Domino 7 Web Administrator - Certificates

Files tab

The Domino 7 Web Administrator provides file-level access to the operating system. The file-level view begins in the Domino data directory and includes all subdirectories of the data directory (Figure 9-37).

On the Files tab, you can see and manage Domino databases and templates, as well as folders and links. You can perform many database management operations in this view, including compacting, signing and managing database ACLs, and viewing available disk space. These functions are all available in the Tools pane.



http://dom1a.cam.itso.ibm.com/webadmin.nsf

Server: **Dom1a/ACME**
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC

Show me: Databases - 20

- Databases - 20
- Templates - 73
- Advanced templates - 58
- Shared templates - 0
- Mailboxes - 1
- All database types - 94
- Database links - 0
- Cluster out of service - 0
- DB2 Databases - 0

Title◇	File Name◇	Physical Path◇		e◇	Spac
Domino Web Administrator (7)	webadmin.nsf	/notes/dom1a/weba		6553600	
Monitoring Results	statrep.nsf	/notes/dom1a/statre		74448896	
Domino LDAP Schema (6)	schema.nsf	/notes/dom1a/sche		3145728	
Reports for Dom1a/ACME	reports.nsf	/notes/dom1a/repor		944640	
ACME's Directory	names.nsf	/notes/dom1a/name		15990784	
Dom1a's Log	log.nsf	/notes/dom1a/log.nsf	R6 (43)	26214400	
Lotus Notes/Domino Smart Upgra	lndsutr.nsf	/notes/dom1a/lndsutr.nsf	R6 (43)	838656	
Lotus Notes/Domino Fault Report	lndfr.nsf	/notes/dom1a/lndfr.nsf	R6 (43)	1064448	
Homepage (7)	homepage.nsf	/notes/dom1a/homepage.nsf	R6 (43)	458752	
Monitoring Configuration	events4.nsf	/notes/dom1a/events4.nsf	R6 (43)	24379392	
Offline Services	doladmin.nsf	/notes/dom1a/doladmin.nsf	R6 (43)	524288	
Domino Domain Monitor (7)	ddm.nsf	/notes/dom1a/ddm.nsf	R6 (43)	5505024	
DB Analysis	dba4.nsf	/notes/dom1a/dba4.nsf	R6 (43)	458752	
Server Certificate Admin	certsrv.nsf	/notes/dom1a/certsrv.nsf	R6 (43)	1331712	
ACME's Certification Log	certlog.nsf	/notes/dom1a/certlog.nsf	R6 (43)	524288	
Catalog (7)	catalog.nsf	/notes/dom1a/catalog.nsf	R6 (43)	1898496	
Local free time info	busytime.nsf	/notes/dom1a/busytime.nsf	R6 (43)	393216	
Java AgentRunner	AgentRunner.nsf	/notes/dom1a/AgentRunner.nsf	R5 (41)	458752	
Administration Requests (6)	admin4.nsf	/notes/dom1a/admin4.nsf	R6 (43)	2621440	
Domino Directory Cache (6)	dbdirman.nsf	/notes/dom1a/dbdirman.nsf	R6 (43)	746496	

/etc/svc/volatile
9.6 GB free (9.6 GB)

/export/home
66.6 GB free (67.3 GB

/notes/dom1a
114 GB free (116.1 GI

/notes/dom2b
114.2 GB free (116.1

/notes/log1a
19.8 GB free (20 GB)

/notes/log2b
19.8 GB free (20 GB)

/tmp
9.6 GB free (10 GB)

/var/run
9.6 GB free (9.6 GB)

root
53.2 GB free (63.4 GB

1 selected file(s) 7 MB (6553600 bytes)

Transferring data from dom1a.cam.itso.ibm.com...

Figure 9-37 Domino 7 Web Administrator - Files

Table 9-1 shows the minimum access level required for a user to access various database functions.

Table 9-1 Minimum Access Control List levels

Database action	**Minimum access level**
Compact	Reader
Delete	Manager
Create full-text index	Designer
Update an index	Reader
Replicate, create a new copy or replica	Reader
Make changes to ACL	Manager

In addition, Maximum Internet name & password access must be set to **Manager** in the database whose ACL you are changing if you use name-and-password authentication to access the database.

Server tab

On the Server tab, the Domino 7 Web Administrator provides the Domino administrator with the ability to:

- Review several representations of Server status
- Analyze server activities
- Review server statistics

On the Status tab, you can see the status of different elements of your Domino environment (Figure 9-38 on page 309).

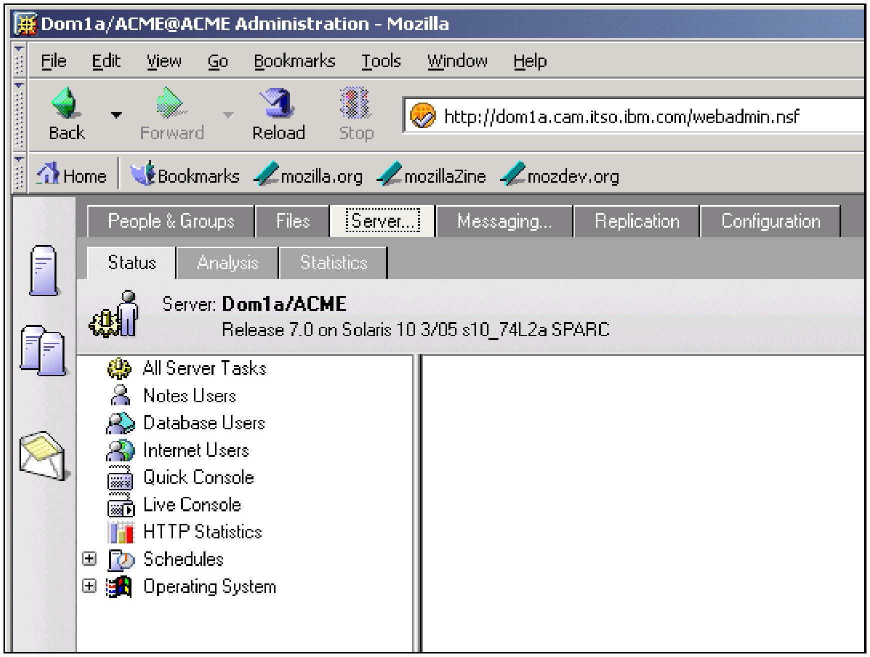


Figure 9-38 Domino 7 Web Administrator - Server - Status

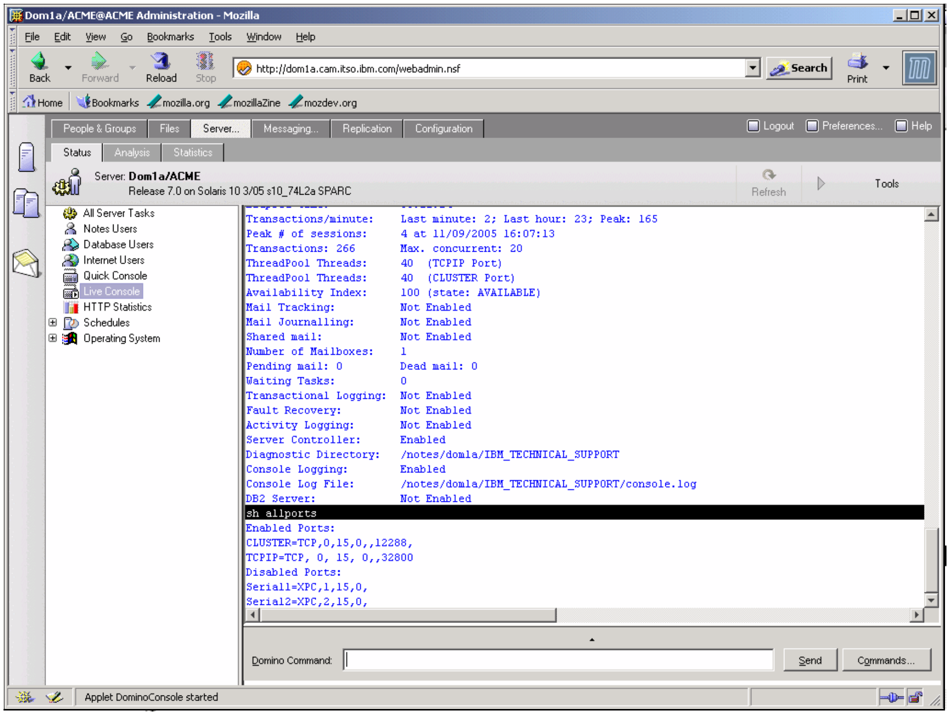
These status elements include:

- Server users: Shows who is using your Domino server.
- Database users: Indicates which databases are being accessed on your Domino server, and by whom.
- Quick Console: Enables you to issue console commands to the server.
- All server tasks: Shows a list of server tasks that are active.
- HTTP statistics: Shows various statistics about your Domino Web server; Figure 9-41 on page 312 shows an example statistics page.
- Schedules: Enables you to view schedules for programs, agents, mail routing, and replication.
- Operation system statistics.

You can perform several tasks by using the links in the Tools pane. These tasks include replicating databases and shutting down and restarting the Domino server.

There are two Domino Console options, the *Quick Console* and the *Live Console*, which you access from the Server Status sub-tab. These consoles mirror the server console on the Server - Status tab of the Domino Administrator.

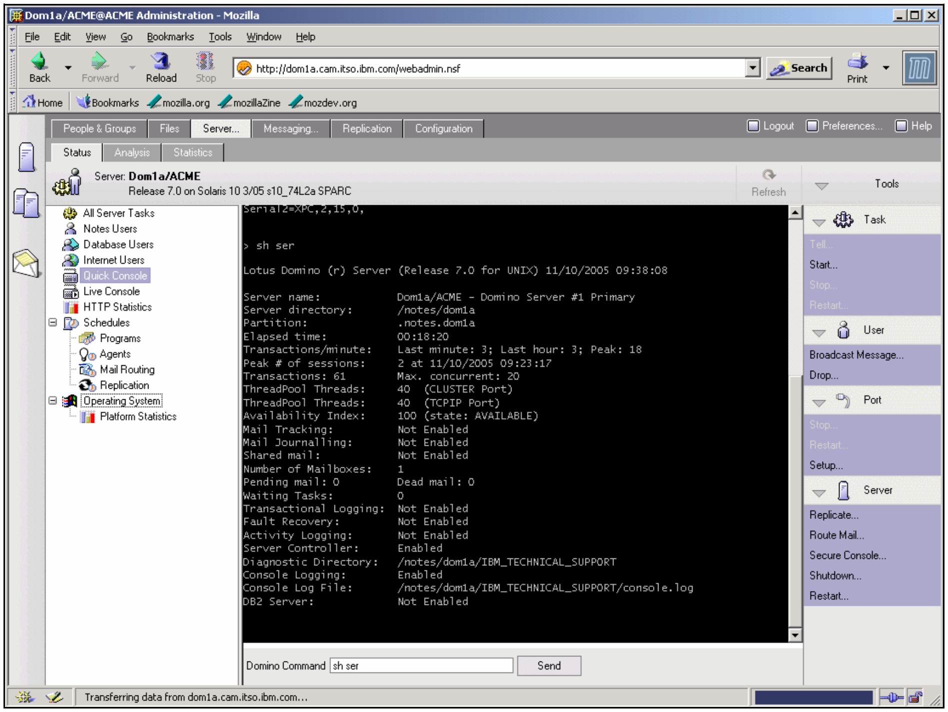
Use the Live Console (Figure 9-39) to send commands to a Web server running under a Server Controller. (See 9.4.2, “Domino (Java) Console” on page 325 for more information about the Server controller.) You can send Controller and shell commands, as well as Domino server commands. To use the Live Console, you must install Java Plug-in 1.4 or higher, and enable it in your Web browser.


Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Status Analysis Statistics
Server: Dom1a/ACME
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC
Refresh Tools
All Server Tasks
Notes Users
Database Users
Internet Users
Quick Console
Live Console
HTTP Statistics
Schedules
Operating System
Domino Command:
Send Commands...
Applet DominoConsole started

```
Transactions/minute:    Last minute: 2; Last hour: 23; Peak: 165
Peak # of sessions:     4 at 11/09/2005 16:07:13
Transactions: 266       Max. concurrent: 20
ThreadPool Threads:     40  (TCPIP Port)
ThreadPool Threads:     40  (CLUSTER Port)
Availability Index:     100 (state: AVAILABLE)
Mail Tracking:          Not Enabled
Mail Journalling:       Not Enabled
Shared mail:            Not Enabled
Number of Mailboxes:    1
Pending mail: 0         Dead mail: 0
Waiting Tasks:          0
Transactional Logging:  Not Enabled
Fault Recovery:         Not Enabled
Activity Logging:       Not Enabled
Server Controller:      Enabled
Diagnostic Directory:   /notes/dom1a/IBM_TECHNICAL_SUPPORT
Console Logging:        Enabled
Console Log File:       /notes/dom1a/IBM_TECHNICAL_SUPPORT/console.log
DB2 Server:             Not Enabled
sh allports
Enabled Ports:
CLUSTER=TCP,0,15,0,,12288,
TCPIP=TCP, 0, 15, 0,,32800
Disabled Ports:
Serial1=XPC,1,15,0,
Serial2=XPC,2,15,0,
```

Figure 9-39 Domino 7 Web Administrator - Server Live Console

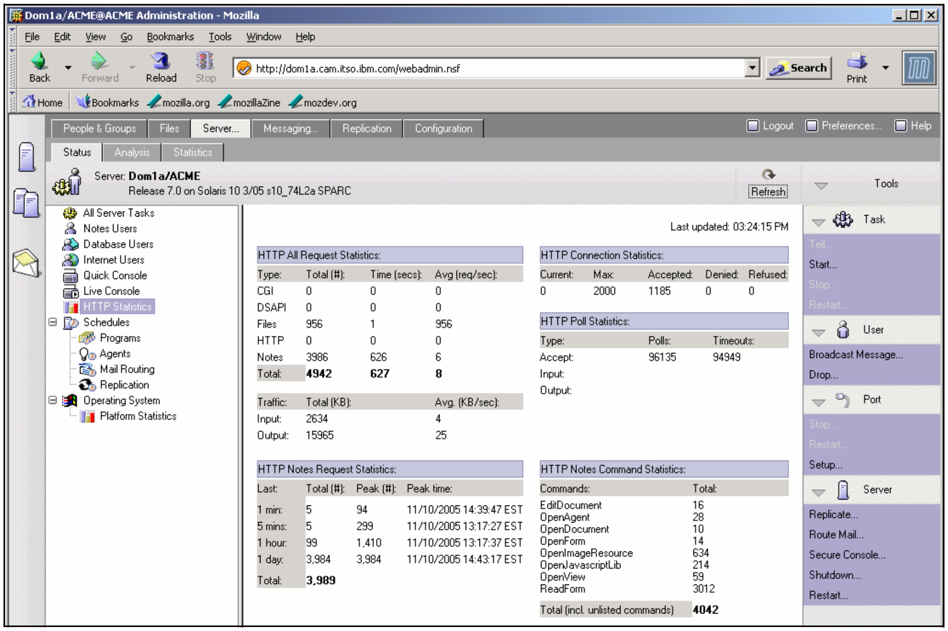
Use the Quick Console (Figure 9-40) to send commands to a Web server that does not run under a Server Controller. You can also use it if you are unable to install or use the Java plug-in in your browser.



```
Serial2=XPC,2,15,0,


> sh ser

Lotus Domino (r) Server (Release 7.0 for UNIX) 11/10/2005 09:38:08

Server name:            Dom1a/ACME - Domino Server #1 Primary
Server directory:       /notes/dom1a
Partition:              .notes.dom1a
Elapsed time:           00:18:20
Transactions/minute:    Last minute: 3; Last hour: 3; Peak: 18
Peak # of sessions:     2 at 11/10/2005 09:23:17
Transactions: 61        Max. concurrent: 20
ThreadPool Threads:     40  (CLUSTER Port)
ThreadPool Threads:     40  (TCPIP Port)
Availability Index:     100 (state: AVAILABLE)
Mail Tracking:          Not Enabled
Mail Journalling:       Not Enabled
Shared mail:            Not Enabled
Number of Mailboxes:    1
Pending mail: 0         Dead mail: 0
Waiting Tasks:          0
Transactional Logging:  Not Enabled
Fault Recovery:         Not Enabled
Activity Logging:       Not Enabled
Server Controller:      Enabled
Diagnostic Directory:   /notes/dom1a/IBM_TECHNICAL_SUPPORT
Console Logging:        Enabled
Console Log File:       /notes/dom1a/IBM_TECHNICAL_SUPPORT/console.log
DB2 Server:             Not Enabled
```

Figure 9-40 Domino 7 Web Administrator - Server Quick Console

Figure 9-41 shows an example of the Domino Server's HTTP Status display.



Last updated: 03:24:15 PM

HTTP All Request Statistics:

Type:	Total (#):	Time (secs):	Avg (req/sec):
CGI	0	0	0
DSAPI	0	0	0
Files	956	1	956
HTTP	0	0	0
Notes	3986	626	6
Total:	**4942**	**627**	**8**

Traffic:	Total (KB):	Avg. (KB/sec):
Input:	2634	4
Output:	15965	25

HTTP Connection Statistics:

Current:	Max:	Accepted:	Denied:	Refused:
0	2000	1185	0	0

HTTP Poll Statistics:

Type:	Polls:	Timeouts:
Accept:	96135	94949
Input:		
Output:		

HTTP Notes Request Statistics:

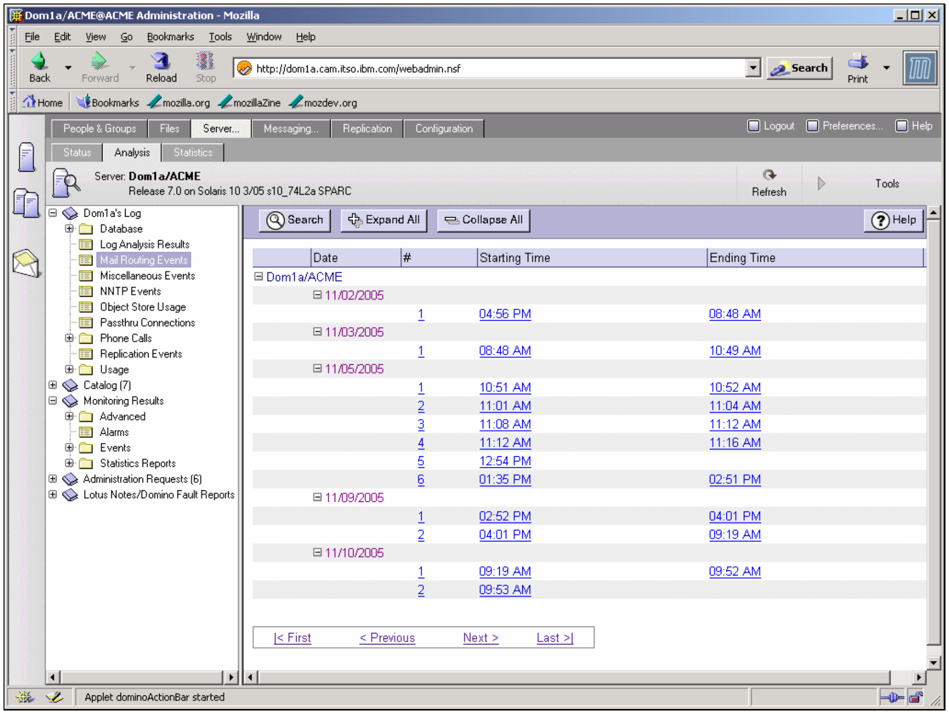
Last:	Total (#):	Peak (#):	Peak time:
1 min:	5	94	11/10/2005 14:39:47 EST
5 mins:	5	299	11/10/2005 13:17:27 EST
1 hour:	99	1,410	11/10/2005 13:17:37 EST
1 day:	3,984	3,984	11/10/2005 14:43:17 EST
Total:	**3,989**		

HTTP Notes Command Statistics:

Commands:	Total:
EditDocument	16
OpenAgent	28
OpenDocument	10
OpenForm	14
OpenImageResource	634
OpenJavascriptLib	214
OpenView	59
ReadForm	3012
Total (incl. unlisted commands)	**4042**

Figure 9-41 Domino 7 Web Administrator -Server HTTP status

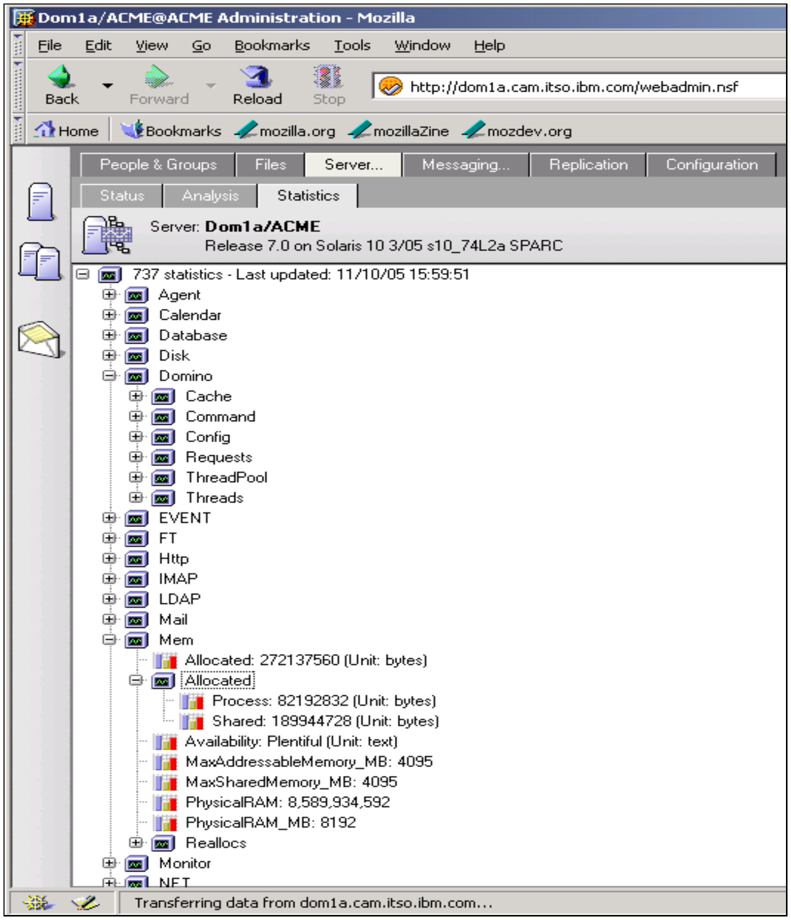
The Server analysis view (Figure 9-42) provides you with a wide variety of representations of information regarding databases, mail routing, replication, logs, and administration requests. See Lotus Domino Administrator 7 help for further information about data analysis.


Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search
Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Status Analysis Statistics
Server: Dom1a/ACME
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC
Refresh
Tools
Dom1a's Log
Database
Log Analysis Results
Mail Routing Events
Miscellaneous Events
NNTP Events
Object Store Usage
Passthru Connections
Phone Calls
Replication Events
Usage
Catalog (7)
Monitoring Results
Advanced
Alarms
Events
Statistics Reports
Administration Requests (6)
Lotus Notes/Domino Fault Reports
Search Expand All Collapse All Help
|< First < Previous Next > Last >|
Applet dominoActionBar started

Date	#	Starting Time	Ending Time
⊟ Dom1a/ACME			
⊟ 11/02/2005			
	1	04:56 PM	08:48 AM
⊟ 11/03/2005			
	1	08:48 AM	10:49 AM
⊟ 11/05/2005			
	1	10:51 AM	10:52 AM
	2	11:01 AM	11:04 AM
	3	11:08 AM	11:12 AM
	4	11:12 AM	11:16 AM
	5	12:54 PM	
	6	01:35 PM	02:51 PM
⊟ 11/09/2005			
	1	02:52 PM	04:01 PM
	2	04:01 PM	09:19 AM
⊟ 11/10/2005			
	1	09:19 AM	09:52 AM
	2	09:53 AM	

Figure 9-42 Domino 7 Web Administrator - Server analysis

The Server tab's Statistics sub-tab shows voluminous statistics about processes running on your system. These statistics include information about agents, databases, http, mail, and the server in general (Figure 9-43).



Server: **Dom1a/ACME**
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC

```
737 statistics - Last updated: 11/10/05 15:59:51
  Agent
  Calendar
  Database
  Disk
  Domino
    Cache
    Command
    Config
    Requests
    ThreadPool
    Threads
  EVENT
  FT
  Http
  IMAP
  LDAP
  Mail
  Mem
    Allocated: 272137560 (Unit: bytes)
    Allocated
      Process: 82192832 (Unit: bytes)
      Shared: 189944728 (Unit: bytes)
    Availability: Plentiful (Unit: text)
    MaxAddressableMemory_MB: 4095
    MaxSharedMemory_MB: 4095
    PhysicalRAM: 8,589,934,592
    PhysicalRAM_MB: 8192
    Reallocs
  Monitor
  NET
```

Transferring data from dom1a.cam.itso.ibm.com...

Figure 9-43 Domino 7 Web Administrator - Server statistics

Messaging tab

The Domino 7 Web Administrator enables you to manage every aspect of Enterprise Mail management from a Web browser. These tasks include:

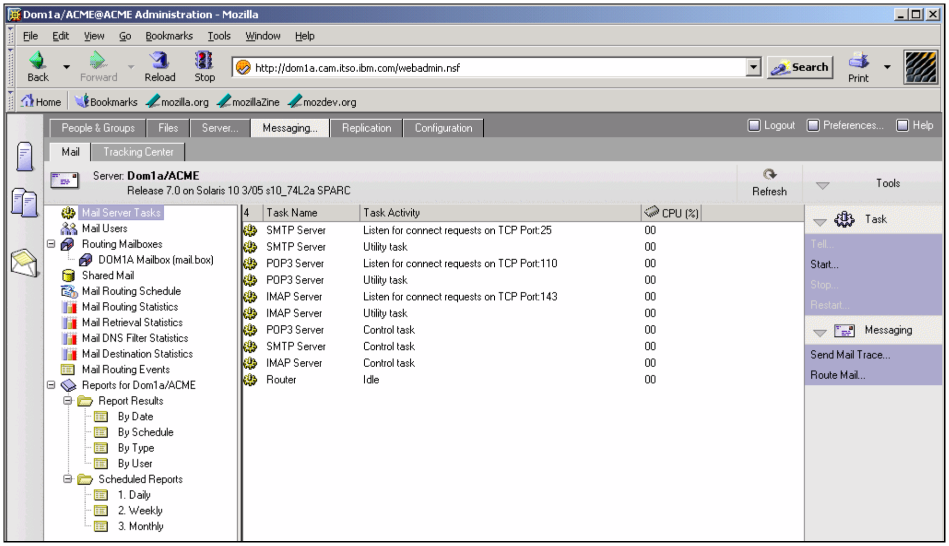
- Mail server tasks
- Mail routing activities and events
- Mail reports

You can access the Routing Events, Shared Mail, and Mail User views. You can examine the contents of the Routing Mailbox and configure multiple Routing Mailbox databases for a Domino server.

Important: Undeliverable (Dead) mail is held in the Routing Mailbox (mail.box) database by default, pending Administrator intervention.

If you have mail tracking enabled on a server, you can generate usage reports on that data. You can also track specific mail messages to determine whether the intended recipient received them. Figure 9-21 on page 286 shows the routing status of messages on the Domino Server. In this case there is no dead or waiting mail.

Within the Messaging tab, you can manage the mailboxes on your server, check mail routing, monitor the logfile, run reports on various messaging usage criteria, and use the Tracking Center tab to track messages. In the window shown in Figure 9-44, you can see the Mail server tasks and the status of our Domino server.


Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Mail Tracking Center
Refresh
Tools
Task
Tell... Start... Stop... Restart...
Messaging
Send Mail Trace... Route Mail...

Server: **Dom1a/ACME**
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC

- Mail Server Tasks
- Mail Users
- Routing Mailboxes
  - DOM1A Mailbox (mail.box)
- Shared Mail
- Mail Routing Schedule
- Mail Routing Statistics
- Mail Retrieval Statistics
- Mail DNS Filter Statistics
- Mail Destination Statistics
- Mail Routing Events
- Reports for Dom1a/ACME
  - Report Results
    - By Date
    - By Schedule
    - By Type
    - By User
  - Scheduled Reports
    - 1. Daily
    - 2. Weekly
    - 3. Monthly

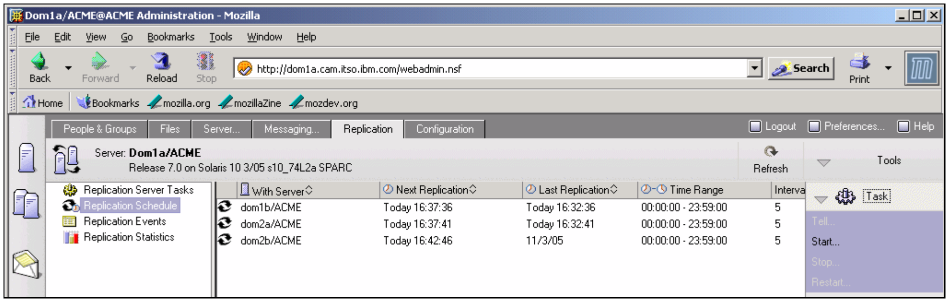
4 Task Name	Task Activity	CPU (%)
SMTP Server	Listen for connect requests on TCP Port:25	00
SMTP Server	Utility task	00
POP3 Server	Listen for connect requests on TCP Port:110	00
POP3 Server	Utility task	00
IMAP Server	Listen for connect requests on TCP Port:143	00
IMAP Server	Utility task	00
POP3 Server	Control task	00
SMTP Server	Control task	00
IMAP Server	Control task	00
Router	Idle	00

Figure 9-44 Domino 7 Web Administrator - Messaging - Mail

Replication

The Domino 7 Web Administrator enables you to control and manage the following replication activities (see Figure 9-45):

- Replication tasks
- Replication schedules
- Replication events
- Replication statistics


Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Refresh
Tools
Task
Tell... Start... Stop... Restart...

Server: **Dom1a/ACME**
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC

- Replication Server Tasks
- Replication Schedule
- Replication Events
- Replication Statistics

With Server	Next Replication	Last Replication	Time Range	Interva
dom1b/ACME	Today 16:37:36	Today 16:32:36	00:00:00 - 23:59:00	5
dom2a/ACME	Today 16:37:41	Today 16:32:41	00:00:00 - 23:59:00	5
dom2b/ACME	Today 16:42:46	11/3/05	00:00:00 - 23:59:00	5

Figure 9-45 Domino 7 Web Administrator - Replication

Configuration

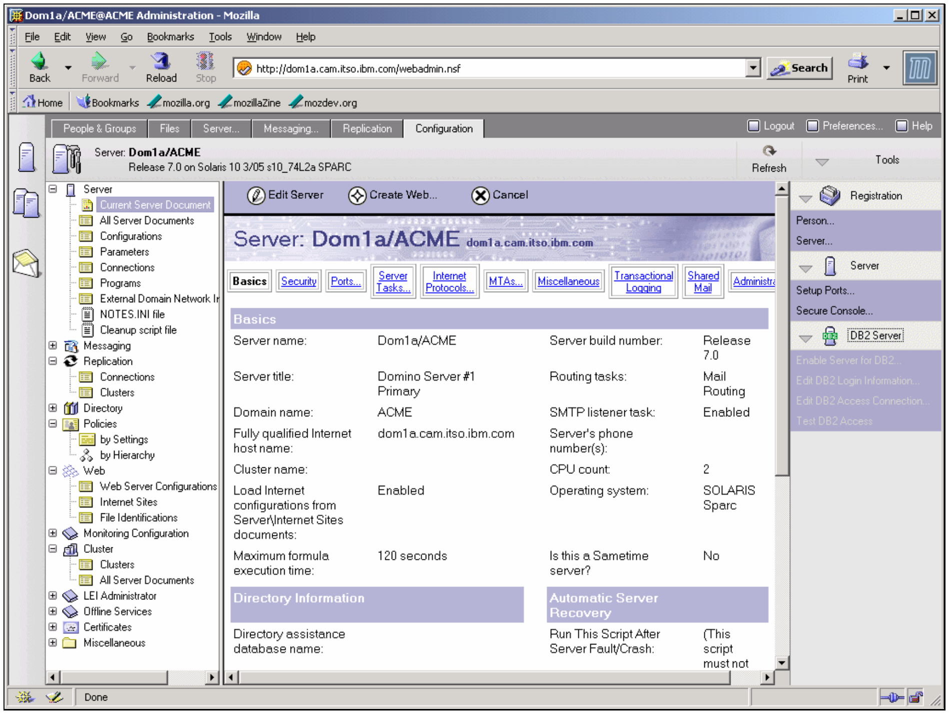
The Domino 7 Web Administrator provides the ability to control and modify several Domino server configuration options from a Web browser. The following configurations are available:

- Server documents, configurations, and connections
- Directory functions
- Web configuration
- Server monitoring
- Cluster management
- Miscellaneous

You can access Servers (server documents), Web Configuration, Clusters, Connections, Domains, Programs, and Configurations views from the Domino Directory.

One of the views available through the Configuration tab is the Current Server Document, which is shown in Figure 9-46. It provides access to your *current* Domino server document, which contains many of the configuration settings that define how that server operates. These settings include:

- Basic information, such as the server name and the host name of your server
- Security settings
- Network and port settings
- Server tasks
- Internet protocols and port assignments
- Mail routing
- Transaction logging


Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Server: Dom1a/ACME
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC
Refresh Tools
Server
Current Server Document
All Server Documents
Configurations
Parameters
Connections
Programs
External Domain Network Ir
NOTES.INI file
Cleanup script file
Messaging
Replication
Connections
Clusters
Directory
Policies
by Settings
by Hierarchy
Web
Web Server Configurations
Internet Sites
File Identifications
Monitoring Configuration
Cluster
Clusters
All Server Documents
LEI Administrator
Offline Services
Certificates
Miscellaneous
Edit Server Create Web... Cancel
Server: Dom1a/ACME dom1a.cam.itso.ibm.com
Basics Security Ports... Server Tasks... Internet Protocols... MTAs... Miscellaneous Transactional Logging Shared Mail Administra
Registration
Person...
Server...
Server
Setup Ports...
Secure Console...
DB2 Server
Enable Server for DB2...
Edit DB2 Login Information...
Edit DB2 Access Connection...
Test DB2 Access
Done

Basics

Server name:	Dom1a/ACME	Server build number:	Release 7.0
Server title:	Domino Server #1 Primary	Routing tasks:	Mail Routing
Domain name:	ACME	SMTP listener task:	Enabled
Fully qualified Internet host name:	dom1a.cam.itso.ibm.com	Server's phone number(s):	
Cluster name:		CPU count:	2
Load Internet configurations from Server\Internet Sites documents:	Enabled	Operating system:	SOLARIS Sparc
Maximum formula execution time:	120 seconds	Is this a Sametime server?	No

Directory Information

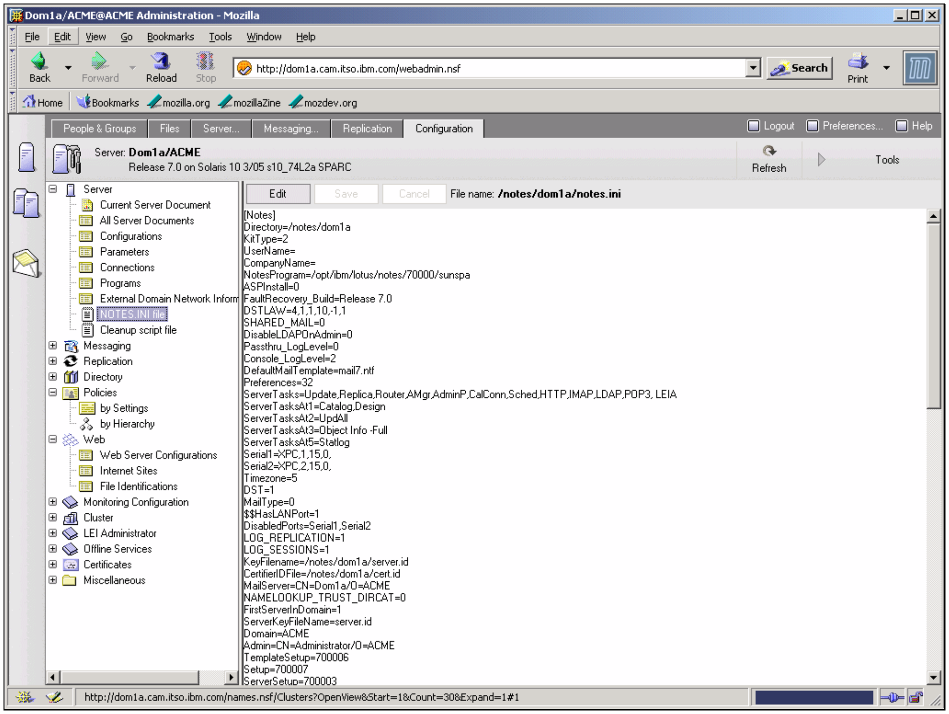
Directory assistance database name:

Automatic Server Recovery

Run This Script After Server Fault/Crash: (This script must not

Figure 9-46 Domino 7 Web Administrator - Configuration - Current Server Document

Figure 9-47 shows how you can open and edit System Files on the remote host system. This display shows how easy it is to update the server's notes.ini file. (See the following Important note about manually editing notes.ini.)


Dom1a/ACME@ACME Administration - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://dom1a.cam.itso.ibm.com/webadmin.nsf
Search Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
People & Groups Files Server... Messaging... Replication Configuration
Logout Preferences... Help
Server: Dom1a/ACME
Release 7.0 on Solaris 10 3/05 s10_74L2a SPARC
Refresh
Tools
Server
Current Server Document
All Server Documents
Configurations
Parameters
Connections
Programs
External Domain Network Inform
NOTES.INI file
Cleanup script file
Messaging
Replication
Directory
Policies
by Settings
by Hierarchy
Web
Web Server Configurations
Internet Sites
File Identifications
Monitoring Configuration
Cluster
LEI Administrator
Offline Services
Certificates
Miscellaneous
Edit Save Cancel
File name: /notes/dom1a/notes.ini
http://dom1a.cam.itso.ibm.com/names.nsf/Clusters?OpenView&Start=1&Count=30&Expand=1#1

```
[Notes]
Directory=/notes/dom1a
KitType=2
UserName=
CompanyName=
NotesProgram=/opt/ibm/lotus/notes/70000/sunspa
ASPInstall=0
FaultRecovery_Build=Release 7.0
DSTLAW=4,1,1,10,-1,1
SHARED_MAIL=0
DisableLDAPOnAdmin=0
Passthru_LogLevel=0
Console_LogLevel=2
DefaultMailTemplate=mail7.ntf
Preferences=32
ServerTasks=Update,Replica,Router,AMgr,AdminP,CalConn,Sched,HTTP,IMAP,LDAP,POP3, LEIA
ServerTasksAt1=Catalog,Design
ServerTasksAt2=UpdAll
ServerTasksAt3=Object Info -Full
ServerTasksAt5=Statlog
Serial1=XPC,1,15,0,
Serial2=XPC,2,15,0,
Timezone=5
DST=1
MailType=0
$$HasLANPort=1
DisabledPorts=Serial1,Serial2
LOG_REPLICATION=1
LOG_SESSIONS=1
KeyFilename=/notes/dom1a/server.id
CertifierIDFile=/notes/dom1a/cert.id
MailServer=CN=Dom1a/O=ACME
NAMELOOKUP_TRUST_DIRCAT=0
FirstServerInDomain=1
ServerKeyFileName=server.id
Domain=ACME
Admin=CN=Administrator/O=ACME
TemplateSetup=700006
Setup=700007
ServerSetup=700003
```

Figure 9-47 Domino 7 Web Administrator - Configuration - Server notes.ini

Important: Exercise caution when manually updating notes.ini on the Domino server. With Domino 7, an Administrator can use structured approaches to change notes.ini *without* having to edit the file manually. For example:

- In the Domino 7 Administrator client, click the **Configuration** tab. In the Navigator pane, click **Server** → **Configurations**, select the correct server and click **Edit Configuration**. In the Configuration Settings document, click the **NOTES.INI Settings** tab and follow the instructions to make your changes.
- In the Domino 7 Web Administrator, click the **Configuration** tab. In the Navigator pane, click the **Server** twistie, then click **Parameters**. Follow the instructions to make your changes.

Help

You can open the Domino 7 Administration Help database at any time, from anywhere in the Administration client. To access help, click **Help** in the main navigator pane or press F1. The Domino 7 Administration Help database contains detailed information about all aspects of setting up and maintaining a Domino server.

Exit Web Administrator

There are two ways to exit the Domino 7 Web Administrator:

- Click **Logout** on the Web Admin display. This returns you to the default server display window (Figure 9-28 on page 296).
- End your browser session.

Troubleshooting

This section describes some known problems and possible solutions. You can use this information as a basis for troubleshooting Web Administrator problems.

- If you are having trouble authenticating with the Domino Web Administrator, ensure that you are logging on with one of the entries specified in the User name field of your Person document, and that you are using the correct password as specified in the Internet password field.

  > **Note:** The short name is valid only if it is added to the User name field.

- Your name should also be listed in the group that has been defined for appropriate access in the ACL of Webadmin.nsf.
- Make sure that the File Protection document for the Web Administration executables is configured properly. File Protection documents protect files on a server's hard drive. They control the access that Web browser clients have to the files. Both the server and administrator should have post and get (read and write) access to the domino/adm-bin directory. For more information about File Protection documents, see "Protecting server files from Web client access" in the Domino 7 Administration Help database.
- Some browser configurations might require two authentications due to the way realms are handled. A realm is a string, typically a URL path, that the server sends to indicate the location, or path, for which the user has been authenticated. When two authentications are required, the remote console and some of the other applets do not function correctly until the second authentication has occurred. Selecting "Live Console" forces a second authentication if it is required.

- If your Domino server ID is using a password and you want to use the Web Administrator to modify database security (such as database ACLs and roles), you might need to set the server ID to not “prompt for a password from other Notes-based programs.” Failure to do so might cause the Domino server to hang (awaiting a password) if the Web Administrator is used to modify database ACLs. To set this, use a Notes client to access the Server ID, select **File** → **Security** → **User Security** to display the User Security pop-up box. On the Security Basics tab, select the **Don’t prompt for a password from other Notes-based programs (reduces security)** check box.
- Your Web browser cache should be set to check documents every time.
- If your Internet browser setting in your Location document is set to Notes with a separate Web browser, make sure that the **Update cache** setting in the **Advanced** → **Web Retriever** sub-tab of the Location document is set to **every time**. This setting overrides the setting in some Web browsers.
- If you have trouble creating databases or database replicas using the Web Administrator, it might be because the Create new databases or Create replica databases field in the Server document is not set correctly.

> **Tip:** If you encounter any problems with the Web Administration application, it is possible that the database has become damaged. Shut down HTTP, delete Webadmin.nsf, and restart HTTP. When HTTP starts, it checks for the existence of Webadmin.nsf, and creates a new one from the template if it does not exist.

9.3 The Domino Character Console

The Domino Character Console (the cconsole program), introduced in Domino R5, provides a way to access the server console from the Solaris command line. You can invoke the cconsole program multiple times simultaneously. You can also run the cconsole program when there is already an operational Domino server console; however, the cconsole input and output might also reflect commands launched from other console processes. The cconsole program ships with Domino 7. To access the cconsole:

1. Log on as the Solaris account you created for running the server (for example, sola1a).
2. Change to your Domino data directory

   ```
   cd /notes/dom1a
   ```

3. On the command line, enter:

   ```
   /opt/ibm/lotus/bin/cconsole
   ```

4. Enter the path to the administrator’s ID file, for example,

   `/notes/dom1a/admin.id`

5. Enter the password.
6. The Domino Console prompt “>” appears, indicating that console commands may now be entered. For example, to issue the Domino **`show tasks`** command, type `show tasks`.
7. To end a console session, type `done` at the console prompt.

See Example 9-1.

Example 9-1 cconsole example

```
$ /opt/ibm/lotus/bin/cconsole
Domino Character Console v0.0
Warning:  You are remotely connected to host dom1a.
If you have not taken precautions to secure this connection,
passwords will be exposed over the network.
Do you want to end this cconsole session? [y/n] n

Enter the full path to your ID file: /notes/dom1a/admin.id

Enter your password:
12/02/2005 09:00:28   Initiating cconsole on dom1a
>
```

Note: The Domino (Java) Console, introduced with Domino 6, can be used when a GUI is available. The Domino Java Console is available either from X11 Windows GUI or from a Windows workstation. The **`cconsole`** command is available to use if you do not have access to a GUI system, and remains popular in many Solaris installations.

In Domino 7, cconsole is located in /opt/ibm/lotus/bin by default. For more about the cconsole command, see the Domino 7 Administrator Help.

9.4 The Domino Server Controller and Domino Console

This section describes the Domino Server Controller and Domino (Java) Console.

9.4.1 Domino Server Controller

The Server Controller is a Java-based program that controls a Domino server. Starting the Server Controller starts the Domino server it controls. When a server runs under a Server Controller, you can send operating system commands (shell commands), Controller commands, and Domino server commands to the Server Controller. For example, from a remote console, you can use Controller commands to kill Domino processes on a server that is hung or to start a Domino server that is down.

You can use the Domino Console, a Java-based console, to communicate with a Server Controller. By default, the Server Controller listens on port 2050.

Restriction: You can run the Domino Console on any platform except Apple Macintosh.

Using the Domino Console, you can send commands to multiple servers. The Domino Console does not require a Notes ID, only a Domino Internet name and password, so you can connect to servers certified by different certifiers without having multiple Notes IDs or cross-certificates. You can customize output to the Domino Console — for example, use local event filters to specify the types of events the Console displays. You can also log server output to log files and customize the appearance of the Console.

Note: The Domino Console functions strictly as a server console. Consequently, the Domino Console does not include the full set of Domino administration features that are available through the Domino Administrator and the Web Administrator, and you cannot use it to open and manage Notes databases.

The files needed to run the Server Controller and to run the Domino Console are provided with Domino and Notes.

You can also use remote consoles in the Domino Administrator and Web Administrator to communicate with a Server Controller.

Starting and stopping the Server Controller

To start the Server Controller, the Domino server, and the Domino Console:

1. Shut down the Domino server, if it is running.
2. Start the Server Controller using the same command you normally use to start the Domino server but append the argument –jc. For example, if you run a server on Solaris from the program directory /opt/ibm/lotus/bin, use the following server start command to launch Domino, start the Server Controller, and run in the background:

   ```
   /opt/ibm/lotus/bin/server -jc &
   ```

Important: The Domino 7 Release Notes state that for the Domino Java Console, running the Server Controller in the background (UNIX systems only) might cause the Controller process not to run (in wait mode). There is currently no programmatic fix available. Although characterized as applying across all UNIX systems, this issue is not known to occur with Solaris. Associated SPRs: JBAA67MQR5

3. The Server Controller runs in its own window. You can minimize a Server Controller window, but do not close or kill the window to stop the Server Controller. Instead, use the Controller Quit command from a console to stop a Server Controller and the server it controls.

When you run a Server Controller, you no longer have access to the traditional console at the server. You can communicate only through the Domino Console or a console in the Domino Administrator or Web Administrator.

Starting the Server Controller using only the argument -jc starts the Domino Server and the Domino Console along with the Server Controller. There are two optional arguments you can specify to change this default behavior: -c and -s. (See options in Table 9-2.)

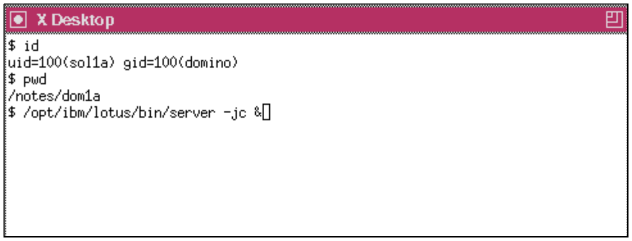
Use -c to prevent the Domino Console from running when you start the Server Controller. You might prevent the Console from running on a slow machine or a machine that is low on memory. If you use this argument and the Domino server ID requires a password, the Domino server starts without running its server tasks. To run the server tasks, you must connect to the Server Controller from a console and specify the server password when prompted.

Use -s to prevent the server from running when you start the Server Controller. Use this argument along with -c so that someone who is directly at the server can start only the Server Controller, and then a remote administrator can start the server and specify a required server password remotely from a console.

Table 9-2 Server Controller launch options

Example	Result
/opt/ibm/lotus/bin/server -jc	Runs the Server Controller, server, and Domino Console
/opt/ibm/lotus/bin/server -jc -c	Runs the Server Controller and the server
/opt/ibm/lotus/bin/server -jc -s	Runs the Server Controller and the Domino Console
/opt/ibm/lotus/bin/server -jc -c -s	Runs only the Server Controller

Figure 9-48 shows an example of launching Domino, the Server Controller, and the Domino Console from an X-Window in our sample environment.



```
$ id
uid=100(sol1a) gid=100(domino)
$ pwd
/notes/dom1a
$ /opt/ibm/lotus/bin/server -jc &
```

Figure 9-48 Launching Server Controller and Domino Console

Note: If you have more than one Domino partition, bind the server controller port, 2050, to each partition's TCP/IP address. See 5.4.1, "Partitioned server networking considerations" on page 181.

9.4.2 Domino (Java) Console

The Domino (Java) Console provides real-time interaction with the Domino server and is often the fastest way to see what is happening with a server. In Domino 7, the Domino Console is available through a new, powerful Java application.

The advantage of the new Java Domino Console feature is that, unlike the Win32 Administration client, you can connect to the Solaris server Domino is installed on, even when the Domino server is not responding.

You can run the Domino Console from any machine on which a Domino server or the Domino Administrator is installed. To use Domino Console to communicate with a Domino server, the server must be running under a Server Controller.

Starting the Domino Console

To start the Domino Console manually:

1. Make sure that the Domino server is installed on the machine.
2. If your Solaris server has graphics, keyboard, mouse, and the X11 Windows software installed, or you have remotely logged on and your DISPLAY environment variable is pointed to a workstation running X11, then the Java console will start on what your DISPLAY environment variable is pointing to. A DISPLAY set to :0.0 indicates that the main local display, *hostname*:0.0 indicates the main display on the workstation called *hostname*.

3. On a Solaris system running the X Window System, you can also run the following command directly from the program directory (/opt/ibm/lotus/bin), or from a directory path that points to the program directory:

   ```
   jconsole
   ```

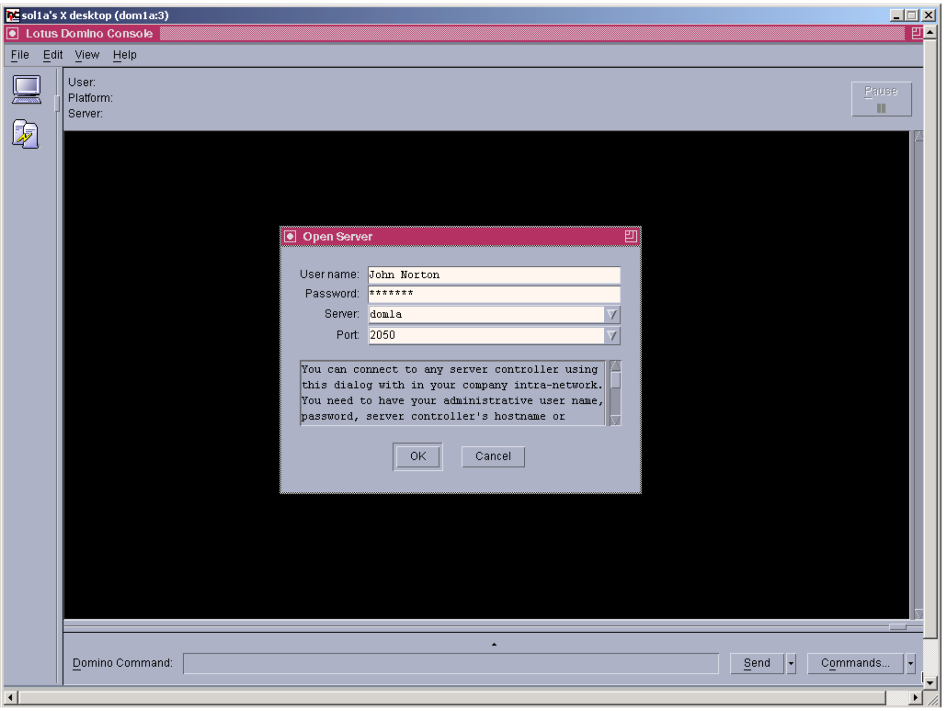
   Note: The Domino Console also starts by default when you start a Server Controller. See the example in Figure 9-48 on page 325.

For information about using the Domino Console, select **Help** → **Help Topics** from the Domino Console menu.

Once the Domino Console launches, you can connect to a new server by **File** → **Open Server** (or press Ctrl+O).

If you have previously connected to the server with this console, you can click the multiple server icon and select it from the list. In the prompt box, enter your Notes name (or shortname) as your user name and your Domino HTTP password in the password field. For a new server, type the name in the server; otherwise, select the server from the pull-down list.

The Domino Console's Open Server dialog box displays (Figure 9-49).



User name: John Norton
Password: *******
Server: dom1a
Port: 2050

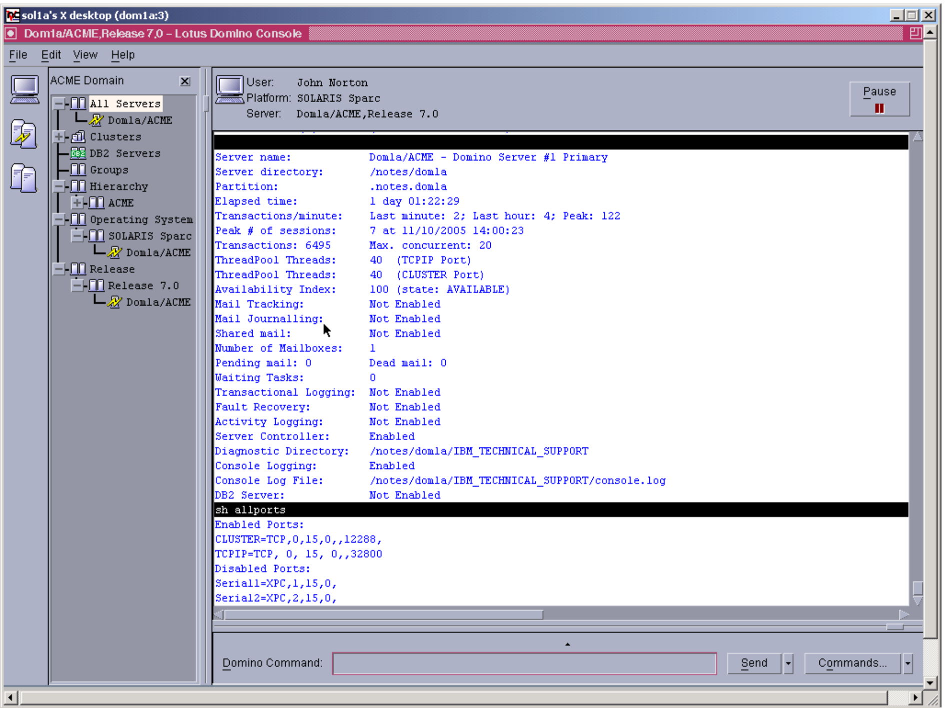
You can connect to any server controller using this dialog with in your company intra-network. You need to have your administrative user name, password, server controller's hostname or

Figure 9-49 Domino Console - Authenticating with a server

Enter your Notes User Name, Internet password, and the name of the Domino Server you want to connect to. The Open Server dialog box provides some information to help you complete these fields.

Click **OK** to continue.

When you successfully authenticate with the server, you are connected to the Domino Console, and you the window shown in Figure 9-50.



User: John Norton
Platform: SOLARIS Sparc
Server: Domla/ACME,Release 7.0

```
Server name:              Domla/ACME - Domino Server #1 Primary
Server directory:         /notes/domla
Partition:                .notes.domla
Elapsed time:             1 day 01:22:29
Transactions/minute:      Last minute: 2; Last hour: 4; Peak: 122
Peak # of sessions:       7 at 11/10/2005 14:00:23
Transactions: 6495        Max. concurrent: 20
ThreadPool Threads:       40  (TCPIP Port)
ThreadPool Threads:       40  (CLUSTER Port)
Availability Index:       100 (state: AVAILABLE)
Mail Tracking:            Not Enabled
Mail Journalling:         Not Enabled
Shared mail:              Not Enabled
Number of Mailboxes:      1
Pending mail: 0           Dead mail: 0
Waiting Tasks:            0
Transactional Logging:    Not Enabled
Fault Recovery:           Not Enabled
Activity Logging:         Not Enabled
Server Controller:        Enabled
Diagnostic Directory:     /notes/domla/IBM_TECHNICAL_SUPPORT
Console Logging:          Enabled
Console Log File:         /notes/domla/IBM_TECHNICAL_SUPPORT/console.log
DB2 Server:               Not Enabled
sh allports
Enabled Ports:
CLUSTER=TCP,0,15,0,,12288,
TCPIP=TCP, 0, 15, 0,,32800
Disabled Ports:
Serial1=XPC,1,15,0,
Serial2=XPC,2,15,0,
```

Figure 9-50 Domino Console - Connected

Table 9-3 identifies some of the common commands you can use from the console; these commands will also work from the Web Admin quick console.

Table 9-3 Common Domino Console commands

Domino Console command (abbreviation)	**Description of the command results**

`show users`
`(sh us)`
	Shows the users connected to the Domino server

`show tasks`
`(sh ta)`
	Shows the tasks currently running

Domino Console command (abbreviation)	Description of the command results

`show cluster`
`(sh cl)`
	Shows how the cluster is performing and current connectivity to cluster members

`show config servertasks`	Shows the current value of the servertasks notes.ini entry. You can use show config to display any notes.ini entry.
`set config servertasks=`	Replaces the existing server tasks notes.ini entry with the values you specify after the equals sign. The values you specify replace the existing ones. (They are not appended.)
`load replica`	Loads an instance of the replicator that remains until you reboot the server. Any load command without options loads another permanent instance of the task, and a load command with options (see the next example) runs, then quits.
`replicate dom2a/ACME names.nsf` (`rep dom2a/ACME names`)	This causes the current server, dom1a/ACME in our case, to replicate the specified database, names.nsf, with the specified server,dom2a/ACME. You must use the full hierarchical name of the server. When replication finishes, the replicator will quit.
`show stat server.users`	Show stat displays the specified Domino statistic. There are hundreds of statistics; consult the event4.nsf database for a description of each statistic.
`restart server` (`res s`)	This restarts the Domino server. If issued from the Web admin quick console, you will not be able to view the restart. If issued from a client connected via the new controller, you can monitor the restart process.

Commands are entered into the Domino Command area at the bottom of the Domino Console. For frequently used commands, you can click **Command** and select from a predefined list. Optionally, you can click the arrow to the right of the Command button and create a customized command list.

Here are the steps to record a customized command:

1. Click the arrow to the right of the Command button and select **Customize**.
2. In the Make a Custom Command dialog box, enter the desired command.
3. Click **Add** to add the command to your list.

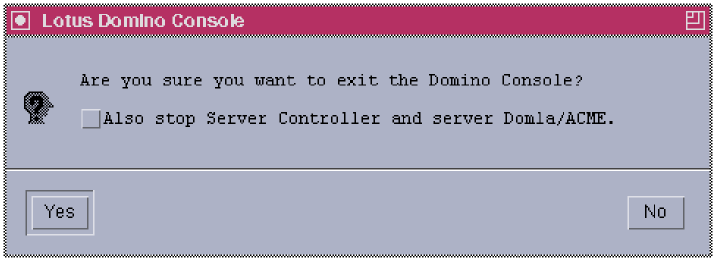
4. Repeat steps 2 on page 328 and 3 on page 328 until you have entered the commands for your list.
5. If you make a mistake or later want to remove a command, highlight the command in the Make a Custom Command display and click **Remove** to remove it from your list.
6. Click **Save** to save and exit the dialog box.

You can now use your custom commands by clicking the arrow to the right of Command and picking the desired command from the list.

In addition to Domino commands, you can send Shell commands if you have the appropriate access. Refer to **Help** → **Help Topics** available with the Domino Console, or the Lotus Domino Administrator 7 Help, for more information.

Stopping the Domino Console

1. From the Domino Console, choose **File** → **Exit**.
2. If the Domino Console is currently connected to a Server Controller, you will see the prompt `Are you sure you want to exit the Domino Console?`(Figure 9-51). To stop a Domino server and Domino Server Controller running locally, select the option **Also stop Server Controller and server <*your ServerName*>**. Click **Yes**.

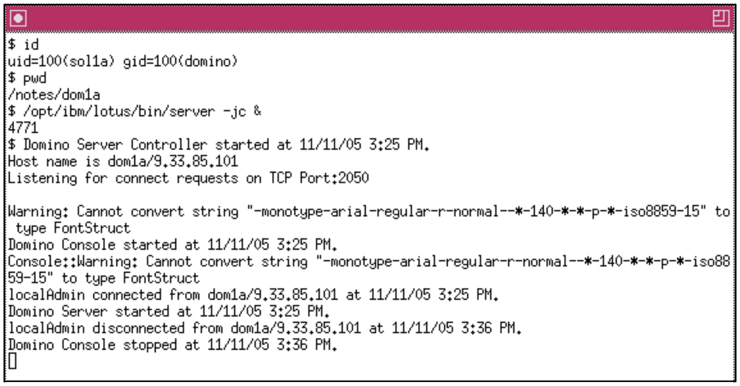


Are you sure you want to exit the Domino Console?

□ Also stop Server Controller and server Domla/ACME.

Figure 9-51 Domino Console - Exit option box

If you left the Exit Option unchecked, then the Domino Console shuts down and you return to the Solaris X-Window from which you launched the Server Controller and Domino Console (Figure 9-52 on page 330).



```
$ id
uid=100(sol1a) gid=100(domino)
$ pwd
/notes/dom1a
$ /opt/ibm/lotus/bin/server -jc &
4771
$ Domino Server Controller started at 11/11/05 3:25 PM.
Host name is dom1a/9.33.85.101
Listening for connect requests on TCP Port:2050

Warning: Cannot convert string "-monotype-arial-regular-r-normal--*-140-*-*-p-*-iso8859-15" to
 type FontStruct
Domino Console started at 11/11/05 3:25 PM.
Console::Warning: Cannot convert string "-monotype-arial-regular-r-normal--*-140-*-*-p-*-iso88
59-15" to type FontStruct
localAdmin connected from dom1a/9.33.85.101 at 11/11/05 3:25 PM.
Domino Server started at 11/11/05 3:25 PM.
localAdmin disconnected from dom1a/9.33.85.101 at 11/11/05 3:36 PM.
Domino Console stopped at 11/11/05 3:36 PM.
```

Figure 9-52 Server Controller - After exiting Domino Console

9.5 Summary

In this chapter we have shown how to connect to your Domino servers using different administration tools: the Domino Administrator client with its tabbed pages, the Web Administrator for administering your server from a browser, the Domino Server Controller and Domino (Java) Console for entering server console commands from a command line, and the Domino Character Console.

10

Security

This chapter offers a starting point for considering how to implement a secure Solaris system that runs IBM Lotus Domino 7.

It is divided in two parts: the Solaris operating environment and the Domino environment.

The Solaris operating environment part focuses on which services you might consider disabling to make a system secure.

The Domino part starts with an overview of Domino and Notes security basics, followed by a discussion about how to protect your Domino server and databases.

© Copyright IBM Corp. 2006. All rights reserved.

10.1 Solaris 10 security

This section describes methods that will help you to secure your Solaris 10 operating system. It will assist you in finding the correct patches for the OS, and suggests making some basic changes to file system permissions, accounts, and the service management facility to better secure your environment. In addition, security as it relates to the cron, the init system, log files, and the **login** command, itself, are incuded.

10.1.1 Solaris patches

Building a secure Solaris operating environment involves installing a new system with the latest version of the Solaris operating environment and applying the latest patches. Each new release of Solaris includes security improvements and additional features to enhance system security. You should always use the latest version of the Solaris operating environment that your applications will support.

Sun provides patches to the Solaris operating environment and unbundled software products when problems are found and corrected. Anyone can download recommended security patches for the Solaris operating environment. For more details, see:

http://www.sun.com/sunsolve

All systems should have the latest recommended security patches installed. Subscribe to the Sun security bulletin mail list to receive notification of important security-related patches. For more information, visit:

http://www.sun.com

Sun provides Maintenance Updates (MU) for the Solaris operating environment. An MU is a tested combination of patches for a specific release of the Solaris operating environment that installs in one quick, easy step. These updates are available only to service contract customers. SunSpectrum service contract customers have access to all patches, MUs, and the patchdiag tool.

The patchdiag tool uses a list of current patches that are available from Sun to examine the local system and determine patches that have not yet been applied. It also checks for new versions of patches that have already been applied. The patchdiag tool should be run on the system at least once a week to determine whether important patches should be applied.

To check which patches are installed in the system, use the Solaris command:

```
showrev -p
```

10.1.2 File system

The Solaris operating environment ships with some file system permissions that should be adjusted for security reasons. For example, many files and directories have the group write bit set. In most instances, this permission is not necessary and should be switched off.

File permissions

You can see the file permission using the **`ls -la`** command. File permission information is in the first column. For example, to see the permissions of the file `billing`, use this command:

```
ls -la billing
-rwxr-xr-x  1 root   bin  42564 Dec 16 12:37 billing
```

In the permission string `-rwxr-xr-x` the first position tells you whether it is a directory (d), a file (-), or a link (l). The next nine bits, divided into three groups of three (rwx), refer to the owner (you), the groups you belong to, and others (meaning everyone else). You can grant members of these three groups the ability to read (r), write (w), or execute (x) a file or directory. Refer to the **`chmod`** command for more details.

File system partitions

When creating operating system file partitions, be sure to allocate adequate disk space for system directories, log files, and applications. Certain server applications or services might require extra disk space or separate partitions to operate effectively without affecting other services.

Typically, there should be separate partitions for:

- / (the root file system)
- /export/home

Note: By default, the Lotus Domino programs directory is installed under /opt.

Usually the Solaris operating environment /var file system contains:

- System log files
- Patch data
- Print, mail, and files for other services

The disk space required for these files will vary over time. Most systems should maintain /var as a separate partition from the root file system. Provide extra space in /var if you intend to store large log files.

The set-user-ID and set-group-ID bits

The set-user-ID and set-group-ID bits (sometimes referred to as SUID and SGID bits) on an executable file indicate to the system that the executable should operate with the privileges of the file's owner or group, for example:

```
-r-sr-xr-x  1 root   bin   24270 Dec 16 12:38 bindsock
```

The flag s in the 4th position shows that the file is a set-user-ID.

An attacker can use the elevated privileges provided by the set-user-ID or set-group-ID mechanism to execute code on the program stack (a "buffer overflow" attack) or to overwrite system files. When these security problems are reported, Sun identifies a fix for them and provides a patch. This is another reason to keep your system up to date with the latest set of patches.

The Lotus Domino bindsock program uses the suid as root. This is done to permit Domino to open ports less than 1024 to the Internet Domino processes, such as IMAP, POP3, HTTP.

To find all set-user-ID and set-group-ID files on a server, use the following find command:

```
find / type f \( -perm -u+s -o -perm -g+s \) -ls
```

Note: Executing this command in the Domino program directory should give the following output:

```
373631 15 -r-sr-xr-x 1 root bin 14504 Dec 16 18:48 ./bindsock
```

10.1.3 Mounting file systems

The Solaris operating environment file system partitions can be mounted with various options that enhance security. To prevent an attacker from using the set-user-ID feature, you can mount the file system in one of the following ways:

- Use the nosuid option
- Mount the file system in read-only mode

Basic recommendations

It is not possible to mount all the file systems with these two options. For example, the /usr partition can be mounted read-only, but it should not be mounted nosuid because some commands in this partition have the set-user-ID bit set.

The same is valid for /opt for Domino: it must have the bindsock program using the suid.

The `/var` partition cannot be set to read-only, but can be set to nosuid. All other partitions should be mounted read-only and with nosuid whenever possible.

It is not possible to mount the root file system (/) with the nosuid option on modern releases of the Solaris operating environment because the root file system is mounted read-only when the system boots and is later remounted read-write. When the remount occurs, the nosuid option is ignored.

10.1.4 Accounts

Managing user and system accounts is an important aspect of Solaris operating environment security. A default Solaris operating environment installation contains several accounts that must be either deleted or modified to strengthen security.

Basic recommendations

Some accounts are not necessary for normal system operation. These accounts include:

smtp	The mail transfer protocol user
nuucp	The UNIX-to-UNIX system copy administration user
listen	The Network Listener Daemon administration user

Use the **passmgmt** command with the -d option to delete accounts in /etc/passwd and /etc/shadow. Here is an example:

```
passmgmt -d smtp
```

This command removes the /etc/passwd and /etc/shadow entries for smtp. The remaining system accounts (except the root account) should also be modified for added security.

System accounts listed in /etc/passwd have no shell listed. Those accounts also have an NP string (meaning “no password”) listed in the /etc/shadow file. By default, this is sufficient. However, some additional steps can be taken to add more security. Use the -l option of the **passwd** command to lock accounts. For example, to lock the uucp account, use the command:

```
passwd -l uucp
```

Also, use the **-e** option with the **passwd** command or edit the /etc/passwd file manually to change the default shell for those accounts to /usr/bin/true. For example:

```
passwd -e uucp
Old shell: /sbin/sh
New shell: /usr/bin/true
```

This prevents an unauthorized user from using the uucp account to start a shell session on your system.

Note: The **/usr/bin/true** command is a UNIX command typically used in shell script to have a true condition.

10.1.5 cron and at security

The cron and at services execute commands at a future time. User submission for the cron service is handled by the **crontab** command. The **at** and **batch** commands are used to submit jobs to the at service.

The cron and at services can be problematic because commands are executed in the future. An attacker might use these systems to implement a “logic bomb” or other type of programmed attack that begins at some point in the future. It is better to restrict access to the at and cron systems to prevent attacks and abuse.

cron configuration

The access control files are stored in the /usr/lib/cron directory:

- cron.deny
- cron.allow

The allow file is checked first to see whether the account is explicitly allowed to use the system. If the file does not exist or the account is not listed in this file, the deny file is checked. If the account is explicitly listed in the deny file, then access is refused. Otherwise, access is permitted. If neither the deny nor the allow files exist, then only the root account can use the **at** or **cron** system. Add only the accounts that need access to the allow file.

At configuration

The at.deny and at.allow files are used to manage access to the at system. The same considerations that apply to the cron allow and deny files are valid for the **at** command.

Usage

The following command lists all scheduled tasks for the current user:

```
crontab -l
```

The Domino user administrator can use the **cron** and **at** Solaris commands to schedule maintenance tasks outside of Domino. For example, the administrator can schedule the Domino server shutdown and do some maintenance procedures, such as starting the compact, fixup, or updall Domino programs on some databases.

10.1.6 Service management facility

The Service Management Facility (also known as smf(5) or simply, SMF) provides a unified method of managing Solaris system services. This section outlines some SMF general concepts along with suggestions and thoughts on using SMF in your current environment.

General concepts

- The smf(5) service model

  The Service Management Facility defines a programming model for providing persistently running applications called services. A service can represent software facilities, such as a set of running processes, a set of system configuration parameters, or a synthetic set of running services. A Solaris service will be started only if it is marked as enabled (by the administrator) and when all of its dependencies are satisfied.

  Taking the time to convert your existing services to smf(5) allows them to take easy advantage of automated restart capabilities due to hardware failure, unexpected service failure, or administrative error. Participation in the Service Management Facility also brings enhanced visibility with svcs(1) (as well as future-planned GUI tools) and ease of management with svcadm(1M) and other Solaris management tools. This usually requires only the creation of a short XML file and making a few simple modifications to the service init script.

- XML versus repository

  A service is usually defined by a service manifest, an XML file that describes a service and any instances that are associated with that service. The service manifest is pulled into the repository either at boot time or by using the svccfg import subcommand. The XML format of the service manifest is specified by the Service description DTD, located at:

  ```
  /usr/share/lib/xml/dtd/service_bundle.dtd.1
  ```

  The repository is where the authoritative copy of service configuration lives. This is where administrators may customize service settings after they are installed on a system.

  The rest of this document covers creating a service manifest, which is the delivery mechanism for all services.

- Instance versus service split

  A service consists of the general service definition and one or more instances that implement the service. An instance’s properties are inherited from the service, unless if the instance specifically overrides them.

  Thus, as general guidance for the rest of this document, all properties that would not be changed by a different copy of your service running (if your service supports that) should be defined at the service level.

  If your service is implemented differently (for example, smtp might be implemented by sendmail, postfix, or qmail) by a different instance, you should locate the properties that are specific to the current implementation at the instance, not the service.

  All properties discussed below may be defined at the instance or service level.

Compatibility and caveats

smf(5) maintains compatibility for most applications started by init(1M) by placement in the /etc/rc?.d directories, and for applications delivered into inetd.conf.

Some init services, however, must be converted to smf(5) to preserve their boot-time ordering. An init service must convert if it affects other infrastructure services, such as the early setup of devices, file systems, or network configuration. A service also should convert if it requires input from the console during the boot process. (Such services are strongly discouraged.)

Writing a service manifest

As stated earlier, the service manifest is an XML file that describes a service and any instances that are associated with that service. This section outlines the steps necessary in writing a service manifest:

1. Name your service.
2. Identify whether your service may have multiple instances.
3. Identify your service model.
4. Identify how your service is started/stopped.
5. Determine faults to be ignored.
6. Identify dependencies.
7. Identify dependents.
8. Insert your service into a milestone.
9. Create, if appropriate, a default instance.
10. Create template information to describe your service.
11. Write or update an administrative command.
12. Remove your script from /etc/rc?.d locations and etc/init.d.

We provide general service categories for naming. These categories are not used by the system, but help the administrator in identifying the general use of the service.

These categories are shown in /var/svc/manifest, and include:

application	Higher-level applications, such as Apache
milestone	Collections of other services, such as name-services
platform	Platform-specific services, such as Dynamic Reconfiguration daemons
system	Solaris system services, such as coreadm
device	Device-specific services
network	Network/Internet services, such as protocols
site	Site-specific descriptions

The service name describes what is being provided, and includes both any category identifier and the actual service name, separated by a slash (/). Service names should usefully identify the service being provided by the administrator.

The instance name describes any specific features about the instance. Most services deliver a “default” instance. Some (such as Oracle) might want to create instances based on administrative configuration choices.

Services that are shipped as part of a product or generally extend beyond a site-specific definition should include either the stock symbol or Java-style reversed domain prefix followed by a comma as part of the category or service name for uniqueness.

As an example of the naming conventions above, the cron service specifies as its prelude:

```
<service
   name='system/cron'
   type='service'
   version='1'>
```

Identify whether your service may have multiple instances.

If multiple binaries of your service running simultaneously on the system would cause an error, you must define it as a single_instance service. This tag tells the restarter to not start up multiple service instances simultaneously, regardless of administrative configuration.

Most configuration and system services require single_instance tags. Services such as Web servers or databases that could run multiple configurations simultaneously (such as use a different database source or run on a different port) should not be specified as single_instance.

Specify after the service block:

```
<single_instance />
```

Identify your service model

In order to provide restart capabilities for services with different run-time characteristics, smf(5) provides a variety of models for services. Currently, these models are provided by the svc.startd and inetd restarters. Additional models may be provided in the future by either these restarters or additional restarters. This document describes the models for svc.startd(1M) and inetd(1M); see the restarter documentation for more detail on the application model it provides.

If your service is started by inetd, see “Write/update an administrative command” on page 346, as we have provided a tool to ease the transition.

svc.startd is a process-based restarter. It provides three distinct models for service processes:

- *Transient* services are often configuration services, which require no long-running processes to provide service. Common transient services take care of boot-time cleanup or load of configuration properties into the kernel.

  Transient services are also used sometimes to overcome difficulties in conforming to the method requirements for contract or wait services. This is not recommended and should be considered a stopgap measure.
- *Wait* services run for the lifetime of the child process and are restarted when that process exits.
- *Contract* services are the standard system daemons. They require processes that, when started, run forever to provide service. Death of all processes in a contract service is considered a service error, which will cause the service to restart.

  The default service model is contract, but may be modified by specifying this in your service manifest for a transient service:

  ```
  <property_group name='startd' type='framework'>
     <propval name='duration' type='astring' value='transient' />
  </property_group>
  ```

  Specify this for a wait service:

  ```
  <property_group name='startd' type='framework'>
     <propval name='duration' type='astring' value='child' />
  </property_group>
  ```

Identify how your service is started and stopped

SMF interacts with your service primarily by its methods. The *stop* and *start* methods must be provided for services that are managed by svc.startd, and can directly invoke either a service binary or a script that handles care of more complex setup. The *refresh* method is optional for svc.startd managed services. Different restarters might require different methods.

Existing init scripts can easily serve as the basis for service methods. We give the following rules and guidance for the methods supported by svc.startd.

All methods

Shell scripts should include /lib/svc/share/smf_include.sh to gain access to convenience functions and return value definitions.

Failures must cause explicit error returns. All non-0 values are considered errors. Additional information (for example, to avoid restart due to configuration errors) may be provided to the restarter with the SMF_EXIT_* definitions.

Method should emit log messages on failure. They will be logged by svc.startd to the service log file, so the administrator can determine what is happening.

The keywords *:kill* and *:true* are available for all method definitions:

- :true simply returns success to the restarter.
- :kill kills all processes started by your service's start method. The list of all processes is determined by the service's contract.

Start methods

A start method is required for all svc.startd-managed services.

start methods are run only when the service is enabled and dependencies are already met. Therefore, start methods should exit with SMF_EXIT_ERR_CONFIG if the service cannot come online due to any configuration error.

If your service is the contract type, the start method must leave your daemon running if returning success, as exiting all processes will cause the service to be restarted.

For contract and transient services, the start method should not return success until service is being provided. This is true for daemons as well; daemons should not fork() then exit() from their initial process; they should wait to return until startup errors have been accumulated and can be reported. Many init scripts used to start up the daemon and return immediately, counting on the fact that the serial boot took "a while" to start dependent services. Now that dependent services are started precisely (often immediately) after your service returns successfully from its start method, imprecise semantics are not acceptable.

If code changes to the daemon/service cannot be made, a positive test for service is required before returning success. If no other options are available, insert an appropriately long sleep() before successful return.

Stop methods

A stop method is required for all svc.startd-managed services.

Stop methods are run in a number of different scenarios, including if a dependency has gone offline, if your service fails, and if an administrator requests disable or restart.

Thus, stop methods should return success if the service is no longer running after execution is complete, even if the service was not running when the execution started. This is because stop methods may be called in error scenarios.

Refresh methods

Refresh methods are optional for all svc.startd-managed services.

Any defined refresh method has very precise semantics; it must reload appropriate configuration parameters from the repository or other configuration source without interrupting service. It must not cause exit of the existing processes for contract or wait services.

Timeouts must be provided for all methods. The timeout should be defined to be the maximal amount of time in seconds that your method might take to run on a slow system or under heavy load. A method that exceeds its timeout will be killed. If the method could potentially take an unbounded amount of time, such as a large filesystem fsck, an infinite timeout may be specified as `0`.

We strongly discourage expecting user interaction (such as by console input) as part of the service methods. Scripts that do so will not work without modification, as the stdin/stdout/stderr are not /dev/console for service methods.

We provide a set of method tokens that are available for use in method specification for commonly used property values. A comprehensive list is available in smf_method(5).

The default method environment is inherited from init(1M), with the PATH set to /usr/sbin:/usr/bin. Variables beginning with SMF_ are reserved for framework use. The SMF_ variables defined in smf_method(5) are provided to all methods; these include SMF_FMRI, SMF_METHOD, and SMF_RESTARTER.

Finally, each method may specify a *method context* to define system and security attributes used during method execution. We recommend starting long-running services with reduced privileges and safe uids and gids when possible.

This is an example of a start method specification:

```
<exec_method
   type='method'
   name='start'
   exec='/lib/svc/method/svc-cron'
   timeout_seconds='60'>
   <method_context>
      <method_credential user='root' group='root' />
   </method_context>
</exec_method>
```

Determine faults to be ignored

If either your service is poorly behaved itself, or it might spawn poorly behaved subprocesses, inform the restarter that certain errors are expected and do not constitute service faults.

You may specify that coredumps from subprocesses should not be considered errors, or that external kill signals are not errors. This is an example of specifying that neither are errors:

```
<property_group name='startd' type='framework'>
   <propval name='ignore_error' type='astring' value='core,signal' />
</property_group>
```

Identify dependencies

This is the most difficult part of service conversion, as most dependencies are not explicitly stated. There are two different types of dependencies: *file* and *service* dependencies.

First, identify what other services are required for yours to be started. For example, does your service require the network to be plumbed, local devices to be configured, name services to be available?

When you have decided what your service is dependent on, you must specify the fault propagation model. For each dependency, you must decide how your service should restart. The following values correspond to the ability to handle restart of the specified dependency, via the restart_on property:

none The dependency is required only for startup. No fault or administrative action requires restart.

fault Restart if the dependency has a fault (core dump, system fault).

restart If the dependency is restarted, your service should also be restarted.

refresh If the dependency is refreshed (its configuration is changed), your service should be restarted.

Dependencies may be specified in groupings. The potential groupings are:

require_all All in the group must be online or degraded before the dependency is started.

require_any Any one of the services in the group must be online or degraded before the dependency is started.

optional_all If the services are enabled and able to run (not in maintenance), they must be online or degraded before the dependency is started.

exclude_all If the service is enabled and online or degraded, the dependency should not be started.

If your service is dependent on a legacy script having run, we strongly recommend that you convert or encourage your vendor to convert the legacy script to an smf(5) service. Barring that, you can specify a dependency on the *milestone* that script is part of. This will never propagate errors from the legacy service, so it only makes sense as a restart_on=none dependency.

Finally, after doing the hard work to determine why a certain dependency was required, write a comment to help future maintainers!

```
<!-- Must be able to resolve hostnames. -->
<dependency
   name='nameservice'
   type='service'
   grouping='require_all'
   restart_on='none'>
      <service_fmri value='svc:/milestone/name-services' />
<dependency>
```

Identify dependents

To deliver a service that is a dependency of another service that you do not deliver, you can specify this in your manifest without modifying the manifest you do not own. That is, dependent specifications are an easy way to have your service run before a service delivered by Sun.

If not all of your dependent services have been converted, you must convert those too, as there is no way to specify a dependent on a legacy script.

To avoid conflicts, we recommend prefacing your dependent name with the name of your service.

For example, if you are delivering a service (mysvc) that must start before syslog:

```
<dependent
   name='mysvc_syslog'
   grouping='optional_all'
   restart_on='none'>
      <service_fmri value='svc:/system/system-log' />
<dependent>
```

Insert your service into a milestone

If your service was previously delivered into an rc?.d directory and other services might be dependent on it, you should make a milestone (that corresponds to your previous delivery location) a dependent.

For example, if your service was previously started at runlevel 2, this clause will ensure that runlevel 2 is not considered complete until your service has started:

```
<dependent
   name='mysvc_multi-user'
   grouping='require_all'
   restart_on='none'>
   <service_fmri value='svc:/milestone/multi-user' />
<dependent>
```

Create, if appropriate, a default instance

If your service does not require additional administrative intervention for configuration before it starts the first time, you should configure a default instance for your service.

If the instance has no configuration differences from the service, this can easily be done:

```
<create_default_instance enabled='false' />
Alternatively, you can explicitly define the instance.
      <instance name='default' enabled='false'>
         <!-- instance-specific properties, methods, etc. go here. -->
      </instance>
```

We recommend that all instances are delivered as disabled unless they are critical to system boot. Customization can then be done by either the administrator or a profile (described elsewhere).

Create template information to describe your service

Document at least a common name in the C locale and a manpage reference. The common name should:

- Be short (40 characters or less).
- Avoid capital letters other than in trademarks such as Solaris.
- Avoid punctuation.
- Avoid the word service (but be sure to distinguish between client and server).

This information is presented by various forms of svcs(1) to provide the administrator with concise detail about your service and where to get more technical information. Common names may be localized.

```
<template>
   <common_name>
      <loctext xml:lang='C'>
      Solaris fault manager
      <loctext>
   <common_name>
   <documentation>
      <manpage title='fmd' section='1M' manpath='/usr/share/man' />
   <documentation>
<template>
```

Write/update an administrative command

If your service already has an administrative command that stops, starts, or restarts your service, update it to use svcadm(1M) or libscf calls. If an administrative command explicitly starts a daemon outside of smf(5), the smf(5) framework will not know that other daemons are running. Problems that will occur include conflicts between daemons, incorrect contracts, and lack of visibility using svcs(1).

Remove your script from /etc/rc?.d locations and /etc/init.d

If you do not remove your init script, it will still be run in legacy mode.

For more information

The DTD is self-documenting. Many questions can be resolved by just reading /usr/share/lib/xml/dtd/service_bundle.dtd on your Solaris 10 system.

Sun delivers many manifests in /var/svc/manifest. These may be used as templates and examples. A few to start with:

- system/utmp is a simple standalone daemon.
- system/coreadm is a simple transient service.
- network/telnet is an inetd(1M)-based daemon.

The following manpages are a helpful start: smf(5), smf_bootstrap(5), smf_method(5), smf_restarter(5), smf_security(5), svc.startd(1M), inetd(1M), inetconv(1M).

Writing an inetd service manifest

Start with inetconv(1M), and include other modifications such as adding templates and refining the name.

10.1.7 The init system

The Solaris operating environment init system manages system services. Some services might not be needed or should be modified to strengthen the security posture of a system.

System services are started by the init system. There are some services that might allow a system to be compromised due to incorrect configuration. To disable services started by init, simply rename or delete the initialization script in the init system run level directory. The run level directories contain the scripts for starting or stopping services for the system run level. The system run level directories and their purposes are listed here:

- /etc/rcS.d single user
- /etc/rc0.d shutdown
- /etc/rc1.d start
- /etc/rc2.d multi-user
- /etc/rc3.d multi-user (default)
- /etc/rc4.d multi-user (unused)
- /etc/rc5.d shutdown and power off
- /etc/rc6.d shutdown and reboot

These directories contain initialization scripts to start or stop services. Initialization scripts that begin with either an S or a K are executed by the init system. S scripts *start* services, and K scripts *stop* or *kill* services. If you rename the scripts, make sure the name does not begin with these letters. Instead of deleting these files, we recommend placing an underscore character (_) at the beginning of the original file name. This makes it easy to enable services that might be needed later. For example:

```
cd /etc/rc.2
mv S99dtlogin _S99dtlogin
```

For security purposes, only required services should be enabled. The fewer services that are enabled, the less likely an attacker will discover a way to exploit the system using an enabled service.

For example, if you would like to disable sendmail, simply type this command:

```
svcadm disable sendmail
```

10.1.8 Log files

Log files are used by the system and applications to record actions, errors, warnings, and problems. They are often useful for investigating system quirks, for discovering the root causes of tricky problems, and for watching attackers.

Log type

There are typically two types of log files in the Solaris operating environment:

- System log files, which are usually managed by the syslog daemon
- Application logs, which are created by the application

It is possible to redirect some events of Lotus Domino in the syslog system file. See Appendix E, “IBM Lotus Domino and syslog” on page 549 for details.

Syslog

The syslog daemon receives log messages from several sources and directs them to the appropriate location based on the configured facility and priority. The facility (or application type) and the priority are configured in the /etc/syslog.conf file to direct the log messages. The destination can be a log file, a network host, specific users, or all users logged on to the system.

By default, the Solaris operating environment defines two log files in the /etc/syslog.conf file. The /var/adm/messages log file contains a majority of the system messages. Save the file and use the following command to force syslogd to reread its configuration file:

```
kill -HUP 'cat /etc/syslog.pid'
```

All of these files should be examined regularly for errors, warnings, and signs of an attack. This task can be automated by using log analysis tools or a simple **grep** command.

Login trace

The /var/adm/loginlog file does not exist in the default of the Solaris operating environment installation, but it should be created. If this file exists, the login program records failed login attempts.

10.1.9 The login command

The **login** command is part of the authentication process to access a local Solaris operating environment account. It is used on the console and by the in.telnetd daemon to determine whether a user may be granted access to the system.

By default, only the root user can log on to a Solaris operating environment system from the console device. The console device is defined by the following entry in the /etc/default/login file:

```
CONSOLE=/dev/console
```

When this line is commented out, the root account can log directly onto the system over the network using Telnet, in addition to the console. This is not secure and should be avoided. Do not alter the default configuration.

10.2 Network service security

The Solaris operating environment is designed to provide customers with full access to most network services by default. This enables administrators and users to install and configure the Solaris operating environment systems as quickly as possible. Customers are encouraged to disable all unnecessary services for performance and security reasons.

There are many possible ways to attack network services. Network weakness can be introduced by many factors, including:

- Programming flaws
- Using weak authentication
- Transferring sensitive data in unencrypted format
- Allowing connections from any network host

These weaknesses open up a system to compromise by an attacker. In addition to vigilance in ridding your system of these problems, safer network service alternatives should be used whenever possible.

Sun has a product for secure network services, based on Kerberos, called the Sun Enterprise™ Authentication Mechanism™ (SEAM product). Kerberos is a centralized network security architecture that uses symmetric encryption and a ticket mechanism to provide strong authentication. The SEAM product also uses strong encryption.

A tool known as Secure Shell (SSH) provides strong authentication and encryption capabilities. Both commercial and open source versions are available.

Access control can be provided, thereby configuring network services to handle only connections from approved systems. Wietse Venema's TCP Wrapper toolkit provides access control and additional security checks. It manages TCP-based services managed from inetd.

10.2.1 Telnet

Telnet is a user-interactive service used to log into and access a remote system on the network. Unfortunately, this service provides little in the way of security. The only authentication information required is user name and password. Neither of these pieces of information is encrypted while in transit, so Telnet service is vulnerable to a variety of attacks including:

- Man in the middle attack
- Session hijacking
- Network sniffing

If you must use a telnet daemon that does not support encryption, TCPWrappers can be used to limit the hosts that may connect to a system. By restricting access to services based on IP addresses, a system can limit its exposure to network attacks.

10.2.2 Remote access services (rsh, rlogin, and rcp)

The default authentication mechanism of the r* daemons (r* is an abbreviation for remote commands) uses the IP address of a system in combination with the user ID for authentication. No additional authentication is required. Considering the ease with which an IP address and user ID might be stolen or misused, this is clearly not a secure mechanism.

> **Important:** The r* commands should never be used in this manner and no servers should offer the service in this manner.

Secure Shell (SSH) can be used to improve the security of the r* commands.

10.2.3 Remote execution service (rexec)

The remote execution server daemon, in.rexecd, is started from the file /etc/inetd.conf when a connection request is made. This daemon provides remote execution facilities based on user name and password information.

When authenticated, the daemon executes the command passed along with the authentication information. As with the in.telnetd daemon, neither the user name nor password is encrypted while transmitted over the network.

This exposes the in.rexecd daemon to the same man in the middle, session hijacking, and network sniffing attacks as the in.telnetd and in.ftpd daemons. For this reason, the in.rexecd entries in /etc/inetd.conf file should be removed.

10.2.4 FTP

The FTP daemon has many of the same problems as the telnet daemon. All authentication information transmitted over the network is in clear text, in much the same fashion as the Telnet protocol. This exposes the FTP protocol to many of the same attack scenarios as Telnet, including man in the middle, session hijacking, and network sniffing.

If you must use FTP, you have to configure the /etc/ftpusers file, which is used to restrict access to the system through FTP. All accounts that are not allowed to use the incoming FTP service should be specified in this file. At a minimum, this should include all system accounts (bin, uucp, smtp, sys, and so forth) in addition to the root account.

Another service, the trivial FTP service (in.tftpd), exists to provide diskless systems with a way to get files on the network. This is less secure than even FTP. By default, it is not enabled in the Solaris operating system.

10.2.5 Managed services: inetd

The inetd service manages many of the minor network services that are available on a system. Its configuration file, /etc/inetd.conf, defines its operation. An ideal secured server should not have an /etc/inetd.conf or run inetd, as the daemons started in the /etc/inetd.conf are frequently not needed.

To disable a service, edit the /etc/inetd.conf file and place a comment character (#) in front of the line containing the service definition. When this is completed, send a HUP signal to the inetd process, using the **kill** command as follows:

```
kill -s HUP pid
```

pid is the Process ID of the inetd process.

This will cause it to reread its configuration file.

Of the daemons started from the /etc/inetd.conf, the remote access services, FTP, TFTP, and Telnet services have already been discussed. The remaining /etc/inetd.conf entries should be removed. The only one that can be left is the netstat, a service that provides a list of current network connections that are useful for troubleshooting network issues.

After removing these services and entries, restart the server inetd and test applications to verify that required functionality has not been affected.

10.2.6 Solaris IP Filter

The Solaris IP Filter is a software package that can be used to provide firewall services. The Solaris IP Filter provides packet filtering and network address translation (NAT), based on a user-configurable policy. Packet filtering rules are configurable in either a stateful or stateless manner. All configuration and management of Solaris IP Filter is performed through a command-line interface.

For further information, see the ipfilter(5) man page. Also, refer to the ipf(1M), ipfs(1M), and ipfstat(1M) man pages and the *System Administration Guide: IP Services*.

10.2.7 Network File System (NFS)

The Network File System (NFS) permits the sharing of file systems on network-connected machines. A Solaris operating environment system can be an NFS server, an NFS client, both, or neither.

From a security perspective, the best option is to not provide NFS services or accept them from any other systems. The following command can be used to disable all clients and server NFS daemons:

```
svcadm disable nfs/client
```

10.2.8 Sendmail

The sendmail daemon is used on a Solaris operating environment system both to forward and to receive mail from other systems. A more secure Mail Transport Agent (MTA) should be used.

The sendmail daemon has been subject to numerous denial of service attacks from the Internet.

In Solaris 10 you can use the Solaris Management Facility and disable sendmail with this command:

```
svcadm disable sendmail
```

10.2.9 Print services

Installing a Solaris operating environment system using the End User, Development, or Entire Distribution cluster also installs the line printing packages.

The Lotus Notes client is no longer available in Release 7 for UNIX platforms, so we do not need to have this service running on the server.

To disable it, you should remove the following line from the /etc/inetd.conf file:

```
printer stream tcp nowait root /usr/lib/print/in.lpd in.lpd
```

The in.lpd entry should also be removed from the /etc/inetd.conf file.

10.2.10 Reducing inetsvc

The inetsvc file contains all of the network services that the Solaris system starts at the OS boot.

Based on the recommendations made in this section, it is possible to construct a minimized /etc/init.d/inetsvc file that contains only the essential components.

By commenting out all of these entries, the resulting script should look like this:

```
#!/bin/sh
/usr/sbin/ifconfig -au netmask + broadcast +
/usr/sbin/inetd -s -t
```

With this minimal file you will have a well secured system.

10.2.11 The Solaris ndd command

You can increase the Network Secure level of your Solaris system using the Solaris **ndd** command. It is used to examine and set kernel parameters, namely the TCP/IP drivers.

Usage

Most kernel parameters accessible through **ndd** can be adjusted without rebooting the system. To see which parameters are available, use the following **ndd** commands:

- `ndd /dev/arp \?`
- `ndd /dev/icmp \?`
- `ndd /dev/ip \?`
- `ndd /dev/tcp \?`

These commands list the parameters for the ARP, IP, ICMP, and TCP drivers. “\?” lists all parameters for the driver and indicates whether the parameter is read-only, write-only, or read and write. The current parameter value or status information can be read by specifying the driver and parameter names.

This example shows the output of an **ndd** command examining the debugging status of the ARP driver. (The output “0” indicates that the option is disabled.)

```
ndd /dev/arp arp_debug
0
```

Parameter values specified by **ndd** are integers, with 0 (zero, meaning disable), 1 (meaning enable), or a large integer to set a time or size value.

Basic recommendations

Setting parameters requires the -set option, the driver name, the parameter name, and the new value.

For example, to enable debugging mode in the ARP driver, use the following **ndd** command:

```
ndd -set /dev/arp arp_debug 1
```

One security use for **ndd** is to disable IP forwarding, the process of routing packets between network interfaces on one system. Systems that allow packet forwarding are targets for attackers, as they provide access to other systems and networks.

Packet forwarding is easily disabled on a Solaris system. Simply creating a file named /etc/notrouter will disable IP forwarding at boot time.

IP forwarding can also be switched on or off while the system is operating, using the **ndd** command. Use this command to disable IP forwarding:

```
ndd -set /dev/ip ip_forwarding 0
```

To view the current IP forwarding table, use the following command:

```
ndd /dev/ip ip_ire_status
```

10.3 Security tools

A lot of security tools can be found over the Internet. In this section we describe some of the more common ones. Always try to use the latest available versions of these tools.

10.3.1 The sudo tool

Sudo (superuser do) enables a system administrator to give certain users or groups the ability to run some or all commands as root while logging all commands and arguments.

Sudo is free software and is distributed under a BSD-style license. It is currently maintained by Todd Miller, and you can find it at:

http://www.courtesan.com/sudo/

10.3.2 TCP Wrapper

First, a little background. The TCP Wrapper tool has been around for many, many years. It is used to restrict access to TCP services based on host name, IP address, network address, and so on. For more details about TCP Wrapper and how you can use it, see tcpd(1M). TCP Wrapper was integrated into the Solaris Operating System starting in the Solaris 9 release, where both Solaris Secure Shell and inetd-based (streams, nowait) services were wrapped.

TCP Wrapper support in Secure Shell was always enabled since Secure Shell always called the TCP Wrapper function host_access(3) to determine whether a connection attempt should proceed. If TCP Wrapper was not configured on that system, access would be granted by default. Otherwise, the rules as defined in the hosts.allow and hosts.deny files would apply. For more information about these files, see hosts_access(4). Note that this and all of the TCP Wrappers manual pages are stored under /usr/sfw/man in the Solaris 10 OS. To view this manual page, you can use the following command:

```
$ man -M /usr/sfw/man -s 4 hosts_access
```

inetd-based services use TCP Wrapper in a different way. In the Solaris 9 OS, to enable TCP Wrapper for inetd-based services, you must edit the /etc/default/inetd file and set the ENABLE_TCPWRAPPERS parameter to YES. By default, TCP Wrapper was not enabled for inetd.

In the Solaris 10 OS, two new services were wrapped: sendmail and rpcbind. sendmail works similar to Secure Shell. It always calls the host_access function and therefore TCP Wrapper support is always enabled. Nothing else has to be done to enable TCP Wrapper support for that service. On the other hand, TCP Wrapper support for rpcbind must be enabled manually using the new Service Management Facility (SMF). Similarly, inetd was modified to use an SMF property to control whether TCP Wrapper is enabled for inetd-based services.

To enable TCP Wrapper support for inetd-based services, use the following commands:

```
inetadm -M tcp_wrappers=true
svcadm refresh inetd
```

This enables TCP Wrappers for inetd-based (streams, nowait) services such as Telnet, rlogin, and FTP (for example):

```
inetadm -l telnet | grep tcp_wrappers
default  tcp_wrappers=TRUE
```

You can see that this setting has taken effect for inetd by running this command:

```
svcprop -p defaults inetd
defaults/tcp_wrappers boolean true
```

You can also use the svccfg(1M) command to enable TCP Wrappers for inetd-based services.

```
svccfg -s inetd setprop defaults/tcp_wrappers=true
svcadm refresh inetd
```

Whether you use inetadm(1M) or svccfg is a matter of preference. You can also use inetadm or svccfg to enable TCP Wrappers on a per-service basis. For example, say you wanted to enable TCP Wrappers for Telnet but not for FTP. By default, both the global and per-service settings for TCP Wrappers are disabled:

```
inetadm -p | grep tcp_wrappers
tcp_wrappers=FALSE

inetadm -l telnet | grep tcp_wrappers
default  tcp_wrappers=FALSE

inetadm -l ftp | grep tcp_wrappers
default  tcp_wrappers=FALSE
To enable TCP Wrappers for telnet, use the following command:
inetadm -m telnet tcp_wrappers=TRUE
Let's check out the settings again:
inetadm -p | grep tcp_wrappers
tcp_wrappers=FALSE

inetadm -l telnet | grep tcp_wrappers
         tcp_wrappers=TRUE

inetadm -l ftp | grep tcp_wrappers
default  tcp_wrappers=FALSE
```

As you can see, TCP Wrappers has been enabled for telnet but none of the other inetd-based services.

You can enable TCP Wrappers support for rpcbind by running the following command:

```
svccfg -s rpc/bind setprop config/enable_tcpwrappers=true
svcadm refresh rpc/bind
```

This change can be verified by running:

```
svcprop -p config/enable_tcpwrappers rpc/bind
true
```

That is all there is to it.

10.3.3 Secure shell (SSH)

In Solaris 10, SSH is already included and only has to be configured.

10.3.4 BART

This section provides and overview of the new Basic Audit and Reporting Tool (BART), including concepts you need to understand before proceeding with steps to automate file integrity checking. BART provides a quick, easy way to collect information about file system objects and their attributes so that you can determine later whether there have been any changes. BART can help you detect accidental or malicious changes to files within an operating system due to either a security incident or a change management incident.

BART can collect such information as an object's UID, GID, permissions, access, control lists, modification time, size, and type. In addition, BART generates an MD5 fingerprint from the contents of a file. BART has two primary modes of operation: create and compare.

Create mode

When it is run in create mode, BART collects file system object information from a system. You can control the scope of collection on a system, including the entire system, under a specified root directory, or just a subset of files. You can even define a more granular policy using a rules file that can be customized to meet your organization's requirements.

When you use BART in create mode, it can read its rules file from either standard input or from a regular file. As BART processes individual file system objects, it records its results in a manifest file. This manifest is directed to standard output by default, although you can easily redirect the output to a file or to another process. BART's ability to read rules from standard input and produce a manifest on standard output are important for the automation of file integrity checking.

Compare mode

To use BART in compare mode, you need two BART manifests and, optionally, a rules file. The first (and original) manifest, called the *control* manifest, is used as your baseline.

The second manifest, called the *test* manifest, is compared against the control (in accordance with a set of rules, if supplied). If a rules file is specified, BART will use the rules it contains to determine how to make the various comparisons. One of the benefits of a rules file is that you can use it to define rules to help eliminate any false alarms in your reports, thereby enabling you to better focus your efforts on the remaining alarms.

Why automate BART?

For customers with both large and small Solaris deployments, there is a growing need to manage cost and complexity. The goal of this BluePrints Cookbook is to highlight how the collection of file system information using BART can be securely automated across any number of systems (with any number of Solaris Containers).

BART automation has several benefits: With a centralized collection authority, you can collect BART manifests across a network of Solaris 10 systems using strong authentication, least privilege, and encryption over the wire.

The rules and manifest files never have to be stored on the system (or Container) being evaluated—they can all be managed and protected on a central authority. Similarly, the comparison process can be performed in relative isolation because the comparison need not be done on the host being evaluated. This approach offers a significant security benefits over other file integrity methods in use today, where artifacts of the collection or comparison process must exist on the system being evaluated.

10.3.5 Containers in Solaris 10

This section reproduces an article by Glenn Brunette (September 2005), which is used by permission. The article with live links can be found at:

`http://www.sun.com/bigadmin/features/articles/container_security.html`

Practical Security Using Solaris Containers in the Solaris 10 OS

In the first article of this two-part series, I would like to highlight the Solaris 10 security model using containers and zones, combined with tools and technologies that are available by default in the Solaris 10 OS. I hope to show how these can provide customers with an enhanced ability to detect and contain security breaches, limit privilege escalation, and minimize installation of root kits, Trojan horses, and other malware. In this way, we can demonstrate how the use of containers, and more specifically zones, can be leveraged as part of a greater defense and in-depth security strategy.

Since a great deal of material is already available on containers and zones, I will not discuss any of the basics. I would like to specifically focus on security using a Solaris Containers model, and show how zones can be leveraged to improve the security of deployed systems and services. If you would like more information on zones in general, see the Big Admin Pages at Sun Microsystems Inc.

The first thing that you will realize is that zones are configured to run with reduced privileges by default. In fact, today the Solaris 10 OS offers no way to alter this default. The privileges that are not available to be used within a zone are:

```
cpc_cpu, dtrace_kernel, dtrace_proc, dtrace_user, net_rawaccess,
proc_clock_hires, proc_lock_memory, proc_priocntl, proc_zone,
sys_config, sys_devices, sys_ipc_config, sys_linkdir, sys_net_config,
sys_res_config, sys_suser_compat, sys_time
```

For a description of each of these privileges, see privileges(5). By preventing these privileges from being used within a zone, you are immediately better off than you would have been in the Solaris 9 OS or if you were to run a service in the global zone in the Solaris 10 OS.

Why is this?

Let's take an example. Let's assume that you are running some kind of exploitable service that an attacker uses to gain shell access to the system as a privileged user. For our example, let's even assume that the attacker has obtained root access in a zone.

Once attackers gain access to the system, the first thing that they would typically want to do is hide the fact that the system or service was breached. By leveraging Solaris auditing (also known as the Basic Security Module or BSM) and configuring it to run from the global zone, you are in a position to monitor and record this breach in a way that (1) attackers do not know that their actions are being monitored and (2) attackers cannot see or change the audit system, its configuration, or its logs. This is a significant improvement over using the global zone for service deployment where an attacker who has root or equivalent privilege would be able to view and even modify the audit records on the system.

In addition to auditing, if extended process accounting has been configured and enabled from the global zone, then the accounting data can still be archived for the local zone even if the attacker turns off process accounting within the zone (which in fact only turns off the zone's own accounting stream).

To further hide their presence, attackers might also try to install a kernel root kit. This type of attack would be thwarted by the zones security model because local zones are not permitted to load or unload kernel modules (since local zones lack the sys_config privilege). So much for kernel root kits. This attack vector would still be valid, however, if you were running the exploited service from the global zone.

Attackers might also attempt to protect their level of access so that they can come back at a later time even if the vulnerability they used initially had been patched. Often this is done through the installation of root kits and Trojan horses. If the system has been configured in a sparse root configuration (which is the default), the attackers are significantly limited as to what they can install or replace since the /usr, /sbin, /lib, and /platform directory trees are mounted read-only and cannot be modified from within the local zone. So much for installing a Trojaned library or version of sshd.

Since attackers cannot install, modify, or remove files under these directory trees, they might look to see what they can modify. Attackers will only be able to access those file systems and devices that have been specifically assigned to the zone (regardless of what other file systems and devices are available to other zones, including the global zone). If any of the file systems are mounted read-only, then the same condition applies as noted above.

Some file systems, such as / (root) must be writable, however. This means that an attacker could create, modify or remove files from those file systems. Remember that normal UNIX file permissions and ACLs would normally apply here, but we have assumed that our attacker has already obtained root-equivalent access in the zone. So, in this worst case, the attacker could destroy the zone's root file system, but this is no worse than what he or she could do in prior versions of the operating system. This is one reason why it is so important to leverage the Solaris 10 privilege model to run services with only the privileges that they require. That way, should a flaw be found and the service exploited, the impact of the damage can hopefully be minimized. But I digress.

Since the root file system is writable, the attacker could install a new run-control script or a service using Service Management Facility (SMF), modify service configuration files, or even add a user or change a password. All of these changes to the system can be monitored and detected, however, through the use of Solaris auditing as well as the Solaris 10 Basic Auditing and Reporting Tool (BART). BART is a file system integrity tool that can be run from the global zone. Just as with Solaris auditing, attackers would not know that they were being monitored or that their changes to the system had been detected.

In fact, the zones security model combined with Solaris 10 capabilities like Solaris auditing and BART do not leave attackers with very much room to conceal the fact that they are on the system. Similarly, resource management controls can also be applied to help prevent individual zones from consuming resources required by other zones or the global zone on the system. This can help mitigate certain types of denial of service attacks. Of course, the success of this model is dependent on customers deploying services in local zones that can leverage the strength of these capabilities and tools.

10.4 Domino and Notes security basics

We now consider Domino and Notes security basics. For detailed information, see *Lotus Notes and Domino Security Infrastructure Revealed*, SG24-5341.

10.4.1 Notes certificates

A Notes certificate is an electronic stamp that verifies to the server that you are who you say you are. In actuality, a certificate is a digitally signed message added by a certifier to a Notes ID file.

When you register users and servers, Domino automatically creates a Notes certificate for each user and server ID.

You can also create Internet certificates for user IDs using a Domino or third-party certificate authority (CA). Domino creates Internet certificates using the X.509 certificate format.

Note: The certificate itself does not contain any private information; it is therefore open to the public and can be distributed anywhere.

10.4.2 Certification hierarchies

Lotus Notes used to provide two types of certification: flat and hierarchical. Organizations using flat names may use several certifier IDs. Each user ID and server ID can include separate certificates generated by each flat certifier ID. Organizations using hierarchical certification have one organization certifier and, optionally, up to four layers of organizational unit certifiers below.

Flat certificates

Before the introduction of hierarchical certificates, flat certificates were the only way to register users and servers. They are supported in Lotus Notes/Domino R5.0 only for compatibility with earlier releases.

New installations are encouraged to start with hierarchical names, and existing flat installations are encouraged to convert to hierarchical, because of the increased security and flexibility of access control, ID file generation and certification, and maintenance.

Hierarchical certificates

In hierarchical certification, an organization might be layered with the organization certifier at the top and up to four layers of organizational unit certifiers below. When users or servers are registered with a certifier, they receive a certificate signed by that certifier and inherit the certification hierarchy of the layers above.

Users and servers may authenticate with each other if they have at least one common ancestral certificate. Entities that do not share at least one common ancestor can still authenticate by going through a cross-certification process.

Cross-certification

Cross-certificates are used to allow users and servers from different hierarchically certified organizations to access servers in other organizations and to verify the digital signature of a user from another organization. Servers store cross-certificates in the Domino Directory. To access servers, users store cross-certificates in their Personal Address Books.

10.4.3 Notes IDs

Domino uses ID files to identify users and to control access to servers. Every Domino server, Notes certifier, and Notes user must have an ID. When an administrator registers users and servers, Domino automatically creates their IDs.

> **Important:** The security of the entire Domino system relies heavily on the secure creation, distribution, administration, and archiving of certificates and Notes IDs or their ID files so that they cannot be compromised. Store ID files on secure media and keep them safe.

Contents of a Notes ID

After the registration process, the ID file contains:

- The user's name and Notes license number
- Two public and private key pairs
- Two certificates for the user
- A certificate for each ancestor certifier

Password protection

ID files should be password-protected to avoid unauthorized use. When you password-protect your ID, a key that is derived from the password encrypts the data on the ID. Then, when you attempt to access mail, open a server-based database, or examine ID file information, you are prompted to enter a password.

10.4.4 Notes validation and authentication

Whenever a Notes client (or Domino server) attempts to communicate with a Domino server for replication, mail routing, or database access, two security procedures use information about the client's ID to verify that the client is legitimate: validation and authentication.

- Validation establishes trust of the client's public key. If validation occurs successfully, authentication begins.
- Authentication verifies the identity of the user. Authentication uses the public and private keys of the client and the server in a challenge/response interaction.

10.5 Protecting a Domino server

You as an administrator have to ensure that all data on your Domino server is protected. From the beginning of server setup, you should always keep security in mind. Basic security settings have to be made as soon as a user or server gains access to the server on the network. If you set up servers for Internet or intranet access, you have to set up additional server security. In addition, set up a firewall server to protect Internet servers from unauthorized access from outside the organization's network. Reverse proxy servers are also recommended to secure HTTP servers, instead of exposing them to the Internet zone.

10.5.1 Protecting access during Domino Server Setup

The remote setup listener can be loaded on the server to provide access for an administrator to perform server setup, but it is possible to run the setup step locally run the set up step using an X.11 terminal session–based installation as seen in 5.3.6, "Local server setup" on page 165.

Note: The field details from the form are sent in clear text format to the server; therefore, ID names and password details are vulnerable during this time. Therefore we recommend using the X.11 terminal-based installation because of security concerns.

The administrator may use FTP to retrieve copies of newly created certifier, server, or administrator ID files. Using an unsecured FTP session means that the contents of the ID files are vulnerable to network sniffers during transit between the server and the receiving machine. Also, FTP and Telnet are known to send passwords in plain text through the network. There are many ways to prevent this from happening. It is highly recommended to utilize a secure shell client for terminal access and a secure file transfer client for file transfers.

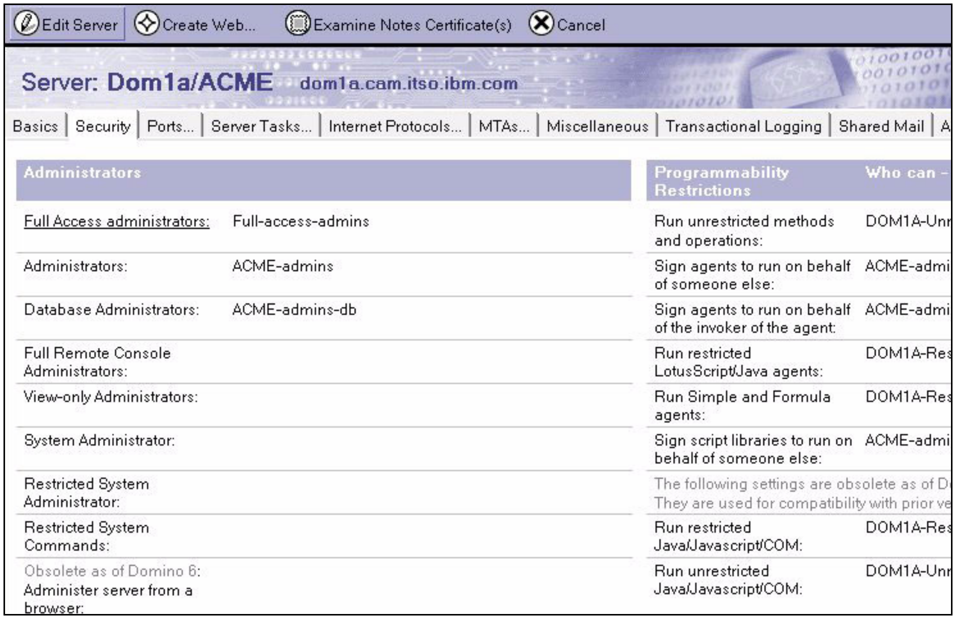
10.5.2 Setting up basic Domino server security

You can use server documents in the Domino Directory to control access to a Domino server. In addition, you can restrict the activities that users and servers may perform on the server. The following fields are on the Server tab.

> **Note:** We recommend that you include groups instead of individual user names in the configuration fields, and avoid using nested groups in order to provide better control of the users included in those groups. Also, it is possible to include organizational units in the configuration fields although we only recommend this for certain fields (such as the Access server field).

Administrators section

A Domino environment has several levels of administrator privileges. We recommend that you define administrator roles within a organization according to the organization business needs and security policies, and then set up this configuration (Figure 10-1).



Server: Dom1a/ACME dom1a.cam.itso.ibm.com

Administrators	
Full Access administrators:	Full-access-admins
Administrators:	ACME-admins
Database Administrators:	ACME-admins-db
Full Remote Console Administrators:	
View-only Administrators:	
System Administrator:	
Restricted System Administrator:	
Restricted System Commands:	
Obsolete as of Domino 6: Administer server from a browser:	

Programmability Restrictions	Who can -
Run unrestricted methods and operations:	DOM1A-Unr
Sign agents to run on behalf of someone else:	ACME-admi
Sign agents to run on behalf of the invoker of the agent:	ACME-admi
Run restricted LotusScript/Java agents:	DOM1A-Res
Run Simple and Formula agents:	DOM1A-Res
Sign script libraries to run on behalf of someone else:	ACME-admi
The following settings are obsolete as of D They are used for compatibility with prior ve	
Run restricted Java/Javascript/COM:	DOM1A-Res
Run unrestricted Java/Javascript/COM:	DOM1A-Unr

Figure 10-1 First part of the security tab from the server document

- Full Access administrator

  A Full Access administrator has Manager access to all databases within the server, regardless of the database ACL. Otherwise, this administrator has the same level of access as the users in the Administrators field.

- Administrators

  Users listed in the Administrator field can:

  - Issue console commands
  - Designate an Administration server for databases
  - Compact and delete databases
  - Create, update, and delete full text indexes
  - Create, update, and delete directories and links
  - Create database replicas and master templates
  - Get and set certain database options, such as quota
  - Use message tracking and track subjects
  - Use cconsole to remotely administer UNIX servers

- Full Remote Console Administrators

  These administrators can issue console commands.

- View-only Administrators

  These administrators can issue informational commands (such as show server or show task).

- System Administrator

  People listed in this field may issue operational system commands. The shell commands run with the Solaris user ID that owns the Domino process.

  > **Attention:** Users included in this field will be able to delete databases and folders by issuing shell commands. Make sure that only authorized persons are included here.

- Restricted System Administrator

  These users can issue restricted operational system commands. These users can issue restricted operating system commands that are listed in the Restricted System Commands field (see below).

- Restricted System Commands

  List of available operational system commands that the Restricted System Administrator list of users can issue.

- Administer server from a browser

  This configurations is already deprecated (in Domino 6 and later).

Configurations for secure applications

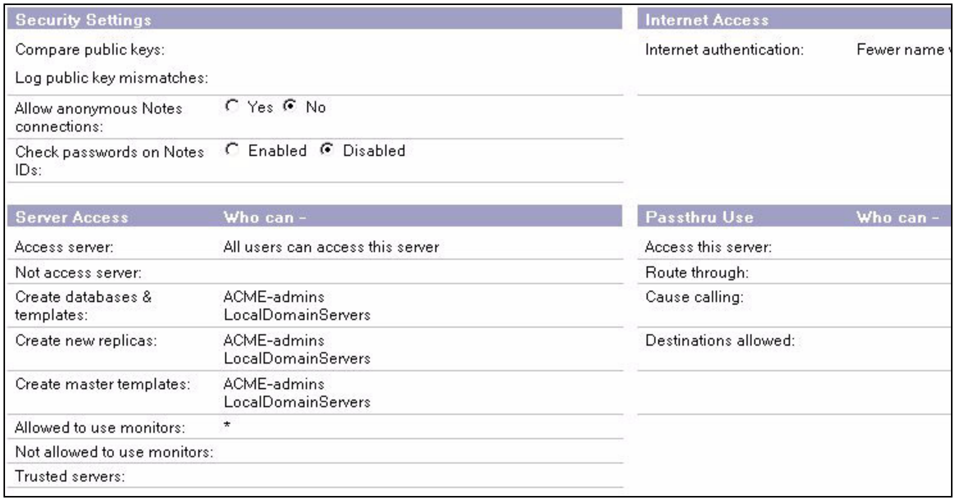
These are some of the fields you should configure in order to secure your server. Securing applications is not part of the scope of this book, so for further information refer to the Lotus Security Handbook, SG24-7017-00 which can be found at:

http://www.redbooks.ibm.com/redbooks/pdfs/sg247017.pdf

- Run unrestricted methods and operations
- Sign agents to run on behalf of someone else
- Sign agents to run on behalf of the invoker of the agent
- Run restricted LotusScript/Java agents
- Run Simple and Formula agents
- Sign script libraries to run on behalf of someone else

The following settings are obsolete as of Domino 6. They are used for compatibility with prior versions only:

- Run restricted Java/Javascript/COM
- Run unrestricted Java/Javascript/COM



Security Settings	
Compare public keys:	
Log public key mismatches:	
Allow anonymous Notes connections:	○ Yes ● No
Check passwords on Notes IDs:	○ Enabled ● Disabled

Internet Access	
Internet authentication:	Fewer name

Server Access	Who can -
Access server:	All users can access this server
Not access server:	
Create databases & templates:	ACME-admins LocalDomainServers
Create new replicas:	ACME-admins LocalDomainServers
Create master templates:	ACME-admins LocalDomainServers
Allowed to use monitors:	*
Not allowed to use monitors:	
Trusted servers:	

Passthru Use	Who can -
Access this server:	
Route through:	
Cause calling:	
Destinations allowed:	

Figure 10-2   Second part from the security tab of the server document

Server Access section

Specify which Notes users and Domino servers are authorized to access the server (whether only users listed in the current Domino Directory can access the server) in these fields:

- Access server
- Not access server

Specify which Notes users and Domino servers are authorized to create databases, replica databases, and master templates on the server:

- Create databases & templates

Internet Access section

Specify what type of names will be accepted during name and password authentication (by restricting the number of available entries, you ensure that a hacker is less likely to find a match by guessing a user name):

- Internet authentication (set to **Fewer name variations with higher security**).

Passthru Use section

Specify which Notes users and Domino servers can access the server as a passthru server and specify the destinations they may access in these fields:

- Access this server
- Route through
- Cause calling
- Destinations allowed

10.5.3 Setting up additional Domino server security

This section outlines additional parameters that can be set for even greater Domino server security.

Restrict Web browser access to the OpenServer URL parameter

Specify whether browser users can see a list of all databases on the server. By default, users cannot display a list of databases even if they have access to the server. On the Internet Protocols → HTTP tab:

- Allow HTTP clients to browse databases (set to **No**).

Control Web browser access to files on their server’s hard drive

This section demonstrates how to specify who is allowed to access files (for example, HTML, GIF, or JPEG) on a server’s hard drive. For more information, see 14.3.5, “Domino file protection” on page 440.

Secure the server with SSL

Set up SSL security for Internet and intranet users to authenticate the server, encrypt data, prevent message tampering, and, optionally, authenticate clients.

For more information about configuring SSL in a Domino HTTP server, refer to “Setting up SSL on a Domino server” in Administrator client help.

Secure the server with name-and-password authentication

When using name-and-password authentication, also known as basic password authentication, Domino asks for a name and password only when an Internet or intranet client tries to access a database on the server. Set up basic password authentication using the following steps:

1. Create a Person document for each user in the Domino Directory on the Domino server.
2. Assign an Internet password to each user.
3. Specify which Internet protocols require a name and password in the appropriate fields on the Ports → Internet Ports tab in the Server document.
4. Set the database ACLs.

> **Note:** You can use basic password authentication with either TCP/IP or SSL on any servers that run an Internet protocol—namely, NNTP, LDAP, POP3, HTTP, SMTP, IIOP, or IMAP.

Using policies, you can now ensure that Internet passwords are strong, and you can synchronize user ID passwords with the Notes Internet password. For more information, refer to “Managing Internet passwords” in Administrator client help.

> **Note:** Password synchronization will be done by the Administration Process, so a delay between the password change and the synchronization is expected, depending on the replication topology.

Secure the server with session-based authentication

There is an additional method for setting up name-and-password authentication for an HTTP server: session-based authentication. Session-based name-and-password authentication offers greater control over user interaction than basic name-and-password authentication, and it enables you to customize the form in which users enter their name and password information. It also allows users to log out of the session without closing the browser.

Set up session-based authentication by completing the following fields on the Internet Protocols → Domino Web Engine tab in the Server document:

- Session authentication
- Idle session timeout
- Maximum active sessions

You can also set up session authentication for Web site documents from the Domino Administrator. Select the **Configuration** tab, expand the **Web** section, and click **Internet Sites**. From there you can select the Web site document that you wish to edit and click **Edit Document**. Click the **Domino Web Engine** tab and under HTTP Sessions, in the Session Authentication field, you can choose the type of authentication that you desire.

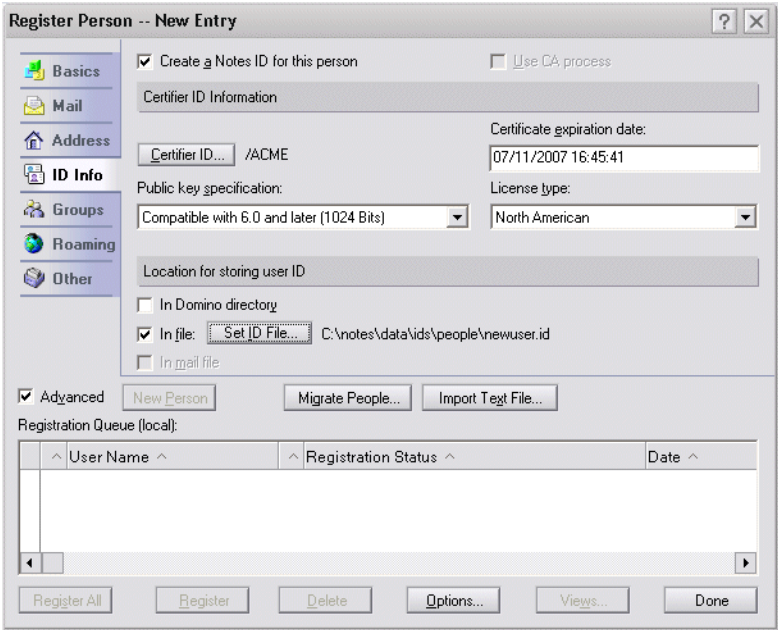
Allow anonymous Internet and intranet client access

Determine whether Internet and intranet users are allowed to access the server anonymously. Use the following steps to do this:

1. Set the Anonymous field for the protocol that you want accessed anonymously on the Ports → Internet Ports tab in the Server document.
2. Include `Anonymous` in the ACL of the database for which you want to give free, anonymous access.

10.5.4 New support to 1024-bit keys

The new 1024-bit keys are supported only by Domino Versions 6 and later (Figure 10-3). This new key size is an enhancement in the encryption strength that extends the power of Domino databases to store confidential information in an organization.



Register Person -- New Entry

☑ Create a Notes ID for this person
□ Use CA process

Certifier ID Information

Certifier ID... /ACME

Certificate expiration date: 07/11/2007 16:45:41

Public key specification: Compatible with 6.0 and later (1024 Bits)

License type: North American

Location for storing user ID

□ In Domino directory
☑ In file: Set ID File... C:\notes\data\ids\people\newuser.id
□ In mail file

☑ Advanced

Registration Queue (local):

Figure 10-3 Registering user with 1024-bit encryption key

Authenticate Web clients using a secondary Domino Directory or LDAP directory

If your organization uses a secondary Domino Directory or an LDAP directory to verify client certificates, you can set up Domino to check those additional directories. To do so, set up the secondary Domino and LDAP directories as trusted domains in the Directory Assistance database.

For more information, see "Authenticating Web SSL clients in secondary Domino and LDAP directories" in the security section of Domino 5 Administrator online help.

Authenticate Web clients for a specific realm

Allow Web users to access a certain drive, directory, or file on a Domino server and prevent Domino from prompting users for a name and password for different realms. Setting a realm for specific applications also protects the Domino server databases and other application directories from unauthenticated use. When a user accesses a page on a Domino Web site, the browser keeps track of user credentials based on the realm that the Domino server sends to the browser. A *realm* is a string (typically a URL path) that the server sends to indicate the location, or path, for which the user has been authenticated.

For example, if your server name is www.acme.com, then www.acme.com is the top-level realm and www.acme.com/doc, www.acme.com/hr, and www.acme.com/marketing are the lower-level realms. If a user authenticates with the server when accessing the home page for www.acme.com, then the user is authenticated for www.acme.com and all lower-level realms.

However, if the user accesses www.acme.com/doc first, enters a name and password and is authenticated, and then accesses www.acme.com/hr, Domino prompts the user for credentials again. This second prompt occurs because the browser examines the list of realms for which Domino has successfully authenticated the user and finds www.acme.com/doc in the browser realm list. Because www.acme.com/hr is not a subdirectory of www.acme.com/doc, Domino requires the user to enter credentials again.

To prevent users from being prompted multiple times for their names and passwords, direct them to access and authenticate with the highest level realm that they need to access. This way, Domino asks users for their credentials only once during the browser session.

You can protect server files from Web access by creating a File Protection document in the Domino Directory.

Specify Web realms by creating Web realm documents in the Domino Directory.

For more information, read “Creating a Web Site authentication realm document” in the Administrator client help.

10.6 Setting up Domino database security

When actual server access and connections to the server have been restricted, access to the data in the databases and applications on the server must be considered.

> **Tip:** To ensure that all security mechanisms are covered, disable all access, then re-enable only the specific areas of access that are known to be required. Having to remember to enable a feature is much less of a risk than having to remember to disable one, as security might already have been breached.

10.6.1 Review database ACLs

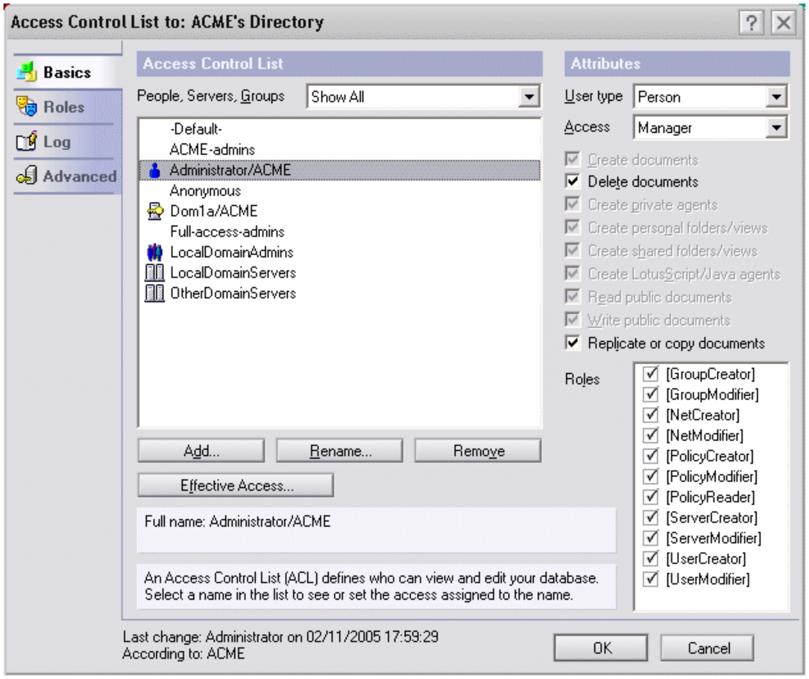
Every database has an access control list (ACL) that specifies the level of access that users and servers have to the database. The access levels are the same for users and servers. Access levels assigned to users determine the tasks that users can perform, and those assigned to servers determine what information within the database the servers can replicate.

You must have Manager access to modify the ACL.

The following areas of database access control should be reviewed and set for all databases and templates on the server:

- Enter an Anonymous entry in the ACL with the appropriate access level.
- Set the Default entry to **No Access**.
- Check appropriate use of Read public documents and Write public documents.
- Set an appropriate Maximum Internet Name & Password access level.
- Use groups instead of single user entries. Groups prevent ACLs from becoming too big and unmanageable.
- Assign user types because they provide an additional level of security.

Consider the use of consistent ACLs.



Access Control List to: ACME's Directory

People, Servers, Groups: Show All

-Default-
ACME-admins
Administrator/ACME
Anonymous
Dom1a/ACME
Full-access-admins
LocalDomainAdmins
LocalDomainServers
OtherDomainServers

User type: Person
Access: Manager

☑ Create documents
☑ Delete documents
☑ Create private agents
☑ Create personal folders/views
☑ Create shared folders/views
☑ Create LotusScript/Java agents
☑ Read public documents
☑ Write public documents
☑ Replicate or copy documents

Roles:
☑ [GroupCreator]
☑ [GroupModifier]
☑ [NetCreator]
☑ [NetModifier]
☑ [PolicyCreator]
☑ [PolicyModifier]
☑ [PolicyReader]
☑ [ServerCreator]
☑ [ServerModifier]
☑ [UserCreator]
☑ [UserModifier]

Full name: Administrator/ACME

An Access Control List (ACL) defines who can view and edit your database. Select a name in the list to see or set the access assigned to the name.

Last change: Administrator on 02/11/2005 17:59:29
According to: ACME

Figure 10-4 Database Access Control List

10.6.2 Consistent ACLs

You can ensure that an ACL remains identical on all database replicas on servers, as well as on all local replicas that users make on workstations or laptops, by selecting **Enforce a consistent Access Control List** in the Advanced section of a database ACL.

You need Manager access to change an ACL. Select **Enforce a consistent Access Control List** on a replica whose server has Manager access to other replicas to keep the access control list the same across all server replicas of a database. If you select a replica whose server does not have Manager access to other replicas, replication will fail because the server has inadequate access to replicate the access control list.

Manager access is awarded to you by default when a database is local because security does not have to be enforced. However, if the “Enforce a consistent access control list” option is selected, your local rights can never exceed the rights you have been assigned on the server. If you have been assigned Author access and the option is enabled, you will have Author access locally, not Manager access.

If a user changes a local or remote server database replica's ACL when the "Enforce a consistent access control list" option is selected, the database stops replicating. The log file records a message indicating that replication could not proceed because the program could not maintain a uniform access control list on replicas.

Enforcing a consistent access control list does not provide additional security for local replicas. To keep data in local replicas secure, encrypt the database.

10.6.3 Extended ACL

An extended access control list (ACL) is an optional directory access-control feature available for a directory created from the PUBNAMES.NTF template — a Domino Directory or an Extended Directory Catalog. An extended ACL is tied to the database ACL, and you access it through the Access Control List dialog box using a Notes 7 or Domino Administrator 7 client. You use an extended ACL to apply restrictions to the overall access the database ACL allows a user — you cannot use it to increase the access the database ACL allows. Use an extended ACL to set access to:

- All documents with hierarchical names at a particular location in the directory name hierarchy (for example, all documents whose names end in OU=West/O=Acme)
- All documents of a specific type (for example, all Person documents)
- A specific field within a specific type of document
- A specific document

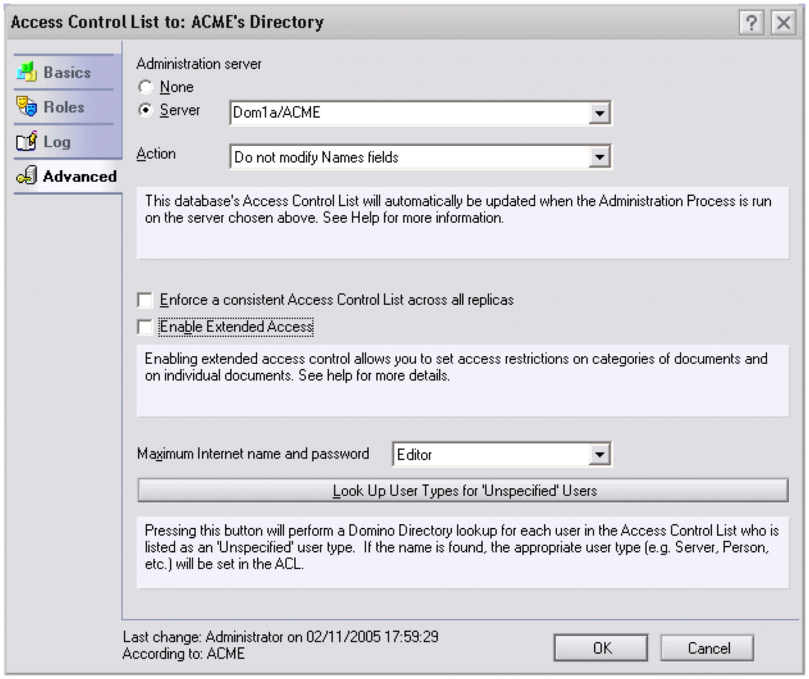
An extended ACL enables you to:

- Delegate your Domino administration; for example, allow a group of administrators to manage only documents named under a particular organizational unit.
- Set access to precise portions of the directory contents.
- Set access to documents and fields easily and globally at one source, rather than requiring you to control access through features such as multiple Readers and Authors fields.
- Control the access of users who access the directory through any supported protocol: Notes (NRPC), Web (HTTP), LDAP, POP3, and IMAP.

Setting xACL

To set xACL:

1. Open the access control list from the Domino Directory database (names.nsf) and select **Advanced** in the left panel.


Access Control List to: ACME's Directory

Administration server
○ None
● Server: Dom1a/ACME

Action: Do not modify Names fields

This database's Access Control List will automatically be updated when the Administration Process is run on the server chosen above. See Help for more information.

□ Enforce a consistent Access Control List across all replicas
□ Enable Extended Access

Enabling extended access control allows you to set access restrictions on categories of documents and on individual documents. See help for more details.

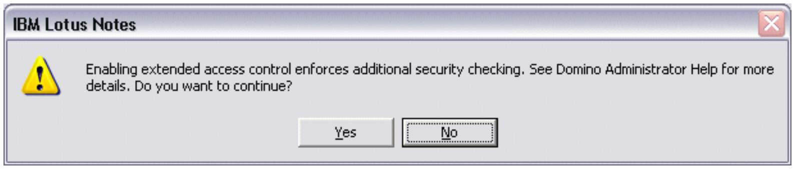
Maximum Internet name and password: Editor

Pressing this button will perform a Domino Directory lookup for each user in the Access Control List who is listed as an 'Unspecified' user type. If the name is found, the appropriate user type (e.g. Server, Person, etc.) will be set in the ACL.

Last change: Administrator on 02/11/2005 17:59:29
According to: ACME

Figure 10-5 ACL advanced panel

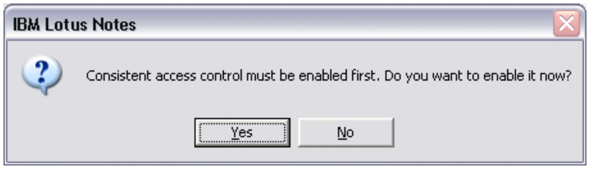
2. Mark the check box for **Enable Extended Access**.


IBM Lotus Notes

Enabling extended access control enforces additional security checking. See Domino Administrator Help for more details. Do you want to continue?

Figure 10-6 Confirming Extended ACL enablement

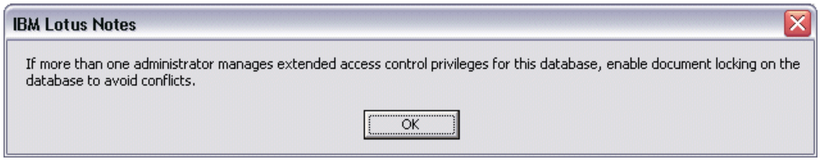
3. Click **Yes** to confirm the configuration. If consistent ACL is not enabled, you need to enable. The system will prompt you to do that.


IBM Lotus Notes

Consistent access control must be enabled first. Do you want to enable it now?

Figure 10-7 Enabling Consistent ACL

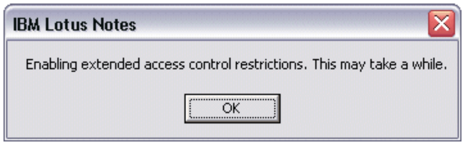
4. Click **Yes** to confirm configuration changes.



If more than one administrator manages extended access control privileges for this database, enable document locking on the database to avoid conflicts.

Figure 10-8 Database conflict disclaimer

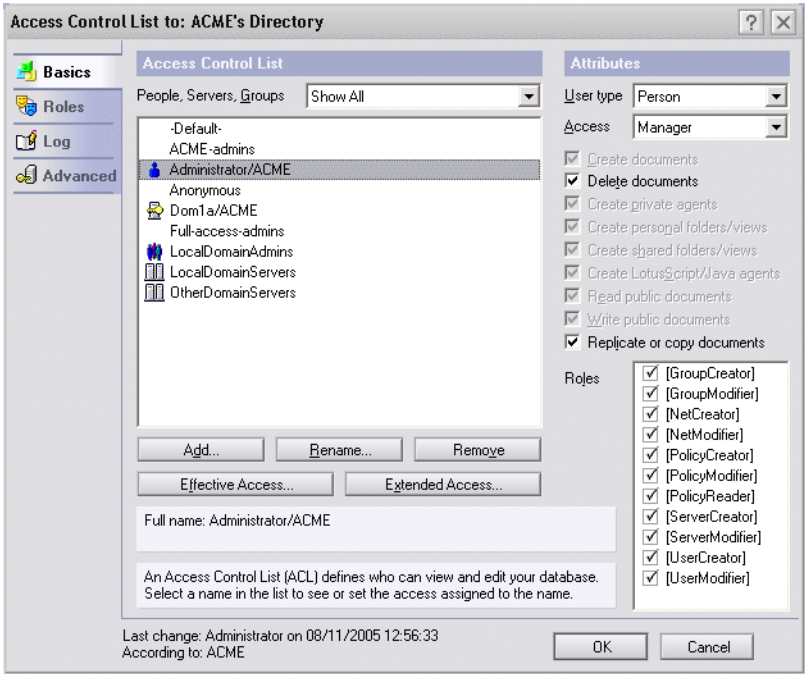
5. Click **OK**.



Enabling extended access control restrictions. This may take a while.

Figure 10-9 Confirmation of extended ACL enablement

Now the Extended Access button should be enabled for Extended access control list configuration (Figure 10-10).



People, Servers, Groups: Show All

-Default-
ACME-admins
Administrator/ACME
Anonymous
Dom1a/ACME
Full-access-admins
LocalDomainAdmins
LocalDomainServers
OtherDomainServers

User type: Person
Access: Manager

☑ Create documents
☑ Delete documents
☑ Create private agents
☑ Create personal folders/views
☑ Create shared folders/views
☑ Create LotusScript/Java agents
☑ Read public documents
☑ Write public documents
☑ Replicate or copy documents

Roles:
☑ [GroupCreator]
☑ [GroupModifier]
☑ [NetCreator]
☑ [NetModifier]
☑ [PolicyCreator]
☑ [PolicyModifier]
☑ [PolicyReader]
☑ [ServerCreator]
☑ [ServerModifier]
☑ [UserCreator]
☑ [UserModifier]

Full name: Administrator/ACME

An Access Control List (ACL) defines who can view and edit your database. Select a name in the list to see or set the access assigned to the name.

Last change: Administrator on 08/11/2005 12:56:33
According to: ACME

Figure 10-10 ACL Advanced with Extended Access button enabled

10.6.4 Mail rules and spam

Spam is always a problem that companies with a vast mail platform have to face. Handling spam within a mail environment usually means increasing security costs in an IT department, so it is best to prevent undesired mail from actually reaching the mail server.

There are many third-party spam solutions that can be used in conjunction with Domino to decrease the amount of undesired mail handled by the server. New anti-spam software is capable of identifying spam using pre-existing signatures or heuristic algorithms based in common spam characteristics. These algorithms have a small percentage of false positives (real mail marked as spam) and this makes it unwise to delete the messages. Instead, a spam folder can be created in each user's mail folder and a mail rule created that moves messages that contain the subject [spam] directly to the spam folder. The user is responsible for checking this folder regularly for real mail in the folder and purging the spam.

Setting up and using message disclaimers

Message disclaimers are notices—usually short text blocks—that are added to e-mail messages. They are often used by organizations in an attempt to protect the organization's legal interests. For example, message disclaimers can be used to limit an organization's exposure to vicarious liability, that is, to limit the organization's responsibility for the actions of its employees. This type of disclaimer informs the message recipient that the organization is not responsible for anything written by the author of the message. Another commonly used type of message disclaimer consists of a warning stating that the message might not be intended for the current recipient and that it might contain confidential information. The disclaimer directs the unintended recipient to dispose of the message without sharing its contents with others.

To enable message disclaimer, refer to "Setting up and using message disclaimers" in Administrator client help.

Restricting SMTP inbound routing with whitelists

Use DNS whitelist filters to help identify legitimate e-mail. When DNS whitelist filters are enabled, the SMTP listener task determines whether a connecting host is a member of a DNS whitelist by relying on the results of a DNS query of a DNS blacklist-style host name. If the query returns an IP address, the host is added to the whitelist and the remaining DNS whitelists are not searched. If the host is not found in the DNS whitelist, processing continues with DNS blacklist filters. If the query returns an error indicating that the host name is not valid, the host is not added to the whitelist and might be subject to blacklist filtering if that is enabled. For more information, refer to "Enabling DNS whitelist filters for SMTP connections" in Administrator client help.

For more about using Domino to prevent spam, refer to *Lotus Domino 6 spam Survival Guide for IBM eServer*, SG24-6930.

10.7 Anti-virus products for Domino

Several anti-virus products are available for Domino 7 running on Solaris. These products are best deployed on the mail and replication gateways and firewall servers. With this architecture, the performance impact of running virus detection is localized to the key gateway servers. Refer to the IBM product pages for Lotus Domino to find out which virus scanners are available for Domino on Solaris.

10.8 Summary

In this chapter we discussed how to implement a secure system for Domino running on Solaris. We considered this issue from a Solaris operating environment point of view and from a Domino application point of view.

11

Solaris 10 administration

This chapter discusses the Solaris 10 Administration tools. These administration tools are divided into System Administration tools and the Sun Management Center.

© Copyright IBM Corp. 2006. All rights reserved.

11.1 System administration tools

Solaris Service Manager

Automatically restarts failed services in dependency order, whether the services failed as the result of administrator error, a software bug, or an uncorrectable hardware error.

- Makes services objects that can be viewed, with the new **`svcs`** command, and managed, with **`svcadm`** and **`svccfg`** commands. You can also view the relationships between services and processes by using **`svcs -p`** for both SMF services and legacy /etc/init.d scripts.
- Makes it easy to back up, restore, and undo changes to services by taking automatic snapshots of service configurations.
- Makes it easy to debug. You can ask questions about services and receive an explanation of why a service is not running by using **`svcs -x`**. Also, this process is eased by individual and persistent log files for each service.
- Enhances administrators' ability to securely delegate tasks to non-root users, including the ability to modify properties and start, stop, or restart services on the system.
- Boots faster on large systems by starting services in parallel according to the dependencies of the services. The opposite process occurs during shutdown.
- Enables you to customize the boot console output either to be as quiet as possible, which is the default, or to be verbose by using **`boot -m verbose`**.
- Preserves compatibility with existing administrative practices wherever possible. For example, most customer and ISV-supplied RC scripts still work as usual.
- Enables you to configure your system services in one of two modes, both represented as smf(5) profiles. The generic_open.xml profile enables all traditional Internet services that were previously enabled by default in the Solaris OS. The generic_limited_net.xml profile disables a large number of services that are frequently disabled during the process of hardening a system. However, this profile is not a replacement for the Solaris Security Toolkit (JASS) tool. See the individual profiles listed at the Sun Web site for details.

Solaris Fault Manager

Predictive Self-Healing systems include a simplified administration model. Traditional error messages are replaced by telemetry events that are consumed by software components. The software components automatically diagnose the underlying fault or defect and initiate self-healing activities. Examples of self-healing activities include administrator messaging, isolation or deactivation of faulty components, and guided repair. A new software component is called Fault Manager, fmd(1M). The Fault Manager manages the telemetry, log files, and components. The new fmadm(1M), fmdump(1M), and fmstat(1M) tools are also available in the Solaris 10 OS to interact with the Fault Manager and new log files.

When appropriate, the Fault Manager sends a message to the syslogd(1M) service to notify an administrator that a problem has been detected. The message, which explains more about the problem impact and appropriate responses and repair actions, directs administrators to a knowledge article on Sun's new message Web site:

http://www.sun.com/msg/

The Solaris Express 6/04 release introduced self-healing components for automated diagnosis and recovery for UltraSPARC-III and UltraSPARC-IV CPU and memory systems. This release also provided enhanced resilience and telemetry for PCI-based I/O.

In the Solaris Express 5/04 release, user-process tracing that uses the pid provider was made available on x86. This feature has been available on SPARC platforms since the introduction of DTrace in the Solaris Express 11/03 release.

The pid provider enables you to trace any instruction in any process either at the level of any function call's entry and return, or at any offset into any function. For complete details, see Chapter 27, "pid Provider," and Chapter 32, "User Process Tracing," in the Solaris Dynamic Tracing Guide.

In the Solaris Express 11/04 release, the plockstat(1M) utility enables you to observe user-level synchronization primitives, such as lockstat(1M) in the kernel. The DTrace plockstat provider is the underlying instrumentation methodology for plockstat(1M). Dtrace plockstat can be used to augment the data recorded by the plockstat utility. See the plockstat(1M) man page for further information.

The Solaris 10 OS has the ability to automatically detect whether your system is 64-bit capable and then boot the appropriate kernel.

Following a new installation of the Solaris 10 software, the boot program automatically loads the 64-bit kernel if it detects your system is 64-bit capable. Otherwise, the program loads the 32-bit kernel.

Following an upgrade installation of the Solaris 10 OS on a system that is configured to load the default 32-bit kernel, the system now automatically determines whether to load the 32-bit or 64-bit kernel. If the system was configured to load a non-default kernel, the system continues to load that non-default kernel. Procedures for customizing a system to load a specific kernel are outlined in Chapter 8, “Shutting Down and Booting a System (Overview)” in System Administration Guide: Basic Administration.

Further documentation about the kernel selection procedure is provided in the Solaris 10 documentation at:

http://docs.sun.com

11.1.1 Package and patch tool enhancements

The Solaris package and patch tools have been enhanced, providing improved performance and extended functionality.

As a part of these enhancements, the **pkgchk** command now provides a new option to assist you in mapping files to packages. To map files to packages, use the **pkgchk -P** option instead of grep pattern /var/sadm/install/ contents. The -P option enables you to use a partial path. Use this option with the -l option to list the information about the files that contain the partial path.

If you installed a previous Software Express release, your system might use a SQL format package database. The SQL database was created in one of the following ways:

- You performed an initial installation of a Solaris Express release prior to the Solaris Express 10/04 release.
- You upgraded to a prior Solaris Express release, and upgraded the package database manually by running pkgadm upgrade.

When you upgrade to the Solaris Express 10/04 release or subsequent releases, the SQL package database is automatically converted back to the ASCII text file format.

See the System Administration Guide: Basic Administration and the pkgchk(1M) man page for further information.

11.1.2 Sun Patch Manager enhancements

The Sun Patch Manager tool (Patch Manager) is the standard tool for managing patches on Solaris systems. Use this tool to apply patches to Solaris systems.

You can access Patch Manager by using the smpatch command-line interface.

Patch Manager has been enhanced with these features:

- PatchPro analysis engine: Patch Manager now incorporates PatchPro functionality to automate the patch management process. This process includes performing patch analysis on systems, then downloading and applying the resulting patches. This automation functionality was previously available for the Solaris 9 release as a separate PatchPro product and is now part of the standard Solaris release. Solaris 9 users should refer to “Solaris Patch Update Feature” as described in What’s New in the Solaris 9 4/03 Operating Environment.

- Local-mode command-line interface: The command-line interface, smpatch, can be used even when the Solaris WBEM services are not running on your system. This capability enables you to use smpatch to apply patches while your system is in single-user mode.
- Patch list operations: Patch Manager enables you to generate, save, edit, order, and resolve patch lists. These lists can be used to perform patch operations, such as downloading and applying patches.

You must install at least the Developer Software Support Group of the Solaris 10 release to use Sun Patch Manager.

11.1.3 System Management Agent

The System Management Agent is a Simple Network Management Protocol (SNMP) agent that provides SNMPv1, SNMPv2c, and SNMPv3 functionality to the Solaris 10 environment. The agent is based on the Net-SNMP open source implementation, with some customizations for the Solaris environment. The agent has all of the necessary base functionality that is required by an SNMP agent. The agent includes support for standard SNMP operations and numerous standard Management Information Bases (MIBs), including MIB-II, Host Resources MIB, and Notification MIB. Additionally, the agent supports the User-based Security Model (USM) and View-based Access Control Model (VACM), as well as AgentX.

The System Management Agent is configured to be the default SNMP agent, but coexists with the Solstice™ Enterprise AgentsTM software in this release.

For further information, see the netsnmp(5) man page or the Solaris System Management Agent Administration Guide and the Solaris System Management Agent Developer’s Guide.

11.1.4 Signed packages and patches

The Solaris software enables you to securely download Solaris packages and patches that include a digital signature by using the updated pkgadd and patchadd commands. A package or a patch with a valid digital signature ensures that the package or patch has not been modified after the signature was applied to the package or patch.

In previous Solaris releases, you could only add signed patches to your system if you used the Solaris patch management tools with PatchPro 2.1.

These are additional software management features in this Solaris release:

You can add a digital signature to a package with the updated **pkgtrans** command. For information about creating a signed package, see the Application Packaging Developer's Guide.

You can download a package or patch from an HTTP or HTTPS server.

A signed package is identical to an unsigned package except for the signature. The package can be installed, queried, or removed with existing Solaris packaging tools. A signed package is also binary compatible with an unsigned package.

Before you can add a package or patch with digital signatures to your system, you must set up a keystore with trusted certificates that are used to identify that the digital signature on the package or patch is valid.

For information about setting up the package keystore and adding signed packages or patches to your system, see the System Administration Guide: Basic Administration.

For information about booting and retrieving Solaris installation images from an HTTP or HTTPS server, see WAN Boot Installation Method.

11.1.5 LDAP command changes

These command changes were made in the Solaris Express 12/03 release.

Several LDAP commands are updated to include full SSL support and extended support for SASL. The modifications also provide support for managing smart referrals, using virtual list views (VLVs), and establishing stronger authentication when binding to the LDAP server.

This upgrade aligns the Solaris LDAP command functionality with Sun's LDAP directory server commands. All Solaris functionality is preserved for backward compatibility. The updated commands are ldapdelete, ldapmodify, ldapadd, ldapsearch, and ldapmodrdn.

Several changes have been made to the LDAP commands. Those changes include the following:

The -M authentication option is obsolete. This option has been superseded by the stronger -o option. The -M option is now used for managing smart referrals.

Search results are now displayed in LDAP Data Interchange Format (LDIF) by default. Use the -r option to display results in the old format, for backward compatibility.

See the ldapdelete(1), ldapmodify(1), ldapadd(1), ldapsearch(1), and ldapmodrdn(1) man pages for details.

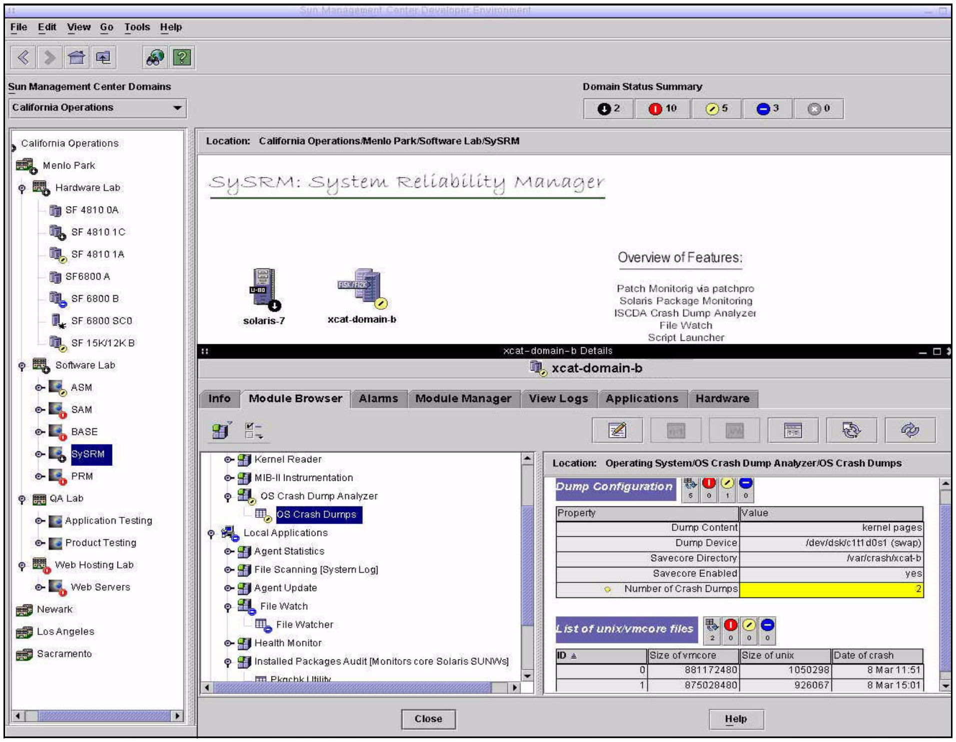
For further information, see the System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP).

11.2 Sun Management Center

Sun Management Center software offers a single point of management for multiple Sun systems, devices and network resources. It works with accompanying software packages: Service Availability Manager, a set of modules that test and measure the availability of network services, System Reliability Manager, a component that enhances reliability, helping to increase service levels and decrease administrative costs, and Performance Reporting Manager, software that adds analysis, reporting, and graphing capabilities.You can find more information at:

http://www.sun.com/software/solaris/sunmanagementcenter

A sample of what the Sun Management Center looks like can be seen in Figure 11-1 on page 386.



Property	Value
Dump Content	kernel pages
Dump Device	/dev/dsk/c1t1d0s1 (swap)
Savecore Directory	/var/crash/xcat-b
Savecore Enabled	yes
Number of Crash Dumps	2

ID	Size of vmcore	Size of unix	Date of crash
0	881172480	1050298	8 Mar 11:51
1	875028480	926067	8 Mar 15:01

Figure 11-1 Sun Management Center example

11.3 Sun Java Web Console

The Sun Java Web Console provides a common location for users to access web-based management applications. Users reach the console by logging in through an HTTPS port, using one of several supported web browsers. The single entry point that is provided by the console eliminates the need to learn URLs for multiple applications. This entry point provides authentication and authorization for all applications that are registered with the console.

All console-based applications conform to the same user interface guidelines. This change enhances ease of use by enabling users to transfer their knowledge of one application to another.

The Java Web Console also provides auditing and logging services for all registered applications.

For more information about the Java Web Console, see the System Administration Guide: Basic Administration.

You can simply start the Java Web Console by typing the following command:

```
smcwebserver start
```

Make sure you have at least one applicaction registered before starting the Java Web Console.

How to connect to via browser to the Java Web Console

Start a Web browser that is compatible with the Java Web Console. Compatible browsers include:

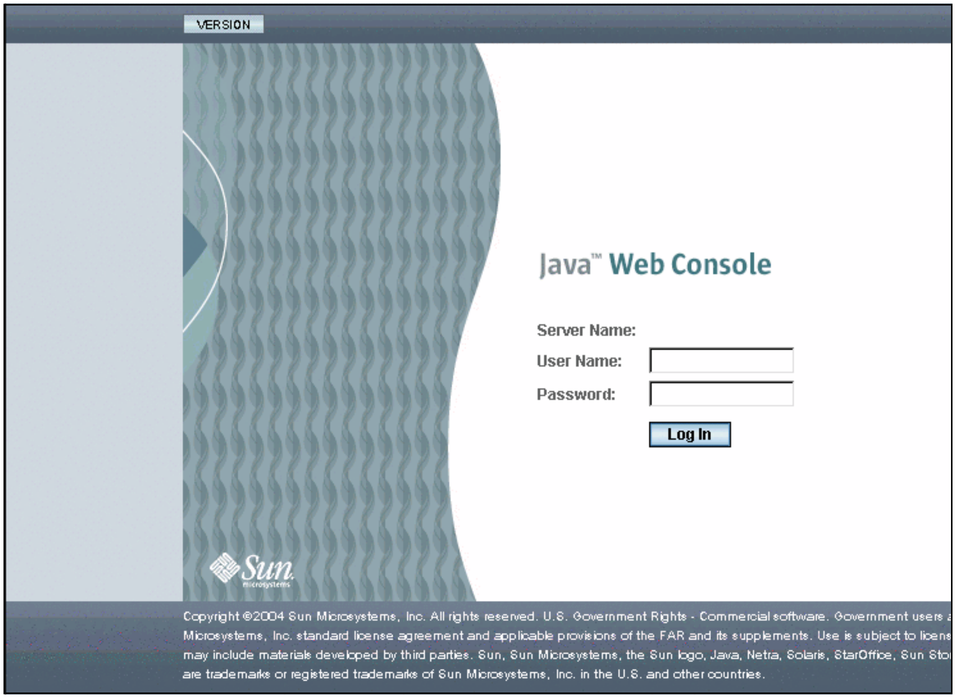
- Mozilla, Version 1.2 or later
- Netscape, 6.2.x, and 7.x

Type a URL in the browser's location field. For example, if the management server host is named dom1b, the URL will be:

```
https://dom1b:6789
```

This URL will take you to the Web Console login page, where you can be authenticated and authorized.

Accept the server's certificate before the Web Console's login page displays.



Copyright ©2004 Sun Microsystems, Inc. All rights reserved. U.S. Government Rights - Commercial software. Government users a
Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements. Use is subject to licens
may include materials developed by third parties. Sun, Sun Microsystems, the Sun logo, Java, Netra, Solaris, StarOffice, Sun Sto
are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Figure 11-2 Java Web Console login

For detailed information about the Java Web Console visit:

`http://docs.sun.com/app/docs/doc/817-1985/6mhm8o5kd?a=view`

11.4 Webmin

What is Webmin?

Webmin is a Web-based interface for system administration for UNIX. Using any browser that supports tables and forms (and Java for the File Manager module), you can setup user accounts, Apache, DNS, file sharing, and so on.

Webmin consists of a simple Web server and a number of CGI programs that directly update system files such as /etc/inetd.conf and /etc/passwd. The Web server and all CGI programs are written in Perl Version 5 and use no non-standard Perl modules.

Almost all development of Webmin was done by Jamie Cameron, though many people have contributed patches and translations into additional languages.

You can download Webmin under the following link:

http://www.webmin.com

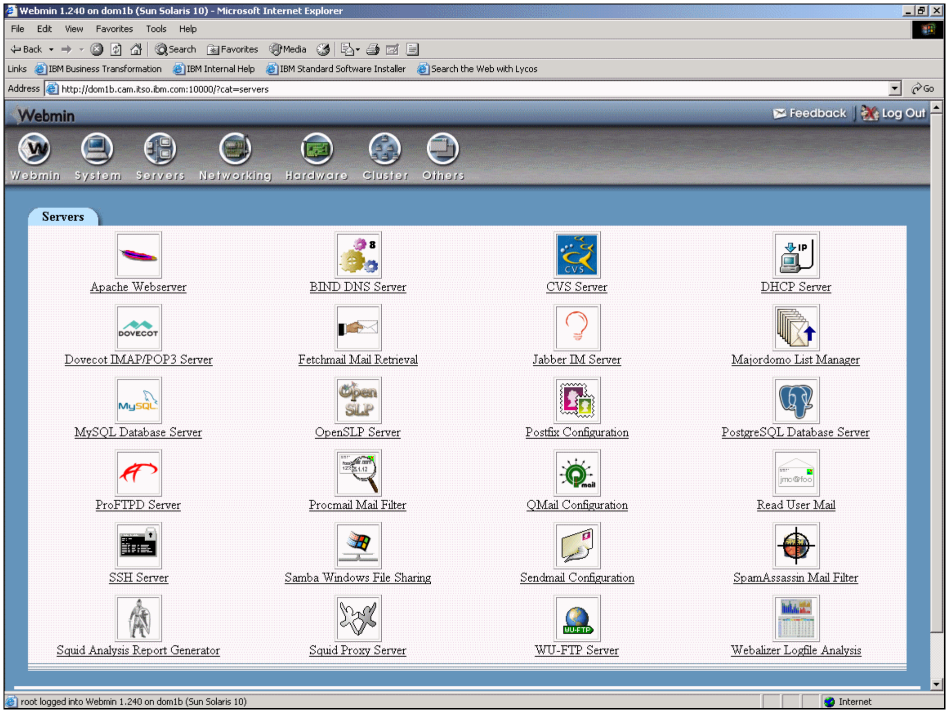
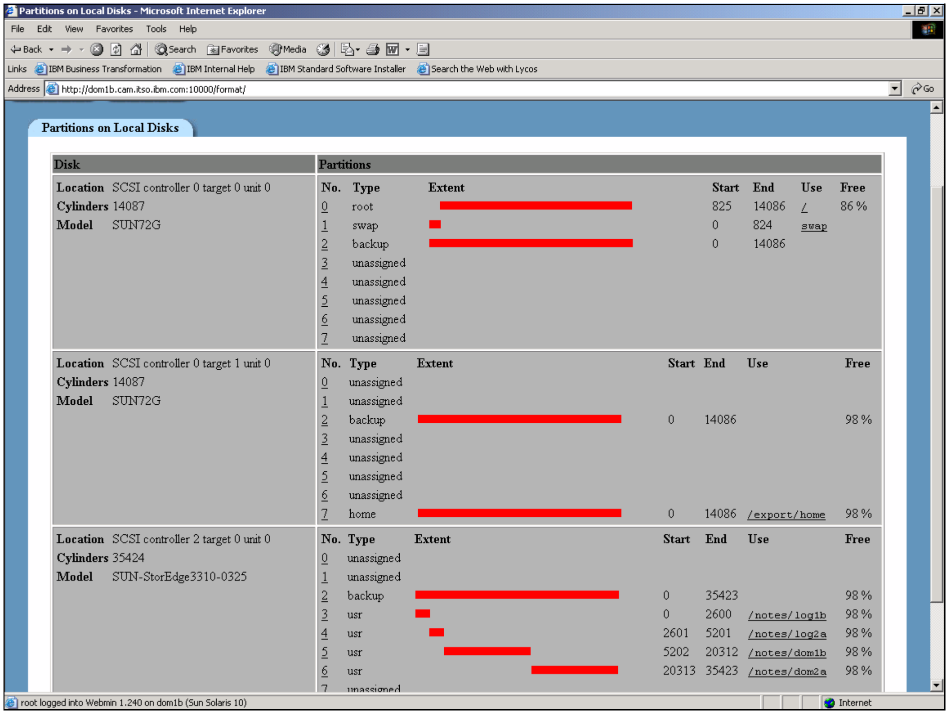

Webmin 1.240 on dom1b (Sun Solaris 10) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links IBM Business Transformation IBM Internal Help IBM Standard Software Installer Search the Web with Lycos
Address http://dom1b.cam.itso.ibm.com:10000/?cat=servers
Go
Webmin
Feedback
Log Out
Webmin
System
Servers
Networking
Hardware
Cluster
Others
Servers
Apache Webserver
BIND DNS Server
CVS Server
DHCP Server
Dovecot IMAP/POP3 Server
Fetchmail Mail Retrieval
Jabber IM Server
Majordomo List Manager
MySQL Database Server
OpenSLP Server
Postfix Configuration
PostgreSQL Database Server
ProFTPD Server
Procmail Mail Filter
QMail Configuration
Read User Mail
SSH Server
Samba Windows File Sharing
Sendmail Configuration
SpamAssassin Mail Filter
Squid Analysis Report Generator
Squid Proxy Server
WU-FTP Server
Webalizer Logfile Analysis
root logged into Webmin 1.240 on dom1b (Sun Solaris 10)
Internet

Figure 11-3 Configure the Server in a wink of an eye


Partitions on Local Disks - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Links
IBM Business Transformation
IBM Internal Help
IBM Standard Software Installer
Search the Web with Lycos
Go
Internet

Address http://dom1b.cam.itso.ibm.com:10000/format/

Partitions on Local Disks

Disk	Partitions						
Location SCSI controller 0 target 0 unit 0 **Cylinders** 14087 **Model** SUN72G	**No.**	**Type**	**Extent**	**Start**	**End**	**Use**	**Free**
	0	root	🟥	825	14086	/	86 %
	1	swap	🟥	0	824	swap	
	2	backup	🟥	0	14086		
	3	unassigned					
	4	unassigned					
	5	unassigned					
	6	unassigned					
	7	unassigned					
Location SCSI controller 0 target 1 unit 0 **Cylinders** 14087 **Model** SUN72G	**No.**	**Type**	**Extent**	**Start**	**End**	**Use**	**Free**
	0	unassigned					
	1	unassigned					
	2	backup	🟥	0	14086		98 %
	3	unassigned					
	4	unassigned					
	5	unassigned					
	6	unassigned					
	7	home	🟥	0	14086	/export/home	98 %
Location SCSI controller 2 target 0 unit 0 **Cylinders** 35424 **Model** SUN-StorEdge3310-0325	**No.**	**Type**	**Extent**	**Start**	**End**	**Use**	**Free**
	0	unassigned					
	1	unassigned					
	2	backup	🟥	0	35423		98 %
	3	usr	🟥	0	2600	/notes/log1b	98 %
	4	usr	🟥	2601	5201	/notes/log2a	98 %
	5	usr	🟥	5202	20312	/notes/dom1b	98 %
	6	usr	🟥	20313	35423	/notes/dom2a	98 %
	7	unassigned					

root logged into Webmin 1.240 on dom1b (Sun Solaris 10)

Figure 11-4 Webmin Storage Usage

12

IBM Lotus Domino 7 Directory services

In this chapter we talk about Domino Directory services.

In addition to the Domino Directory itself, Domino provides three directory service features: Directory Catalog, Directory Assistance, and the LDAP service. These features help users find user names, e-mail addresses, and other information in the Domino Directory.

The Directory Catalog consolidates key information about users and groups from one or more Domino Directories into a small, lightweight database. Lotus Notes users can use a local replica of the Directory Catalog—a Mobile Directory Catalog—to quickly address mail to users throughout the organization, even if the organization uses a large directory or multiple directories. In organizations with multiple Domino Directories, a Directory Catalog on a server combines these directories into a single database so that a server can look up names in one database rather than in multiple Domino Directories.

Directory Assistance is a feature that helps manage user name lookups in organizations that use multiple Domino Directories, alone or in combination with third-party LDAP directories. A Directory Assistance database associates each Domino or LDAP directory with specific hierarchical names so that when looking up a name, Domino first searches the directory that contains names in that hierarchy.

© Copyright IBM Corp. 2006. All rights reserved.

Extended Directory Catalog combines advantages of the Domino Directory and the Directory Catalog by aggregating entries from multiple Domino directories into a single directory database.

You can set up a Domino server to run the Lightweight Directory Access Protocol (LDAP) service to enable LDAP clients to search for and modify information in the Domino Directory. The Domino LDAP service is LDAP V3 compliant.

12.1 The Domino Directory

The Domino Directory is the heart of the Lotus Domino architecture. Because of this, it is important to understand what it is and how it works. For a deeper understanding of the directory capabilities of the Domino Directory, see *Getting the Most From Your Domino Directory,* SG24-5986. Among the pertinent features of the Domino Directory are the characteristics in the following list. The Domino Directory is:

- A database that is automatically created when you set up the first Domino server in a domain. The file name is names.nsf.
- Replicated to all Domino servers in a domain, which means that all servers operate with the same Domino Directory.
- Automatically replicated to a new server that is added to a domain.
- The central registration and configuration database in a domain.
- A directory of information about users, servers, groups, and other objects that you might include in the directory yourself—for example, printers.
- A database that administrators use to manage the Domino system. For example, administrators create documents in the Domino Directory to connect servers for replication or mail routing, to register users and servers, to schedule server tasks, and so on.
- Referred to as the Public Address Book (PAB) or Name and Address Book (NAB) in previous releases of Domino and Notes.

> **Important:** The Lotus Domino infrastructure relies heavily on a correctly configured Domino Directory. Changing or deleting documents may have serious consequences on the operation of the Domino environment. Therefore, safeguarding the Domino Directory from unauthorized access is vital.

12.1.1 Documents in the Domino Directory

The Domino Directory contains documents that control directory services, manage server tasks, and define server-to-server communication, among other things. Domino automatically creates some documents when you perform certain administrative tasks. For example, Domino creates a new Person document when you register a user. Table 12-1 on page 394 explains the different types of documents in the Domino Directory.

Table 12-1 Types of Domino Directory documents

Document	Description
Certificate	Describes a certifier ID, including public key information
Configuration Settings	Configures mail, LDAP, and the notes.ini file
Connection	Provides server and domain information for connecting servers for mail routing, replication, and news feeds
Domain	Defines a domain used in mail routing: Foreign, Non-adjacent, Adjacent, Foreign X.400, Foreign SMTP, Foreign cc:Mail, Global
External Domain Network Information	Contains names and addresses of servers in a secondary domain; enables Notes clients to connect to servers in the secondary domain
Group	Defines a list of users and servers for use in mail addressing, ACLs, and server access lists
Holiday	Defines holiday documents that users can download to their calendars
Location	Contains communication and other location-specific settings for use from a client
Mail-In Database	Defines the location and properties of a database that can receive mail
Person	Describes a user (Notes or non-Notes) in the directory
Program	Schedules Domino server tasks and other programs to run at specific times
Resource	Defines a resource that Notes clients can reserve by using the calendaring and scheduling feature
Server	Specifies server configuration settings, including server name, cluster name, security methods, ports, server tasks, Internet protocol, MTA, transactional logging, and so on
User Setup Profile	Defines a standard set of configuration options for Notes clients, including connections, server accounts, replicas, bookmarks, and so on
File Identification	Verifies or associates a specific MIME type with an application
Aggregation Configuration	Specifies configuration settings for extended directory catalog

12.2 The Directory Catalog

A Directory Catalog consolidates entries for users, groups, mail-in databases, and resources from one or more Domino directories into a single, lightweight, quick-access database.

Typically, you create a server Directory Catalog and a Mobile Directory Catalog.

12.2.1 Server Directory Catalog

You create a server Directory Catalog so that Domino servers can search one database to find names in multiple Domino Directories.

Benefits of the server Directory Catalog include:

- When users are connected to the network, directory searches are done against the Directory Catalog instead of the multiple Domino directories that exist on the server. This also reduces network traffic and open database sessions.
- This single Directory Catalog database is significantly smaller than all other Domino directories combined.
- Administrators can choose the attributes included in the Directory Catalog, and can create multiple Directory Catalogs with different content or sort orders.
- The Directory Catalog is fully LDAP-enabled and can be searched using standard LDAP clients.

12.2.2 Mobile Directory Catalog

You can use a User Setup Profile to create a replica of a Directory Catalog, known as a Mobile Directory Catalog, on Notes clients so users can quickly address mail to anyone in your organization, even when the senders are disconnected from the network.

Notes users can also create the Mobile Directory Catalog manually for themselves.

A User Setup Profile defines a standard set of configuration options for Notes clients, including connections, server accounts, replicas, bookmarks, and so on.

Type-ahead addressing searches the Mobile Directory Catalog rather than Domino directories on a server. This reduces network traffic. When type-ahead is activated, every time you type an address manually, Notes displays the first name it finds that matches the letters you type so that you can select a name rather than type the entire name.

12.2.3 Directory Catalog size

A Directory Catalog can combine entries from many Domino directories and still be very small. For example, several Domino directories that together contain more than 350,000 users and total 3 GB in size, when combined in a Directory Catalog, are likely to be only about 50 MB. In general, each entry in the Directory Catalog is slightly more than 100 bytes.

12.2.4 Setting up a Directory Catalog

To set up either a server Directory Catalog or a Mobile Directory Catalog complete these procedures:

1. Prepare a server for the source Directory Catalog.
2. Create and configure the source Directory Catalog.
3. Run the Dircat task.
4. Perform one of the following steps:
   a. If you configured the Directory Catalog for server use, set up the Directory Catalog on servers.
   b. If you configured the Directory Catalog for mobile use, set up the Mobile Directory Catalog on Notes clients.

Prepare a server for the source Directory Catalog

A source Directory Catalog is the replica of a Directory Catalog that the Directory Cataloger—the Dircat task—initially populates and then continues to update when changes occur in the full secondary Domino directories.

Perform the following steps:

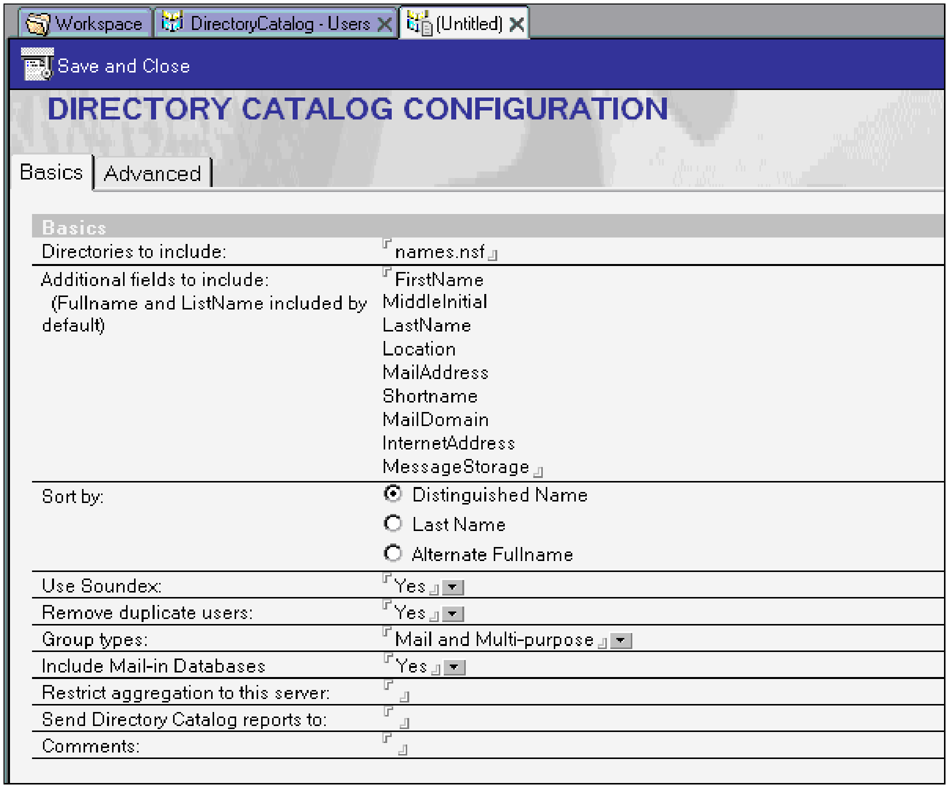
1. Create a replica of each secondary Domino Directory that you want to include in the Directory Catalog. Use unique file names for these replicas.
2. Set up replication between your source Directory Catalog server and the secondary Domino Directory servers.

For more information, see “Preparing a server for a source Directory Catalog” in the “Domino Directories” section of Domino 7 Administration online help.

Create and configure the source Directory Catalog

Perform the following steps from the Domino Administrator client or Notes client to create and configure the source Directory Catalog:

1. Choose **File** → **Database** → **New** and enter the server name that you prepared for the source Directory Catalog.
2. Select the Directory Catalog template (dircat.ntf), and click **OK**.
3. Open your new Directory Catalog.
4. Choose **Create** → **Configuration** from the menu to bring up the Directory Catalog Configuration document.



Basics	
Directories to include:	names.nsf
Additional fields to include: (Fullname and ListName included by default)	FirstName MiddleInitial LastName Location MailAddress Shortname MailDomain InternetAddress MessageStorage
Sort by:	● Distinguished Name ○ Last Name ○ Alternate Fullname
Use Soundex:	Yes
Remove duplicate users:	Yes
Group types:	Mail and Multi-purpose
Include Mail-in Databases	Yes
Restrict aggregation to this server:	
Send Directory Catalog reports to:	
Comments:	

Figure 12-1 Directory Catalog Configuration

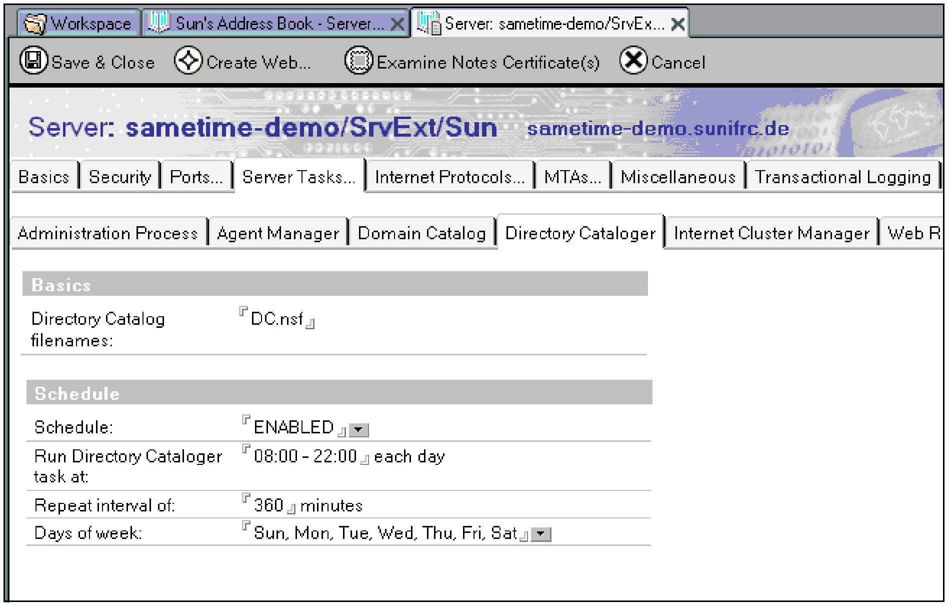
5. On the Basics tab, in the field for Directories to include, list the file names of the Domino Directories to be included in the Directory Catalog (for example, names1.nsf, names2.nsf, names3.nsf, names4.nsf).

6. In the field for Restrict aggregation to this server, enter the name of the Domino server that runs the Directory Catalog Task to ensure that the Dircat task runs on only one server.
7. Close and save the document.

Running the Dircat task on schedule

Run the Dircat task to initially populate the source Directory Catalog and later to keep the entries in the source Directory Catalog synchronized with corresponding entries in the full Domino Directories. Use the following steps to run the Dircat task:

1. Open the Server document in edit mode for the server that stores the source Directory Catalog.
2. Click the **Server Tasks** → **Directory Cataloger** tab (Figure 12-2).



Basics

Directory Catalog filenames: DC.nsf

Schedule

Schedule: ENABLED

Run Directory Cataloger task at: 08:00 - 22:00 each day

Repeat interval of: 360 minutes

Days of week: Sun, Mon, Tue, Wed, Thu, Fri, Sat

Figure 12-2 Directory Cataloger schedule

3. Make entries in the appropriate fields.

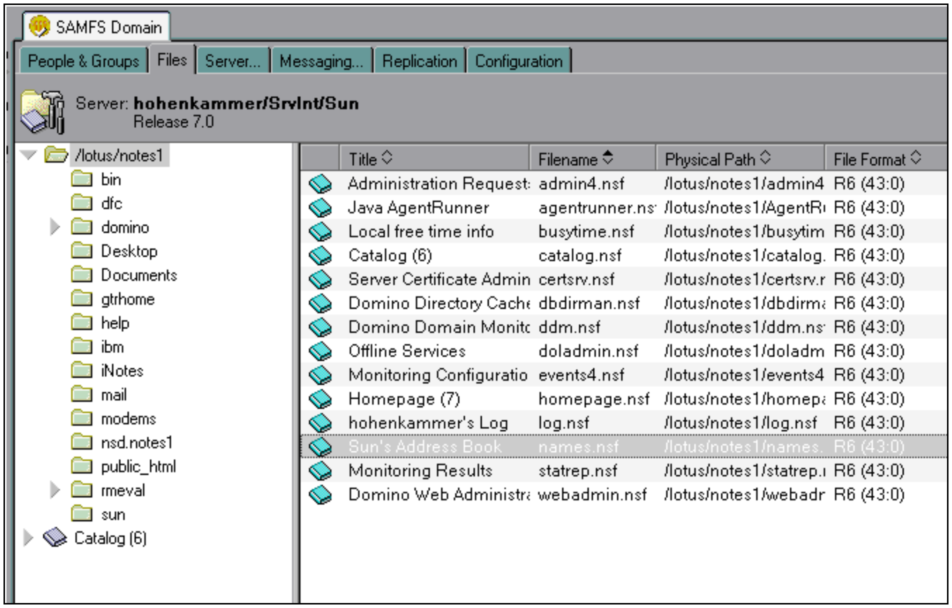
Note: Always run the Dircat task on the server that stores the source Directory Catalogs. If you run it on more than one server, replication conflicts occur. To ensure that the Dircat task runs only on one server, use the configuration field for Restrict aggregation to this server.

Setting up the Directory Catalog on a server

If you have configured and built a source Directory Catalog for server use, set up the Directory Catalog on the servers throughout your organization that will use it. In addition to setting up the Directory Catalog, we also recommend that you set up Directory Assistance.

Use the following steps to set up the Directory Catalog on the servers.

1. Make sure you have already run the Dircat task to build the source Directory Catalog.
2. Create a replica of the source Directory Catalog on other servers in the domain that will use the catalog. Use the same file name as the source Directory Catalog for each replica. Domino automatically creates a full-text index for each replica.
3. From the Domino Administrator, in the server pane on the left, select a server that is in the same domain as the source Directory Catalog. If you do not see the server pane, click the Servers icon.
4. Click the **Files** tab.
5. Select the Domino Directory, and double-click to open it.



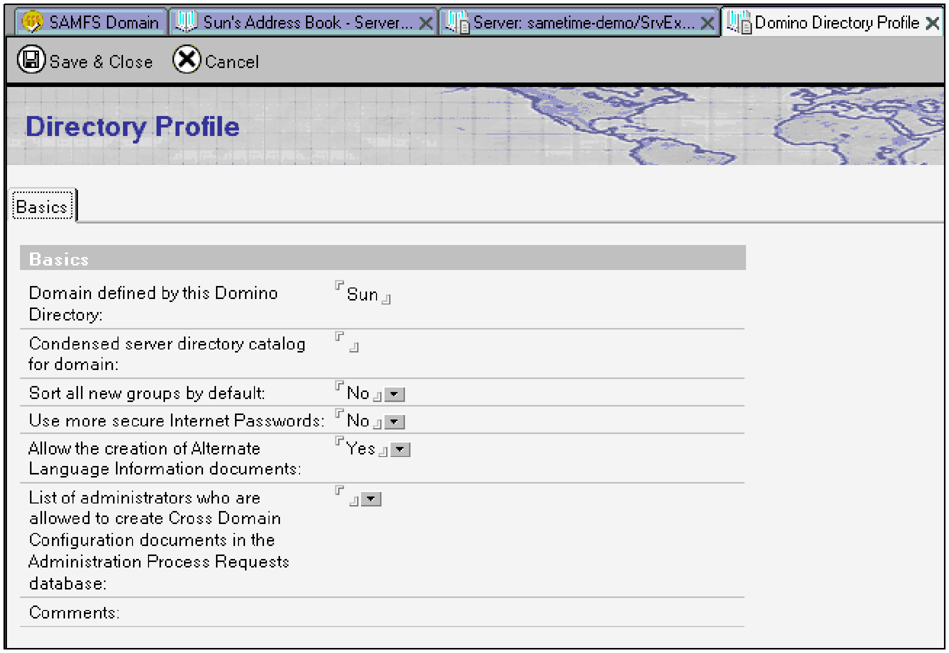
Server: **hohenkammer/SrvInt/Sun**
Release 7.0

Title	Filename	Physical Path	File Format
Administration Request:	admin4.nsf	/lotus/notes1/admin4	R6 (43:0)
Java AgentRunner	agentrunner.ns	/lotus/notes1/AgentR	R6 (43:0)
Local free time info	busytime.nsf	/lotus/notes1/busytim	R6 (43:0)
Catalog (6)	catalog.nsf	/lotus/notes1/catalog.	R6 (43:0)
Server Certificate Admin	certsrv.nsf	/lotus/notes1/certsrv.r	R6 (43:0)
Domino Directory Cache	dbdirman.nsf	/lotus/notes1/dbdirma	R6 (43:0)
Domino Domain Monitc	ddm.nsf	/lotus/notes1/ddm.ns	R6 (43:0)
Offline Services	doladmin.nsf	/lotus/notes1/doladm	R6 (43:0)
Monitoring Configuratio	events4.nsf	/lotus/notes1/events4	R6 (43:0)
Homepage (7)	homepage.nsf	/lotus/notes1/homepa	R6 (43:0)
hohenkammer's Log	log.nsf	/lotus/notes1/log.nsf	R6 (43:0)
Sun's Address Book	names.nsf	/lotus/notes1/names.	R6 (43:0)
Monitoring Results	statrep.nsf	/lotus/notes1/statrep.i	R6 (43:0)
Domino Web Administra	webadmin.nsf	/lotus/notes1/webadr	R6 (43:0)

Figure 12-3 Editing the Directory Profile

6. Choose **Actions** → **Edit Directory Profile**.

7. This opens the window shown in Figure 12-4. In the field for Directory catalog database name for domain, enter the file name you chose for the Directory Catalog, and click **Save and Close**.



Basics

Domain defined by this Domino Directory:	Sun
Condensed server directory catalog for domain:	
Sort all new groups by default:	No
Use more secure Internet Passwords:	No
Allow the creation of Alternate Language Information documents:	Yes
List of administrators who are allowed to create Cross Domain Configuration documents in the Administration Process Requests database:	
Comments:	

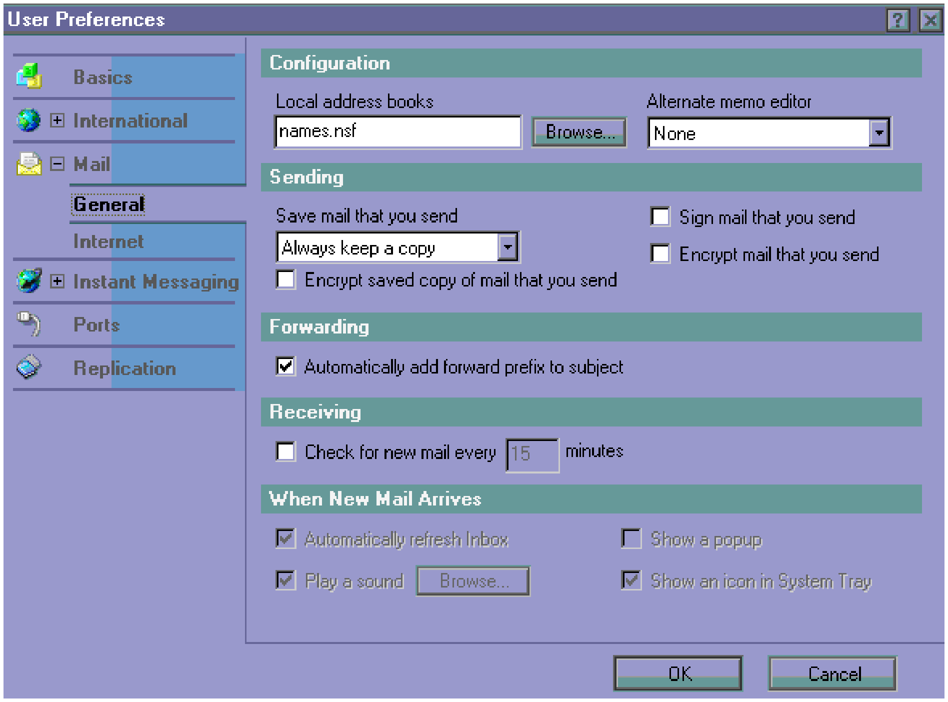
Figure 12-4 The Domino Directory Profile document

8. Make sure there are connection documents that schedule replication between the server storing the source Directory Catalog and the servers on which you create replicas of the Directory Catalog. Scheduling replication ensures that replicas remain synchronized with the source Directory Catalog.
9. Wait for the file name to replicate to a particular server's replica of the Domino Directory, or force the replication.
10. Restart the servers that have replicas of the Directory Catalog so the servers detect the file name. Enter `Restart Server` from the remote server console of the Domino Administrator client. The Domino server stops and restarts after a short delay.

Setting up Mobile Directory Catalogs

If you have configured and built a source Directory Catalog for mobile use, you can create a User Setup Profile to set up the Mobile Directory Catalog on Notes clients. The User Setup Profile performs two tasks:

- It creates a replica stub (an empty replica) of the Mobile Directory Catalog. Replication between the Notes client and the Domino server populates the Mobile Directory Catalog and keeps it updated.
- It appends the Mobile Directory Catalog's file name to the contents of the "Local address books" field in the user preferences for mail (Figure 12-5).



Configuration

Local address books: names.nsf

Alternate memo editor: None

Sending

Save mail that you send: Always keep a copy

□ Encrypt saved copy of mail that you send

□ Sign mail that you send

□ Encrypt mail that you send

Forwarding

☑ Automatically add forward prefix to subject

Receiving

□ Check for new mail every 15 minutes

When New Mail Arrives

☑ Automatically refresh Inbox

□ Show a popup

☑ Play a sound

☑ Show an icon in System Tray

Figure 12-5 Verifying the Local address books setting in User Preferences

Note: If you do not use a User Setup Profile, each Notes user must manually perform these two procedures.

For more information, see "Setting up the mobile directory catalog" in the "Domino Directories" section of the Domino 7 Administration online help.

12.3 Directory Assistance

A new server gets its primary Domino Directory for its domain during the setup process. Each server stores its own primary Domino Directory under the file name names.nsf. Directory Assistance is a feature that enables users and servers to locate information in a directory that is not a server's primary Domino Directory.

You can set up Directory Assistance for:

- Secondary Domino Directories
- LDAP directories, including those on third-party servers

Include secondary Domino Directories in Directory Assistance to:

- Use the Domino Directories to authenticate Web clients that use the Domino Web service
- Allow Notes users to easily address mail to users registered in the directories
- Extend LDAP client searches to secondary Domino Directories

Include LDAP directories in Directory Assistance to:

- Use the directories to authenticate Web clients that use the Domino Web service
- Use one directory to verify Web clients' membership in groups in the directory
- Refer LDAP clients that connect to a Domino LDAP service to the directories
- Allow Notes users to use mail addresses of users in the LDAP directories

12.3.1 Setting up Directory Assistance

To set up Directory Assistance in a Domino domain, complete these steps:

1. Set up a Directory Assistance database.
2. Set up Directory Assistance for each secondary Domino Directory.
3. Set up Directory Assistance for each LDAP directory.

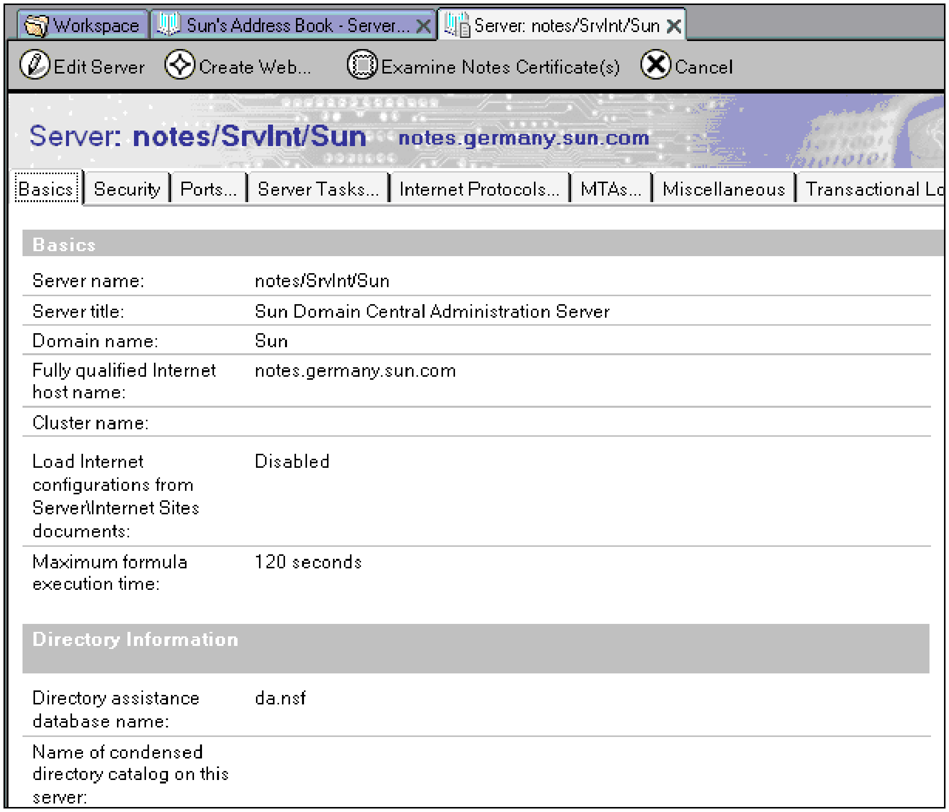
Each step is described in detail in the following sections.

Setting up a Directory Assistance database

1. Create a Directory Assistance database from the Directory Assistance template (da50.ntf).
2. Replicate the database to each server that needs it.

3. Identify the Directory Assistance database on servers that need it. Add the replica file name of the Directory Assistance database to the “Directory Assistance database name” field on the Basics tab in Server documents in the Domino Directory. You can manually enter the file name of the Directory Assistance database on one server document, or use the administration Process to add the file name of the Directory Assistance database to multiple server documents.

   Figure 12-6 shows the Server document after the Directory Assistance database has been added.



Basics

Server name:	notes/SrvInt/Sun
Server title:	Sun Domain Central Administration Server
Domain name:	Sun
Fully qualified Internet host name:	notes.germany.sun.com
Cluster name:	
Load Internet configurations from Server\Internet Sites documents:	Disabled
Maximum formula execution time:	120 seconds

Directory Information

Directory assistance database name:	da.nsf
Name of condensed directory catalog on this server:	

Figure 12-6 Setting up Directory Assistance

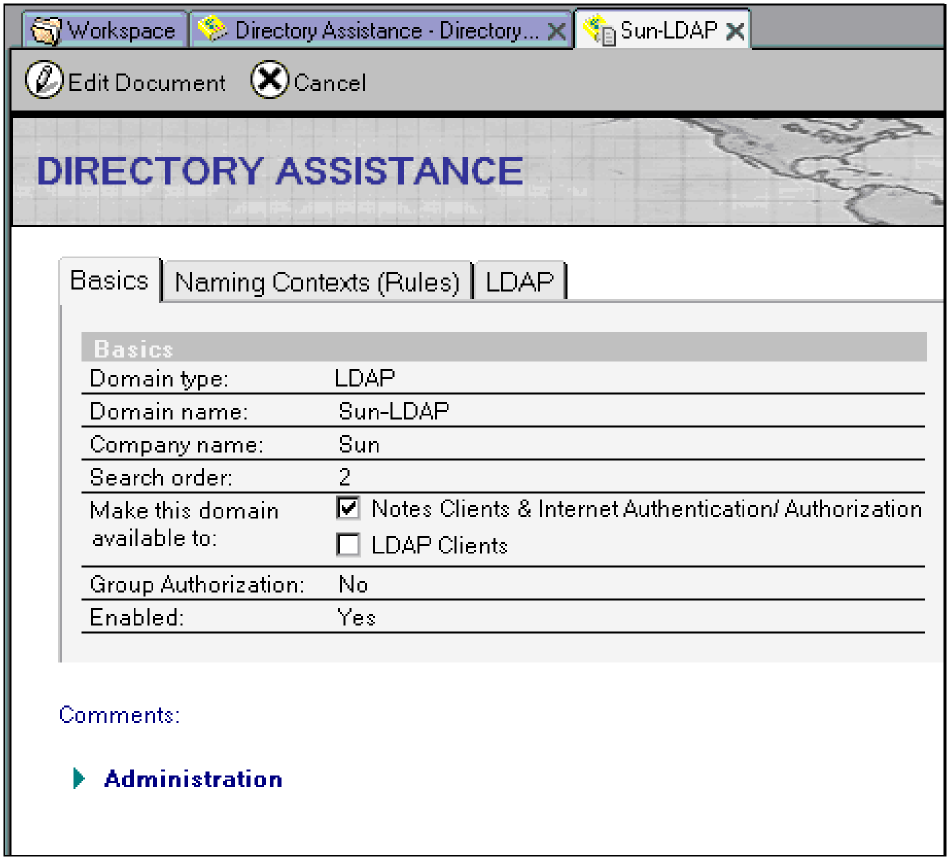
For more information, see the “Domino Directories” section of the Domino 7 Administration online help.

Setting up Directory Assistance for each LDAP directory

To set up Directory Assistance for an LDAP directory, configure a single Directory Assistance document for the directory to do one or more of the following tasks:

- Authenticate Web clients using credentials in an LDAP directory.
- Verify membership in a group that is stored in an LDAP directory.
- Refer LDAP clients to an LDAP directory.
- Use an LDAP directory to verify mail addresses on behalf of Notes users.

Figure 12-7 shows an example of a Directory Assistance document for referring LDAP clients to an LDAP directory.



Basics

Domain type:	LDAP
Domain name:	Sun-LDAP
Company name:	Sun
Search order:	2
Make this domain available to:	☑ Notes Clients & Internet Authentication/ Authorization ☐ LDAP Clients
Group Authorization:	No
Enabled:	Yes

Comments:

Figure 12-7 Configuring Directory Assistance for LDAP

12.4 Extended Directory Catalog

The Extended Directory Catalog feature is new to Domino 7 and, as stated in the release notes, it combines advantages of the Domino Directory and the Directory Catalog by aggregating entries from multiple Domino directories into a single directory database. The Extended Directory Catalog is created by means of the same process as the Standard Directory Catalog, but instead of using the DIRCAT50.NTF, the Extended Directory Catalog uses the PUBNAMES.NTF (Domino Directory) template to create the target database and therefore it retains the full set of indexed views and other features of the Domino Directory. This enables the enterprise to maintain a single consolidated server-based directory structure that responds rapidly to a variety of search patterns and can contribute to enhanced mail router performance.

This hybrid design based on the Domino Directory provides more flexibility and faster responses locating entries because a server can virtually always use views to quickly look up names. In contrast, to look up names in a standard Server Directory Catalog created from the DIRCAT50.NTF template, a server must do full-text searches—a slower lookup process than view lookups—when the name formats do not correspond to the “Sort by” configuration setting. Because the Extended Directory Catalog contains the views that are in a standard Domino Directory and combines multiple directories into one database, it can be quite large. Therefore, do not replicate the database to Notes clients and use as few replicas on servers as feasible.

Servers use Directory Assistance to determine the locations of an Extended Directory Catalog. One Directory Assistance document, and therefore one set of naming rules, applies to all of the directories that are aggregated into an Extended Directory Catalog.

12.4.1 How to set up Extended Directory Catalog

Follow these steps to set up an Extended Directory Catalog:

1. If you currently use the standard Server Directory Catalog, disable it by removing its file name from the “Directory Catalog database name on this server” field in the Basics tab of the Server documents. If you have specified the file name there rather than in Server documents, remove its file name from the “Directory catalog database name for domain” field in the Public Directory Profile document.
2. On the server that runs the Dircat task, select **File** → **Database** → **New** to create the Extended Directory Catalog from the PUBNAMES.NTF template. Give the database a unique file name and title; do *not* give it the file name NAMES.NSF. In our lab we chose the name extended.nsf.

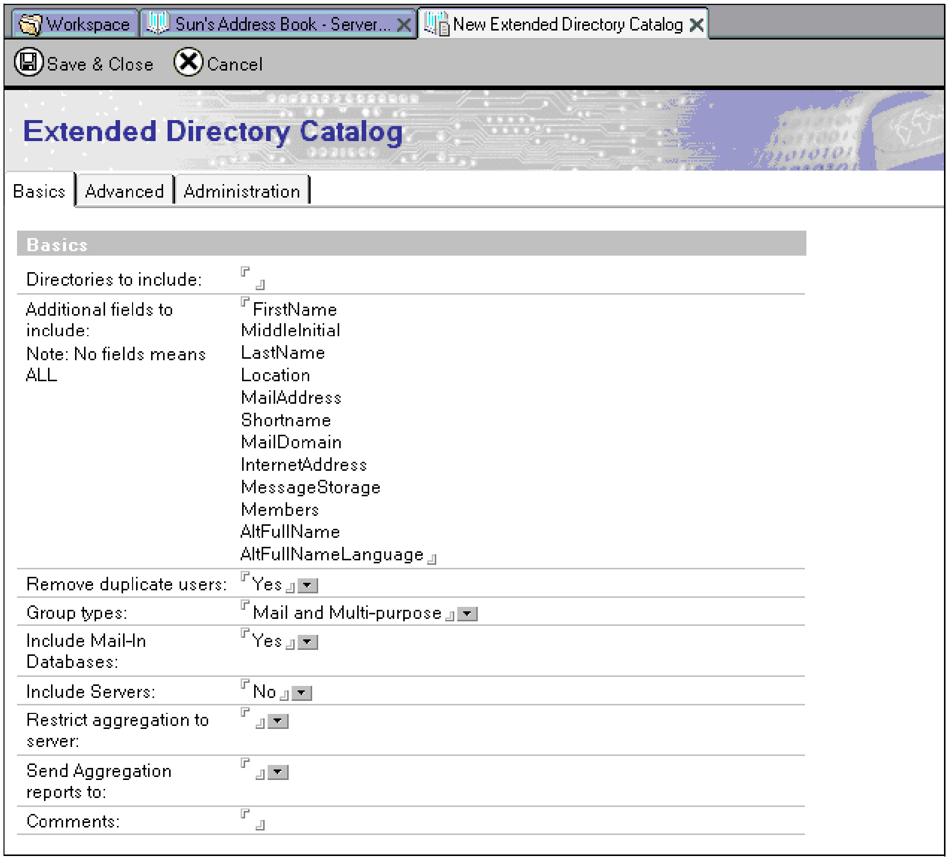
Note: It is not necessary to create a full text index.

3. In the ACL of the database you created, set the Default access to `Reader`.
4. Open the database you created, and choose **Create → Aggregate Configuration**. Fill out the Configuration document, and click **Save and Close**.

   This document has most of the same configuration choices as the Configuration document that is used in the standard Server Directory Catalog. However, if you want to include Server documents in the Extended Directory Catalog, select the Include Servers option. Also, there is no “Sort by” option—the Extended Directory Catalog retains all indexed views in the Directory, so this option is unnecessary. The Server - Aggregate Directory Configuration view shows the saved configuration document. Keep these points in mind when you configure an Extended Directory Catalog:

   – Do not aggregate the primary Domino Directory into an Extended Directory Catalog.

   – If the “Additional fields to include” configuration field is blank, the Dircat task aggregates all fields from the source directory documents. To use the Extended Directory Catalog for Web user authentication, you must use the “Additional fields to include” configuration field to aggregate additional fields. To use names and passwords to authenticate Web users, add the HTTP password field to the configuration. To use X.509 client certificates to authenticate Web users, add the UserCertificate field. Figure 12-8 on page 407 shows an example configuration we used in our lab.


Workspace
Sun's Address Book - Server...
New Extended Directory Catalog
Save & Close
Cancel
Extended Directory Catalog
Basics
Advanced
Administration

Basics

Directories to include:	
Additional fields to include: Note: No fields means ALL	FirstName MiddleInitial LastName Location MailAddress Shortname MailDomain InternetAddress MessageStorage Members AltFullName AltFullNameLanguage
Remove duplicate users:	Yes
Group types:	Mail and Multi-purpose
Include Mail-In Databases:	Yes
Include Servers:	No
Restrict aggregation to server:	
Send Aggregation reports to:	
Comments:	

Figure 12-8 Aggregated Address Configuration - basic settings

5. To build the Extended Directory Catalog, run the Dircat task against the database you created. In our example, this was `load dircat extended.nsf`. Given the larger size of the Extended Directory Catalog, expect the Dircat task to take longer to run against an Extended Directory Catalog than it does on a Standard Directory Catalog. You can improve Dircat performance by selecting No for the “Remove duplicate users” option. If you select No, then entries with identical names are all included in the Directory Catalog and users choose between the duplicates. Selecting No avoids the building of a particular view used to ensure the removal of entries with duplicate names.
6. If you use Directory Assistance, open the Directory Assistance database and remove the Directory Assistance documents for all directories that you included in the Extended Directory Catalog. If you do not currently use a Directory Assistance database, create one from the DA50.NTF template,

replicate it to servers, and add its file name to the Directory Assistance database name field in the Basics tab of Server documents.

7. In the Directory Assistance database, create a Directory Assistance document for the Extended Directory Catalog. Choose **Add Directory Assistance**, fill out the configuration fields, then click **Save and Close**. Keep the following points in mind:
   - For Domain type, select Notes, not LDAP. For Domain name, make up a unique domain name.
   - Do not specify the name of the primary domain. If you want to trust the directory catalog for Web user authentication, include a rule that is Trusted for Credentials.
   - In the Replicas tab, specify one or more replicas of the Extended Directory Catalog. In a large domain, it is important that there be more than one replica for performance and failover reasons.
8. Replicate the updated Directory Assistance database to the servers in the domain that will use it. Then restart the servers to load the new Directory Assistance information or wait five minutes for the servers to restart themselves.

12.5 Domino LDAP service

The Lightweight Directory Access Protocol (LDAP) is an open industry standard. LDAP defines a standard method for accessing and updating information in a directory. LDAP is gaining wide acceptance as the directory access method of the Internet and therefore is also becoming strategic within corporate intranets.

12.5.1 What is Domino LDAP service?

Domino 7 includes a wide range of LDAP features, including support for LDAP V3. For more details, see the IBM product pages regarding LDAP and Lotus Domino.

Lotus Domino 7 includes two types of support for LDAP:

1. You enable the LDAP Service on a Domino server by starting the LDAP task on it. Users can execute directory operations, such as searching or modifying Domino Directory entries using an LDAP client.
2. Domino supports several LDAP features that you can use with a third-party LDAP directory server. The LDAP Service is not required to use these features.

Lotus Domino 7 LDAP service features

Domino 7 supports the following service features of LDAP V2 and V3:

- Different access protections, including anonymous access to specified fields, user and password authentication, SSL and X.509 certificates, and others.
- Support of third-party LDAP clients

  LDAP support in Domino makes directory information highly accessible. It enables any LDAP client, whether POP3, IMAP, a browser, or a common mail client, to use the Domino Directory to look up names and addresses.
- Add, delete, and modify directory entries

  By default, LDAP write access to the Domino Directory is not allowed. You can enable LDAP write access to the Domino Directory by editing the Directory settings.
- Schema

  The schema for an LDAP directory defines how information is stored as entries in a directory. The smallest piece of information in a schema is an attribute. Attributes correlate to Domino Directory fields. Groups of related attributes are known as object classes. Object classes correlate to Domino Directory forms and subforms. The default Domino LDAP service schema includes many standard LDAP attributes and object classes, as well as some that are specific to Domino.
- Searches based on alternate languages

  You can create Alternate Language Information documents that allow LDAP users to search Person entries and retrieve the results using their native languages.

For more information about LDAP features in Domino, see “The Domino LDAP service” in the “Domino Directories” section of the Domino 7 Administration online help.

For more information about LDAP, see *Understanding LDAP*, SG24-4986.

12.5.2 Setting up Domino LDAP service

The Lotus Domino 7 LDAP server task can be installed automatically when you install Lotus Domino 7 or it can added at any time afterward. There is no need to install additional software to enable Lotus Domino to function as an LDAP server. There is also very little extra configuration needed.

To turn Lotus Domino into an LDAP server, set up the Domino server and set up security for the server, then use the following steps to implement the Domino LDAP service.

1. Create a full-text index for the replica of the Domino Directory on the server that runs the LDAP service.
2. Start the Domino server and the LDAP task.
3. If your organization uses more than one Global Domain document, you must specify the one that the LDAP service uses to return users' Internet addresses to LDAP clients. Open the Global Domain document. In the "Use as default Global Domain" field, choose **Yes**. A Global Domain document is used to specify the settings for all used LDAP directories.
4. Set up LDAP clients to connect to the LDAP service. To use the Domino LDAP service, each LDAP user, whether Notes or non-Notes, must set up the client to connect to the LDAP service. For more information, see "Setting up users to use the LDAP service" in the "Domino Directories" section of the Domino 7 Administration online help.
5. (Optional) Customize the default LDAP service configuration. In most cases, the LDAP service functions correctly when using the default settings.
6. To check whether you set up the LDAP service correctly, use an LDAP client or the **ldapsearch** utility to issue a query to the LDAP service. Use of the **ldapsearch** utility is described later in this chapter.
7. To allow clients to connect to the LDAP service over the Internet, connect the server that runs the LDAP service to an Internet service provider (ISP) and register the server's DNS name and IP address with the ISP.

Note: TCP/IP port 389 and TCP/IP port 636 are the industry-standard ports for LDAP connections over TCP/IP and SSL, respectively. You should use the default port numbers in most cases. Firewalls must pass traffic on these ports.

12.5.3 Starting and stopping the LDAP server task

There are three options for starting the LDAP server:

- If you selected LDAP when you installed Lotus Domino, the LDAP server task starts automatically.
- If you did not select LDAP when you installed Lotus Domino, you can start it manually using the following command at the server console:

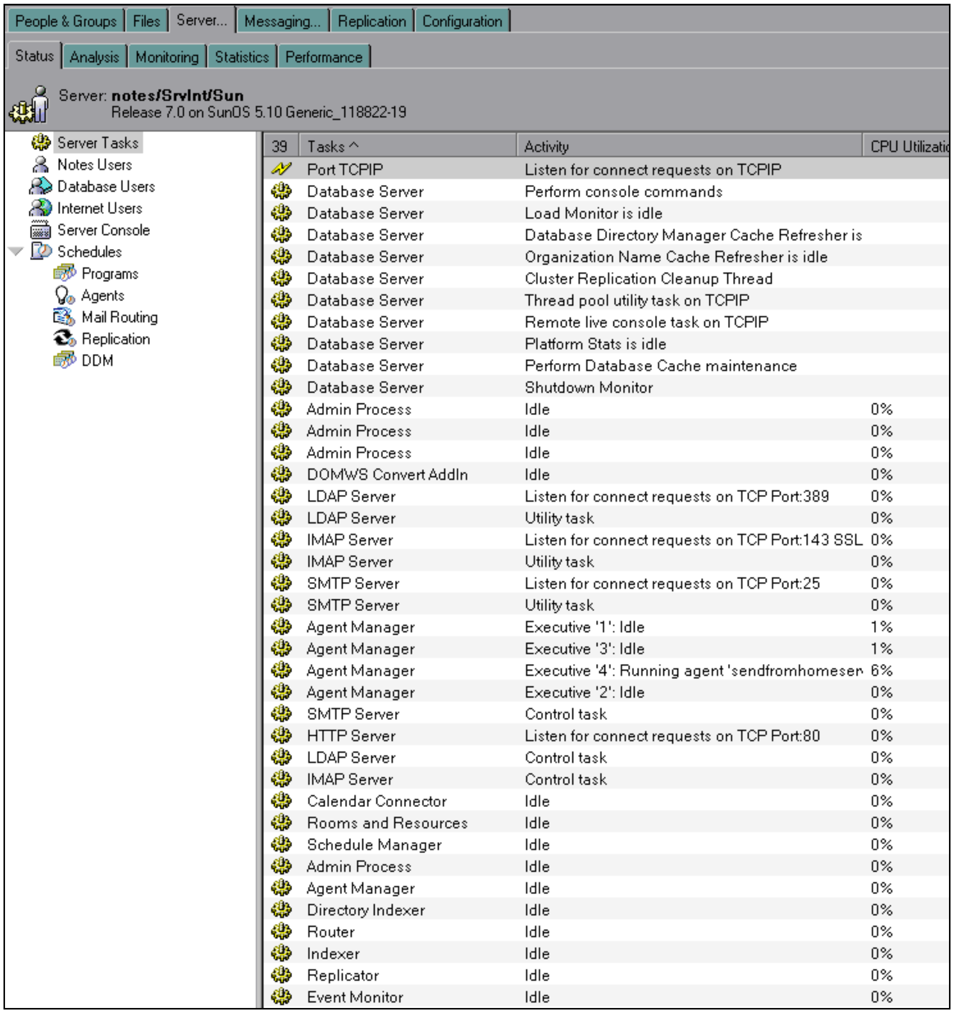
```
load ldap
```

- To start the LDAP server task automatically at Lotus Domino Server startup, add LDAP to the ServerTasks entry in notes.ini. For example:

```
ServerTasks=LDAP, REPLICA, ROUTER, UPDATE, ...
```

You can verify that the LDAP server is running by using the **show tasks** command at the server console.

Figure 12-9 shows the result of the **show tasks** command.



Server: **notes/SrvInt/Sun**
Release 7.0 on SunOS 5.10 Generic_118822-19

39	Tasks ^	Activity	CPU Utilizati
	Port TCPIP	Listen for connect requests on TCPIP	
	Database Server	Perform console commands	
	Database Server	Load Monitor is idle	
	Database Server	Database Directory Manager Cache Refresher is	
	Database Server	Organization Name Cache Refresher is idle	
	Database Server	Cluster Replication Cleanup Thread	
	Database Server	Thread pool utility task on TCPIP	
	Database Server	Remote live console task on TCPIP	
	Database Server	Platform Stats is idle	
	Database Server	Perform Database Cache maintenance	
	Database Server	Shutdown Monitor	
	Admin Process	Idle	0%
	Admin Process	Idle	0%
	Admin Process	Idle	0%
	DOMWS Convert AddIn	Idle	0%
	LDAP Server	Listen for connect requests on TCP Port:389	0%
	LDAP Server	Utility task	0%
	IMAP Server	Listen for connect requests on TCP Port:143 SSL	0%
	IMAP Server	Utility task	0%
	SMTP Server	Listen for connect requests on TCP Port:25	0%
	SMTP Server	Utility task	0%
	Agent Manager	Executive '1': Idle	1%
	Agent Manager	Executive '3': Idle	1%
	Agent Manager	Executive '4': Running agent 'sendfromhomeser	6%
	Agent Manager	Executive '2': Idle	0%
	SMTP Server	Control task	0%
	HTTP Server	Listen for connect requests on TCP Port:80	0%
	LDAP Server	Control task	0%
	IMAP Server	Control task	0%
	Calendar Connector	Idle	0%
	Rooms and Resources	Idle	0%
	Schedule Manager	Idle	0%
	Admin Process	Idle	0%
	Agent Manager	Idle	0%
	Directory Indexer	Idle	0%
	Router	Idle	0%
	Indexer	Idle	0%
	Replicator	Idle	0%
	Event Monitor	Idle	0%

Figure 12-9 Verifying that the LDAP server is running from the server console

To shut down the LDAP server, you have several options:

- Shut it down manually by executing the command **`tell ldap quit`** at the server console.
- Shut down the entire Domino server.
- Deactivate the automatic startup by removing LDAP from the ServerTasks entry in notes.ini and then restarting the Lotus Domino server.

The **`show tasks`** console command should no longer show LDAP entries.

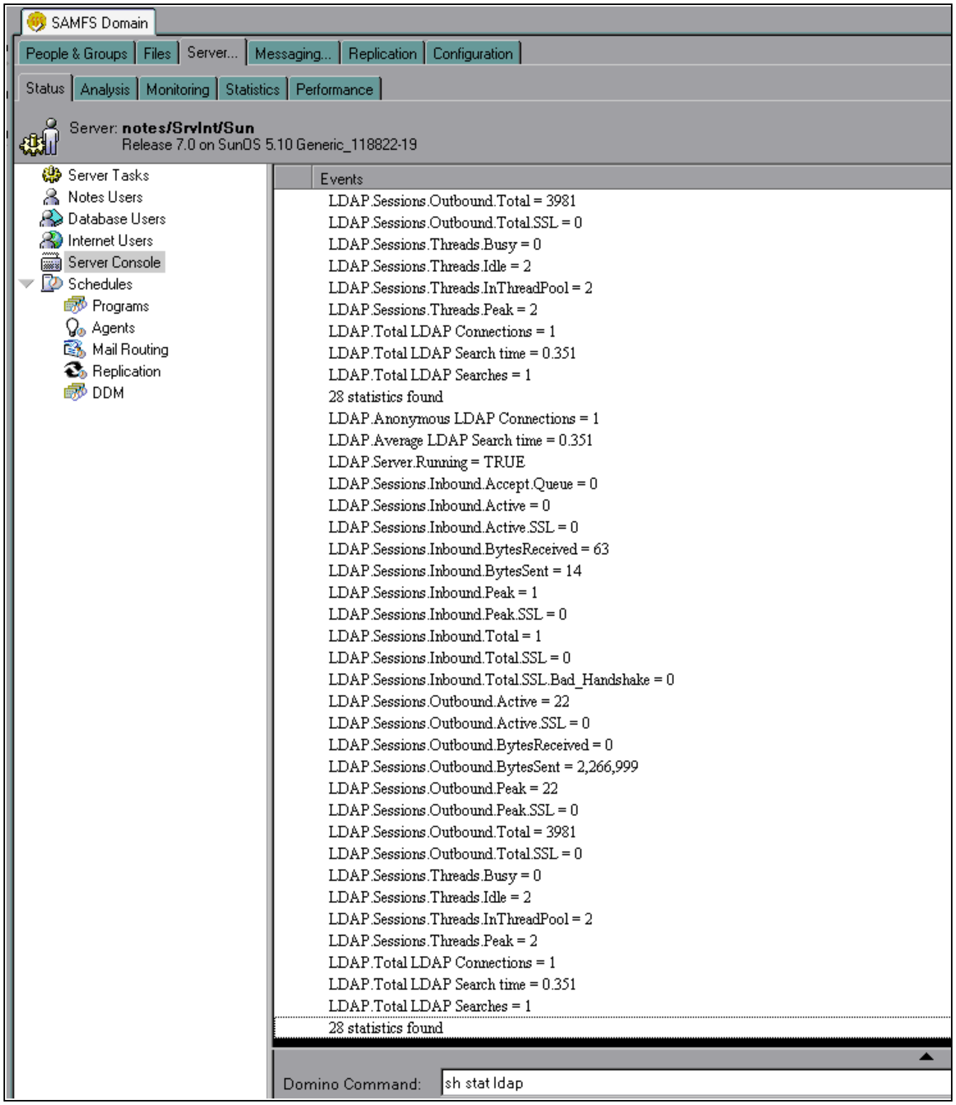
12.5.4 Showing LDAP statistics

There are several ways to display LDAP statistics:

- On a remote console
- On a browser, with the Web Administrator
- On the Server → Status tab

To view LDAP statistics on a remote console, perform the following steps:

1. Open the Domino Administrator client.
2. Select **Server** from the server list.
3. Click the **Status** tab under the Server tab.
4. Click **Console** to open the remote console.
5. Enter the command **`sh stat ldap`** in the command line and press Enter. This displays the window shown in Figure 12-10 on page 413.



Server: **notes/SrvInt/Sun**
Release 7.0 on SunOS 5.10 Generic_118822-19

```
LDAP.Sessions.Outbound.Total = 3981
LDAP.Sessions.Outbound.Total.SSL = 0
LDAP.Sessions.Threads.Busy = 0
LDAP.Sessions.Threads.Idle = 2
LDAP.Sessions.Threads.InThreadPool = 2
LDAP.Sessions.Threads.Peak = 2
LDAP.Total LDAP Connections = 1
LDAP.Total LDAP Search time = 0.351
LDAP.Total LDAP Searches = 1
28 statistics found
LDAP.Anonymous LDAP Connections = 1
LDAP.Average LDAP Search time = 0.351
LDAP.Server.Running = TRUE
LDAP.Sessions.Inbound.Accept.Queue = 0
LDAP.Sessions.Inbound.Active = 0
LDAP.Sessions.Inbound.Active.SSL = 0
LDAP.Sessions.Inbound.BytesReceived = 63
LDAP.Sessions.Inbound.BytesSent = 14
LDAP.Sessions.Inbound.Peak = 1
LDAP.Sessions.Inbound.Peak.SSL = 0
LDAP.Sessions.Inbound.Total = 1
LDAP.Sessions.Inbound.Total.SSL = 0
LDAP.Sessions.Inbound.Total.SSL.Bad_Handshake = 0
LDAP.Sessions.Outbound.Active = 22
LDAP.Sessions.Outbound.Active.SSL = 0
LDAP.Sessions.Outbound.BytesReceived = 0
LDAP.Sessions.Outbound.BytesSent = 2,266,999
LDAP.Sessions.Outbound.Peak = 22
LDAP.Sessions.Outbound.Peak.SSL = 0
LDAP.Sessions.Outbound.Total = 3981
LDAP.Sessions.Outbound.Total.SSL = 0
LDAP.Sessions.Threads.Busy = 0
LDAP.Sessions.Threads.Idle = 2
LDAP.Sessions.Threads.InThreadPool = 2
LDAP.Sessions.Threads.Peak = 2
LDAP.Total LDAP Connections = 1
LDAP.Total LDAP Search time = 0.351
LDAP.Total LDAP Searches = 1
28 statistics found
```

Domino Command: sh stat ldap

Figure 12-10 Viewing LDAP statistics from the server console

To view LDAP statistics with the Web Administrator, use the following steps:

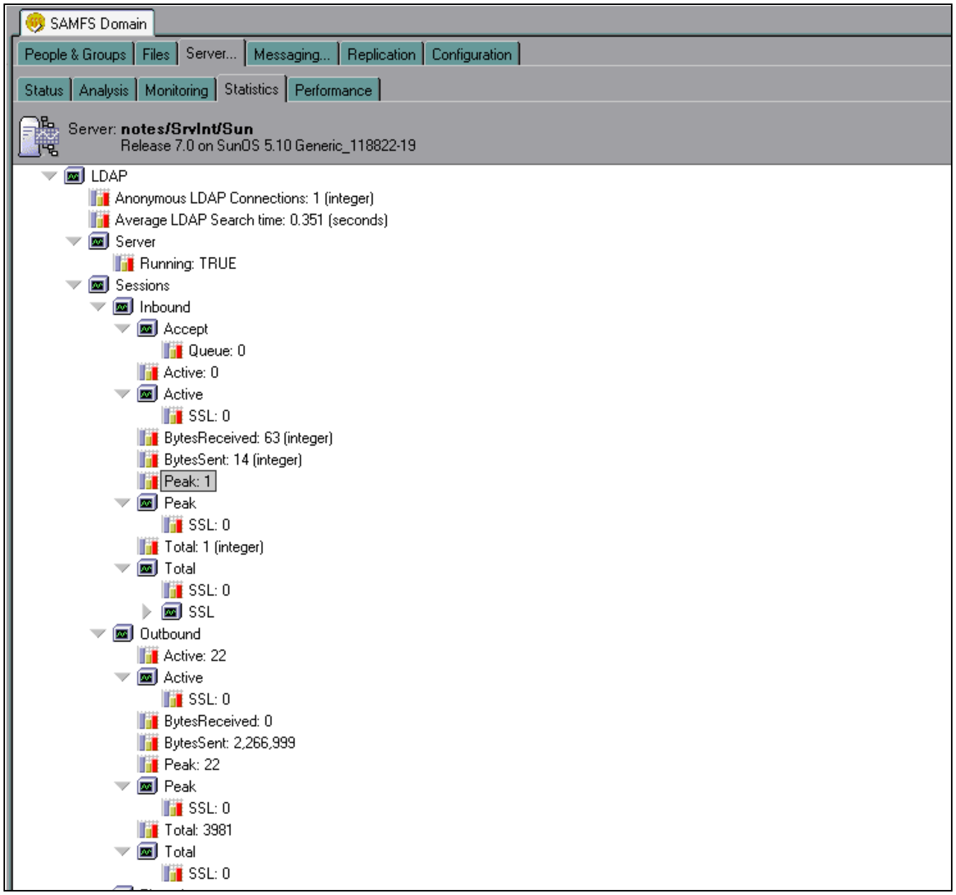
1. Start the Web browser.
2. Connect to the Domino server's Web Administrator:

   `http://dominoserver/webadmin.nsf`

3. Use the console command system to **`sh stat ldap`**

To view LDAP statistics on the Server → Status tab, use the following steps:

1. Open the Domino Administrator client.
2. Select **Server** from the server list.
3. Click the **Status** tab under the Server tab.
4. Expand **LDAP** to view LDAP statistics. The window in Figure 12-11 appears.



Server: **notes/SrvInt/Sun**
Release 7.0 on SunOS 5.10 Generic_118822-19

- LDAP
  - Anonymous LDAP Connections: 1 (integer)
  - Average LDAP Search time: 0.351 (seconds)
  - Server
    - Running: TRUE
  - Sessions
    - Inbound
      - Accept
        - Queue: 0
      - Active: 0
      - Active
        - SSL: 0
      - BytesReceived: 63 (integer)
      - BytesSent: 14 (integer)
      - Peak: 1
      - Peak
        - SSL: 0
      - Total: 1 (integer)
      - Total
        - SSL: 0
        - SSL
    - Outbound
      - Active: 22
      - Active
        - SSL: 0
      - BytesReceived: 0
      - BytesSent: 2,266,999
      - Peak: 22
      - Peak
        - SSL: 0
      - Total: 3981
      - Total
        - SSL: 0

Figure 12-11 Viewing LDAP statistics, Administration client

12.5.5 Using the ldapsearch utility to search LDAP directories

Domino provides a command-line search utility, **ldapsearch**, that enables you to use LDAP to search entries in the Domino Directory on a server that runs the LDAP service, or to search entries in a third-party LDAP directory. Note that you do not have to enter the command on a machine that runs the Domino LDAP service. The ldapsearch utility connects to the server that you specify and returns results according to the search criteria. It is available on Domino server and Notes client platforms.

Notes:

- To use this tool, the notes.ini file must be included in your path statement.
- Solaris also has an **ldapsearch** command. Depending on the order of your path, you may be using the Solaris version, /bin/ldapsearch instead of the Domino command at /*Domino Program Dir*/bin/ldapsearch.

Performing a search with the ldapsearch utility

Enter the following command:

```
ldapsearch parameters searchfilter attributes
```

In this sequence:

- *parameters* are case-sensitive command-line parameters.
  For more information, see “Using parameters with ldapsearch” in the “Domino Directories” section of Domino 7 Administration online help.
- *searchfilter* is a required search filter that causes **ldapsearch** to find only entries that meet specific attribute criteria.
- *attributes* are options that limit the values that ldapsearch returns. Separate each attribute with a space. If you do not specify one or more attributes, **ldapsearch** returns all attributes.

Example 12-1 shows the result of the **ldapsearch** command:

```
ldapsearch -h saturn.lotus.com objectClass=*
```

The search connects to the LDAP service on host saturn.lotus.com and returns all attributes and values.

Example 12-1 LDAP search results

```
$ cd /notes/dom1b
$ ldapsearch -h dom1b “objectClass=*
CN=ACME-admins
cn=ACME-admins
mail=ACME-admins@cam.itso.ibm.com
```

```
objectclass=dominoGroup
objectclass=groupOfNames
objectclass=top
member=CN=Administrator,O=ACME

CN=ACME-admins-db
cn=ACME-admins-db
mail=ACME-admins-db@cam.itso.ibm.com
objectclass=dominoGroup
objectclass=groupOfNames
objectclass=top

CN=ACME-admins-full-access
cn=ACME-admins-full-access
mail=ACME-admins-full-access@cam.itso.ibm.com
objectclass=dominoGroup
objectclass=groupOfNames
objectclass=top
member=CN=Administrator,O=ACME
member=CN=Carolynn McCarthy,O=ACME
member=CN=Craig Swain,O=ACME
member=CN=John Norton,O=ACME
member=CN=Rodrigo Castello Branco,O=ACME
member=CN=Uwe Wiest,O=ACME

CN=Administration Requests
cn=Administration Requests
mail=Administration_Requests%ACME@cam.itso.ibm.com
maildomain=ACME
objectclass=dominoServerMailInDatabase
objectclass=top
--More--(3%)
```

12.5.6 Exporting Domino Directory information

You can export Domino Directory information in a format that can be understood by other LDAP-compliant directories by extracting the Domino Directory information into a text file. The extraction leaves the data in Lightweight Data Interchange Format (LDIF), the RFC-compliant format used by LDAP servers and clients. LDIF defines a universally understood format used by LDAP servers to build their respective schema.

Use the following **ldapsearch** command to extract the Domino Directory information to a text file. In a more enhanced environment, this would be:

```
ldapsearch -h LDAPservername -b dc=sun “(&(givenname=Uwe*) (sn=Wiest*)“
>filename.txt
```

For example:

```
ldapsearch -h LDAPservername -b dc=sun “(&(givenname=Uwe*) (sn=Wiest*)“
>dir.txt

more dir.txt

cn=Uwe Wiest (92756)/ou=people/dc=sun
```

The text file that is created can then be imported to another LDAP server.

12.6 Summary

In this chapter we have given an overview of Domino Directory services.

We described the primary Domino Directory (names.nsf) with its documents, how to set up a directory catalog, directory assistance, extended directory catalog, and the Domino LDAP service. Finally, we explained how to use the **ldapsearch** utility and to export Domino Directory information.

13

Backup strategy for IBM Lotus Domino 7 on Solaris

Backup strategies for Domino have been in place since early implementations. In this chapter we discuss the different mechanisms for backing up Domino in a Solaris environment.

© Copyright IBM Corp. 2006. All rights reserved.

13.1 Backup strategy

There are two basic methods to back up Domino:

- Offline backup

  Shut down the server, back up your files, then restart the server. This is the most reliable and inexpensive type of backup procedure. This accomplishes all the necessary file integrity results with very little cost. The downside to this is that it cannot be done on critical systems that require 24/7 operation.

  - One way to have Domino still in production during offline backup is to have a Domino cluster where one server is shut down during the backup procedure. This can be done during non-peak hours of operation. Be aware that you lose all cluster benefits for this server, such as failover or load-balancing, during the backup time. After the server resumes its place in the cluster, a replication has to be set to synchronize the data that was created on the other cluster members during the backup period.
  - A second method to accomplish this is to run a scheduled replication to another Domino partition. This could be in addition to the Domino cluster. You may consider replicating the data off-site, which would provide a level of Disaster Recovery. Like the cluster method, you then bring down Domino on this backup partition and back up the databases. The advantages to this method are that you maintain your high-availability cluster and have more time to back up the third partition. If you restart Domino on this backup partition, you will have an online copy of the backup that the administrators can use to recover data without reloading backup tapes.
  - Third, depending on your storage technology, you may be able to quickly take a snapshot of your Domino data while Domino is down and quickly get your Domino server back in production. The snapshot can then be backed up.

- Online backup

  Online backup provides a way to back up your data and still have your system in production. This option becomes more and more important with the requirement of 24/7 operation becoming more common. There are different options to perform an online backup. We recommend that you utilize the features provided by the backup/recovery APIs in Domino 7. You can then use third-party tools that take advantage of these APIs.

13.2 Offline backup

In this section we discuss common offline backup tools and procedures.

13.2.1 Using Solaris backup utilities for offline backup

Several utilities that are provided with your Solaris OS can be used to perform backups:

- CPIO: This utility is a UNIX system backup procedure that has been in existence since the early implementations of the UNIX operating system. Files can be backed up and restored from disk or tape.
- TAR: This utility is a UNIX system file archive procedure that has gained popularity on all UNIX platforms.
- UFSDUMP/ UFSRESTORE: This utility is used specifically for backing up file systems on the Solaris OS. There are many options that can be used with this procedure, and it can be a quick way to back up your Domino servers without purchasing any additional software.
- DD: This is one of the original "dump" utilities that is used on a UNIX system to write files to disk and tape. It is not very user friendly, but it can be useful in experienced hands.

Consult your Solaris product manuals or online documentation for detailed procedures for backing up files and directories using these utilities.

13.2.2 Using third-party tools for offline backup

You can use third-party backup tools for offline backup. Many of these tools also support optional features that support the Lotus backup APIs but you can choose not to purchase or use these optional features and use the tool for offline Domino backup. Many third-party tools work with the concept of a backup server where the backup devices are and backup client software that is loaded onto the system that is being backed up. This adds the benefit of multiple servers sharing the same backup server, and is referred to as using a *backup network* design.

13.2.3 Backup device options

Another consideration when backing up files on a Solaris system is which of the available backup devices to use when you back up on the same machine and are not using a backup network.

Almost all devices configured on a Solaris system are in the /dev directory and are linked to special files in the /devices directory. When you install the Solaris system, the special files are created based on the devices that are attached to your system. If you add additional devices, such as a tape drive or tape library, you will need to configure the drive in the Solaris OS before you can use it with any software that you have installed.

The standard backup devices are disk, tape, and floppy. Although use of floppy disks is rare these days, we include it because this is still a supported device.

An example of the type of name associated with each of the devices follows:

- Floppy - /dev/rdiskette
- Tape - /dev/rmt/0
- Disk - /dev/dsk/c0t0d0s0

When you attach a tape drive to your Solaris system, you should use the following steps to ensure that the device is recognized by the Solaris OS.

1. If the tape drive is a SCSI device, set the SCSI ID before connecting the device.
2. Connect the tape device with the appropriate cable that came with your tape drive, or consult the manufacturer for the correct cable.
3. Reboot your system with the -r option to finish reconfiguration of the devices.

   The command is **`reboot – -r`**
4. Change to the /dev/rmt directory and type the following command: **`ls -la`**

   This command produces a list of device names that were created for your tape drive. The characters following the drive number have special meaning to the device and should be used as instructed by the software or the Solaris utility you are using.

For further instructions on setting up the device to back up your Domino data using UNIX utilities, consult the Solaris product manuals or online documentation. For instructions for backup with a separately purchased third-party product, consult the documentation provided by the manufacturer.

13.3 Backup management

In this section we discuss management issues related to backing up files, such as why you still need backups even if you are replicating your databases, how to establish backup cycles, and how to implement incremental backups with the transaction logging feature enabled in Domino 7.

13.3.1 Backup versus replication

Your Domino implementation may include clustering of your Domino servers so you can replicate your databases to another system or disk. Or you may use scheduled replication to keep additional copies of databases at certain points in time. What we want to point out in this section is that replication does not replace the need to have reliable backups of your databases.

It is true that in the event of disk failure or disaster recovery a replica of a database is a quick way to recover the information that was lost, but there are other times when a database may have to be recovered from a previous day or week. Here are some cases when you would need a backup of data:

- Information that was in a database was changed and this was discovered at a later date. Replication has already overwritten the changed information on the other Domino servers or cluster partners.
- A database has become corrupted on the server; this was not discovered prior to corruption replicating to the cluster or other replicas.
- An Adminp request was issued and approved to perform deletion of databases through your servers. This was discovered but could not be stopped prior to user databases being deleted.
- A user has inadvertently deleted all mail in their database and did not inform the administrator in time to stop replication.

These are just a few examples of why a reliable backup to your databases is an important part of your Domino implementation planning.

13.3.2 Backup cycles

When planning for your backup, it is a good idea to develop a backup cycle that will work for your organization. You should consider the following issues when determining a good backup cycle for your office:

- Budget allotment for tapes and life cycle of tape usage
- Company policy for mail retention and archiving
- Amount of data to be backed up per server
- Time available for backup

13.3.3 Incremental backups versus full backups

The Domino 7 transaction logging feature enables incremental backups of the transaction logs. You need to have at least one full backup of your databases. For recovery reasons it is better to do full backups on a frequent basis (for example, once a week) and between the full backups do an incremental backup of the transaction logs.

In this section we discuss the pros and cons to consider when choosing to use either an incremental backup or a full backup solution. Transaction logging is an essential part of the Domino server because it provides performance optimizations, speeds the recovery from an abnormal Domino shutdown, and uses the log used for backup. We discuss the ways in which transaction log backups and full backups can be used; you must determine which way suits your particular situation. You should review the documentation about transaction logging in the Administration Guide for Domino 7 to get a full understanding of the operation of transaction logs.

Domino 5 introduced transaction logging but the databases must be in the Domino 5 or later on-disk structure (ODS).

With this feature enabled, the system captures database changes and writes them to the transaction log. Then, if a system or media failure occurs, you can use the transaction log and a third-party backup utility to recover your databases.

A single transaction is a series of changes made to a database on a server. An example of a transaction might include opening a new document, adding text, and saving the document.

When you enable transaction logging, you must select the type of logging that you want to occur. You can choose from circular logging (which is the default), archive (recommended), and linear logging.

- *Circular logging* continuously reuses the log files and overwrites old transactions. You are limited to restoring only the transactions that are stored in the transaction logs. If this implementation is selected, full nightly backups are required. The maximum size of circular transaction logs is 4 GB in total. If the overall size of your transactions exceeds this size, the oldest logs will be overwritten. Be aware that you can lose data if the backup procedure is not scheduled appropriately (meaning that the logs are full and overwritten before you backed them up). This must be monitored—especially in heavy loaded environments. Each backup takes longer to perform, but the restore process is more efficient because only the most recent (or other appropriate) full backups have to be restored. You cannot archive the transaction log if circular logging is used. Therefore, if you lose both the database and the recovery log, you will only be able to recover the database at its state at the last backup.
- *Archival logging* does not reuse the log files until they are archived. A log file can be archived when it is inactive, which means that it does not contain any transactions necessary for a restart recovery. Use a third-party utility to copy and archive the existing logs. The archive log files will be created incrementally according to a set schedule. With this implementation, incremental backups of the transaction logs can be accomplished daily, with full backups run, for instance, once a week or when a situation occurs that changes the database instance ID. A full backup once a week reduces the

number of transaction log extents to be processed during a restore. It also reduces the number of transaction logs and therefore the disk space required to store them. The disk you dedicated for transaction logging has to be large enough because it can cause severe trouble if the server runs out of disk to write transactions into the logs. This has to be monitored.

- *Linear logging* reuses the log files and overwrites old transactions for log size greater than 4 GB. Linear logging is similar to circular logging, except that it allows more than 4 GB. Use linear logging if the size of the log needed between full database backup intervals is greater than 4 GB and you are not using archive media.

The next consideration for setting up transaction logging is the way the database instance IDs are created and maintained.

When you enable transaction logging, Domino assigns a database instance ID (DBIID) to each Domino database. When Domino records a transaction in the log, it includes the DBIID. During recovery, Domino uses the DBIID to match transactions to databases. Some database maintenance activities, such as compaction with options, cause Domino to assign a new DBIID to a database. From that point forward, all new transactions recorded in the log use the new DBIID. The previous transactions have a different DBIID, so you would not be able to restore any data from the old logs. When these situations occur you will need to perform a full backup of your databases.

Note: When the Domino server is installed, compaction of databases is performed daily by default. Change the compact task to a weekly housekeeping procedure and create a full backup of your databases after compaction is complete.

Cases when Domino assigns a new DBIID to the transaction logs, requiring a new full backup, include:

- Transaction logging is enabled for the first time.
- A Compact server task with options is run.
- Fixable is run on any databases that were corrupted.
- The log path or maximum log size is changed.
- A Domino database is moved from one logged server to another logged server, or from an unlogged server to a logged server.

As you can see from this list, there are considerations for implementing incremental backups at your location. Close analyses of all variables should be accomplished before making a final decision about your backup method. Whether you decide to perform incremental or full backups, test your procedures regularly to ensure the accuracy of the data to be restored. In most cases you will have a mixed environment with full and incremental backups running each day.

13.3.4 Online backup tools

In previous sections we discussed transaction logs and other considerations. Next you need to select a backup tool that can take advantage of the Lotus backup API and features included with transaction logging. In general, the third-party tools have three major parts:

1. The backup server, where the media devices such as tape drives exist and backup management usually takes place.
2. The client software, which is loaded onto each Domino server and sends the data to the backup server.
3. The add-on feature that implements the Domino-specific features.

Refer to your vendor's documentation for more information.

13.4 Planning for successful backups

After you have selected your backup software, you should take time to consider the issues that will affect a successful backup strategy. Considerations include:

- Will you be backing up across the network, and if so, will the bandwidth on your network be able to handle the load?
- Schedule your backups during non-peak hours. Your server performance will diminish if backup is running during high-volume access periods.
- How many servers and databases will be backed up? Run test backups and estimate the amount of time you will need to complete your backups. Will you have enough time to complete them during scheduled hours?
- For servers with terabytes of data, architect your Domino directories as multiple file systems. Each of these can be backed up individually on a rotating basis so that you will have more flexibility in the use of the backup tape capacity. If multiple file systems are not an option in your environment, use folders in your data directory.
- Consider the backup media you will be using, the cost of the media, and how much will be needed annually. Include this in your budget plans.

- Be sure to complete the weekly maintenance for your databases before running your weekly backups if you have implemented transaction logging with incremental backups. Remember that the DBIID will change when compact with options and fixup are run on your databases.
- When considering your backup volume, be sure to take into account your transaction log size. The daily log size varies because it depends on the number of transactions in a database and the number of databases on a server. We recommend performing tests based on the user behavior in your company and monitoring the size of your transaction logs. Numbers usually range from 10% to 35% of the total database size for each server, but this is only an average from different environments and it might not adapt to your environment.
- Be sure to test the restore of your databases to ensure accurate data.
- Document your backup procedures and, if you are not the Domino administrator, inform the administrator of the effect transaction logging has on backup levels.
- If you use transaction logging with archive log enabled, be sure that the archive logs are recycled when not valid (when DBIID changes).
- Be sure you understand the throughput capabilities of any tape device you will use. If your backup is taking a long time to complete, you may find that the throughput on your tape drive is the cause of your bottleneck.
- You can increase your throughput on a library by adding tape drives.
- If you are using single tape drives, consider having more than one.
- Software compression during backup can increase CPU utilization.
- When performing a restore with transaction logging:
  - Restore the database from the full backup first.
  - Next, restore all transaction logs for the database.

13.4.1 Sample schedule

It is common to follow this schedule in existing environments:

- Schedule daily incremental backups of the transaction log. Use the backup utility daily to back up the transaction log.
- Schedule archiving of transaction log files. If you use the archive logging style, use a third-party backup utility to schedule archiving of log files.
- Schedule weekly full database backups. Each week, it is recommended to run the Compact task with the option to reduce file size. Because this compaction style changes each database’s DBIID, you should schedule compaction with a full database backup.

13.4.2 Backup using Lotus C API for Domino 7

In this section we describe the Lotus C API for Domino and Notes, which can be used to write your own software to back up and restore the transaction logs in Domino 7.

If transaction logging is enabled on the server, all Domino 5 and later format databases in the server data path are logged by default. The Domino administrator can disable logging for a particular database. Earlier database versions are not supported by transaction logging. All logged transactions go into a single transaction log, consisting of one or more files or extents. Transaction logging may be of circular style, linear style, or archive style. Transaction logging must be enabled in order to implement the recovery of databases via the API's backup and recovery functionality.

See the documentation available for the Lotus C API Toolkit and the C++ API Toolkit for a full technical description of the functions and sample programs that are available. Documentation is available online in the Technical Library area of the following Web site:

http://www.lotus.com/ldd/

The API enables the backup products to perform the following functions:

- Online backup of databases
- Maintain multiple backup versions of databases
- Archive transaction log extents (if archival logging is used)
- Restore any version of a database and apply changes since the backup from the transaction log
- Restore databases to a specific point in time
- Restore one or more archived transaction logs
- Expire database backups automatically based on version limit and retention period
- Archive inactive transaction log extents when they are no longer needed for restore
- Automate scheduled backups

13.4.3 Considerations for backup software

When you select third-party software, there are some features that relate to your Domino server that should be considered. Your evaluation of the software should determine whether it provides the following capabilities:

- Online full and incremental backup of Domino databases.

- Offline full and incremental backup of Domino databases.
- Selective network port addressing for backup across a LAN. This is valuable if you have installed a private network for your clustering. You can back up your servers without using the bandwidth necessary for the Domino server functions.
- Automatic discovery of new Domino databases.
- Automatic recognition of DBIID change to select full instead of incremental backup for transaction logging.
- Software determines which transaction logs are aged (obsolete) and informs you, deletes logs, or reuses the logs.
- Online recovery of an entire Domino database.
- Offline recovery of single or multiple Domino databases.
- Automated backup scheduling for Domino server.
- Automated backup scheduling by Domino databases.
- Centralized administration of distributed Domino environment.

13.5 Vendor solutions

Quite a few third-party software companies offer backup software for the Domino server on the Solaris platform. Many vendors have products that support the Domino C API for backing up the transaction logs.

To find out which third-party products are currently supported, visit the Lotus IBM Business partner Web site at:

http://www.lotus.com/partner

13.6 Summary

In this chapter we described the types of backups that can be performed, from simple, inexpensive procedures to the use of third-party software. The configuration of devices that can be used for backup and the strategies to consider when planning a successful backup routine were also presented.

14

IBM Lotus Domino 7 as a Web server

In this chapter we describe how to configure a Domino server to work as a Web server.

We discuss in detail a number of changes that were implemented in the HTTP task for Domino 7 that improved performance and scalability over previous versions.

© Copyright IBM Corp. 2006. All rights reserved.

14.1 Solaris Operating System configuration

Considering the temporary nature of connections under the HTTP protocol (each request opens a connection, sends the message, returns the response, and closes the connection), particular care must be taken in configuring the TCP/IP part of the Solaris Operating System.

14.1.1 Basic recommendation

It is possible that some other HTTP server could be running on your system, such as Netscape or Apache. The only precaution is to check whether other HTTP daemons are running on the Solaris system using the default port 80.

Use the **ps -ef** command and pipe the output to the **grep** command to check this:

```
ps -ef | grep http
```

Note: The UNIX **grep** command searches a file for a pattern. It also reads from the standard input so it can be used in a pipeline command.

You should not see any HTTP-related task running on your system.

Use the **netstat** command to see whether any daemons are using port 80:

```
netstat -an | grep ":80"
```

In this case, the command should not have any output. If daemons are listening on port 80, you may see output such as:

```
tcp 0 0.0.0.0:80 0.0.0.0:* LISTEN
```

Generally you can have other HTTP processes running on your system, listening on different ports. Running other HTTP systems on the same Solaris server is not recommended if you want to have a high performance Domino Web server.

14.2 Domino Web server configuration

The configuration of the HTTP server in Domino 7 is a very easy task. Most of the work is done at Domino installation time if you check the options to install the HTTP task.

If you choose to install the HTTP task, you will find the HTTP name in the notes.ini file to the ServerTasks entry:

```
ServerTasks=replica,router,update,amgr,adminp,HTTP
```

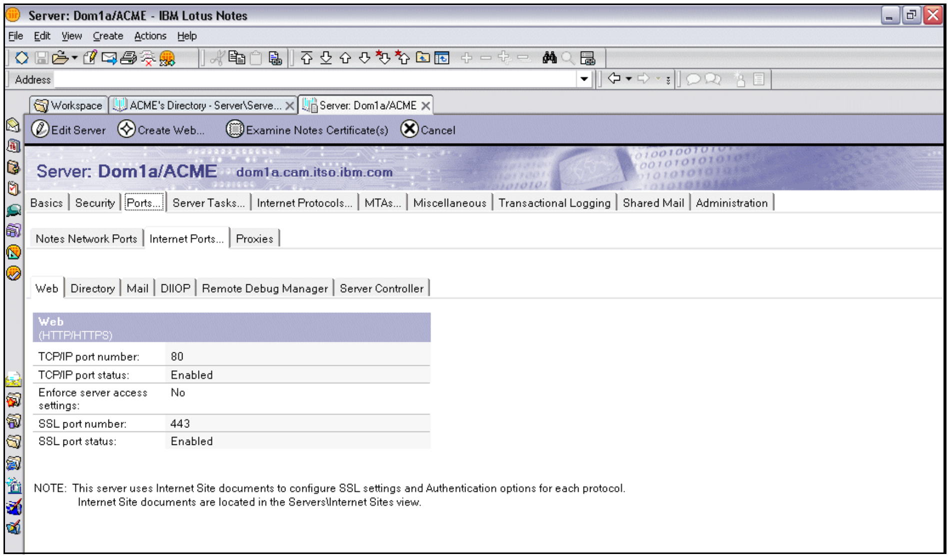
> **Tip:** The content of the notes.ini file is *not* case sensitive, so there is no problem if the name of the task is written with capitals and the effective name of the binary file is http. Remember that UNIX *is* case sensitive.

14.2.1 Settings on a Domino Web server

To change the settings of the Domino Web server, use the following steps:

1. Start the Domino Administrator.
2. Choose the server you want to reconfigure.
3. Click the **Configuration** tab.
4. Choose **Server** → **All Server Documents**.
5. Double-click the Domino server you want to change or select the server and click **Edit Server**.
6. To change the Domino Web server port, click **Ports** → **Internet Ports** in the server document. The Web tab should be selected by default.

   It is best to use the default port 80 for a non-secure Web server and port 443 for a secure Web server.



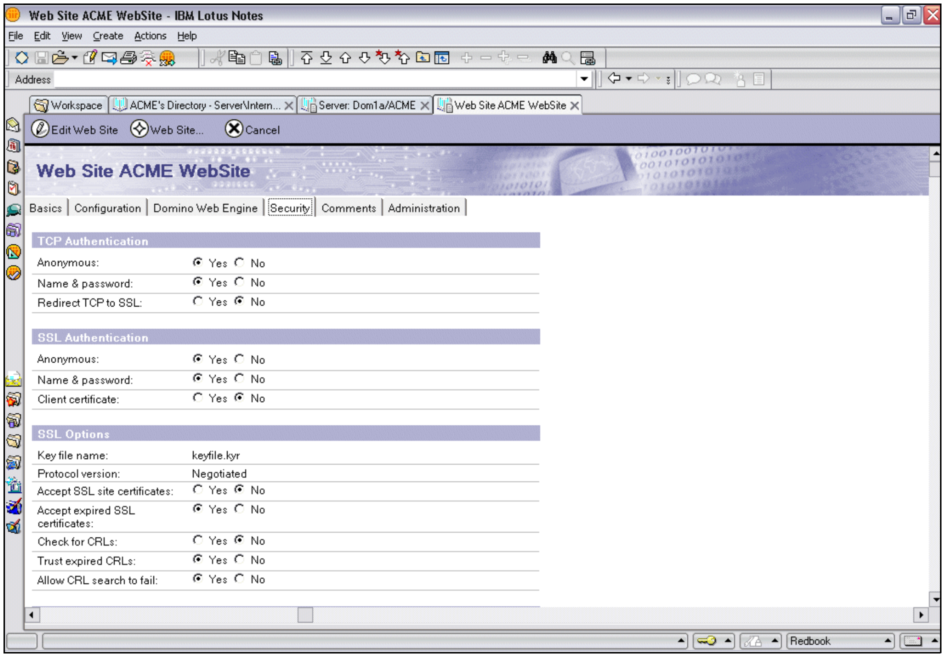
Web (HTTP/HTTPS)	
TCP/IP port number:	80
TCP/IP port status:	Enabled
Enforce server access settings:	No
SSL port number:	443
SSL port status:	Enabled

NOTE: This server uses Internet Site documents to configure SSL settings and Authentication options for each protocol.
Internet Site documents are located in the Servers\Internet Sites view.

Figure 14-1 Web server configuration

> **Note:** The secure server will not run until you create a server certificate. See “Setting up SSL on a Domino server” in Domino 7 Administration online help.

Under Domino 6, other configuration parameters were available to be edited on this server document; however, with Domino 7, those parameters have been moved to the servers\Internet sites view as shown in Figure 14-2.



Web Site ACME WebSite

TCP Authentication

Anonymous:	● Yes ○ No
Name & password:	● Yes ○ No
Redirect TCP to SSL:	○ Yes ● No

SSL Authentication

Anonymous:	● Yes ○ No
Name & password:	● Yes ○ No
Client certificate:	○ Yes ● No

SSL Options

Key file name:	keyfile.kyr
Protocol version:	Negotiated
Accept SSL site certificates:	○ Yes ● No
Accept expired SSL certificates:	● Yes ○ No
Check for CRLs:	○ Yes ● No
Trust expired CRLs:	● Yes ○ No
Allow CRL search to fail:	● Yes ○ No

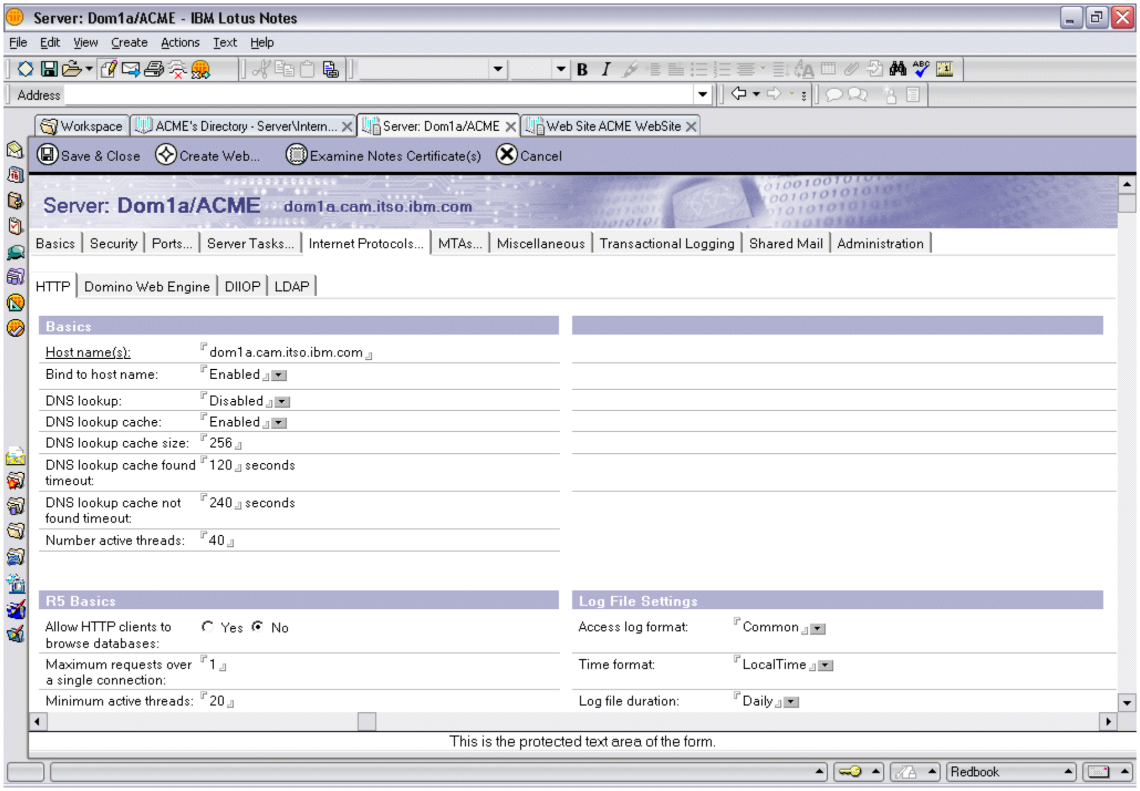
Figure 14-2 Security tab from the Internet site document

Here you can also choose whether you want to allow name and password authentication for clients connecting over TCP/IP; the default is Yes. Also specify whether you will allow anonymous connection over TCP/IP; again, the default is Yes. The same is true for the SSL protocol.

Going back to the server document, select **Internet Protocols** → **HTTP** (see Figure 14-3 on page 435). In this section, you should make at least the following changes:

- In the Basics section, enter a host name and enable the **Bind to host name** option for a Domino partitioned environment. The **Number of active threads** parameter, which is discussed later in this chapter, should be set.
- In the R5 Basics section, the **Maximum requests over a single connection** parameter, which is discussed later in this chapter, should be set.

- ► In the Enable Logging To section, enable either log files or Domlog.nsf if you want to create statistics about access to your Web server (for example, by whom, how much, and which pages were accessed). Enabling either type of logging will affect server performance.
- ► In the Mapping section, customize the Home URL. It should be either a Notes database or an HTML file.


Server: Dom1a/ACME - IBM Lotus Notes
File Edit View Create Actions Text Help
Address
Workspace
ACME's Directory - Server\Intern...
Server: Dom1a/ACME
Web Site ACME WebSite
Save & Close
Create Web...
Examine Notes Certificate(s)
Cancel
Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transactional Logging | Shared Mail | Administration
HTTP | Domino Web Engine | DIIOP | LDAP
Redbook

Server: Dom1a/ACME dom1a.cam.itso.ibm.com

Basics

Host name(s):	dom1a.cam.itso.ibm.com
Bind to host name:	Enabled
DNS lookup:	Disabled
DNS lookup cache:	Enabled
DNS lookup cache size:	256
DNS lookup cache found timeout:	120 seconds
DNS lookup cache not found timeout:	240 seconds
Number active threads:	40

R5 Basics

Allow HTTP clients to browse databases:	○ Yes ● No
Maximum requests over a single connection:	1
Minimum active threads:	20

Log File Settings

Access log format:	Common
Time format:	LocalTime
Log file duration:	Daily

This is the protected text area of the form.

Figure 14-3 Web server Internet protocol specifications

14.2.2 Starting, stopping, and refreshing the Domino Web server

There are two ways to start the Domino 7 Web server:

- ► Manually, by entering `load http` at the server console
- ► Automatically at Lotus Domino 7 start-up, by adding it to the ServerTasks in notes.ini.

Note: You can start only one HTTP task per Domino server. You have to use the Domino partitions feature to have more than one HTTP task running on the Solaris server.

To stop the Web server, enter the command `tell http quit` at the server console, or remove HTTP from the ServerTasks in notes.ini to stop it from starting at the next restart of the Domino server.

Type the command `tell http restart` at the server console to refresh the Web server, and if you made changes in the Domino Directory related to the HTTP configuration.

Tip: You can use the `server -c` Domino command to send a Domino Console command from a Solaris prompt. Type `server -c "tell http quit"` to stop the HTTP task from a Solaris prompt.

14.3 Security on the Web server

In this section we describe the Web security features in Domino 7. Some new security features were added to Domino 7, including HTTP protocol security options.

14.3.1 Internet certificates

Domino certificate authorities can also issue Internet certificates to Notes users, Internet clients, and Internet servers. The Domino certificate authority issues signed X.509 format certificates that uniquely identify the requesting client or server. Internet certificates are required when sending encrypted or electronically signed S/MIME mail messages and when using SSL to authenticate a client or server.

S/MIME is a protocol used by clients to sign mail messages and send encrypted mail messages over the Internet to users of mail applications that also support the S/MIME protocol.

Domino 7 provides native X.509 V3 support along with the Notes certificate.

14.3.2 Browsing Domino databases via the Internet

A common security issue is accessing the log.nsf database via a Web browser, for example:

```
http://dom1a.cam.itso.ibm.com/log.nsf
```

Although the log.nsf database does not contain critical information, a Domino system that allows access to the system log is not secure.

To avoid this you have to change the ACL of the database to either:

- Default No Access

  or

- Anonymous No Access

You have to do one or the other in *each* Domino database in your data directory that must be kept inaccessible to Internet users.

14.3.3 Session authentication

A *session* is the time during which a Web client is actively logged on to a server. Session-based name-and-password security includes additional functionality that is not available with basic name-and-password security.

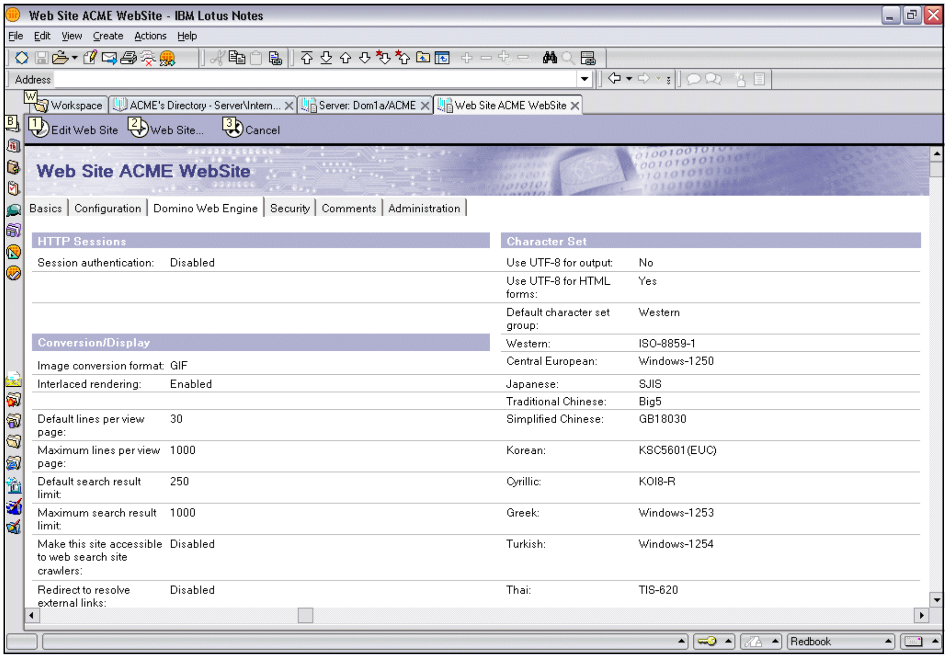
Session-based authentication creates a temporary *cookie* that stores the user name and password on the browser client. As the user traverses the site, responses for name and password are provided by the cookie.

This cookie passes the user credentials for every database within the Domino site, thus alleviating concerns of realm-based authentication.

> **Tip:** If you wish to retain realm-specific logins, session-based authentication cannot be used.

When a user logs in to the Web site, the credentials are passed to every database hosted by the server. The user login information, however, is not shared across virtual hosts or virtual servers; it is based on the host name of the URL request.

You can configure session authentication on the Domino Web Engine tab of the Internet sites, in the Domino Web engine tab (Figure 14-4).



Web Site ACME WebSite

HTTP Sessions

Session authentication:	Disabled

Conversion/Display

Image conversion format:	GIF
Interlaced rendering:	Enabled
Default lines per view page:	30
Maximum lines per view page:	1000
Default search result limit:	250
Maximum search result limit:	1000
Make this site accessible to web search site crawlers:	Disabled
Redirect to resolve external links:	Disabled

Character Set

Use UTF-8 for output:	No
Use UTF-8 for HTML forms:	Yes
Default character set group:	Western
Western:	ISO-8859-1
Central European:	Windows-1250
Japanese:	SJIS
Traditional Chinese:	Big5
Simplified Chinese:	GB18030
Korean:	KSC5601(EUC)
Cyrillic:	KOI8-R
Greek:	Windows-1253
Turkish:	Windows-1254
Thai:	TIS-620

Figure 14-4 Session authentication settings in the Internet sites document

With the Session Authentication feature enabled, you can use the following command to find out who is using a Web browser to access your Domino 7 server:

```
tell http show users
```

The command produces this output:

```
11/24/2005 11:00:07 AM There are 2 current HTTP user sessions
11/24/2005 11:00:07 AM User Name IP Address Expires
11/24/2005 11:00:07 AM dom1a 9.95.35.56 11:29:52 AM
11/24/2005 11:00:07 AM dom1a 9.95.35.56 11:29:28 AM
```

The session authentication feature is based on the cookie mechanism; it enables a Web server to store pieces of information on the client computer through the Web browser. These pieces of information, known as cookies, are stored on the client machine.

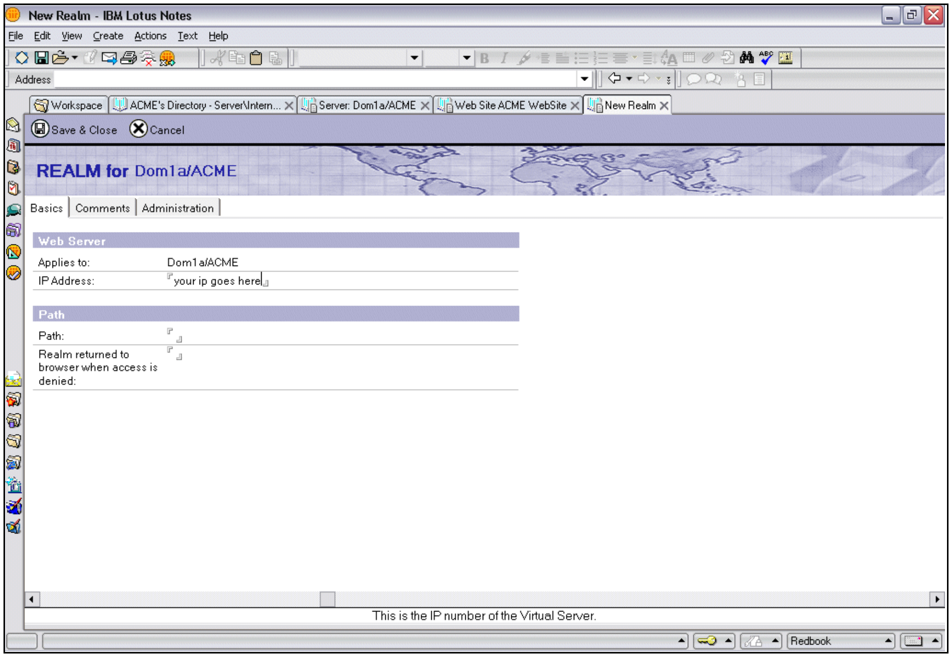
Tip: To return the value of a cookie, add a computed field called `HTTP_COOKIE` to your form using an empty string as a formula. This field will be populated with the cookie information. You can then use the field HTTP_COOKIE in other formulas on the page.

14.3.4 Domino Web realms

To minimize the need for a Web user to repeatedly supply a password, Domino administrators can set up Web realms on the server. *Realms*, based on ACLs, are zones of file protection on a Web site.

The browser automatically stores and sends the credentials for pages in the same realm, so the user can move throughout the Realm after supplying the password just once.

Access the page for setting up realms by selecting the server document you wish to modify, then choose **Web** → **Create Realm**. Figure 14-5 shows the resulting window.



Applies to: Dom1a/ACME

IP Address: your ip goes here

Path:

Realm returned to browser when access is denied:

This is the IP number of the Virtual Server.

Figure 14-5 Web realm: Basic setting

Provide information for the Path field to permit user navigation of the directory defined in the Realm.

Note: Refer to Domino Administration 7 help for additional information about configuring Realms.

14.3.5 Domino file protection

In Domino 7, File Protection documents stored in the Domino Directory database are the basis for configuring browser access control to files.

You can enforce file system security for files that browser users can access. For example, for HTML, JPEG, and GIF, you can specify the level of access for these types of files and the names of the users who can access them.

You can apply file system protection on CGI scripts, servlets, and agents. However, the file protection does not extend to other files accessed by the scripts, servlets, or agents.

For example, you can apply file protection on a CGI script that restricts access to a group named Web Admins. However, if the CGI script executes and opens other files (or causes other scripts to be executed), the File Protection document is not checked to determine whether Web Admins has access to these files.

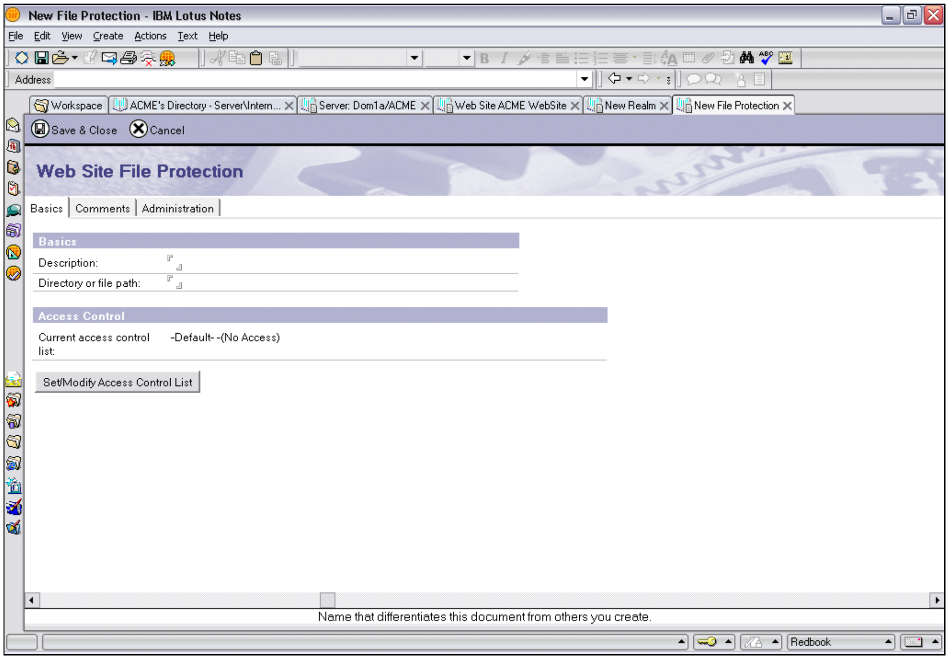
File protection also does not extend to files in the following directories, which contain default image files and Java applets that are used by the HTTP Web server and other applications (for example, mail databases):

- /notes/dom1a/domino/java, accessed via Web browser using the path http://dom1a.cam.itso.ibm.com/domjava
- /notes/dom1a/domino/icons, accessed via Web browser using the path http://dom1a.cam.itso.ibm.com/icons

File system protection does apply, however, to files that access other files, such as HTML files that open image files. If a user has access to the HTML file but does not have access to the JPEG file that the HTML file uses, Domino does not display the JPEG file when the user opens the HTML file.

You have to consider setting up File Protection documents for each directory Web users are able to access. There is no file protection for an upgraded or new Domino 7 server until you create File Protection documents.

You do this by choosing **Web** → **Create File Protection**. Figure 14-6 on page 441 shows the resulting window.


New File Protection - IBM Lotus Notes
File Edit View Create Actions Text Help
Address
Workspace
ACME's Directory - Server\Intern...
Server: Dom1a/ACME
Web Site ACME WebSite
New Realm
New File Protection
Save & Close
Cancel
Basics
Comments
Administration
Set/Modify Access Control List
Redbook

Web Site File Protection

Basics

Description:

Directory or file path:

Access Control

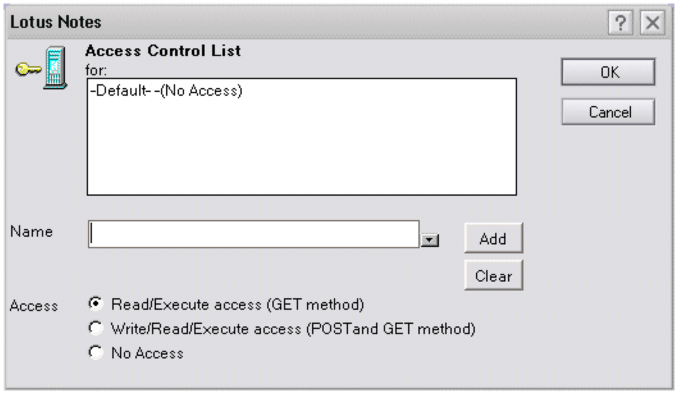
Current access control list: -Default- -(No Access)

Name that differentiates this document from others you create.

Figure 14-6 File Protection: Basic setting

The ability to set file protection might be needed in mixed environments, where you have some data in the Notes databases and other data in text files. These protection settings apply to all Web servers on a Lotus Domino 7 server.

You can only grant access to users specified in the server's Domino Directory, even if you are allowed to enter any user. You assign these permissions by clicking **Set/Modify Access Control List** in the Access Control tab.



Access Control List for:

-Default- -(No Access)

Name

Access
● Read/Execute access (GET method)
○ Write/Read/Execute access (POSTand GET method)
○ No Access

Figure 14-7 Access Control List for file protection

You can assign a user to one of three access levels:

- Read/Execute access (GET method)
- Write/Read/Execute access (POST and GET method)
- No Access

In the Name field, specify the user name by typing or by using the Domino Directory lookup. After assigning the appropriate access permission, click **OK** to apply this user to the Access Control List. To remove a user, click the name and click **Clear**.

14.3.6 HTTP protocol security

Domino 7 is better equipped to fend off cyberattacks. Several new protocol-related security settings have been added to the Server document under the Internet Protocols → HTTP tab. These new settings are designed to discourage attacks that probe for buffer overflows or request parsing errors.

The new settings for HTTP protocol security are:

- Maximum URL length
- Maximum number of URL path segments
- Maximum number of request headers
- Maximum size of request headers
- Maximum size of request content

Maximum URL length is the URL length that can be received from HTTP clients such as Internet browsers. This length includes the query string, which defaults to 4 KB. We do not recommend increasing this limit unless your applications require extremely long query strings.

Maximum number of URL path segments limits the number of segments allowed. For example:

> http://dom1a.cam.itso.ibm.com/a/b/c/d/e/f/g/h/i/j/k/l/m/n/o/.........etc.

The default value for this setting is 64.

Maximum number of request headers helps to protect against buffer overflow probes. By default, the Domino 7 HTTP task allows only 48 headers.

Maximum size of request headers limits the actual size or total length of the header in the request. The default setting is 16 KB.

Maximum size of request content restricts the amount of data that can be contained in a request such as a form. The default value is 10 MB. The “Maximum POST data” setting from Domino R5 can be found in the Web site document at the Internet Sites view in the Domino Web Engine tab.

Note: Refer to the Domino Administration 7 Help for additional configuration information about these HTTP security settings.

14.4 Troubleshooting

The HTTP process usually operates without incident. However, this section describes a few issues that are specific to HTTP process troubleshooting.

14.4.1 HTTP does not respond

To check whether the HTTP process has hung or simply is overloaded by a lot of client requests, a good basic test you can do is to Telnet to the process in the right port, by default port 80.

For example, if your Domino server is running on a host named itsoredhat and listening on the default port 80, you have to run the command:

```
telnet dom1a.cam.itso.ibm.com 80
```

The command output is:

```
Trying 9.33.85.101...
Connected to dom1a.cam.itso.ibm.com.
Escape character is ’^]’.
```

Now you can issue an HTTP command, for example **`get`**:

```
Trying 9.33.85.101...
Connected to dom1a.cam.itso.ibm.com.
Escape character is ’^]’.
get
```

Note: The **`get`** command should return the HTML header information from your default homepage. This header should include references to Domino and your operating system.

In this case the **`get`** command receives an answer from the HTTP process; if HTTP was hanging, the **`get`** command would not receive any responses.

Note: This technique can be implemented as well for the other Domino Internet processes, such as IMAP, LDAP, and POP3, by choosing the appropriate port number (for example, 143 for IMAP) and the appropriate protocol command (for example, **`hello`** for IMAP).

14.4.2 Using the tell command

Domino 7 utilizes a console command that helps in troubleshooting if HTTP hangs. This command is **`tell http Show Thread State`**.

When entered at the Domino Console, this command displays the current status of each active thread, and which URL, if any, the thread is processing.

Following is a sample output for three threads. The first two threads are idle; the third thread (0xf9) is processing the URL
`GET /reference.nsf/ Refresh?OpenAgent HTTP/1.0`

```
> tell http show thread state
06:37:09 PM HTTP Thread State: Thread: [fb] State: [Worker waiting for
work] Other Info:
06:37:09 PM HTTP Thread State: Thread: [fc] State: [Worker waiting for
work] Other Info:
06:37:09 PM HTTP Thread State: Thread: [f9] State: [Worker processing
request] Other Info: GET /reference.nsf/Refresh?OpenAgent HTTP/1.0
```

If the HTTP process is in a hung or partially hung state, this command can be used to determine whether a particular thread has been processing the same URL for too long. If the thread processes the same request or URL for more than a few minutes, then the thread is likely hung. You can check this by repeating the command after a few minutes.

In many cases, if the HTTP task is hung, the Domino administrator can attempt to shut down the HTTP server task, but the task does not always shut down gracefully. In Domino 7, when an administrator issues the command **`tell http quit`**, if HTTP is waiting for a hung thread to complete during shutdown, HTTP outputs this thread ID and the URL it is working on to the console. For example:

```
> tell http quit
04/28/2002 06:37:51 PM HTTP Waiting For Thread: Thread: [f9] State: [Worker
processing request] Other Info: GET /reference.nsf/Refresh?OpenAgent
HTTP/1.0
```

This information can be used to determine the hung thread and which URL the thread is processing. This is similar to the use of the req*.log files (described in the following section). The thread ID can be correlated against the req*.log file that pertains to that thread.

14.4.3 HTTP thread debugging

Additional diagnostics for the Domino HTTP process are available and can be enabled when troubleshooting HTTP problems.

A request log file can be created for each worker thread by placing the parameter `debugthreadlogging on` in the httpd.cnf configuration file. When this is enabled, a file is created for each active thread, with information about each processed request appended to the file as requests are made to the server (roughly 10-15 lines per request). These files can be extremely useful to pinpoint causes of HTTP crashes or hangs.

As an alternative to placing `debugthreadlogging on` in the httpd.cnf, administrators can enter the following command at the server console:

```
tell http debug thread on
```

This dynamically sets the thread logging debug flag, and the server begins to create thread logs immediately. However, this debug flag remains in effect only until the HTTP server is restarted. This method of turning on debug does not place the parameter in the httpd.cnf file.

The created files are named req###.log, where ### is the thread ID for the active thread, and they are written to the Domino data directory. For example, req111.log corresponds to the lwp-id 111 from the nsd.

These req*.log files do not contain a date/time stamp, so they must be used in conjunction with Domino logging (DOMLOG.NSF or Access logs). However, each line of the logged request displays the number of milliseconds since the HTTP process last started (the bold number in the Start Request line). This enables you to determine the amount of time that each phase of the request process takes.

Note: Use these variables only for debugging. They have a significant impact on Domino server performance when they are enabled.

14.5 Domino 7 console tell commands

Lotus Domino 7 has **`tell`** commands that can be used for the HTTP process. These commands are issued on the server console. Some of the commands are:

- **`tell http show users`**
- **`tell http show thread state`**
- **`tell http restart`**
- **`tell http show security`**
- **`tell http show virtual servers`**
- **`tell http quit`**

tell http show users

This command can be used only if the server is configured to use session-based tracking for the Web. Session tracking is a feature of session-based authentication. To enable it, edit the server document in the Domino Directory. In the Internet Protocols section, select **Domino Web Engine**. By default, the entry for "Session authentication" is disabled. Select **Enabled** to allow the HTTP task to report on authenticated users. This command shows the User Name, IP address, and time of expiration (30 minutes by default). This will reflect only users who are authenticated and cannot be used to track anonymous users.

tell http show thread state

This command lists the current state of each active thread (as well as the accept thread and logger thread). If the thread is processing a request, the output of this command will indicate the URL being processed.

tell http restart

This command causes the HTTP task to shut down and reload. This is the equivalent of **`tell http quit`** followed by **`load http`**. This command also is valid for the other Domino processes.

tell http show security

This command outputs current status about the use of SSL for the server and each virtual server.

tell http show virtual servers

This command outputs the current configuration for virtual servers.

tell http quit

This command causes the HTTP task to shut down.

14.6 Virtual servers and host

If you are a corporate intranet administrator who provides services to multiple customers, you can set up *virtual servers* on a single Domino Web server. A single Domino Web server can then host several Web sites. Using virtual servers enables you to maintain separate sites without incurring the expense of additional hardware and software.

You can configure each site in Domino with its own IP address, default home page, customized Web server messages, and HTML, CGI, and icons directories. The Domino data directory, however, is not individually configured for each virtual server; it is shared by all virtual servers.

The difference between a virtual server and a virtual host is that *virtual servers* have different IP addresses and different host names; *virtual hosts* use the same IP address but different host names.

> **Note:** Refer to system administration documentation for your operating system environment for installing and configuring additional network interface cards and IP addresses. This document only addresses Domino-specific configuration settings.

14.6.1 Create virtual server or host

To create a virtual server or host: In the Domino Directory, select the Domino server and choose **Web** → **Create Virtual server** from the menu bar.

You will be asked whether you want to create a virtual host or a virtual server. Choose **Virtual Host**. Creating a Virtual Server is almost the same, except you will be asked for the IP address instead of the host name.

On the Basics tab, enter the host name of your added virtual host.

On the Mapping tab, specify the path names mapping to the HTML directory, the Icon directory, the CGI directory, and the home URL, such as a Domino Web server configuration. This tab is the same for both server types.

On the Security tab, you can designate some security settings for your virtual servers, such as whether name and password or anonymous authentication can be used.

You can also customize the SSL settings to comply with your company's security policies. For more about SSL, refer to the Domino Administrator 7 Help.

14.6.2 Create URL mapping and redirection

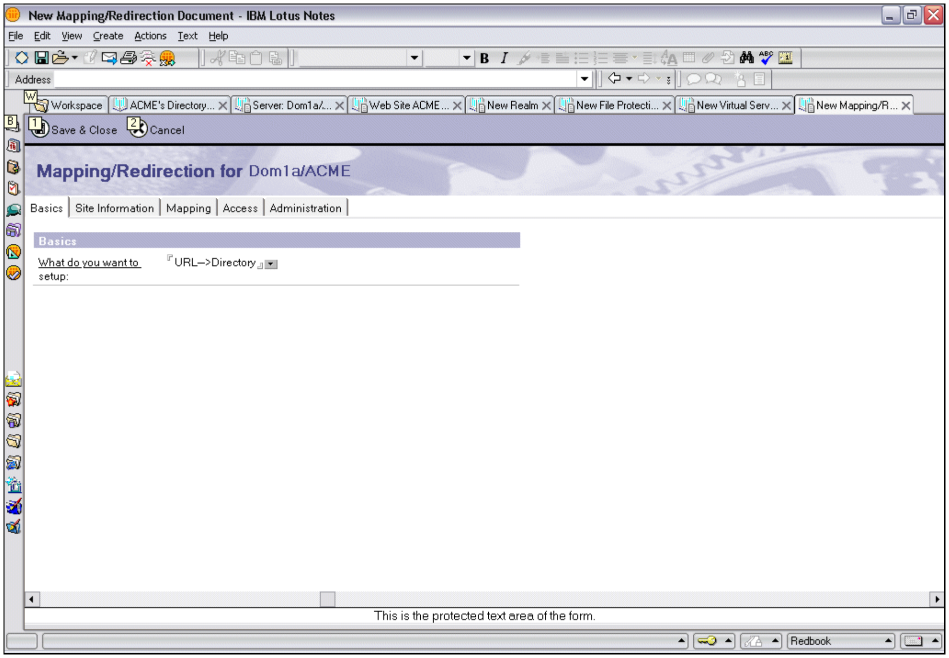
There are three different types of URL mappings. Depending on the type you choose, you will get three or four tabs to configure the mapping.

URL-to-URL mapping (shown in Figure 14-8 on page 448) enables you to define an alias name for URL paths. For example, you can map /MyPictures to /images.

URL-to-Directory mapping enables you to specify which URL path should be mapped to which real directory on your server. For example, if all of the images you are using in your Web pages are in /web/images, you have to create a directory mapping /web/images to /YourPictureDirectory to be able to access these pictures through the Internet. If you have defined a URL-to-directory mapping, you will also have to specify whether your data can only be read or if it should be executable.

URL-to-Redirection URL. Using this, you can move pages to a different server without making the old URL invalid.

Figure 14-8 shows the options for the Basics tab.



Mapping/Redirection for Dom1a/ACME

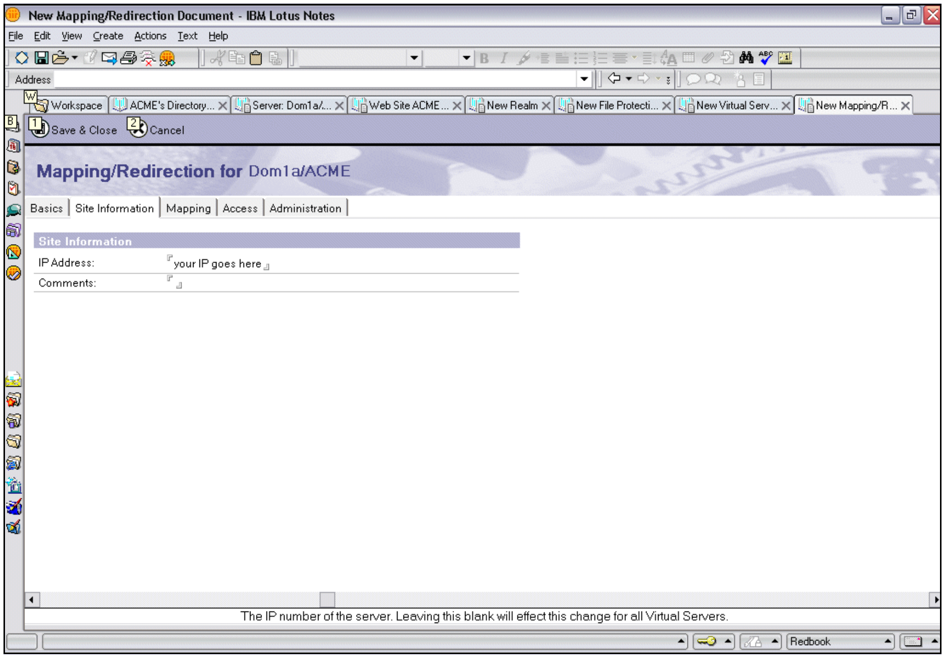
Basics

What do you want to setup: URL-->Directory

This is the protected text area of the form.

Figure 14-8 URL mapping/redirection document: Basics

Figure 14-9 shows the Site Information tab. For each choice, specify in the Site Information tab which virtual server is affected by this mapping.



Mapping/Redirection for Dom1a/ACME

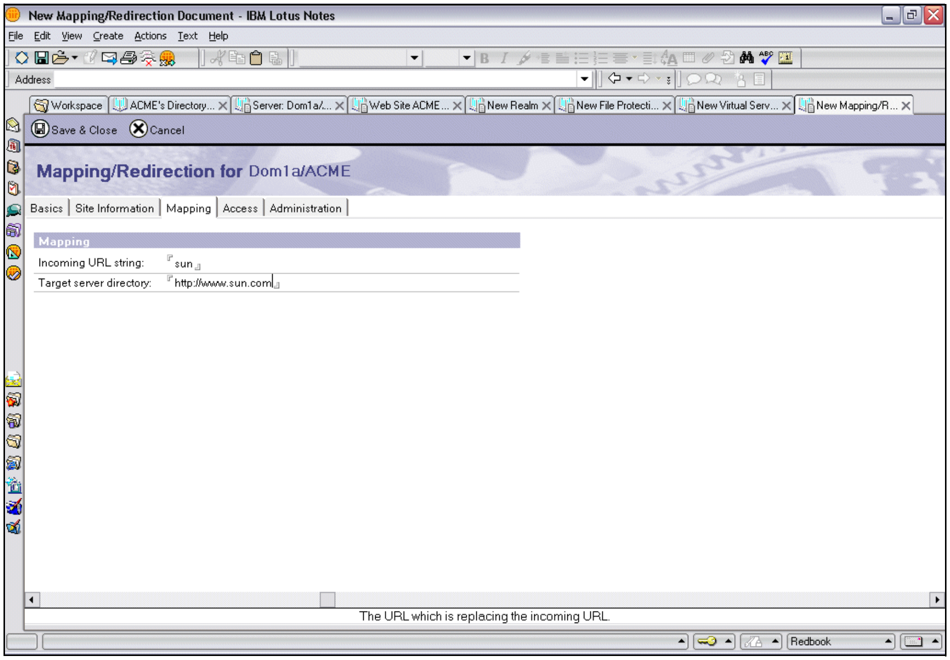
Site Information

IP Address:	your IP goes here
Comments:	

The IP number of the server. Leaving this blank will effect this change for all Virtual Servers.

Figure 14-9   URL mapping/redirection: Site Information

Figure 14-10 shows the options available under the Mapping tab. On the Mapping tab, specify the actual mapping.



Mapping/Redirection for Dom1a/ACME

Mapping

Incoming URL string: sun

Target server directory: http://www.sun.com

The URL which is replacing the incoming URL.

Figure 14-10 URL/Mapping redirection: Mapping

14.7 Domino and Java

At the time of this book was written, Lotus Domino 7 included a Java Virtual Machine (JVM™) based on Sun Microsystemss JDK. The JVM is automatically installed in the Domino program directory.

If you have configured the HTTP server task to support Java servlets, the task will load the JVM when the HTTP task is started. This configuration is available in the Server document under the Internet Protocols → Domino Web Engine tab.

14.7.1 Java servlets

A servlet is a Java program that runs on a Web server in response to a browser request. Servlets for Domino must conform to the Java Servlet API Specification, an open standard published by Sun Microsystems, Inc.

Configuring

On a Domino 7 server, Java servlet support is disabled by default. In order to enable Java servlets, edit the server document and go to the Domino Web Engine tab, then find the section labeled Java Servlets. Set the appropriate value for the Java servlet support field. There are three options:

- None.
- Domino Servlet Manager (which initializes the Domino JVM and starts the servlet manager).
- Third party Servlet manager (which initializes the Domino JVM only). In order to use a third-party servlet manager, you must install the appropriate software (such as IBM WebSphere), which will in turn place lines in the HTTPD.CNF file to allow the servlet manager to plug in to the Domino HTTP server.

Running

The basic steps to run a servlet in Domino 7 are as follows:

1. In the Servlet URL Path field, enter the URL path you wish to use to indicate that the resource is a servlet (the string `/servlet` is the default).
2. Create a directory under the /notes/dom1a/domino directory (for example, domino/servlets) where you wish to store your servlets.
3. Edit the Class Path field to include the location of your specific servlet. You can specify .jar and .zip files in this field.
4. Copy the class files to the /notes/dom1a/domino/servlets directory.
5. Issue the server console command **`tell http restart`** to reload the HTTP server. In your Web browser, enter a URL that contains the servlet name (without the file extension), such as:

    ```
    http://hostname/servlet/HelloWorldServlet
    ```

Note: The addition of any servlets to the servlet directory requires a restart of HTTP before the servlet manager will recognize the new servlet.

14.8 Domino log and analysis tools

Domino 7 makes logging even easier for Internet service providers (ISPs) as well as the rest of us. Domino 7 can now create text files that include the IP address or host name of the server that the user requests. This way, you can more easily use the logs to create statistics for virtual servers. To use this feature, you must enable Extended log format for the access log file in the server document.

To create separate statistics for virtual servers, analysis tools still have to sort the entries in the log file according to the different virtual servers' IP addresses or host names.

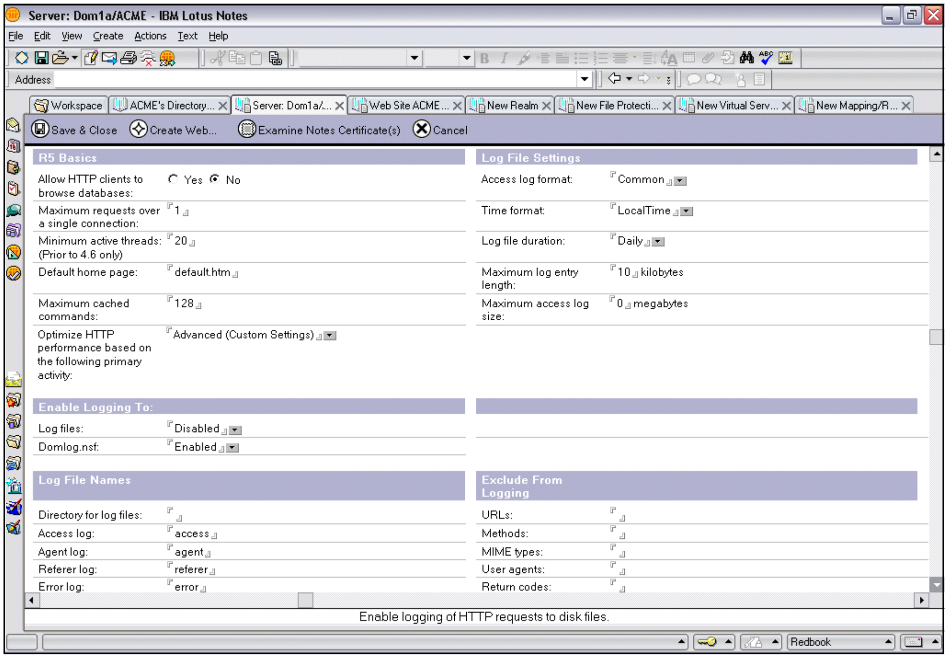
14.8.1 Domino Web log

To set up logging on your Domino server, simply enable one of the logging methods in the HTTP section of the server document in the Domino Directory. (Because logging is very server intensive, it is disabled by default.)

If you enable logging to domlog.nsf, the database is created automatically the next time you start the server. If you enable logging to text files and specify a directory for the files, Domino automatically creates the access log and error log files.

You can select the format for the access log files (Common or Extended Common) and the time format (LocalTime or GMT). Remember that the Common format records only access information, and the Extended format tracks access, agent, and referred information in the access log file. You can then specify different names for the log files.

Figure 14-11 on page 453 shows the logging fields in the server document.



R5 Basics

Allow HTTP clients to browse databases:	○ Yes ● No
Maximum requests over a single connection:	1
Minimum active threads: (Prior to 4.6 only)	20
Default home page:	default.htm
Maximum cached commands:	128
Optimize HTTP performance based on the following primary activity:	Advanced (Custom Settings)

Log File Settings

Access log format:	Common
Time format:	LocalTime
Log file duration:	Daily
Maximum log entry length:	10 kilobytes
Maximum access log size:	0 megabytes

Enable Logging To:

Log files:	Disabled
Domlog.nsf:	Enabled

Log File Names

Directory for log files:	
Access log:	access
Agent log:	agent
Referer log:	referer
Error log:	error

Exclude From Logging

URLs:	
Methods:	
MIME types:	
User agents:	
Return codes:	

Enable logging of HTTP requests to disk files.

Figure 14-11 Domino Web logs

Logging fields

With Domino 7, you can specify whether you want Domino to create new log files daily, weekly, monthly, or never. The log file duration applies to all log files on the server. In addition, only one log file is maintained per Web server, including servers set up as virtual servers. The name that Domino gives to the log file depends on the duration settings and the file names you specify in the server document.

In the Exclude from Logging section, you can prevent logging for specific types of requests. For example, if you do not want to log image requests on your server, enter `*.gif` in the URLs field and `image/gif`, `image/jpeg`, and `image/bmp` in the MIME types field.

You can also prevent logging for:

- Specific HTTP methods
- User agents
- Status return codes
- Hosts and domains

14.8.2 Domino Log database analysis

When you enable logging to the Domino Log database, Domino automatically creates the database using the template domlog.ntf. The basic design of the database includes one form for log entries and one view for displaying them, called Requests. The Requests view shows all records in the order that they were created. To analyze the entries in your Domino Log database, you can either use a Notes tool or one of several solutions from Lotus Business Partners. You can customize the database with additional views, create agents to notify you when specific events occur (such as when a certain number of unsuccessful login attempts occur), or modify the database to generate reports.

15

IBM Lotus Domino Web access

Domino supports several client types that allow users access to their e-mail, including Notes, IMAP, POP, Web browser, and Microsoft Outlook client. In this chapter we look at the Domino Web Access component.

© Copyright IBM Corp. 2006. All rights reserved.

15.1 High-level overview

Domino Web Access is a powerful way to access Domino's core messaging, collaboration, and PIM functions through a Web browser while allowing users to work both online and offline. Companies can let current Notes users access Domino-based messaging, PIM, and collaborative services using Domino Web Access from a Web browser, as well as giving features to new users without requiring them to run the Notes client. In addition, a company can use the Domino Web Access technology, to reach customers and business partners without requiring them to run anything but a Web browser.

Application Service Providers (ASPs) and Internet Service Providers (ISPs) can also use this Web client. Using Domino Web Access, they can give small to medium-sized businesses messaging, collaboration, and PIM features, including the ability to work both online and offline. When used with Domino Off-line Services (DOLS), which enables users to work with Domino Web applications offline, ASPs and ISPs can give customers access to Domino-based intranet applications.

Domino Web Access builds on the previous-generation WebMail template in its use of Domino Off-line Services. With Domino Web Access, users can work from a disconnected Web session to manage e-mail messages, contacts, calendars, and to-do items. Domino Web Access can also work in conjunction with the Notes client or independently of the Notes client while offering many Notes core messaging features. Users can move between Domino Web Access and the Notes client, using Notes when at their desks and using Domino Web Access when they only have access to a Web browser, all of which is supported by a single Domino infrastructure.

Domino Web Access provides users with almost universal access to their Notes mail and IM functions. They can access that information from any location, such as an Internet café, an Internet kiosk, or another user's PC. Domino Web Access is also well-suited for users who routinely share a PC.

For administrators, Domino Web Access provides a simple client that is easy and cost-effective to manage and deploy, all from within the same Domino infrastructure that you may already manage. The thin-client and server-based deployment model, as well as the absence of training requirements, enable companies to get users up and running quickly.

15.2 Design goals

Domino Web Access is designed to take advantage of the latest Internet technologies. Based on XML, DOM level 2, DHTML, and XSL, Domino Web Access uses these technologies to deliver an advanced Web client experience. Additionally, the Web client can be integrated into sites easily using the current Notes 7 client, so that users can enjoy interoperability between the two clients.

Domino Web Access utilizes sophisticated JavaScript components, providing a very rich user interface within a Web browser. These components include date, time, and duration controls; an outline control; tabs within forms that do not require data moving back and forth between server and client; hover and right-click menus; and a sophisticated Notes-like view component. Most Web applications break up large lists into multiple pieces or pages, but the virtual list view component enables users to view all documents on a single page, navigable through a virtual scroll bar. Portions of the view are retrieved from the server in XML format and incorporated into the virtual list as needed.

15.2.1 System requirements

The following sections list the requirements for using the Domino Web Client.

Client requirements

- Recommended for better performance: Pentium IV 1 GHZ with 512 MB of memory (Windows and Linux clients)
- Minimum: Pentium III 400 MHz with 128 MB of memory (Windows client); Pentium III 500 MHz with 192 MB of memory (Linux client)

Client operating systems

- Windows 2000 Professional
- Windows XP

Client operating systems for Mozilla

- Novell SUSE Linux Enterprise Server (SLES) 8
- Novell SUSE Linux Enterprise Server (SLES) 9

Supported browsers

- Win32 Internet Explorer 6.0
- Mozilla 1.4.1 and 1.7.x (Linux clients only)
- Mozilla Firefox 1.0 on Win32 and Linux (supported by the DWA7 mail template only; not supported by iNotes6 templates)

Attempting to access Domino Web Access through unsupported browsers results in the display of an unsupported browser notice. Netscape 4.x users may see hangs or crashes when encountering the Domino Web Access unsupported browser page. If you are a Netscape 4.x user and you encounter these problems, you should open your mail file using the WebMail UI directly through the &ui=webmail switch. This is documented in the topic “Switching to WebMail” in the Domino Web Access help.

> **Note:** Domino Web Access does not work if JavaScript or session cookies are disabled.

Certified proxy servers

- SunOne Portal Server 6.2
- IBM WebSphere Edge Server 2.0.2 efix 49
- Tivoli Access Manager 5.1

Adobe Acrobat

Adobe Acrobat Reader, Version 4.0 or higher to print calendars.

Offline support

Domino Web Access overcomes one of the largest problems facing large customers wanting to give their users browser-based access to their applications: the ability to seamlessly work offline. For Notes 7 users, running the Web client gives them an alternate means to replicate (or synchronize) their mail database and to work offline using a browser instead of the Notes client.

When using Domino Web Access for the first time, users will notice an `Online/Offline` link in the upper-right corner of the browser window. Selecting that link opens a Web page that offers options for downloading the offline components, including the Domino Synch Manager, as well as the contents of your NSF (Notes) files. Synchronizing content between the local system and the server is then as convenient as two mouse clicks. Synchronizing delivers a comparable experience to replication using the Notes client.

User interface

Another goal with Domino Web Access was to present the user with an intuitive Web interface, helping corporate customers to offer a powerful new tool with little retraining for users.

The Domino Web Access user interface provides two means of moving between components of the Web client, as well as performing actions. The Task Bar is the higher menu bar, providing users with access to any of the six components on the Web client including mail, calendar, to-do items, contacts, notebook, and the

Welcome Page. (In the Notes 7 client, access to these functions is gained via the icons along the left of the screen.) These roll-down menus enable users to move directly to the part of the application they desire with a single click, such as pulling up a five-day calendar view while working in the mail inbox.

The Action Bar provides users with the contextual tools to work within the application components of the Domino Web Access client. The roll-down menu is always available to users regardless of what part of the application they are working in, including open messages and calendar items. This menu gives them the ability to create a new message, calendar entry, to-do item, contact, notebook page, or folder—with a single click. Each component of the client, mail, calendar, contacts, and other features has additional component-specific Action Bar menus. Users can also access some contextual menu items with right-clicks.

The Welcome Page is a user-customizable page that presents a main point of entry into the components of the Notes client, such as mail and contacts, as well as Web pages. Users can define rules for prioritizing messages displayed on the Welcome Page, add links to important Web sites or online documents, and check who is online (if the optional Sametime collaboration server is running).

Domino Web Access includes several user interface conventions that greatly enhance the experience of users. The product opens a new window whenever a user opens a mail message, calendar entry, to-do item, contact, or notebook entry. This enables the user to more quickly take follow-up action to an event. In the instance a user receives a mail message that requires scheduling a group meeting, sending a memo, and following up on multiple action items, having the flexibility to create those new items while viewing the original message makes the user more productive. Domino Web Access also includes a virtual scroll bar for easier viewing of large lists and navigation within its components.

Server-based administration

Because Domino Web Access runs on Domino/Notes 7, administrators will find the same strong management tools they are accustomed to with the Web client.

Administrators can set mail quotas and enable archiving as they would with a normal Notes client.

For the user, advanced features such as delegating mail, calendar, and contacts are available, as is the ability to set time format display options and reset the HTTP password. Mail that has been read in Notes appears as read in Domino Web Access, and vice versa.

New features for WebMail users

Domino Web Access includes a wide range of new features that improve the user experience for WebMail users as well as a few enhancements that are not currently in the Windows-based Notes client.

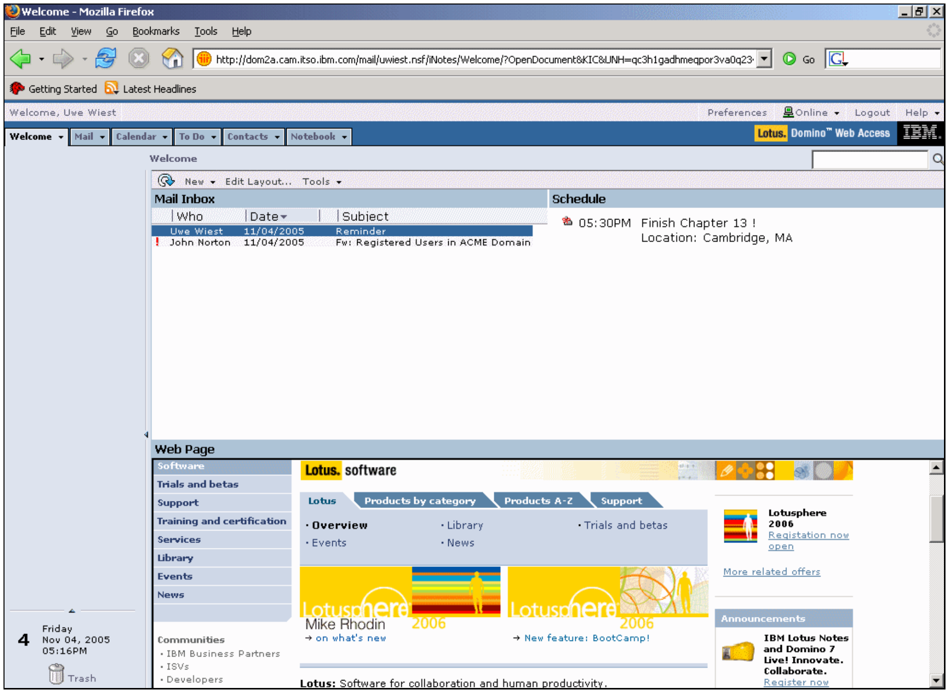
15.3 Domino Web Access activation

This section deals specifically with the activation of a mailbox using Domino Web Access.

15.3.1 Domino Web Access activation of a mailbox

To enable a user's mailbox to use Domino Web Access, simply replace the template of the user's mail database. Use the Domino Web Access (7) template for this purpose. After the change of template, the user's mailbox will be Domino Web Access enabled.

If everything was set up correctly you should see the result as shown in Figure 15-1.



http://dom2a.cam.itso.ibm.com/mail/uwiest.nsf/iNotes/Welcome/?OpenDocument&KIC&UNH=qc3h1gadhmeqpor3va0q23

	Who	Date	Subject
	Uwe Wiest	11/04/2005	Reminder
!	John Norton	11/04/2005	Fw: Registered Users in ACME Domain

05:30PM Finish Chapter 13 !
Location: Cambridge, MA

4 Friday
Nov 04, 2005
05:16PM

Lotus: Software for collaboration and human productivity.

Figure 15-1 Domino Web Access

16

Enterprise integration

This chapter discusses the installation of IBM Lotus Domino Enterprise Connection Services (DECS) as well as the Lotus Enterprise Integrator® (LEI). In addition, it discusses running each of them and offers some troubleshooting tips and techniques.

© Copyright IBM Corp. 2006. All rights reserved.

16.1 Domino Enterprise Connection Services

Domino Enterprise Connection Services (DECS) is an add-in task that is forms-based for easy setup. DECS provides the capability to integrate live data from enterprise systems (DB2, Oracle, Sybase, EDA/SQL, and ODBC).

The DECS add-in server task waits for user-initiated events, then passes them to the Domino Extensions Manager, which makes the query on behalf of the user. Results are then transparently returned to the user as if the Domino server had processed the transaction.

16.1.1 Installation

DECS is shown as an option during the IBM Domino 7 Server setup process. By checking this box you are telling the server to configure the notes.ini for DECS. If you would like to install DECS on a server that is already up and running, you only need to change a few things in the notes.ini. To configure the server to load DECS on startup, add the `decs task` to the `Servertasks=` line in the notes.ini:

```
Servertasks=Replica,Router,Update,Stats,AMgr,Adminp,Sched,CalConn,Event,htt
p,decs
```

Also add the following line at the end of the notes.ini:

```
EXTMGR_ADDINS=decsext
```

Tip: If the server returns an error such as `DECS: DECS Server Extension Manager library is not being initialized. Make sure the DECS Server is properly installed and the line 'EXTMGR_ADDINS=libdecsext.so' is in the notes.ini file`, and the `EXTMGR_ADDINS=` line appears to be correct, the path might not reflect the binary directory. In this case, either add the binary directory to the path of the Notes user (recommended), *or* specify the full path to the decs extensions. Typically, this would be the following line:

```
EXTMGR_ADDINS=/opt/lotus/notes/latest/sunspa/libdecsext.so.
```

16.1.2 Running DECS

To load DECS on the Domino server, simply type this at the server console:

```
load decs
```

The server responds with the message `Connection Server Started` along with the current date and time.

To shut down the DECS server, type this at the server console:

```
tell decs quit
```

The server console responds with the message `Connection Server Shutdown Complete` together with the current date and time.

16.2 Lotus Enterprise Integrator

IBM Lotus Enterprise Integrator for Domino (LEI) enables users to access data across multiple platforms. With LEI, users can work with corporate data, irrespective of where the data actually resides. This lets you leverage your existing store of company knowledge without having to port this information to a common platform or application. LEI consists of two major components, the LEI Server and the LEI Administrator. The LEI Server monitors the LEI Administrator database for LEI activities to execute. The LEI Administrator (a Notes application) lets users create activities and connections.

In this document we introduce some topics about LEI in a Solaris environment. This publication does not intent to be a main LEI resource. If you need more information about LEI, refer to:

`http://www.ibm.com/software/sw-lotus/products/product4.nsf/wdocs/enterpriseintegrator`

16.2.1 Installation

Installation of LEI on a Solaris server can be straightforward if you set up your environment properly. Be sure that all requirements of the install documentation are fulfilled accordingly.

Software prerequisites to install LEI 7:

- Solaris 10
- Notes 7 client to administer the LEI Administrator database
- Domino 7 server to manage the LEI Administrator database
- Client libraries of the external systems to be accessed must be installed on the LEI server machine as well as the Domino server machine, if separate.
- An X Window system server environment
- X Window system client libraries

Before you use the LEI installer, you must do the following:

- Ensure that Domino 7 is installed and running.
- Set the correct access controls in the names.nsf file (Domino Directory, formerly referred to as the Name and Address Book or NAB) on the Domino

server. See “Setting Access Controls in the Domino Directory” in the LEI installation guide for details.

- Establish the correct access rights in your Notes ID file. See “Establishing Access Rights in Your Notes ID File” in the LEI installation guide for details.
- Ensure that all needed environment variable are set and exported. See “Setting and Exporting Environment Variables” in the LEI installation guide and the following section in this chapter for details.
- Ensure that you have loaded and configured X Window system software. See “Configuring Screen Display for LEI Installation” in the LEI installation guide for details.
- If the Domino server on the system that you are installing LEI onto is running Domino Enterprise Connection Services (DECS), shut down the DECS service. DECS cannot be running when you install LEI.
- Share the Notes ID across applications.
- Ensure that the user ID of the user who is installing LEI is resident in the Domino Directory group LocalDomainAdmins; otherwise, LEI installation will fail.

Installation considerations

The following information is also useful when preparing to install LEI.

You do not have to uninstall past versions of LEI before installing the current Domino or LEI version.

The LEI Administrator, script vault, and data files should be backed up prior to uninstalling a previous LEI release or upgrading LEI to the current LEI release.

If you have a Beta or trial version of the current LEI release, the installation utility will detect it and you will be prompted to upgrade. If you choose to proceed with an upgrade, the LEI program files will be upgraded to the new version.

If DECS is installed, its activities are automatically upgraded during LEI installation.

LEI installation copies all LEI program files and updates the appropriate notes.ini file. The LEI Administrator database and other cluster databases are created on the specified Domino server. If you are installing into an existing cluster, the LEI Administrator is opened and an LEI configuration document is created for the new server.

If you configure the LEI server to run as an add-in task, it will start when you restart the Domino server.

Setting up environment variables

From our experience, most of the problems during LEI installations are related to environment variables not being set properly. This setup may vary, depending on your system configuration, but basically the .profile of the Solaris user that is running the Domino processes looks similar to Example 16-1.

Example 16-1 Domino user .profile

```
LOTUS=/opt/ibm/lotus; export LOTUS
LANG=C; export LANG
Notes_ExecDirectory=/opt/ibm/lotus/notes/70000/sunspa; export
Notes_ExecDirectory
LIBPATH=/opt/IBM/db2/V8.1/lib/:/opt/IBM/db2/V8.1/bin:/lib:/usr/lib:/notes/dom1a
:$Notes_ExecDirectory; export LIBPATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$LIBPATH; export LD_LIBRARY_PATH
DB2INSTANCE=db2inst1; export DB2INSTANCE
```

This .profile already includes the necessary paths to use LEI and connect to a DB2 server. The last line is used by the DB2 administration client in our example. This configuration should be modified to reflect the database that you want to connect to.

To enable the LEI to access the DB2 database, a DB2 client must be installed.

16.2.2 Running LEI

To load LEI on the Domino server, type the following line at the server console:

```
load leia

11/10/2005 09:53:08   LEI: Initializing Lotus Enterprise Integrator
11/10/2005 09:53:08   LEI:  (Release 7.0)
11/10/2005 09:53:09   LEI: LEI started
```

Also it is possible to include LEI to load at the server start, as a server task in the notes.ini file:

```
ServerTasks=Update,Replica,Router,AMgr,AdminP,CalConn,Sched,HTTP,IMAP,LDAP,
POP3, LEIA
```

The last item is from the ServerTasks, and it loads the LEI initialization script.

16.2.3 LEI Activities

The Lotus Connector for DB2 supports the following LEI activities:

- Direct Transfer
- Source/destination connections
- Destination metadata creation (Create Target Metadata)
- Command
- Archive
- Advanced RealTime (Virtual Documents and Virtual Agents), Virtual Fields, and DECS Real Time
- Create, Open, Update, and Delete events
- Replication
- Master and Target connections
- Scripted
- Polling
- Java

For more information about LEI activities, refer to “Enterprise Integrator for Domino (LEI) Activities and User Guide,” which you can find by clicking the line for your version number at the LEI support page:

`http://www.lotus.com/ldd/notesua.nsf/find/lei`

16.3 Troubleshooting

Troubleshooting LEI can be challenging because it involves several systems. Isolating the problem is usually the best approach to resolution. Some tools assist the Domino Administrator in checking for database connectivity, but there is not much information available, for example, in the case of network problems.

16.3.1 Using the dctest tool

You can verify the connectivity with your remote database system by using the **`dctest`** program supplied with Domino.

You can find the program in the Domino program directory /opt/ibm/lotus/notes/latest/sunspa.

From the Solaris user that is running the Domino processes, issue the command:

```
dctest
```

You can use the **dctest** tool to test connectivity with the following databases:

- Lotus Notes
- Oracle Server
- ODBC
- Sybase Server
- DB/2

After you choose the system that you want to test, you will be prompted for your user name, password, and host string.

This tool is useful for checking whether the library paths were set up correctly, or if the Domino user has access to these libraries. If **dctest** cannot find one of the required libraries, it will display an error message with the library name that could not be found.

To search for the library, you may use the UNIX **find** utility by issuing:

```
find / -name nameofthelibrary
```

Make sure those libraries are accessible by the Domino Solaris user as well as the shared libraries. Refer to 16.3.3, “Checking the shared library” on page 468.

The DCTEST must come back successfully for LEI to operate properly. If it does not, you must resolve any issues with your backend client before Domino can continue troubleshooting the issue.

16.3.2 Using the contest tool

You can verify the connector validity with your backend system using the **contest** program supplied with Domino.

You can find the program in the LEI program directory, by default in /opt/lotus/lei.

The **contest** tool is an additional testing program, similar in concept to the connector-specific test program LCTEST.

contest must be run with a running LEI server. It attempts to connect by using connections defined in the currently running LEI server’s Administrator database.

contest tests the ability to make a connection through the information found in the Connection document.

Log in with the user that is running the Domino processes to use the command. The syntax for using **contest** is as follows:

```
contest [-p] <connector1> <connector2>...<connectorn>
```

The -p option displays the connector properties.

For example, this command tests an Oracle connection as defined in LEI:

```
contest -p <Oracle connection name>
```

> **Tip:** Typing `contest` with no input parameters results in Help information being displayed.

16.3.3 Checking the shared library

Use the Solaris **ldd** command to determine whether the shared library can be loaded. The **ldd** command lists dynamic dependencies of executable files or shared objects. Example 16-2 shows the output from entering this command:

```
ldd /opt/IBM/db2/V8.1/lib/db2xbsa.so
```

Example 16-2 Output from the Solaris ldd command

```
libdb2e.so.1 =>  /opt/IBM/db2/V8.1/lib/libdb2e.so.1
        libm.so.1 =>     /usr/lib/libm.so.1
        libsocket.so.1 =>        /usr/lib/libsocket.so.1
        libnsl.so.1 =>   /usr/lib/libnsl.so.1
        librt.so.1 =>    /usr/lib/librt.so.1
        libdl.so.1 =>    /usr/lib/libdl.so.1
        libresolv.so.2 =>        /usr/lib/libresolv.so.2
        libaio.so.1 =>   /usr/lib/libaio.so.1
        libthread.so.1 =>        /usr/lib/lwp/libthread.so.1
        libkstat.so.1 =>         /usr/lib/libkstat.so.1
        libCrun.so.1 =>  /usr/lib/libCrun.so.1
        libCstd.so.1 =>  /usr/lib/libCstd.so.1
        libdb2install.so.1 =>    /opt/IBM/db2/V8.1/lib/libdb2install.so.1
        libdb2locale.so.1 =>     /opt/IBM/db2/V8.1/lib/libdb2locale.so.1
        libdb2g11n.so.1 =>       /opt/IBM/db2/V8.1/lib/libdb2g11n.so.1
        libdb2icuglue.so.1 =>    /opt/IBM/db2/V8.1/lib/libdb2icuglue.so.1
        libdb2osse.so.1 =>       /opt/IBM/db2/V8.1/lib/libdb2osse.so.1
        libdb2genreg.so.1 =>     /opt/IBM/db2/V8.1/lib/libdb2genreg.so.1
        libdb2trcapi.so.1 =>     /opt/IBM/db2/V8.1/lib/libdb2trcapi.so.1
        libdb2dstf.so.1 =>       /opt/IBM/db2/V8.1/lib/libdb2dstf.so.1
        libdb2dascmn.so.1 =>     /opt/IBM/db2/V8.1/lib/libdb2dascmn.so.1
        libc.so.1 =>     /lib/libc.so.1
        libmp.so.2 =>    /lib/libmp.so.2
        libmd5.so.1 =>   /lib/libmd5.so.1
        libscf.so.1 =>   /lib/libscf.so.1
```

```
libpthread.so.1 =>       /usr/lib/libpthread.so.1
libkvm.so.1 =>   /usr/lib/libkvm.so.1
libdb2osse_db2.so.1 =>   /opt/IBM/db2/V8.1/lib/libdb2osse_db2.so.1
libdoor.so.1 =>  /lib/libdoor.so.1
libuutil.so.1 =>         /lib/libuutil.so.1
libelf.so.1 =>   /lib/libelf.so.1
libm.so.2 =>     /lib/libm.so.2
/usr/lib/cpu/sparcv8plus/libCstd_isa.so.1
/platform/SUNW,Sun-Fire-V240/lib/libc_psr.so.1
/platform/SUNW,Sun-Fire-V240/lib/libmd5_psr.so.1
```

16.3.4 leiclean

A shell script is provided with LEI installations on Solaris platforms to clean up LEI resources following an abnormal termination of LEI. The shell script, named leiclean, is located in the LEI binary directory (/opt/lotus/lei by default).

It should be used with caution. It kills all LEI processes owned by the Solaris user who executes the shell script and frees all shared memory and semaphores currently in use by that user.

Use this script only after an abnormal termination of LEI. In addition to terminating all LEI processes, the removal of shared memory and semaphores could affect any other programs that are currently running under the same Solaris user ID. In particular, this includes the Domino server and any other Notes API programs that the same Solaris user ID is currently executing.

If you execute LEI and the Domino server under the same Solaris user ID (as you must to use RealTime), an abnormal termination by either process may halt the other.

17

Diagnostics and troubleshooting

When problems arise, the pressure is on to get the server back up and running smoothly. The best time to prepare for troubleshooting and data collection is before a problem has occurred. Having the correct data to provide to support when reporting a problem can significantly reduce the time to resolution. IBM Technical Support refers to a reported problem as a *Problem Management Record (PMR)*.

Before problems occur, it is helpful to have read or least be familiar with the information in the Domino documentation. You can download information about Domino 7 or view Help databases at:

`http://www.lotus.com/ldd/doc`

The goal of this chapter is to provide information about how to collect the appropriate data when reporting a PMR.

This chapter addresses three major topics:

- How to recognize when a problem is serious enough to open a PMR with IBM Technical Support. When opening a PMR, it is necessary to collect data to leverage the support resource most effectively. This chapter covers details about collecting the necessary data and transmitting it to IBM Technical Support.

© Copyright IBM Corp. 2006. All rights reserved.

- Steps that can be taken on the client side to quickly isolate and fix some common problems.
- The importance of implementing recovery procedures in your company. This includes providing some sample scripts that can be tailored to your environment.

Notes:

- The script provided in 5.7.4, “Shutting down from the Domino Administrator” on page 206” automatically shuts down the server. If the server hangs or crashes, the script will use `nsd` **-kill** to bring the server down and clean up after the abnormal shutdown. The log file can be found in the directory defined for nsd-logs (by default *Domino data directory*/IBM_TECHNICAL_SUPPORT).
- The location of the Domino binary directory and the Domino data directory are configurable on install. All examples in this chapter are presented with the assumption that the paths chosen in Chapter 5, “Installing Lotus Domino 7 on Sun Solaris 10” on page 77, were used. Change these paths as necessary to match your configuration.

17.1 General Lotus support procedures

In general, if you are having problems with your Domino server, you should open a call with Lotus support. The support center will be able to help you collect data to resolve your problem. The usual procedure is:

1. Collect data about the problem, which usually involves running the NSD tool (which we describe in 17.2, "The nsd and memcheck tools" on page 475).
2. Clean up the Domino partition that failed using the NSD tool with the -kill option.
3. Restart Domino.
4. Gather the requested information to Lotus support.

17.1.1 Packaging the files for Lotus support

This section describes the common procedures to package files for IBM Technical Support. By default, the NSD tool stores the nsd files in the *Domino data directory*/IBM_TECHNICAL_SUPPORT directory with names in the following format:

```
nsd_SUNSPA_user_yyyy_mm_dd@hh_mm_ss.log
```

where:

- `SUNSPA` indicates Sun SPARC version of Domino.
- `user` is the Solaris account name.
- `yyyy_mm_dd` is the date.
- `hh_mm_ss` is the time.

Using our first Domino partition on the first Sun server in our Redbooks Lab as the example:

- `/notes/dom1a/IBM_TECHNICAL_SUPPORT` is our nsd directory.
- `nsd_SUNSPA_dom1b_2005_11_16@14_49_56.log` is an example of an nsd file in the directory.

When installing the sample start/stop scripts from this book, you are asked what name you wish to use for the console output file. By default, the current console log will have the file name `coutput` in the Domino data directory. Also, the script will rename the console file so that when the server starts you will be able to retrieve past console output files. By default, these files are also in the Domino data directory and have a name in this format:

```
coutput.upto.dd.mm.yy-hhmm
```

In this sequence:

- `dd.mm.yy` is the date.
- `hhmm` is the time of day

The following commands show an example of creating a single tar file with the current console output and all of the nsd files, for the dom1a partition:

```
cd /notes/dom1a
tar cvf PMR_nnnn.tar coutput IBM_TECHNICAL_SUPPORT/nsd_*
```

This tars up the files to one file called `PMR_nnnn.tar`, which you can FTP to IBM Technical Support (Be sure to use binary mode to transfer the files.)

If you do not use the script in this book, look for the console.log file to supply to support. Each time the server is stopped and restarted, the previous console.log is renamed in the following format:

```
console_servername_yyyy_mm_dd@hh_mm_ss.log
```

For example:

```
console_dom1b_2005_11_17@14_51_30.log
```

If a memory dump was requested by support, look for the memory dump file in the following format:

```
console_servername_yyyy_mm_dd@hh_mm_ss.dmp

memory_dom1b_2005_11_11@14_31_10.dmp
```

If semaphore debug was requested by support, look for the semaphore output file in the format SEMDEBUG.TXT.

17.1.2 Transferring files to support

When a PMR is opened with IBM Technical Support, the support representative asks for the relevant diagnostic information that you have collected and tells you how to transmit the information to IBM into the Centralized Customer Data Repository. It is necessary to have a PMR to transfer data, as the PMR is used to track and find PMR data.

Details about using the IBM Centralized Customer Data Repository procedure are available online at:

http://www.ibm.com/de/support/ecurep/index.html

Data can be transferred via secure FTP with SSL/TLS or by way of an e-mail gateway.

17.1.3 Common mistakes seen by support

If you encounter problems when generating and sending files to IBM Technical Support, you may have made one or more of the following common errors:

- Not using binary mode to transfer the files via FTP.
- Running nsd with options (nsd -info for example) instead of nsd with no options.
- Running nsd -kill before running nsd with no options. nsd -kill kills Domino server without any data collected.

17.2 The nsd and memcheck tools

Notes System Diagnostic (nsd) is a script that gathers diagnostic information that can be used to troubleshoot problems and verify that the server is correctly configured. The nsd tool is included with the Domino server installation.

Overview of data collected by nsd and memcheck tools:

1. NSD header: Contains basic information about NSD and the Domino server it is being run on.
2. Notes Memory Analyzer: Contains basic information about Notes Memory Analyzer, such as memcheck and the Domino server it is being run on.
3. Notes Process Summary: Detailed process tree for Domino processes running on the Domino server instance.
4. Notes Process Info: Call stack listings, memory maps for all Domino processes running on the Domino server instance.
5. OS Process Table: Extended process table of the entire physical system.
6. Notes Memory Analyzer: Detailed command line used to launch memcheck including processes being analyzed.
7. Notes Memory Analyzer: Details about shared memory including maximum usage, shared handle usage, and top 10 shared memory blocks. Additional details on open database by process ID and thread ID as well as NSF Major Blocks, server information, file descriptor data, event data, semaphore data, the last 10 lines of the server console, static pool data, NIF collection data, per-process pool dump and top 10 private blocks, and virtual thread data.
8. IPC Data: Memory-mapped files and `ipcs` data.
9. System Information: System name, resource limits, swap information, system configuration, physical memory, processors, kernel information, load objects, tunable OS values, patches, vm stats, and /etc/system information.

10. Network Information - /etc/resolv.conf, /etc/nsswitch.conf, network kernel configuration, network routing, network memory, network connections.
11. Environment: Domino user shell environment, pid.nbf, mmap.nbf, mq.nbf, exec.nbf, and ini.nbf.
12. Directory Listings: Domino executable and library files and data directory listings.
13. Summary: Location of the nsd, length of nsd script run time, and generated information/warnings/errors.

17.2.1 Running nsd

You must be in the Domino partition's data directory to run nsd. You can run nsd as the Solaris user for that Domino partition or as root. For most problems, you will run the nsd as the Solaris user.

Many different options can be used with nsd to alter the type of information gathered.

Because nsd is constantly evolving and changing, new options may be added in the future. The -help option shows a complete list for the version of nsd you have installed:

```
/opt/ibm/lotus/bin/nsd -help
```

Example 17-1 shows the output from this command.

Example 17-1 nsd help

```
Usage: /opt/ibm/lotus/bin/nsd [options] [ core_file | pid ]

Options:

    -batch                 (run in batch mode -- don't write to tty)
    -info                  (just report system info)
    -noinfo                (don't report system info)
    -fs                    (report data directory file systems)
    -nofs                  (don't report data directory file systems)
    -nolog                 (don't log output to log file)
    -nodbx                 (don't collect process debug info)
    -ver*sion              (just show version header)
    -ps                    (show process tree)
    -stacks                (show process stacks only)
    -kill                  (kill all/user notes processes and cleanup IPCs)
    -memcheck              (run the Notes memory checker only)
    -nomemcheck            (don't run the Notes memory checker by default)
    -dumpmem               (generate shared memory dump)
    -lsof                  (run lsof only -- list Notes open files)
    -nolsof                (don't run lsof by default)
    -user <user_id>        (operate only on notes process run by 'user_id')
    -exec_path <dir[:dir]*> (add additional directories to the search path)
    -ins    <dir>          (specify an alternative Notes install directory)
    -help                  (show this help list)
    -help <option>         (where option is any one of the above)
    -help gen*eral         (general info about the script and how it works)
    -help lim*itations     (general info on script limitations)
    -help update           (list script version update info)
```

Notable options include:

- -kill

  Issuing nsd -kill kills all Notes processes and clean up IPCS resources related to those processes.

  Any time the server cannot be shut down with a graceful quit from the console or a server -q from the command line or the start/stop script, nsd -kill should be run to ensure that the environment is clean for server restart.

- -info

  The command nsd -info skips attaching to the processes with a debugger and obtaining a trace. This is useful when you are only gathering system information and do not need any process-level information for diagnosis.

Tip: You may want to run nsd -info for each Domino partition (while Domino is running) and print the resulting log file to document how your system is currently set up.

17.2.2 Running memcheck

Memcheck is a utility that primarily gathers information about the current state of the Domino memory pools. The data from memcheck is combined with the nsd output file if nsd is run without any optional flags. Memcheck gathers the following information:

- Details about shared memory including maximum usage
- Details about shared handle usage
- Top 10 shared memory blocks
- Open database by process ID and thread ID as well as NSF Major Blocks
- Server information
- File descriptor data
- Event data
- Semaphore data
- Last 10 lines of the server console
- Static pool data

- NIF collection data
- Per-process pool dump and top 10 private blocks
- Virtual thread data

The memcheck utility is run automatically by the nsd tool unless you use the -nomemcheck option with nsd. Attempt to run nsd with memcheck if possible as the resulting nsd will provide significantly more information for support to review.

The memcheck information is stored in a section of the nsd log file. By default, these logs are stored in Domino data directory/IBM_TECHNICAL_SUPPORT directory with names in the following format:

```
nsd_SUNSPA_user_yyyy_mm_dd@hh_mm_ss.log
```

In this sequence:

- `nsd` indicates this is an nsd log file.
- `SUNSPA` indicates Sun SPARC version of Domino.
- `user` is the Solaris account name.
- `yyyy_mm_dd` is the date.
- `hh_mm_ss` is the time.

Using our first Domino partition on the first Sun server in our Redbooks Lab as the example:

- `/notes/dom1a/IBM_TECHNICAL_SUPPORT` is our nsd directory.
- `nsd_SUNSPA_dom1b_2005_11_16@14_49_56.log` is an example of an nsd file in the directory.

The -memcheck option for nsd runs just the memcheck and stores the results in a memcheck log file in the same directory as the nsd log files. They are named in the following format:

```
memcheck_SUNSPA_user_yyyy_mm_dd@hh_mm_ss.log
```

In this format:

- `memcheck` indicates that this is a memcheck log.
- `SUNSPA` indicates Sun SPARC version of Domino.
- `user` is the Solaris account name.
- `yyyy_mm_dd` is the date.
- `hh_mm_ss` is the time.

For example, nsd -memcheck on our dom2b partition:

```
memcheck_SUNSPA_dom2b_2005_11_17@10_49_27.log
```

17.2.3 Enhancements to nsd/memcheck for D7

- New input arguments that show which pid/tid has faulted:

```
Input arguments : -batch -crashpid 18777 -crashtid 0 -wrapper
```

- The process that faulted is now listed first in the NSD log (but not the thread).
- Memory maps are now included for each process, depending on what the operating system provides. Solaris provides library and other memory address ranges:

```
<@@ Notes Process Info -> Process: http -> Memory maps for pid 18777 @@>
    18777:/opt/ibm/lotus/notes/70000/sunspa/http
    00010000       8K r-x--  /opt/ibm/lotus/notes/70000/sunspa/http
    00020000       8K rwx--  /opt/ibm/lotus/notes/70000/sunspa/http
    00022000    3960K rwx--    [ heap ]
    00400000   12288K rwx--    [ heap ]
    E4700000    1128K r-x--
/opt/ibm/lotus/notes/70000/sunspa/libftgtr40.so
    E497A000       8K rwx-R    [ anon ]
    E4980000    2216K r-x--
/opt/ibm/lotus/notes/70000/sunspa/liblsxbe.so
    FF800000    3584K rwx--    [ stack ]
    FFB80000      24K -----    [ stack ]
    FFB86000     488K rwx--    [ stack ]
```

- New to memcheck Boot Time:

```
Server Boot Time     = Fri Nov  4 14:49:48 2005
```

- The process and thread that triggered the crash is listed:

```
StaticHang = [    http:18777]/[    http:18777:   14] (0x4959/0x0/0xe)
```

- Last 10 Console Log messages will be in the nsd/memcheck output if DEBUG_OUTFILE is set in notes.ini.
- POSIX Message Queue Information: The Fault Recovery code in Domino 7 uses Posix Message Queues on Solaris instead of System5 Message Queues. Sys5 queues suffered from painfully low default values on Solaris so if you did not read the release notes and bump the values in the /etc/system file, then you usually got errors on Domino when you ran out of message queues. Posix Message Queues do not have this limitation. Unfortunately you cannot see them when you run an **ipcs** command, so a utility is shipped with Domino called posixq, which NSD uses to include the info in the log file:

```
<@@ IPC Data -> -- POSIX Message Queue Information -- @@>
PID Queue: /notes.dom1bPID
        mq_open returned 278288
        mq_msgsize is 16
        mq_maxmsg is 2048
        mq_curmsgs is 36
```

- A new **isa** command is included:

```
<@@ System Information -> Instruction Set Architecture @@>
64-bit sparcv9 kernel modules
```

17.3 Reviewing and using data from output files

In addition to collecting information for IBM Support, the Domino Administrator can find useful information in the nsd log. It is possible to find open databases by process, check the last lines of the server console, and even review shared memory specifics, among many other possibilities. The next three sections give examples of the type of information found in the nsd/memcheck output file.

17.3.1 Finding Open Databases in memcheck

One of the best features of the memcheck output is to show, for each Domino process/thread, which Domino databases are being used and what activity is being done on the database.

You have to search for the string `Open Databases` in the nsd and memcheck output file.

Example 17-2 shows the data found in the memcheck output file after searching for the string `Open Databases` from our dom1b partition, and Example 17-3 on page 481 shows the data found in the nsd output file after searching for the string `Open Databases` from our dom1b partition.

Example 17-2   Searching for Open Databases in dom1b using memcheck

```
<@@ ------ Notes Memory Analyzer (memcheck) -> Open Databases (Time 14:50:11)
------ @@>
../notes/dom1b/ddm.nsf
        Version    = 43.0
        SizeLimit  = 0, WarningThreshold = 0
        ReplicaID  = 0x852570a7:0x0a75e934
        bContQueue = NSFPool [  00022fa5]
        FDGHandle = 0xf02101b8, RefCnt = 4, Dirty = Y
        DB Sem     =  (FRWSEM:0x0244) state=0, waiters=0, refcnt=0, nlrdrs=0
Writer=[       :    0]
       SemContQueue ( RWSEM:#0:0x029d) rdcnt=-1, refcnt=0 Writer=[        :
0] n=0, wcnt=-1, Users=-1,  Owner=[
 :    0]

        By: [   event:18699:   14] DBH=    96, User=CN=dom1b/O=ACME
```

Example 17-3 Searching for Open Databases on dom1b using the nsd

```
###### thread 14/15 :: event, pid=18699, lwp=14, tid=14 ######
##################################
[1]  fcf40b68 pollsys  (0, 0, f92b13d8, 0)
[2]  fcedcea8 poll     (0, 0, 1388, 10624c00, 0, 0) + 7c
[3]  fd2fa464 unix_usleep (0, ff0390d0, ff28378c, 0, 4e200, 2710) + 44
[4]  fd283d38 OSStaticMem (2b7, fbc00000, fbc00000, fbc00000, 10, 2b70) + b58
[5]  fd281b64 OSStaticMemBeginInit (0, c176, 14, f92b196c, fd2cd5cc, 1deba44) +
a4
[6]  fd24d6b0 NotesSDKTData (0, 0, 103c, 8128, fbb294e0, 1044) + 30
[7]  fd24e304 AddInDayHasElapsed (1, ff0390d0, 2dc00, 56f18, d289c8, 2ddd8) + 4
[8]  00056f94 DDMBackgroundThread (f9d08ea4, 1, 38, 1, 1, f92b1e30) + bf4
[9]  fd2b1298 ThreadWrapper (fbb294e0, ff07a588, ff0390d0, 2c2d4, 0, 4c00) +
1d8
[10]  fcf3fd9c _lwp_start (0, 0, 0, 0, 0, 0)I
```

In the example, the event process is waiting for periodic events to happen to interact with the ddm.nsf database.

17.3.2 Finding the last lines of the server console file

In Example 17-4, the router process is already running.

Example 17-4 Router process running as shown in the memcheck file output

```
<@@ ------ Notes Memory Analyzer (memcheck) -> Last 10 Console Log Messages
(Time 14:50:11) ------ @@>

        11/04/2005 14:49:51   RnRMgr: Done validating schedule database
        11/04/2005 14:49:51   Mail Router is already running
        load router
        > 11/04/2005 14:49:51   LDAP Schema: Finished loading
        11/04/2005 14:49:51   LDAP Server: Started
        11/04/2005 14:49:51   Mail Router is already running
        load router
        > 11/04/2005 14:49:52   Mail Router is already running
```

17.3.3 Determining information about shared memory usage

In Example 17-5 on page 482, the running Domino instance had 73,984,946 bytes of total addressable memory allocated with 67,166,432 bytes of shared memory mapped. Of the 67,166,432 bytes of shared memory, 19,681,280 was in use by BLK_UBMBUFFER (the NSF Buffer Pool).

Example 17-5 Seeing the shared memory from the memcheck data

```
<@@ ------ Notes Memory Analyzer (memcheck) -> Shared Memory Analysis (Time
14:50:11) ------ @@>

Number of Shared Pools = 16
Number of Small Shared Pools = 9
SharedDPoolSize = 8126464
SmallSharedDPoolSize = 524288
Amount of memory allocated in all handle tables = 73984946
Amount of shared memory mapped from the system = 67166432

<@@ ------ Notes Memory Analyzer (memcheck) -> Memory Usage Summary -> Top 10
Shared Memory Block Usage (Time 14:50:11) --
---- @@>

BY SIZE

  Type  TotalSize    Handles    Typename
-----------------------------------------------------------
0x82cd   19681280          5  BLK_UBMBUFFER
0x834a    3145730          3  BLK_GB_CACHE
0x8a05    2520000          1  BLK_NET_SESSION_TABLE
0x8f57    1242714         19  BLK_ISERV_CONFIG_PARAMS
0x8f56    1242714         19  BLK_ISERV_CONFIG_RECORDS
0x826c    1111902         17  BLK_EXTMGR
0x826d    1048576          1  BLK_NSF_DIRMANPOOL
0x8252    1048576          1  BLK_NSF_POOL
0x8311    1048576          1  BLK_NIF_POOL
0x8a08    1048576          1  BLK_SESSION_POOL
-----------------------------------------------------------
BY HANDLE COUNT

  Type    Handles  TotalSize    Typename
-----------------------------------------------------------
0x8604        194       2392  BLK_TEXTLIST
0x8439        165     152718  BLK_BPOOL_PERPROCESS_INFO
0x841c        155     205140  BLK_VARRAY_CHUNK
0x841b        154       4936  BLK_VARRAY
0x8405         74       5402  BLK_IDTABLE
0x8100         67      76782  BLK_OS_NAME
0x8301         34      25406  BLK_FORMULA
0x82d2         28      28728  BLK_BUCKETDESCPAGE
0x8438         26      12516  BLK_BPOOL_SHARED_INFO
0x8321         24       5584  BLK_COLLECTION_GROUP
```

17.4 Showing the memory dump

The server console command **show memory dump** can be used to report data about shared memory, semaphore usage, and private memory. The file generated by the server console command is in this format:

```
memory_dom1b_2005_11_17@15_22_00.dmp
```

This is an overview of data collected in the memory dump file:

- Dump of Shared Handle Table: Lists shared handles by block ID and size.
- Dump of Shared Pools: Dump of usage statistics for shared memory pools.
- Quickpool Dump: Dumps usage statistics of Quickpools.
- Number of shared pool allocations per request size.
- Number of DPool allocations per block type.
- Dump of Shared Semaphore Table: Allocated semaphores by type and process ID, summary of semaphore usage.
- Dump of Handle Table for ProcessID: Per-process listing of private handles by block ID and size.
- Dump of Pools for ProcessID: Per-process dump of usage statistics for private memory pools.
- LotusScript Memory Usage for Process: Per-process dump of LotusScript memory usage if the process uses LotusScript.

17.4.1 Reviewing data in the memory dump file

This section reviews some of the data in the memory dump.

Memory utilization

The data contained in the Dump of Shared Pools and Dump of Pools for ProcessID provides interesting data about how much memory Domino is using. Low values for pool utilization (less than 50%) for large amounts of memory (greater than 1 GB for shared memory) can indicate potential memory fragmentation.

Example 17-6 Dump of Shared Pools

```
16 system shared memory pools
58 MB total pools size
46 MB total pools used

79.96% pool utilization
1.48 pools visited per allocation
```

```
     0.47 pools skipped
     1.02 pools searched
1.23 free blocks searched per allocation
1.28 free blocks searched per free
```

Reviewing semaphore data in the memory dump file

The information in the section titled “Dump of Shared Semaphore Table” provides an overview of the semaphore usage of the Domino Server instance.

Example 17-7 Dump of Shared Semaphore Table

```
SEM       #     Type  Package Name     Event  ProcessID
SEM       1   0x4117  PKG_0x1+23         n   0x000063DF
SEM       2   0x4117  PKG_0x1+23         n   0x000063DF
SEM       3   0x4124  PKG_0x1+36         n   0x000063DF
SEM       4   0x4144  PKG_0x1+68         n   0x000063DF
...
SEM     342   0x3A48  PKG_0x3A+72        y   0x000064DE
SEM     343   0x3A48  PKG_0x3A+72        y   0x000064DE
SEM     344   0x3A4C  PKG_0x3A+76        y   0x000064DE
SEM     345   0x3A49  PKG_0x3A+73        y   0x000064DE
SEM     346   0x4117  PKG_0x1+23         n   0x00006617
SEM     347   0x0429  PKG_0x4+41         y   0x00006617
SEM     348   0x034D  PKG_0x3+77         y   0x00006617
SEM     349   0x034E  PKG_0x3+78         y   0x00006617

Summary:
Total Semaphores Allocated=350
Total Active Semaphores=349
Total Event Semaphores=247
Total Non-Event Semaphores=102
```

17.4.2 Using data in the memory dump file for further investigation

If, after reviewing a memory dump, there is a block ID that appears to be used frequently, the block might be leaked (allocated and never freed). To determine whether a block is being leaked, debug trapleaks can be used. See 17.8.3, “Using Debug_Trapleaks to look for potential memory leaks” on page 508.

17.5 Solaris Operating System tools

Solaris 10 has a variety of tools that both the customer and support find useful.

17.5.1 Solaris snoop tool

There is a useful tool on Solaris called **snoop**, which is used to capture and inspect network packets.

- To see which information at the network level your Domino server is receiving, enter the command:

  ```
  snoop -d device -o filename
  ```

  device is the network interface name (for example bge0 on our lab machines), and *filename* is the output file.

- To read a file created by **snoop** use the -i option and redirect the output to a text file:

  ```
  snoop -i ./filename > filename.txt
  ```

- You can also capture the packets coming from a specific node on your network by adding the IP address to the command in this way:

  ```
  snoop -d device -o filename ip_address
  ```

  For example, to use **snoop** to capture only the packets coming from a Notes client that has IP address 9.33.88.39:

  ```
  snoop -d bge0 -o n7_client_test 9.33.88.39
  ```

- Process and display the information with the following commands:

  ```
  snoop -i n7_client_test > n7_client_test.txt
  more n7_client_test.txt
  ```

  In this case you should see the following lines in your output file, where D=1352 is the destination port of the Domino server and S=2101 is the port number of the client. This example shows five packets:

  ```
  1   0.00000   9.33.88.39 -> dom1a       TCP D=1352 S=2101 Push
  Ack=3033838779
   Seq=1578610597 Len=18 Win=16082
  2   0.00239        dom1a -> 9.33.88.39   TCP D=2101 S=1352 Push
  Ack=1578610615
   Seq=3033838779 Len=50 Win=49640
  3   0.00070   9.33.88.39 -> dom1a       TCP D=1352 S=2101
  Ack=3033838829 Seq=
  1578610615 Len=0 Win=17520
  4   0.17285   9.33.88.39 -> dom1a       TCP D=1352 S=2101 Push
  Ack=3033838829
   Seq=1578610615 Len=140 Win=17520
  ```

```
5   0.00108        dom1a -> 9.33.88.39   TCP D=2101 S=1352 Push
Ack=1578610755
 Seq=3033838829 Len=296 Win=49640
```

> **Note:** You must be in the root to use the **snoop** command.

The **snoop** command can provide a lot of information. For further details, see the product documentation.

17.5.2 ping

The **ping** tool is largely used to check server connectivity. It uses the ICMP protocol to check whether a target server is alive. Relaying only on **ping** can be a little dangerous, because between the servers a router or firewall can exist that does not let ICMP packager flow through. In this case the packages will not reach the target server and you will receive a time-out message exactly equal to the one you would receive if the server were down or unreachable for some reason.

This is the syntax:

```
ping hostname/ip_address
```

17.5.3 traceroute

traceroute is used to map routing problems. It prints the nodes that a connection has to go through to reach a target server or host. It relays on UDP protocol by default, but ICMP can be used as an alternative.

This is the syntax:

```
traceroute hostname/ip_address
```

17.5.4 nslookup

nslookup is largely used to diagnose name resolution problems. Issue this command from the problem server to check whether it is capable of resolving the target host or server name. You can also use **nslookup** to consult DNS tables for MX hosts within domains.

This is the syntax:

- Checking a host name IP address:

  ```
  nslookup hostname
  ```

- Checking an IP address assigned name (requires that a reverse DNS feature be configured in the DNS server):

  ```
  nslookup ip_address
  ```

- Starting nslookup shell:

  ```
  nslookup
  ```

At this point, you can type in the server host name in order to resolve the DNS name. You can also check on the MX of a domain using the nslookup shell and issuing this command:

```
set type=mx
```

When you type in a server host name, you are presented with the mail servers that are responsible for receiving the message at the desired domain.

17.5.5 telnet

telnet is a remote terminal client, and it is handy because it enables you test connectivity at the application layer. In our case, we check whether a specific port at the target server is accessible. This is useful when you have connectivity problems and ICMP is blocked across the network segment.

This is the syntax:

```
telnet hostname/ip_address port
```

17.5.6 netstat

This tool shows the network status, varying by the options you choose. You can check which ports are being used and which hosts are connected to the listening port. For more information, in the shell, type **man netstat**.

17.5.7 Route

Route helps you check the routing tables from a given server and manually manipulate the tables when needed. For more information, in the shell, type **man route**.

17.6 Troubleshooting Domino availability problems

Availability problems typically are evidenced by a server that eventually gets the job done but is far slower than anticipated. Other availability problems, crashes, and hangs are identical from an end-user perspective, because the client in every case will fail to establish a connection with the server.

Depending on the source of the problem, the type of information that leads to resolution can vary widely. Refer to Chapter 6, “Tuning and monitoring Domino servers on Solaris” on page 207 for details about tuning and monitoring your server.

17.6.1 Domino outages and automation to manage failures

This section outlines Domino crashes and hangs along with suggested diagnostics and remedies. It also discusses automation that will help you to better manage failures. Additionally, the Setting Up Fault Recovery and Automatic Data Collection features are covered, as well as using the semaphore debugging tools.

Domino crash

When Domino detects a situation that should not occur, it is designed to call “Panic,” also referred to as a server crash. The purpose of panic is twofold: to collect data and to prevent further problems by stopping Domino when an unknown state has happened. When Panic has been called, an error message appears with text describing the condition. On Solaris the signal handler picks up that panic has happened. The signal handler can be used to control the data collection and server recovery via a tool referred to as Fault Recovery.

Example 17-8 Sample crash as reported to the server console and corresponding NSD

```
[18077:00077-00075]  Thread=[18077:00077-00075]
Stack base=0xF1C20540, Stack size = 11160 bytes
PANIC: OSUnlockWriteSem: Unlocked a write sem that was not mine!
[18077:00077-00075] F9749DC4
/local/ibm/opt/lotus/notes/70000/sunspa/libnotes.so! OSFormatStackFrame +0x83c
F974948C /local/ibm/opt/lotus/notes/70000/sunspa/libnotes.so! OSWalkStack
+0x15c
F97428EC /local/ibm/opt/lotus/notes/70000/sunspa/libnotes.so! Panic +0x434
F96CD01C /local/ibm/opt/lotus/notes/70000/sunspa/libnotes.so! OSUnlockWriteSem
+0xd4
F973D154 /local/ibm/opt/lotus/notes/70000/sunspa/libnotes.so! OSLoadProgramExt
+0xcc4
F974C038 /local/ibm/opt/lotus/notes/70000/sunspa/libnotes.so!
PSGetDominoProcessInfo +0x1628
```

```
F974B2C8 /local/ibm/opt/lotus/notes/70000/sunspa/libnotes.so!
PSGetDominoProcessInfo +0x8b8
00127400 /local/ibm/opt/lotus/notes/70000/sunspa/server! PSMain +0x108
0012EB38 /local/ibm/opt/lotus/notes/70000/sunspa/server! PlatformStatsTask
+0x740
0002EBAC /local/ibm/opt/lotus/notes/70000/sunspa/server! Scheduler +0x89c
F970697C /local/ibm/opt/lotus/notes/70000/sunspa/libnotes.so! OSProcessIsGUI
+0x304
Stack base = 0xf1c20540, Stack size = 12936 bytes
Fatal Error signal = 0x0000000b PID/TID = 18077/75
7/21/2004 2:23:8  Running NSD
```

Example 17-9   NSD snippet from the same crash

```
##################################
###### thread 74/78 :: server, pid=18077, lwp=75, tid=75 ######
###################################
[1]  f939dc8c read     (0, f1c1d1bc, 100)
[2]  f8f5dd88 read     (0, f1c1d1bc, 100, 67000000, 6700, f939ef2c) + 5c
[3]  f96c339c OSFatalTermination (1, 0, 0, 5400, fb873148, f939ef2c) + 254
[4]  f96c3104 fatal_error (b, f1c1d8d0, f1c1d618, 0, 0, 0) + 2d4
[5]  f8f65fec __sighndlr (b, f1c1d8d0, f1c1d618, f96c2e30, 0, 0) + c
[6]  f8f5fdd8 call_user_handler (b, f1c1d8d0, f1c1d618, 0, 0, 0) + 234
[7]  f8f5ff88 sigacthandler (b, f1c1d8d0, f1c1d618, f93bc000, 0, 0) + 64
[8]  --- called from signal handler with signal 11 (SIGSEGV) ---
[9]  f939e694 _lwp_kill (b, fb6db894, fb6d4230, f1c1e140, f1c20540, 2b98) + 8
[10]  f9742b40 Panic    (fb6d4230, 0, 25378, f8f5dacc, 0, f939ef2c) + 688
[11]  f96cd01c OSUnlockWriteSem (f7eb81e4, 67, f1c1e3b4, 100, f1c1e720,
f7ebf9c4) + d4
[12]  f973d154 OSLoadProgramExt (f1c1ed22, 0, 0, 4, f1c1fb98, f974b3d0) + cc4
[13]  f974c038 SolarisProcessStats (f333c468, f1c1fc0a, 2c899c, 2, f06, 1de708)
+ b48
[14]  f974b2c8 PSGetDominoProcessInfo (f333c468, f1c1fc8c, ff, 100, 0, 0) + 8b8
[15]  00127400 PSMain   (f333c468, f1c1fe28, 3, 174348, f1c1fe28, 37) + 108
[16]  0012eb38 PlatformStatsTask (f1c1fecc, f1c1fec8, f1c1ff0c, 0, 0, 0) + 740
[17]  0002ebac Scheduler (0, 0, 0, 0, 0, 0) + 89c
18]  f970697c ThreadWrapper (0, 0, 0, 0, 0, 0) + 2d4
[19]  f8f65c94 _lwp_start (0, 0, 0, 0, 0, 0)
###################################
```

Domino hang

A hang occurs when the Domino instance becomes unresponsive. The period of time that the Domino instance remains unresponsive depends on the severity of the hang. A hang could last a minute or two, several minutes, more than a hour, or, in an extreme case, the server will not recover.

In situations where a hang lasts minutes, the best approach to take is to use the semaphore debugging tools that are built in to Domino. These tools are covered in 17.8, “Troubleshooting techniques, tools, and tips” on page 502.

If the server outage lasts an unreasonable amount of time, specific steps should be taken to manually collect data from the server.

If a hang occurs when shutting down the server, the “Monitoring server shutdown” can be set up before the event to ensure data collection.

Fault recovery

The fault recovery system automates the job of gathering information from, cleaning up, and restarting the faulted server. Fault recovery enables a server to clean itself up from several different failures and then restart itself.

The general idea is that by recovering the faulted server quickly, end users will not notice that the server has been down. This minimizes server downtime and reduces Notes administration. Each fault is logged to a file. At the time of a fault, user-defined actions can be invoked through a user-defined external script, which is also known as the cleanup script. With both fault recovery and cleanup scripting implemented, customers can minimize downtime and maximize data collection painlessly.

Monitoring server shutdown

Domino’s Shutdown Monitor task ensures that Domino terminates when requested to do so; that is, the server does not hang while attempting to shut down. When you request a server shutdown, the System Monitor task monitors the shutdown activity. If no activity occurs for a specified amount of time, Domino automatically acts as though the server has crashed and takes appropriate action, including collecting data about the state of the server and then terminating the server. An NSD log is generated before the server terminates.

Automatic Diagnostic Data Collection Tool

In addition to being able to automate server restart, the Domino administrator can automate data collection in the Domino environment with the Automatic Diagnostic Data Collection Tool, also known as Automatic Data Collection (ADC).

This tool collects diagnostic data after server and client crashes and sends the collected data to a mail-in database when the server or client restarts. You can then use the collected data to determine the cause of the crash. Data is stored in Fault Report documents. A single mail-in database should be used to cover each domain. You can store all of the Fault Report documents from all client and server crashes in a domain in one database, or you can create one database for server crashes and one database for client crashes. You specify the mail-in database when you set up this feature. The collected data from client crashes can be sent to the customer's local Automatic Data Collection databases, enabling customers to quickly identify duplicate problems encountered at their site, or the data can be sent to the same database as the server data.

ADC helps eliminate the instances where an Administrator or user may not be able to capture the proper data on a client or server crash.

17.6.2 Setting up and using fault recovery

You can set up fault recovery to automatically handle server crashes. When the server crashes, it shuts itself down and then restarts automatically, without any administrator intervention. A fatal error such as an operating system exception or an internal panic terminates each Domino process and releases all associated resources. The startup script detects the situation and restarts the server. If you are using multiple server partitions and a failure occurs in a single partition, only that partition is terminated and restarted.

Domino records crash information in *Domino data directory*/IBM_TECHNICAL_SUPPORT. When the server restarts, Domino checks to see whether it is restarting after a crash. If it is, an e-mail is sent automatically to the person or group in the "Mail Fault Notification to" field. The e-mail contains the time of the crash, the server name, and, if available, the FAULT_RECOVERY.ATT file, which includes additional failure information from an optional cleanup script.

The fault-recovery system is initialized before the Domino Directory can be read. During this initialization, fault-recovery settings are read from the notes.ini file, and later read from the Domino Directory and saved back to the notes.ini file. Any changes to the Domino Directory or the notes.ini file become effective when the Domino server is restarted. To disable the reading of the Domino Directory and subsequent update to the notes.ini file, use the notes.ini setting `FaultRecoveryFromIni=1`.

Operating systems and fault recovery

Because fault recovery runs after an exception has occurred, it cannot rely on Domino's internal facilities. Instead, fault recovery makes heavy use of operating system features.

Enabling fault recovery

1. From the Domino Administrator, click the **Configuration** tab, and expand the **Server** section.
2. Open the Server document, click **Edit Server**, and click the **Basics** tab.

3. In the Fault Recovery section, check **Automatically Restart Server After Fault/Crash Enabled**.

Specifying a cleanup script for fault recovery

You can create an optional script that runs before any other cleanup takes place. Use the FAULT_RECOVERY.ATT file to collect the information from the script.

1. From the Domino Administrator, click the **Configuration** tab, and expand the **Server** section.
2. Open the Server document, click **Edit Server**, and click the **Basics** tab.
3. In the Fault Recovery section, complete the fields in Table 17-1.

Table 17-1 Information needed for fault recovery cleanup script

Field	Action
Run This Script After Server Fault/Crash	Enter the entire script name, including any extensions. Do not try to enable NSD from this field. **Note:** Directory separators (slashes) in the file name portion are converted for the operating system, but slashes in optional arguments are not converted.
Run NSD To Collect Diagnostic Information	Enable this field to activate NSD when there is a fault or crash.
Cleanup Script/NSD Maximum Execution Time	Enter the number of seconds for the cleanup script to run. Default is 300 seconds (5 minutes). Maximum is 1800 seconds.
Maximum Fault Limits	Enter the number of restarts allowed during a specified time limit — for example, 3 crashes within 5 minutes. If the number of crashes exceeds the time limit, the server exits without restarting.
Mail Fault Notification to	Enter a user or group name. When the server restarts, Domino checks if it is restarting after a crash and sends e-mail to the person or group.

Using transaction logging for recovery

Transaction logging is an integral part of recovering from system and media failures. Using transaction logging provides insurance against system failure, but creating regular backups is essential so that you can recover data after a failure.

System failure recovery

A system failure causes the server to stop and requires you to restart the server. During restart, Domino automatically performs database recovery. The system uses the transaction logs to apply full transactions and undo partial transactions that were not written to disk for databases that were open during the system failure. When you restart a server after a system failure, Domino automatically restores the affected databases.

Media failure recovery

A media failure causes databases to be damaged or lost. To recover, you use the third-party backup utility to restore database backups and transactions from the transaction log files. The backup utility you choose must use the backup and recovery methods of the Domino C API Toolkit (Release 5 or later).

17.6.3 Automatic Diagnostic Data Collection Tool

Fault Analyzer is a server add-in task that processes all new crashes as they are delivered to the Automatic Data Collection mail-in database. For each new crash, the Fault Analyzer task searches the database containing the Fault Report documents and determines whether the stack matches a crash that has already been seen by a user or server at that customer site. The Automatic Data Collection database lists all Fault Reports, as well as Response documents for any duplicate occurrences of the same crash, and indicates whether the duplicate occurrence is an exact match or a partial match of the original crash. The duplicate occurrences response documents are the Exact Match Fault Report and the Partial Match Fault Report documents. The Partial Match Fault Report document also includes a percentage match that indicates the percentage of the report that matches the original Fault Report for the crash.

Use the fields on the Diagnostics tab of the Server Configuration Settings document to specify whether the Fault Analyzer task is enabled on a server. When Fault Analyzer is enabled, at server startup, Domino reads the Server Configuration Settings documents and desktop policy documents in the local Domino Directory. If any document has a Fault Reports database specified, Domino determines whether the database resides on the local server and, if so, Domino adds it to its list of databases to monitor. Every 10 seconds the process determines whether the data modified time of any of the monitored databases has changed and, if so, Fault Analyzer scans for new unprocessed documents to try to match.

An occurrence count and unique ID count are updated in the parent Fault Report document for the crash. The occurrence count is the total number of times a crash has occurred; the unique ID count is the number of clients and servers on which that problem has been reported.

The Administrator section of the Fault Report document contains a Resolved field that you can use to mark a crash as resolved for all versions of clients and servers reporting to the database, or resolved for specific versions that you identify by release level (for example, Domino Notes 6.5.1) or by hot fix numbers (for example, 652HF10).

When a fault is marked as resolved, clients and servers that crashed with the same signature and that are at a version level for a fault that is to be resolved are not marked as a duplicate. Instead, the Fault Report document is kept as a parent document. The views display a check mark next to resolved documents.

The following files that were previously stored in the Domino data directory are now stored in the diagnostics directory, IBM_TECHNICAL_SUPPORT, located in the Notes/Domino data directory:

```
nsd output
memcheck output
core files
memory dump files (created in the format memory_<platform>_<machine
name>_<date>@<time>.dmp instead of memory.dmp)
notes_child_pid
```

To prevent the diagnostic files from becoming quite large and using a significant amount of disk space, you can specify the number of days that these files can be stored before they are deleted by the automatic diagnostic collection tool.

Setting up automatic diagnostic data collection on the server

Use the Server Configuration document to set up automatic diagnostic data collection on the server. You can also enable or disable Fault Analyses from this same tab on the Server Configuration Settings document.

1. From the Domino Administrator, click the **Configuration** tab.
2. Click **Server** → **Configurations**.
3. Select the Server Configuration document you want to edit and click **Edit Configuration**.
4. Click the **Diagnostics** tab and complete the fields shown in Table 17-2.

Table 17-2 Automatic diagnostic data collection (server) setup fields

Field	Action
Mail-in Database for diagnostic reports	Click in this field, then select the mail-in database to which you want the diagnostic report for server crashes mailed. Click **OK**.
Maximum size of diagnostic message including attachments (in MB)	Enter the maximum size of the entire message that automatic diagnostic data collection will create, including all attachments — NSD, console output, user defined files, and so forth.

Field	Action
Maximum size of NSD output to attach (in MB)	Enter the maximum size of the NSD log that can be attached to the document created by automatic diagnostic data collection. (Automatic diagnostic data collection collects data and then creates documents in a mail-in database.)
Maximum amount of console output file to attach in (KB)	Use the default value of 10240, or enter another value between 10 MB and 1 KB. 10240 is the upper limit. This value represents the portion of the CONSOLE.LOG file to be sent, beginning with the end of the file and moving toward the beginning.
Diagnostic file patterns	Enter a file name pattern that Domino will search for. If the pattern is located and it is listed in the file, DIAGINDEX.NBF, the file will be attached to the message that is sent to the mail-in database. DIAGINDEX.NBF contains all of the files associated with the crashing instance of the client or server. For example, this is a file pattern: addin_log*.txt. These files would be located based on that pattern: addin_log1.txt, addin_log_2004_11_23@16_21_20.txt, and so forth.
Remove diagnostic files after a specified number of days	Choose one of these: No (Default): Never automatically delete the diagnostic files created on the server. Yes: Enter the number of days after which the diagnostic files on the server are to be deleted. Displays the field `Number of days to keep diagnostic files`.
Number of days to keep diagnostic files	Accept the default value of 365 days, or enter another value representing the number of days after which the diagnostic files are to be deleted from the server. (This field displays only if you chose Yes for “Remove diagnostic files after a specified number of days.”)

Setting up automatic diagnostic data collection on clients

Use the desktop policy settings document to set up automatic diagnostic data collection on clients. If you have already created a desktop policy settings document, open that document and complete the fields on the Diagnostics tab. If you have not already created a desktop policy settings document, complete the entire procedure to create the document. See “Creating a desktop policy settings” in Lotus Domino Administrator 7 Help.

Options on the policy document for ADC

On the Diagnostics tab, if you want to enable automatic diagnostic collection on clients, complete the fields in Table 17-3 on page 496.

Table 17-3 Automatic diagnostic data collection (client) setup fields

Field	Action
Mail-in database for diagnostic reports	Click the arrow in the field, select the database to which the diagnostic reports from client crashes are to be mailed, and click **OK**.
Prompt user to send diagnostic report	Choose one of these: Yes: (Default) Prompt the user whether to send a diagnostic report to the mail-in database after a client crash. No: Make this feature transparent to the user. The diagnostic report is automatically sent to the mail-in database by a background process.
Prompt user for comments	Choose one of these: Yes: Display to the user a message box for entering information as to what they were doing when the client crashed. Choose Yes only if you chose Yes in the "Prompt user to send diagnostic report" field. No: Choose No to prevent the user from entering any comments.
Amount (in KB) of diagnostic output file to send	Use the default value of 10240, or enter another value between 10 MB and 1 KB. 10240 is the upper limit. This value represents the portion of the CONSOLE.LOG file to be sent, beginning with the end of the file and moving toward the beginning of the file.
Diagnostic file patterns	Enter a file name pattern that Domino will search for. If the pattern is located and it is listed in the file DIAGINDEX.NBF, the file will be attached to the message that is sent to the mail-in database. DIAGINDEX.NBF contains all of the files that are associated with the crashing instance of the client or server. For example, this is a file pattern: addin_log*.txt. These files are located based on that pattern:addin_log1.txt, addin_log_2004_11_23@16_21_20.txt, and so forth.
Remove diagnostic files after a specified number of days	Choose one of these: No: (Default) Never automatically delete the diagnostic files on the client. Yes: Choose Yes to enter the number of days after which the diagnostic files are to be deleted from the client. Displays the field "Number of days to keep diagnostic files."
Number of days to keep diagnostic files	Accept the default value of 365 days, or enter another value representing the number of days after which the diagnostic files are to be deleted from the client. (This field displays only if you chose Yes for "Remove diagnostic files after a specified number of days.")

17.6.4 How to research whether a crash or hang has been fixed

Go to this Web page:

http://www.ibm.com/developerworks/lotus

In the center column Support section, click **Lotus Software Fix Lists**. On the Fix Lists page, click **Lotus Notes/Domino**. From here, click **Notes/Domino Fix List**.

Expand the release of interest and the area of interest (for example, **6.5.4** and **Server**). You may have to click the Next link at the bottom of the pane to see all subject areas.

Under Server, a list sorted by SPRs (Software Problem Reports) shows one-line descriptions, such as:

```
JNON6B2QWG This fix prevents an intermittent session hang on Solaris. A
workaround to this problem is to reboot the Domino server to free the
session. ...
```

Clicking the SPR number provides more detail, including references to technotes. Click the **Technote** tab for detailed public information about the problem reported in the SPR:

```
Domino 6.x on UNIX has idle user sessions that hang and cannot be dropped

Technote (FAQ)

Problem:
Intermittently the Domino UNIX 6.x server has idle user sessions that hang
and cannot be dropped. The Administrator must reboot the Domino server to
free the hung user. When the customer runs the "show user debug", the
session is present. Attempting to drop the user from the Admin client
fails; it also fails when issuing a "drop all" from the server. The
customer has the following parameters in the Notes.INI:
Server_MaxSessions=
Server_Session_Timeout=

Solution:
This issue was reported to Quality Engineering as SPR# JNON6B2QWG and has
been fixed in Domino 6.5.4 Fix Pack 1 (FP1).
Excerpt from the Lotus Domino Release 6.5.4 Fix Pack 1 fix list (available
at http://www.ibm.com/developerworks/lotus):
Server
SPR# JNON6B2QWG - This fix prevents an intermittent session hang on
Solaris. A workaround to this problem is to reboot the Domino server to
free the session.
Refer to the following document on the Upgrade Central site for details
about the fix pack, and how to obtain it:
```

```
Upgrade Central: Planning your upgrade to Lotus Notes/Domino 6.0.5 and
6.5.4, including Fix Packs (# 1201845)

Related information:
Severe Performance Slowdown on IOCP on Endp_AcquireToke
```

17.7 Maintaining the Domino environment

To prevent problems on the Domino server instances, it is important to schedule daily, weekly, and monthly maintenance. The following section highlights necessary tasks to keep the Domino environment running smoothly.

17.7.1 Server maintenance

As a Domino administrator, a major part of your job is maintaining each server that you administer. Be sure that:

- The server is backed up regularly.
- Users can access the server quickly and consistently.
- Mail is routed properly.
- Administration Process requests are carried out.
- Databases are replicating correctly.
- Server hardware is functioning.

Server maintenance checklist

Table 17-4 lists the server maintenance tasks that you should complete daily, weekly, or monthly to ensure that a server runs efficiently.

Table 17-4 Server maintenance tasks

Task	Frequency
Back up the server	Daily, weekly, monthly
Monitor mail routing	Daily
Run Fixup to fix any corrupted databases [a]	At server startup and as needed[a]
Monitor Administration Requests database (ADMIN4.NSF)	Weekly
Monitor databases that need maintenance	Weekly
Monitor replication	Daily

Task	Frequency
Monitor modem communications	Daily
Monitor memory	Monthly
Monitor disk space	Daily, weekly, monthly
Monitor server load	Monthly
Monitor server performance	Monthly
Monitor Web server requests	Monthly

a. If the database is in Domino 5 or later format and you are not using transaction logging, you can use the Fixup task to repair the corrupted database. If the database is in Domino 5 or later format and you are using transaction logging, you cannot run the Fixup task on that database, because the Fixup task interferes with the way transaction logging keeps track of databases. Instead, you must restore the corrupted database from a backup.

17.7.2 Database maintenance

This section outlines some of the database maintenance tasks that help to keep databases in good working order.

Scheduling regular database tasks

Table 17-5 lists tasks that should be a regular part of database maintenance.

Table 17-5 Database maintenance tasks

Task	Frequency
Monitor replication, if a database replicates	Daily
Check for and consolidate replication or save conflicts	Daily for large active databases; weekly for other databases
Monitor database activity	Weekly
Monitor database size	Weekly
Run the updall task to update all views and full-text indexes	Daily. Occurs by default daily at 2 a.m.[a]
Run the Designer task to keep databases that inherit design from master templates in sync with the master templates	Daily. Occurs by default daily at 1 a.m. [a]

Task	Frequency
Run the Compact task	Weekly or monthly with the -B argument and in conjunction with a certified backup utility.[a]
Monitor the database cache	Occasionally, to ensure that the NSF Buffer Pool is sized correctly.

[a] Backup software can enable databases to be online while backup occurs. Be sure to not run maintenance tasks at the same time a backup is scheduled for the same database. For example, if updall is running on names.nsf at 2 a.m., do not schedule backup at the same time—the result will be that both tasks will take a very long time to complete and the system resources required to complete both requests will be very taxing on memory. It is possible to exhaust memory resources by double-scheduling maintenance tasks on a set of large databases.

Protect databases with transaction logging

Transaction logging is used to:

- Schedule regular backups. Backups based on transaction logs are faster and easier than full database backups that do not use transaction logging.
- Recover from a media failure. If you have a media failure, you can restore the most recent full backup from tape, then use the transaction logs to add the data that was not written to disk.
- Recover from a system crash. When the server restarts, it runs through the end of the transaction logs and recovers any writes that were not made to disk at the time of the crash. Logged databases do not require a consistency check.

More about transaction logging:

- Avoid running fixup with transaction logging enabled. Transaction logging tracks database changes via DBIID, database instance ID. If fixup is run, a new DBIID will be assigned to the DB and all of the transaction logs for the database will have the prior DBIID. If fixup must be run, be sure to take a new full backup of the database. The new full backup captures the database in its current state with the new DBIID. Then, if you have to restore the database, Domino needs only the new transactions that contain the new DBIID.
- Run compact with -b as it is the only switch that will not change the DBIID of a database if transactional logging is enabled. If another switch is used with compact, a new DBIID will be assigned and a new full backup must be done.
- View logging provides a way to maintain consistent views in failure conditions and enables media recovery to update those views. View logging is transaction logging support for Notes views and folders. All updates to Notes views or folders are recorded in the transaction log for recovery purposes.

- To enable view logging, use Domino Designer. In Designer, open a view or folder, select the **Advanced** tab, and check **Logging - Include updates in transaction log**.

17.7.3 Upgrade to the latest Domino Server maintenance release

It is important to plan for upgrading the Domino Server to obtain the latest set of fixes and improvements to the product. Upgrading helps the administrator to avoid finding problems that have already been reported and fixed.

Upgrade Central provides everything you need for planning and deploying the next release of your Lotus software, including Fix Lists, system requirements, product documentation, and installation instructions. Find the latest updates for all Lotus software, including availability dates for future MRs, on the Upgrade Central Web page at:

http://www.ibm.com/software/lotus/support/upgradecentral/index.html

17.7.4 IBM Lotus Notes Smart Upgrade

If, after reviewing the fix lists for Notes client fixes, the administrator has determined that users with the domain could benefit from a Notes client upgrade, the task can be automated.

IBM Lotus Notes Smart Upgrade automates the task of upgrading Notes clients. Lotus Notes Smart Upgrade uses policy and settings documents to help manage updates. You create policy documents in the Domino Directory to distribute standard settings and configurations across groups, departments, or entire organizations. See Table 17-6.

Smart Upgrade can be configured to notify users to update their Notes clients to later releases. For more information, look for “Using IBM Lotus Notes Smart Upgrade” and “Creating a desktop policy settings document” in Domino Administrator 7 Help.

These Smart Upgrade tab options are available on the policy document.

Table 17-6 Smart Upgrade tab options

Option	**Description**
Deploy version	If you use Smart Upgrade, enter the Notes version to which you want users to upgrade.
Upgrade deadline	If you use Smart Upgrade, use *mm/dd/yyyy* format to enter the date by which users must upgrade. If users to do not upgrade by this date, the upgrade happens automatically.

Option	Description
Remind me every hour after "upgrade deadline" has passed	Check this field if you want to send an hourly reminder to users who have not updated their clients by the deadline set in the "Upgrade deadline" field.
Mail-in Database for Smart Upgrade reports	Enable Smart Upgrade Tracking for the user by selecting the mail-in database name.
Remove Smart Upgrade tracking files after a specified number of days	Choose one: Yes: Automatically deletes the Smart Upgrade tracking files when the specified time period for maintaining files is exceeded and the Notes Client is restarted. When field appears, enter number of days. No: Keeps Smart Upgrade tracking files after the specified time for maintaining the files is exceeded. The files are not deleted.
Number of days to keep Smart Upgrade Tracking reports files	Enter the number of days to keep the Smart Upgrade Tracking files before they are deleted. Default is 365 days. **Note:** This field appears only if you choose Yes for "Remove Smart Upgrade Tracking files after a specified number of days."

It is also possible to do a silent upgrade using Smart Upgrade. Optional arguments are commonly used to run a silent Smart Upgrade requiring no user input during the upgrade, or to launch an upgrade that is almost silent requiring almost no input from users. See "Running a silent upgrade using optional arguments" in the Domino Administrator 7 Help for more information.

Note: Smart Upgrade Kits are available only in global English. In a non-English environment, the Notes Client Web Kit can be substituted for the Smart Upgrade Kit.

17.8 Troubleshooting techniques, tools, and tips

This section covers techniques for collecting more information for specific Domino failures, including:

- Basic settings: DEBUG_THREADID and DEBUG_OUTFILE
- How to debug the different types of server hangs
  - Debugging server slowdowns using semaphore debugging tools
  - Debugging server hangs: Collecting required data in when the Domino Server hangs for an extended period of time
- Using Debug_Trapleaks to look for potential memory leaks

- Using Debug_Checkmarkers to search for potential memory overwrites
- Network level debug: LOG_SESSIONS, LOG_CONNECTIONS, DEBUG_TCP_ALL
- Client/server conductivity: CLIENT_CLOCK, SERVER_CLOCK and snoop
- Agent/application: LOG_AGENTMANAGER, DEBUG_AMGR
- View/indexing logging: LOG_UPDATE, LOG_VIEW_EVENTS

17.8.1 Basic settings: DEBUG_THREADID and DEBUG_OUTFILE

DEBUG_THREADID=1 should always be set in notes.ini. It provides the process ID and thread ID for each entry in the Domino Server Console log.

If the Domino server console data is not being logged to a text file, make sure to set up DEBUG_OUTFILE.

DEBUG_OUTFILE=
Domino data directory/IBM_TECHNICAL_SUPPORT)/console.log

The variable DEBUG_OUTFILE contains the filename where the debug information will be stored. DEBUG_OUTFILE also enables NSD to collect the last 10 lines to the Domino server console log.

> **Tip:** To view the output of the debug outfile on the screen, use the UNIX command:
>
> ```
> tail -f Domino data directory/IBM_TECHNICAL_SUPPORT/console.log
> ```
>
> The screen shows the last lines of the file.

17.8.2 How to debug the different types of server hangs

A crash is a fault detected by the application, and a *hang* is when the server appears to have stopped processing entirely but no messages are seen on the console indicating a problem.

Hangs can be thought of as either *recoverable* or *unrecoverable*.

A recoverable hang or server slowdown is one where after a period of time the server resumes servicing client requests, routing mail, responding to HTTP requests, and so forth. These are typically caused by an overloaded server or by insufficient resources, slower-than-required I/O devices, and the like.

Unrecoverable hangs, true Domino Server hangs, never clear themselves and a restart of the server is required to resume normal service. Unrecoverable hangs are typically caused by resource contention between one or more applications, processes, or threads.

Part of the difficulty in diagnosing hangs is that there is no “break point” indicating the nature of the problem, so a holistic approach is usually required to pinpoint the underlying problem.

When hangs occur, you can test whether the Domino application is responding by using Telnet to port 1352 on the Domino server.

If the server is not hung, you will see the message `Connection established`.

If it is hung, you will see `could not connect to remote host` or `connection refused`.

Debugging server slowdowns

This section describes using semaphores and enabling and using DEBUG_SHOW_SEM to assist in debugging server slowdowns.

Domino semaphore debugging

Notes/Domino uses semaphores and a lock manager (software flags/locks) to ensure that certain activity completes before other activities can begin. Performance issues often occur because a thread has an activity requiring a semaphore to be locked, causing other threads to back up while waiting for access to a critical resource. The threads waiting for a semaphore can be from the same process or from multiple processes. Enabling semaphore debugging is a method commonly used to work on Domino server slowdowns.

Debug_ThreadID=1 is required when using semaphore debugging.

Note: Semaphore timeouts do not always indicate a performance problem. It is not uncommon for semaphore timeouts to occur on a busy server.

Enabling and using DEBUG_SHOW_SEM

New to Domino 7, DEBUG_SHOW_SEM set in the notes.ini collects statistics about semaphore usage. With the ini setting enabled, using **`sh sem`** at the server console will produce a dump of semaphore statistics:

```
> sh sem
Semaphore statistics; 12/01/2005 01:09:01 - 12/01/2005 01:11:50
SpinHits=249 SpinAvgIterToHit=61 SpinDelays=(31,0 ms) SpinMaxDelay=96
SpinMaxDelayMask=127 FRWSemReadExt=(0,0)
       31    0 msec intervals
```

```
        2    1 msec intervals
        2    2 msec intervals
        1    3 msec intervals
...
        0   95 msec intervals
        1   96 msec intervals
#    Max          Total      Avg    Type Description
1      0 ms           0 ms     0 ms CA20 Port DriverVar Array semaphore
spin lock
7    281 ms         561 ms    80 ms 030B Collection semaphore
1      5 ms           5 ms     5 ms 02B0 Zero-user database cache
9      0 ms           0 ms     0 ms 8921 Task table semaphore spin lock
21    51 ms        1050 ms    50 ms 02A2 Semaphore controlling
per-process init/termination in NSF
1      0 ms           0 ms     0 ms C12C
1      0 ms           0 ms     0 ms 0110
3      0 ms           0 ms     0 ms 012E
4     21 ms          21 ms     5 ms 412C
223   1077 ms        3119 ms    13 ms 091E Scheduler semaphore
17      0 ms           0 ms     0 ms 83F5 Database offline exclusive
sempahore spin lock
1      0 ms           0 ms     0 ms 82C7  spin lock
2      0 ms           0 ms     0 ms 8244 database semaphore spin lock
1    102 ms         102 ms   102 ms 034C NAMELookup Thread Queue.
2      5 ms           5 ms     2 ms 4245 open database queue semaphore
```

The bottom part of the **sh sem** output lists information about the number of times a given semaphore was used, as well as the max wait time, total wait time, average wait time, type in hex, and description.

The information can be used by taking a base line **sh sem** when the server has been up for a while with no slowdowns, and after a slowdown has happened a second **sh sem** can be taken. High values for average wait times or excessive usage and total wait time can indicate a problem.

DEBUG_SHOW_TIMEOUT and DEBUG_SEM_TIMEOUT

Set the following two parameters in the notes.ini file:

```
DEBUG_CAPTURE_TIMEOUT=1
DEBUG_SHOW_TIMEOUT=1
```

Other parameters:

DEBUG_SEM_TIMEOUT=X (default 30000, which is in milliseconds, so 30000 translates to 30 seconds). Use as instructed by your support provider to change how long a semaphore must time out before being reported.

The first two parameters are necessary for capturing additional performance details, enabling Lotus Support to determine whether a slowdown is due to some threads holding on to a semaphore for a long period of time. There should be little impact on performance when setting these parameters.

When a server slowdown occurs, any semaphore timeout data that is traced via these two debug parameters is written into a file named SEMDEBUG.TXT, which is located in the Domino data directory, and the Domino Console log file (text logging, *not* log.nsf).

> **Note:** The SEMDEBUG.TXT file is created only if a semaphore timeout occurs. Any time this happens, collect an NSD output and send this file to Lotus Customer Support.

Output of SEMDEBUG.TXT for UNIX:

```
THREAD [01676:00001] WAITING FOR RWSEM 0x412C (@EE100210)
(R=0,W=1,WRITER=05067:00001,1STREADER=05067:00001) FOR 30000 ms
THREAD [01684:00001] WAITING FOR RWSEM 0x412C (@EE100210)
(R=0,W=1,WRITER=05067:00001,1STREADER=05067:00001) FOR 30000 ms
```

What does the output mean?

The output shown has the following meaning:

- 0x412C indicates the type of semaphore.
- [01684:00001] The first number (01684) indicates the process ID. The second number (00001) is the thread ID.

You can match this number with the NSD stack trace, as shown in Example 17-10.

Example 17-10 Finding the cause of a system slowdown NSD output

```
[1] 1684:/opt/lotus/notes/latest/sunspa/tmmscan <-- fatal thread
###### thread 1/4 :: tmmscan, pid=1684, lwp=1 ######
[1] eed396a0 lwp_sema_p (228a30)
[2] eed396a0 __lwp_sema_wait (228a30, 1d670, 0, 0, 0, 0) + 8
[3] eefc779c _park  (228990, 228a30, 0, 1, eefe6240, 0) + a0
[4] eefc7554 _swtch  (2289a0, 228b90, 228a10, 228a0c, 228a08, 228a04) + 2cc
[5] eefc5f8c _cond_timedwait_cancel (efffdd90, efffdd78, efffdd70, 228990, eefe52b0, 0) + 1e4
[6] eefd3420 _ti_sleep (1e, eefe52b0, eefe52b0, effff2e3, effff154, f8000600) + 100
[7] ef0776e4 fatal_error (b, ef663dd4, ef657598, efffde50, 228a04, 2289e4) + 2c0
[8] eefd2f20 __libthread_segvhdlr (b, efffe4b0, efffe1f8, efffe138, eefe52b0, 2289e4) + e0
[9] eefd2334 sigacthandler (b, efffe4b0, 228990, eefe52b0, efffe1f8, eefd2e40) + 6e0
[10] 000201d0 KC_ScanStart (efffeec0, 3ae18, efffeec0, efffeec4, efffeec8, efffeecc) + 13a0
```

```
[11] 000157b0 AddInMain (22, 1, effff144, ef7ed2b8, ef7ec9c0, 0) + d00
[12] 0002fb40 NotesMain (1, effff144, effff144, 0, 0, ef7c16e1) + 40
[13] 0002fa60 notes_main (0, 0, 0, 1, effff144, 0) + a8
[14] 000147ec _start  (0, 0, 0, 0, 0, 0) + dc
```

In this way you can identify the thread that caused the semaphore timeout issue.

You can also check a semaphore timeout at the server console reading the Domino statistics. To view this statistic, type the following command at the server console:

```
sh stat sem.timeouts
```

If a semaphore timeout occurred, you will see a Sem.Timeouts statistic similar to:

```
Sem.Timeouts = 430D:58 0A13:42 030B:28 0116:26 0A12:21
```

Note: A single semaphore timeout is not always a symptom of performance issues. You should be concerned only if you experience a lot of them.

DEBUG_SHOW_BLOCKINGTHREADCALLSTACK

Setting DEBUG_SHOW_BLOCKINGTHREADCALLSTACK to 1 in the notes.ini turns on the ability to display callstacks for a thread that was holding a semaphore that was blocking other threads. When the blocking thread releases the lock, the callstack for the thread is dumped.

Debugging server hangs

If the server is still not responding after a reasonable period of time has gone by (10 minutes or so), issue the following commands:

1. Log in as the Solaris user who owns the Domino partition.
2. Make the Domino data directory the working directory (for our Redbooks Lab system: **`cd /notes/dom1a`**).
3. Run the NSD script, which is in your Domino program directory (for our Redbooks Lab systems: /opt/ibm/lotus/bin/nsd).

   The NSD diagnostic script scrolls its output to the screen while it writes to a log file. The name of the log file displays when the script completes.
4. Run the NSD script again: /opt/ibm/lotus/bin/nsd

   The additional NSD captures thread-level information that can provide more insight about whether this is actually a hang, or if the server appears to be in a hung condition but is actually taking longer than usual to process requests.

5. Run NSD a final time: /opt/ibm/lotus/bin/nsd -kill

   This shuts down all server tasks and cleans up.

6. After enabling DEBUG_SHOW_TIMEOUT, DEBUG_SEM_TIMEOUT and DEBUG_SHOW_BLOCKINGTHREADCALLSTACK semaphore debug data will be available in semdebug.txt, if the hang happens again.
7. Restart the Domino server.

The NSD log files should be either tarred (Solaris **tar** command) or zipped (Solaris **gzip** or **zip** commands) to reduce the size. By default, the NSD files are stored in *Domino data directory*/IBM_TECHNICAL_SUPPORT.

It can also be useful to send along the Domino Console log if your startup script creates one. The sample scripts in this book do create a console log called `coutput` in the Domino partition's data directory.

By enabling DEBUG_SHOW_TIMEOUT, DEBUG_SEM_TIMEOUT, and DEBUG_SHOW_BLOCKINGTHREADCALLSTACK, semaphore debug will be available if the hang happens again. In this event, be sure to collect at least two NSDs as described above as well as the Domino Console log and semdebug.txt file for IBM Technical Support.

We discussed the nsd tool in detail in 17.2, "The nsd and memcheck tools" on page 475.

17.8.3 Using Debug_Trapleaks to look for potential memory leaks

Debug_Trapleaks prints out information about private memory handles and private memory blocks allocated by a process for its own exclusive use) that are still allocated when the process terminates. It also includes shared memory handles and shared memory blocks (handles and memory blocks allocated by a process but accessible to all Notes processes) when the last process terminates. This means that to get information about a leak, the process (if the leak is on private handles/blocks) or the server (if the leak is on shared handles/blocks) must quit cleanly because trap_leaks compares what was allocated to what is left at program end. If there is a crash, trap_leaks will not be able to report leaks.

This must be set to enable debug_trapleaks:

```
DEBUG_OUTFILE=<Domino data directory>/IBM_TECHNICAL_SUPPORT)/console.log
debug_threadid=1
Debug_Trapleaks=blockID[,blockID[,blockID...]]
Debug_Trapleaks_ShowStack=1
DEBUG_SHOWLEAKS=1
DEBUG_DUMP_FULL_HANDLE_TABLE=1
```

Using an example based on the memcheck Top 10 data in this Chapter, we set `Debug_Trapleaks=blockID[,blockID[,blockID...]]`, where blockID="Type".

Example 17-11 on page 509 shows the Top 10 Shared Memory Block Usage. Using blockID=0x834a, where 0x834a is the Type for BLK_GB_CACHE, also known as Group Cache, you can see that there is no known leak at this time.

Example 17-11   Top 10 Shared Memory Block Usage

```
<@@ ------ Notes Memory Analyzer (memcheck) -> Memory Usage Summary -> Top 10
Shared Memory Block Usage (Time 14:50:11) --
---- @@>

BY SIZE
Top 10

Type  TotalSize    Handles    Typename
-----------------------------------------------------------
0x82cd   19681280          5  BLK_UBMBUFFER
0x834a    3145730          3  BLK_GB_CACHE
0x8a05    2520000          1  BLK_NET_SESSION_TABLE
0x8f57    1242714         19  BLK_ISERV_CONFIG_PARAMS
0x8f56    1242714         19  BLK_ISERV_CONFIG_RECORDS
0x826c    1111902         17  BLK_EXTMGR
0x826d    1048576          1  BLK_NSF_DIRMANPOOL
0x8252    1048576          1  BLK_NSF_POOL
0x8311    1048576          1  BLK_NIF_POOL
0x8a08    1048576          1  BLK_SESSION_POOL:

      Debug_Trapleaks=834a
```

Note that `debug_trapleaks` expects the number to be hexadecimal without the leading `0x`. The value must be in hex.

Be sure to shut down the server cleanly when a memory leak is suspected.

17.8.4 debug_checkmarkers and potential memory overwrites

Checkmarkers is a special debug created to aide in troubleshooting memory corruption caused by a memory overwrite. Memory overwrites can be caused by Domino or other third-party applications.

The name explains it all: Checkmarkers are at the beginning and end of each memory allocation. When memory is allocated, the checkmarkers code tests the first and last bytes of the memory allocation for consistency. When Notes memory is written, markers are put at the start (FFFE) and end (FFFF) so that this can be checked. If corruption is found, then Domino will panic immediately instead of waiting for the memory to be used (which could take days, weeks, or even months.) Yes, checkmarkers will cause Domino to crash sooner, but this is what we want. It gets us closer to the actual problem by dumping the faulting stack. This helps isolate the cause and sometimes provides information to help reproduce the problem.

Only enable `debug_checkmarkers=1` in notes.ini if the server is crashing or there is evidence that there is a memory overwrite. An example of a memory overwrite is a single Domino task or multiple tasks crashing with a memory operation as one of the last calls in the callstack prior to calling panic or fatal error on a Domino server instance that still has plenty of memory available for use.

17.8.5 Network level debug to set in the notes.ini

Setting network debug in the notes.ini results in a Domino Server performance loss. Only use the settings when necessary.

```
LOG_SESSIONS=1 will generate a message for every new and closed session
LOG_CONNECTIONS=1 will generate a message for every tcpip connection made
DEBUG_TCP_ALL=1 will generate a lot of information about server network
activity and should only be used when necessary due to performance losses.

[07D8:000A-0C24] 03/25/2004 03:56:34.13 PM cmd_open> hEndp: 13C40001h
iError = 0000h
[07D8:000A-0C24] 03/25/2004 03:56:34.43 PM TCPEndp_GetServByName> exit
dwNtvErr = 00000000h
[07D8:000A-0C24] 03/25/2004 03:56:34.58 PM cmd_SendTranPvdrMsg> MAPSERV
lotusnotes
[07D8:000A-0C24] 03/25/2004 03:56:34.58 PM cmd_SendTranPvdrMsg> exit hEndp:
13C40001h wMsg: 1003h iError = 000Dh
[07D8:000A-0C24] 03/25/2004 03:56:35.08 PM Tcp_GetListenAddress> Binding to
port: 1352, QLen = 0
> 03/25/2004 03:56:35.08 PM TCPEndp_ConvertToNativeSockAddr> Exit Status
0000h
[07D8:000A-0C24] 03/25/2004 03:56:35.08 PM TCPEndp_MakeSocket> enter
[07D8:000A-0C24] 03/25/2004 03:56:35.08 PM TCPEndp_MakeSocket> Post
x_socket: Skt: 0000061
```

Network error with many Domino server instances running on a single Solaris system

On a system with many partitioned servers each, the server starts to report the following error on the console:

```
[12718:00010-00008] 16.11.2005 13:00:02   ERROR INITIALIZING STREAMS
DRIVER!!
It might not have not been installed on the system.
```

```
[12718:00010-00008] 16.11.2005 13:00:02
71 iocp_CreateStreams> Unable to
open CompletionPort device FD
error=11
[12718:00010-00008] 16.11.2005 13:00:02   Listener task exited: Failed
to create an IOCP port
```

When this error appears, they find that port 1352 is not responding to any requests. The does not affect all servers.

The problem is with the number of open channels. The maximum number of open channels (system-wide) is 64, and can be modified by listen_devmap_size in /etc/system:

```
set listen:listen_devmap_size=128
```

17.8.6 Client/server activity

Set `CLIENT_CLOCK=1` and `Debug_Outfile=c:\windowsclient.log` in notes.ini to log information about client activity.

Table 17-7 Common Remote Procedure Calls (RPCs) being sent to the server

RPC	Description
Open_Session	Authenticate with the server and establish a session
Open_Database	Find and open a database
Open_Note	Send contents of a note (design element or design document)
Open_Collection	Open a view
Read_Entries	Send a list of information from a view or search; usually follows Open_Collection
Find_By_Key	A view lookup via DBLookup
Get_Special_Note_ID	Send info from the ACL
Close_dB	Close database session

With SERVER_CLOCK enabled in the notes.ini, the server will log most of the NSF transactions (the same information as CLIENT_CLOCK, but for the server). When set to 1, NSF transactions are written to the server's console but do not get written to LOG.NSF.

- Dynamically enable the SERVER_CLOCK=1 parameter in notes.ini for the server when the high CPU usage is seen:

  ```
  set config SERVER_CLOCK=1
  ```

- Allow the server to run with the parameter enabled for 15 minutes.
- Then immediately disable the parameter, because the debug will generate significant logging in the server console:

```
Sample Debug_Outfile output with SERVER_CLOCK=1
> 96-07-12 14.13.43     Opened session for Alex Pulaski/USA/Lotus (Build
138)
44022650 START_SERVER 940 ms (590 ms NETIO) 3TCPIP 000201FF Rcvd 388
Sent 352
44023620 OPEN_DB 0 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 126 Sent 210
> 44023720 OPEN_COLLECTION 120 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 32
Sent 580
> 96-07-12 14.13.44 Opened session for Celeste Dell’Era/USA/Lotus (Build
138)
> 44023900 READ_ENTRIES 130 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 46 Sent
24110
44024190 CLOSE_COLLECTION 0 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 12 Sent
0
> 44025150 DB_REPLINFO_GET 0 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 14
Sent 32
44025190 DB_REPLINFO_GET 0 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 14 Sent
32
> 44025220 DB_INFO_GET 0 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 14 Sent
140
44025220 OPEN_NOTE 0 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 28 Sent 1046
> 44025780 OPEN_COLLECTION 60 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 120
Sent 12276
> 44026220 GET_MULT_NOTE_INFO_BY_UNID 30 ms (0 ms NETIO) 3TCPIP 000201FF
Rcvd 840 Sent 226
44026280 UPDATE_FILTERS 0 ms (0 ms NETIO) 3TCPIP 000201FF Rcvd 48 Sent
12
29845360 SEARCH 11760 ms (0 ms NETIO) TCPIP 000E1A3D Rcvd 86 Sent 68
(now searching notesdata directory)
```

If one of the operations takes an excessive amount of time, the cause of the delay should be investigated.

For example:

```
29845360 SEARCH 11760 (0 ms NETIO) TCPIP 000E1A3D Rcvd 86 Sent 68
(now searching notesdata directory)
```

SEARCH took a long time, 11760 microseconds, and was consuming considerable CPU cycles as seen by tools such as **vmstat**.

17.8.7 Agent, view/indexing, and replication logging flags

The following parameters and flags are used in notes.ini.

Debug_AMgr=value

This logs information depending on the flag used for value.

Description of flags:

c To output agent control parameters

e To output information about Agent Manager events

l To output agent loading reports

m To output agent memory warnings

p To output agent performance statistics

r To output agent execution reports

s To output information about Agent Manager scheduling

v Verbose mode, which outputs more messages about agent loading, scheduling, and queues

Use an asterisk (*) to output all of the flags above (same as turning on all the flags).

> **Note:** Having all debugging flags turned on has approximately 5% performance cost on average user response time. (This will vary.)

Log_AgentManager=value

Description: Specifies whether the start of agent execution is recorded in the log file and shown on the server console:

0 Do not log agent execution events

1 Log agent execution events (partially and completely successful)

LOG_UPDATE=1

Description: Enables logging of more information when updall is updating views

Example:

- If LOG_UPDATE is off, updall reports this to the server console:

```
> set config LOG_UPDATE=0
> 12/01/2005 03:21:08   LOG_UPDATE changed to 0.
> load updall
> 12/01/2005 03:21:17   Index update process started
12/01/2005 03:21:17   Updating views in AgentRunner.nsf
```

- If LOG_UPDATE is on, updall reports this to the server console:

```
> set config LOG_UPDATE=1
> 12/01/2005 03:21:41   LOG_UPDATE changed to 1.
> load updall
> 12/01/2005 03:21:53   Index update process started
12/01/2005 03:21:53   Updating views in AgentRunner.nsf
12/01/2005 03:21:53   Updating views in AgentRunner.nsf
12/01/2005 03:21:53   Finished updating views in AgentRunner.nsf
```

LOG_VIEW_EVENTS

Description: Logs messages when views are rebuilt.

Example:

When LOG_VIEW_EVENTS is off, updall -r reports to the server console:

```
> set config LOG_VIEW_EVENTS=0
> 12/01/2005 03:34:17   LOG_VIEW_EVENTS changed to 0.
> load updall -R
> 12/01/2005 03:34:21   Index update process started
12/01/2005 03:34:21   Updating views in AgentRunner.nsf
12/01/2005 03:34:21   Updating views in dfc/dfc100.nsf
12/01/2005 03:34:21   Updating views in homepage.nsf

LOG_VIEW_EVENTS is on updall -r will report the following to server
console:
> set config LOG_VIEW_EVENTS=1
> 12/01/2005 03:36:30   LOG_VIEW_EVENTS changed to 1.
> load updall -R
> 12/01/2005 03:36:35   Index update process started
12/01/2005 03:36:35   Updating views in AgentRunner.nsf
12/01/2005 03:36:35   Updating views in dfc/dfc100.nsf
12/01/2005 03:36:35   Informational, rebuilding view - user specified
REBUILD (reading /notes/dom1b/dfc/dfc100.nsf default view note Title:'')
12/01/2005 03:36:35   Updating views in homepage.nsf
```

Log_Replication

Description: Specifies whether the start and end of replication sessions are recorded in the Notes Log and displayed on the console:

0	Do not log replication events
1	Log replication events
2	Log replication activity at the database level
3	2 + activity at the note level
4	3 + activity at the field level

17.9 Conclusion

The goal of this chapter is to provide information about how to collect the appropriate data when reporting a PMR. Examples and suggestions for collecting data have been provided. The chapter serves as starting point for understanding available features and options. There are many more notes.ini settings for logging and troubleshooting Domino. Be aware that using the notes.ini settings can have performance penalties and should be removed when they are no longer required. Contact IBM Lotus Support for more information about additional troubleshooting, notes.ini settings, and guidance on resolving issues, as the information covered here is continually evolving.

A

TCP/IP networking

This appendix provides additional details about TCP/IP networking with Solaris and includes:

- Cross-references to other sections in this book with network information
- Installing additional network interfaces
- Private LAN IP addresses
- Crossover cable

© Copyright IBM Corp. 2006. All rights reserved.

A.1 Cross-references to other network information

We provide information about TCP/IP networking and IBM Lotus Domino in many other chapters and appendixes of this book:

- In 4.5, “Network configuration” on page 47, we discuss basic TCP/IP setup using our Redbooks Lab as the example.
- In 5.4.1, “Partitioned server networking considerations” on page 181, we discuss network port contention and binding ports for Domino partitions.
- In 8.3, “Configuring network resources for partitioning” on page 255, we discuss separate host names and IP addresses and the alternative method of port mapping for partitioned servers.
- In Appendix F, “IBM Lotus Domino IP resolve process” on page 557, we discuss the Name to Address resolve process.

A.2 Installing additional network interfaces

Solaris servers have one or more built-in network interfaces. These interfaces usually support 10 Mbps, 100 Mbps, and 1000 Mbps, and both full and half-duplex operation. These interfaces auto-sense what setting to use based on the hub or switch they are plugged into. Check the documentation that came with your server or at:

http://www.sun.com/docs

Often a single 100 Mbps or 1000 Mbps connection will have enough capacity to support all of your users or your cluster network, but you may want additional interface cards. For example, you would want an additional card to provide a higher level of availability where you can continue to operate even if an interface fails. There may be other reasons such as your organization’s topology that would require additional network interface cards.

A.2.1 Installing the network card

The following steps describe how to install an additional network card in your system.

1. Shut down Domino and any other applications.
2. Log in as the root user and execute the **`touch /reconfigure`** command. This causes Solaris to check for newly installed devices at the next system boot.
3. Enter the **`init 5`** command to shut down Solaris and turn off the system power. (Most Sun servers can turn off their own power; if yours is an older

model you may need to turn off the power manually after the console prompt appears.)

4. Physically install the new network card in the system, following the instructions that came with the card.
5. Turn on the system power. Most servers are configured to reboot automatically when power is reapplied; if this has been disabled on your system, enter the **`boot`** command when the console prompt appears.

> **Note:** Usually, all that is required to install a new network card is to put it into the server and perform a “reconfiguration boot,” either by creating the /reconfigure file beforehand as described above, or by entering the **`boot -r`** command at the console prompt. On some occasions, with new cards that Solaris may not recognize or with cards from third parties, you may need to install driver software. Refer to the documentation that came with your hardware.

A.2.2 Configuring the network interface

With Solaris, each host name and IP address requires a network interface. This interface can either be a separate *physical* interface or multiple *logical* interfaces on a physical network card.

Interface name is a string in this format:

```
physical-unit
physical-unit:logical-unit
```

For example: bge0 refers to the first physical interface, and bge0:1 refers to a logical interface that shares the same hardware.

Each network interface needs to know its host name and IP address. To do this, create a file called /etc/hostname.*interface-name*. This file must contain the host name to be associated with this interface name. The first network “hostname” file is created by the system on install.

To create the appropriate interface files on your server:

1. Log in to the server as root.
2. Using your editor of choice, create the interface files and put the appropriate host name in each. See 4.5.3, “Configuring the Redbooks Lab” on page 51 for examples of these interface files.
3. Start your new network configuration either by rebooting the server or using a series of **`ifconfig`** commands as described in 4.5.3, “Configuring the Redbooks Lab” on page 51.

A.3 Private network IP addresses

For the IP numbers for private LANs such as the cluster connection, you can select a private IP setting from the list set aside by the Internet Corporation for Assigned Names and Numbers (ICANN). Note that these are non-routeable on the Internet. Refer to RFC 1918 - Address Allocation for Private Internets for more information at:

http://www.faqs.org/rfcs/rfc1918.html

The network addresses reserved for private networks are:

- 10.0.0.0 - 10.255.255.255 (Class A)
- 172.16.0.0 - 172.31.255.255 (Class B)
- 192.168.0.0 - 192.168.255.255 (Class C)

For our Redbooks Lab example, we picked a Class C network for our private LAN that we used for our Domino cluster and the storage array consoles.

- Host address 192.168.1.*xxx* (*xxx* is the last octet of the host address.)
- Network 192.168.1
- Netmask 255.255.255.0
- Broadcast address 192.168.1.255

A.4 Crossover cable

If you have just two clustered systems, the easiest way to connect them is with an Ethernet cross-cable. If there are more than two systems, the cluster network cards should be connected to a hub or switch.

Crossover cables can be purchased. If you wish to make your own, a crossover cable has pin assignments of:

- 1 - 3
- 2 - 6
- 3 - 1
- 6 - 2

B

Using System V shared memory

Each running instance of IBM Lotus Domino consists of several cooperating processes that share information with each other by placing it in memory areas that are accessible to all the processes. Domino on Solaris can use either of two mechanisms to implement memory sharing. If you take no special action Domino uses *mmap'ed files*, which are convenient and easy to manage. This appendix describes how to use *System V shared memory*, an alternative that is somewhat trickier to manage but offers some advantages.

You can switch all of your Domino partitions to System V shared memory at the same time, or you can change them one by one. If you operate some lightly loaded partitions with highly variable loads, it may be convenient to let them continue to use mmap'ed memory indefinitely.

© Copyright IBM Corp. 2006. All rights reserved.

B.1 Shared memory mechanisms

By default, Domino on Solaris shares data between its processes by using special files that are made part of the processes' memory with the UNIX *mmap* system call; hence the name *mmap'ed files*. These files ordinarily reside in the /tmp directory and have names such as:

```
.NOTESMEM_please_do_not_remove.xxxxxxxx
```

Although they appear to be ordinary disk files, the files actually reside in physical memory so the Domino processes can access their contents quickly. Domino creates some of these files when it starts and adds more as its memory needs increase; the automatic size adjustment means this mode of memory-sharing needs little or no intervention to work well.

Alternatively, Domino can use *System V shared memory*, named for the early UNIX version that introduced the capability. With this method, Domino does not put its shared data in files but in *shared memory segments*. Domino allocates all of the memory segments it will ever use when it first starts up, and cannot add more segments if its need for memory grows. Therefore, the burden of choosing the proper amount of memory falls on the administrator.

Because System V memory is harder to manage than mmap'ed files, why would you choose to use it? There are two principal reasons to prefer System V memory: it gives better performance and can give better reliability.

- Domino can use *large pages* to address the contents of System V memory. This technique makes more efficient use of a scarce CPU resource called the Translation Look-aside Buffer (TLB), meaning that the CPU spends less time adjusting its memory-mapping hardware and more time actually computing. The result is lower CPU utilization and faster response times, especially on newer multi-threaded processors such as the UltraSPARC T1.
- The System V method also enables Domino to use *intimate shared memory*, another technique that improves TLB efficiency and reduces CPU overhead.
- With mmap'ed files, a Domino process that decides that it needs more memory creates a new file and tells the other processes to start using it. If any process is unable to access the newly created file, a panic ensues and the entire Domino partition shuts down abruptly. This failure mode does not occur with System V memory, because all of the memory segments are created at the outset. If a newly started process cannot attach to all of the segments, that process will be unable to start but the other processes will continue to run and the Domino partition will not panic.
- The mmap'ed files in /tmp are vulnerable to well-intentioned but misguided attempts to "clean up old files." If a Domino server has been running for a few weeks and a routine maintenance procedure (possibly a periodic **cron** job)

decides to remove the “stale” .NOTESMEM_* files, Domino will die horribly. Shared memory segments are immune to this kind of accidental damage.

B.2 Sizing System V shared memory

There is no simple formula to determine how much shared memory a Domino partition will require, yet it is important to allocate a suitable amount. Allocate too little and Domino may perform inefficiently or even be unable to service users' requests; allocate too much and other consumers of memory may be starved and run inefficiently or not at all. This is the tricky part of managing System V shared memory.

One way to determine how much shared memory a Domino partition needs is to let it run for a while using the self-adjusting mmap'ed files, observe how large the files grow, and then size the System V shared memory accordingly. This subsection explains how.

Begin by setting up the Domino partitions as if System V memory did not exist, controlling memory use with PercentAvailSysResources or NSF_Buffer_Pool_Size_MB as described in 6.1.3, “Domino tuning” on page 211. Operate the servers until they have been through at least one period of peak load, when their appetite for shared memory will have been greatest. Then observe three quantities: the peak size of the NSF buffer pool, the upper limit on the buffer pool's permitted size, and the total amount of shared memory allocated.

1. At the console of each Domino partition, enter the **`show stat database`** command. The Database.Database.BufferPool.Peak.Megabytes statistic reports the largest size the NSF buffer pool attained, and Database.Database.BufferPool.Maximum.Megabytes is the maximum size to which the buffer pool is permitted to grow.
2. If the peak size is substantially less than the maximum, this Domino partition can probably make do with less memory than it has been allotted. If the peak size is very close to the maximum allowed, it may mean that Domino could make productive use of more memory, especially if Database.Database.BufferPool.PerCentReadsInBuffer is less than 95 or so. If it appears that the memory allotted does not match the memory used, adjust PercentAvailSysResources or NSF_Buffer_Pool_Size_MB accordingly and begin again.
3. With Domino still running, enter this command in a Solaris console window:

   ```
   ls -l /tmp/.NOTESMEM* | awk '/username/ {s+=$5} END {print s}'
   ```

   Replace *`username`* with the name of the Solaris user account that operates the Domino partition. The first part of this line lists all of the .NOTESMEM* mmap'ed files. The second selects just those files belonging to *username*, adds their sizes, and prints the total in bytes. Divide this total by 1048576 to convert the total to megabytes.

After you have determined the total shared memory size and a suitable upper limit for the NSF buffer pool, proceed to the next section to reconfigure the partition so it will use System V shared memory.

B.3 Enabling System V shared memory

Shut down the Domino partition, then make these changes to its notes.ini file:

- Remove or comment out the PercentAvailSysResources setting, if present.
- Set NSF_Buffer_Pool_MB to the maximum permitted size of the NSF buffer pool, as determined in the preceding section.
- Set ConstrainedSHMSizeMB to the total size of the mmap'ed files as determined in the preceding section. It is prudent to add a safety margin of 300 to 400 MB, but there is no point in making the shared memory more than 900 MB larger than the NSF buffer pool.
- Set DEBUG_Enable_Sys_V_SHM to `1`.
- Set Mem_EnablePreAlloc to `1`.

Save the notes.ini changes and restart the Domino partition. When Domino restarts, it should use System V shared memory. To verify that it is doing so, enter the **`ipcs -m`** command in a Solaris terminal window. The output should look similar to:

```
$ ipcs -m
IPC status from <running system> as of Mon Nov 28 12:23:53 EST 2005
T         ID      KEY        MODE        OWNER    GROUP
Shared Memory:
m         61   0xff0d1001 --rw-rw----    sol1a   domino
m         60   0xf8e86807 --rw-rw----    sol1a   domino
m         59   0xf8e86806 --rw-rw----    sol1a   domino
m         58   0xf8e86805 --rw-rw----    sol1a   domino
m         57   0xf8e86804 --rw-rw----    sol1a   domino
m         56   0xf8e86803 --rw-rw----    sol1a   domino
m         55   0xf8e86802 --rw-rw----    sol1a   domino
m         54   0xf8e86801 --rw-rw----    sol1a   domino
m         53   0xf8e86800 --rw-rw----    sol1a   domino
m         13   0xc26a1368 --rw-rw---- db2inst1  db2grp1
m         12   0          --rw------- db2fenc1 db2fgrp1
```

Nine of the shared memory segments that are listed in this example belong to the Solaris user account sol1a, which operates the dom1a partition in our Redbooks

Lab. This demonstrates that the dom1a partition is in fact using System V shared memory.

If **`ipcs -m`** does not show any shared memory segments belonging to the Domino partition, double-check the spelling of the parameters that you added to notes.ini. All three of ConstrainedSHMSizeMB, MEM_EnablePreAlloc, and DEBUG_Enable_Sys_V_SHM must be specified; if any of them is absent or misspelled, Domino will continue to use mmap'ed files.

Because Domino allocates all of its System V shared memory at startup instead of starting small and adding more memory as needed, the total amount of memory claimed by Domino is usually a little greater for System V than for mmap'ed files. Keep a careful eye on the `sr` statistic reported by the **`vmstat`** utility, as described in 6.2, "Monitoring Solaris performance" on page 213.

> **Note:** In Solaris 10 it is not necessary to adjust any /etc/system tuning parameters to use System V shared memory.

C

Domino Server starting and shutting-down scripts

The following scripts are examples of install, post-install, and start/stop scripts.

© Copyright IBM Corp. 2006. All rights reserved.

C.1 Install script

```
###########################################################################
# Sun Microsytems Inc.
#
# File:           install
# Description:    installscript for Sun's Lotus Domino Start/Stop Script
#
# Copyright 2005, Sun Microsystems, Inc. All rights reserved.
###########################################################################


###########################################################################
# Constants
###########################################################################

# Try to find the directory where the Domino executables were installed.
# Look for an .install.dat file in /opt/ibm/lotus and then in /opt/lotus;
# if unable to find it in either place, then look for the directories
# themselves.  If even that doesn't succeed, create and use /opt/ibm/lotus.

if [ -f /opt/ibm/lotus/.install.dat ]; then
   OPTLOTUS=/opt/ibm/lotus
elif [ -f /opt/lotus/.install.dat ]; then
   OPTLOTUS=/opt/lotus
elif [ -d /opt/ibm/lotus ]; then
   OPTLOTUS=/opt/ibm/lotus
elif [ -d /opt/lotus ]; then
   OPTLOTUS=/opt/lotus
else
   OPTLOTUS=/opt/ibm/lotus
   mkdir -p ${OPTLOTUS}
fi

# This file will hold configuration information.  If you move it to
# another location, edit the postinstall and lotusdomino scripts
# to match.

DOMSUN_CFG=${OPTLOTUS}/domsun.cfg

# Try to find out how many partitions were installed.

if [ -f ${OPTLOTUS}/.install.dat ]; then
   NUM_DOMINO_PARTITIONS='grep -c "data_UNIX_user = " ${OPTLOTUS}/.install.dat'
else
   NUM_DOMINO_PARTITIONS=0
fi
```

```
# Gather information from the user.

/usr/bin/clear
echo
echo "You will be asked a few questions regarding the configuration"
echo
echo "The following are the recommended settings:"
echo
echo "o One Solaris account per Domino partition"
echo "o Solaris account names are domino1, domino2, ..."
echo "o All Solaris accounts belong to the notes group"
echo
echo "${NUM_DOMINO_PARTITIONS} partitions were found on this system"
echo
echo


num_partitions='ckstr -p "Enter number of Domino partitions
[${NUM_DOMINO_PARTITIONS}]: " -e "Enter a number between 1 and 4
(recommended)." -r "[1-n]" -d "${NUM_DOMINO_PARTITIONS}"' || exit $?

cat >$DOMSUN_CFG <<EOF
NUM_DOMINO_PARTITIONS=${num_partitions}
EOF


# Default values

count=1
while [ ${count} -le ${num_partitions} ]; do
  echo
  echo "User                      = domino${count}"
  echo "Group                  = notes"
  echo "Home                  = /lotus/domino${count}"
  echo "Data directory            = /lotus/domino${count}/notesdata"
  echo "NSD log directory         =
/lotus/domino${count}/notesdata/IBM_TECHNICAL_SUPPORT"
  echo "Lotus binaries directory  = ${OPTLOTUS}/bin"
  echo
  count='expr ${count} + 1'
done

default_settings='ckyorn -p "Use defaults [n] ? " -d "n"' || exit $?

default_settings='echo ${default_settings}|tr [A-Z] [a-z]'

if [ "X${default_settings}" = "Xy" ]; then
```

```
  count=1
  while [ ${count} -le ${num_partitions} ]; do

    user=domino${count}
    group=notes
    home=/lotus/${user}
    data=${home}/notesdata
    nsdlog_dir=/lotus/nsd-logs/${user}
    lotusbin_dir=${OPTLOTUS}/bin

    cat >>$DOMSUN_CFG <<EOF

# Configuration Settings for partition ${count}

NOTES_USER_${count}_NAME=${user}
NOTES_USER_${count}_GROUP=${group}
NOTES_USER_${count}_HOME=${home}
NOTES_USER_${count}_NOTES_DATA=${data}
NOTES_USER_${count}_NSDLOG_DIR=${nsdlog_dir}
NOTES_USER_${count}_LOTUSBIN_DIR=${lotusbin_dir}
EOF

    count='expr ${count} + 1'
  done
else

  # User has not selected the defaults. So prompt user for all values
  count=1
  while [ ${count} -le ${num_partitions} ]; do

# In this section we let the user override the default values

    user=domino${count}
    user='ckstr -l 8 -p "Enter Solaris account for partition ${count}
[${user}]: " -e "Enter less than 8 characters" -d "${user}" -h "One Solaris
user per Domino parition. ${user} (recommended)."' || exit $?

    group='ckstr -l 8 -p "Enter group name for Solaris account ${user} [notes]:
" -e "Enter less than 8 characters" -d "notes" -h "notes (recommended)."' ||
exit $?

    home=/lotus/${user}
    home='ckstr -p "Enter home directory for Solaris account ${user} [${home}]:
" -d "${home}" -h "${home} (recommended)."' || exit $?

    data=${home}/notesdata
    data='ckstr -p "Enter data directory for partition ${count} [${data}]: " -d
"${data}" -h "${data} (recommended)."' || exit $?
```

```
    nsdlog_dir=${data}/IBM_TECHNICAL_SUPPORT
    nsdlog_dir='ckstr -p "Enter nsd-log directory for partition ${count}
[${nsdlog_dir}]: " -d "${nsdlog_dir}" -h "${nsdlog_dir} (recommended)."' ||
exit $?

    lotusbin_dir=${OPTLOTUS}/bin
    lotusbin_dir='ckstr -p "Enter Lotus binaries directory for partition
${count} [${lotusbin_dir}]: " -d "${lotusbin_dir}" -h "${lotusbin_dir}
(recommended)."' || exit $?

    cat >>$DOMSUN_CFG <<EOF

# Configuration Settings for partition ${count}

NOTES_USER_${count}_NAME=$user
NOTES_USER_${count}_GROUP=${group}
NOTES_USER_${count}_HOME=${home}
NOTES_USER_${count}_NOTES_DATA=${data}
NOTES_USER_${count}_LOTUSBIN_DIR=${lotusbin_dir}
NOTES_USER_${count}_NSDLOG_DIR=${nsdlog_dir}
EOF

    count='expr ${count} + 1'
  done
fi


echo "Configuration file was saved successfully. Installing Script ..."

./postinstall

exit 0
```

C.2 The postinstall script

```
############################################################################
# Sun Microsystems Inc.
#
# File:           postinstall
# Description:    The postinstall script.
#
# Copyright 2005, Sun Microsystems, Inc. All rights reserved.
############################################################################

DOMSUN_CFG=/opt/lotus/domsun.cfg
if [ -f /opt/ibm/lotus/domsun.cfg ]; then
   DOMSUN_CFG=/opt/ibm/lotus/domsun.cfg
```

```
fi
. ${DOMSUN_CFG}

echo "  ${NUM_DOMINO_PARTITIONS} Domino partitions have been configured"


count=1
while [ ${count} -le ${NUM_DOMINO_PARTITIONS} ]; do

echo " Settings for Domino Unix User ${count} "

  var=NOTES_USER_${count}_NAME
  cmd='echo "\$ ${var}"|sed 's/ //''
  user='eval "echo ${cmd}"'

  var=NOTES_USER_${count}_GROUP
  cmd='echo "\$ ${var}"|sed 's/ //''
  group='eval "echo ${cmd}"'

  var=NOTES_USER_${count}_HOME
  cmd='echo "\$ ${var}"|sed 's/ //''
  home='eval "echo ${cmd}"'

  var=NOTES_USER_${count}_NOTES_DATA
  cmd='echo "\$ ${var}"|sed 's/ //''
  data='eval "echo ${cmd}"'

  var=NOTES_USER_${count}_LOTUSBIN_DIR
  cmd='echo "\$ ${var}"|sed 's/ //''
  lotusbin_dir='eval "echo ${cmd}"'

  var=NOTES_USER_${count}_NSDLOG_DIR
  cmd='echo "\$ ${var}"|sed 's/ //''
  nsdlog_dir='eval "echo ${cmd}"'

echo "User ${user}"
echo "Group ${group}"
echo "Homedir ${home}"
echo "Homedata ${data}"
echo "Lotusbin ${lotusbin_dir}"
echo "NSDLOG Dir ${nsdlog_dir}"

echo " "
echo "Done with this user"



  PROFILE_FILE_ORIG=${home}/.profile
  PROFILE_FILE=${home}/.profile_Dom_Sun
  echo "Creating ${PROFILE_FILE} for ${user} ..."
  echo
  cat > ${PROFILE_FILE} <<EOF
############################################################################
# File:           .profile
# Description:    The profile file required for proper functioning of
#                 the lotusdomino script
#
# Copyright 2005, Sun Microsystems, Inc. All rights reserved.
############################################################################
NOTESDATA_DIR=${data}
NSD_LOGDIR=${nsdlog_dir}
LOTUSBIN_DIR=${lotusbin_dir}

PATH=\$PATH:/usr/bin:/usr/sbin:/usr/proc/bin:$lotusbin_dir:

EDITOR=/bin/vi

export PATH NOTESDATA_DIR LOTUSBIN_DIR NSD_LOGDIR EDITOR

EOF

  echo "  chown ${user}:${group} ${PROFILE_FILE}"
  chown ${user}:${group} ${PROFILE_FILE} >/dev/null 2>&1 &

  echo "  chown ${user}:${group} ${PROFILE_FILE_ORIG}"
  chown ${user}:${group} ${PROFILE_FILE}

  echo
  echo "Creating ${PROFILE_FILE} for ${user} ... done."

  echo "Modifying ${home}/.profile for ${user} to source ${PROFILE_FILE} ..."
  echo

  # Set .profile to source ${PROFILE_FILE}
  if [ ! -f ${PROFILE_FILE_ORIG} ]; then
    echo "  touch ${PROFILE_FILE_ORIG}"
    touch ${PROFILE_FILE_ORIG}

    echo "  chown ${user}:${group} ${PROFILE_FILE_ORIG}" >/dev/null 2>&1
    chown ${user}:${group} ${PROFILE_FILE_ORIG} >/dev/null 2>&1

    echo "  chown ${user}:${group} ${PROFILE_FILE_ORIG}" >/dev/null 2>&1
    chown ${user}:${group} ${PROFILE_FILE_ORIG} >/dev/null 2>&1
  fi

  echo "  echo \". ${PROFILE_FILE}\" >> ${PROFILE_FILE_ORIG}"
  echo ". ${PROFILE_FILE}" >> ${PROFILE_FILE_ORIG}
  echo "touch ${home}/.hushlogin; chmod 444 ${home}/.hushlogin" >/dev/null 2>&1
  touch ${home}/.hushlogin; chmod 444 ${home}/.hushlogin >/dev/null 2>&1

  echo
  echo "Modifying ${home}/.profile for ${user} to source ${PROFILE_FILE} ...
done."

count='expr ${count} + 1'

echo " "

done


# Copy the lotusdomino script to /etc/init.d

echo " Copy Script to /etc/init.d "

cp ./lotusdomino /etc/init.d
chown root:sys /etc/init.d/lotusdomino;chmod 555 /etc/init.d/lotusdomino

echo "Finished copy job. Changed ownership and rights"

# Create the RC links to start and stop all Domino partitions automatically

echo "Now linking the new script into the RC directories"

echo " "

echo "ln /etc/init.d/lotusdomino /etc/rc3.d/S99lotusdomino" >/dev/null 2>&1
ln /etc/init.d/lotusdomino /etc/rc3.d/S99lotusdomino >/dev/null 2>&1

echo "chown root:sys /etc/rc3.d/S99lotusdomino;chmod 555
/etc/rc3.d/S99lotusdomino" >/dev/null 2>&1
chown root:sys /etc/rc3.d/S99lotusdomino;chmod 555 /etc/rc3.d/S99lotusdomino
>/dev/null 2>&1

echo "ln /etc/init.d/lotusdomino /etc/rc0.d/K00lotusdomino" >/dev/null 2>&1
ln /etc/init.d/lotusdomino /etc/rc0.d/K00lotusdomino >/dev/null 2>&1

echo "  chown root:sys /etc/rc0.d/K00lotusdomino;chmod 555
/etc/rc0.d/K00lotusdomino" >/dev/null 2>&1
chown root:sys /etc/rc0.d/K00lotusdomino;chmod 555 /etc/rc0.d/K00lotusdomino
>/dev/null 2>&1

echo "ln /etc/init.d/lotusdomino /etc/rc1.d/K00lotusdomino" >/dev/null 2>&1
ln /etc/init.d/lotusdomino /etc/rc1.d/K00lotusdomino >/dev/null 2>&1
```

```
echo "chown root:sys /etc/rc1.d/K00lotusdomino;chmod 555
/etc/rc1.d/K00lotusdomino" >/dev/null 2>&1
chown root:sys /etc/rc1.d/K00lotusdomino;chmod 555 /etc/rc1.d/K00lotusdomino
>/dev/null 2>&1

echo "Finished installing domino start/stop script"
echo "Your server(s) will start and stop automatically at boot and shutdown."

exit 0
```

C.3 Start/stop script

```
#!/bin/sh
###########################################################################
# File:           lotusdomino
# Description:    Start stop script for Lotus Domino
#
# Copyright 2005, Sun Microsystems, Inc. All rights reserved.
###########################################################################

DOMSUN_CFG=/opt/lotus/domsun.cfg
if [ -f /opt/ibm/lotus/domsun.cfg ]; then
   DOMSUN_CFG=/opt/ibm/lotus/domsun.cfg
fi
. ${DOMSUN_CFG}

###############################################################################
#
# check_dosfile():
# This function is used to check if the notes.ini contains the DOS-ish
# line-feed+carriage-return-combination to signal end-of-line
# If any of these are found, the command "dos2unix" is called to automagically
# convert notes.ini to Unix-format.
###############################################################################
#

check_dosfile()
{
    DOSFILE='nawk '/\r$/  { print NR }' $DATA | wc -m'
    if [ $DOSFILE -gt 0 ]; then
   echo "\nConverting $DATA from DOS to Unix format...\c"
   dos2unix $DATA $DATA
   echo "- Done."
    fi
}
```

```
################################################################################
#
# chkpid():
# Function chkpid() is used to check out if there are any remaining processes
# left for a given user.
# The function is always called after a "server -q" command, which is the usual
# way to shut down Lotus Domino server/servers. After the function is started
# it sets a timer (CNT=300 (5 min.)), a loop is started which waits for one
# second and increases variable NUM, if variable NUM reaches the value of
# variable CNT the function ends. Function chkpid() is also terminated if
# variable PROCS equals to zero, the "break" action of the "else" statement in
# the test argument is executed, which breaks the previous started
# "while do done" loop.
# The variable: $1 in this function always refers to the Lotus-Notes-User
# which runs this Domino-Server, whether it is partitioned or not.
################################################################################
#

chkpid()
{
  echo
  CNT=300
  NUM=0
  while [ $CNT -ne $NUM ]; do
    PROCS='ptree $1 | awk 'END{print NR}''
    if [ $PROCS -gt 0 ]; then
      NUM='expr $NUM + 1'
      sleep 1
    else
      break
    fi
  done
}
################################################################################
# chkenv():
# The function chkenv() is used to check installation environment and
# to set variables which are needed for status output.
# The following environment checks are done by chkenv() in the
# following order:
# 1.  check for existing homedirectory for the LNSU.
# 2.  check if homedirectory of LNSU is unique in system passwd.
# 3.  check if the NOTESDATA_DIR is set correctly in the .profile
#     and if the NOTESDATA_DIR exists.
# 4.  check if LNSU uses Bourne Shell.
# 5.  check for existing .hushlogin file in homedirectory of LNSU.
# 6.  check for existing .profile file in homedirectory of LNSU.
# 7.  check for existing notes.ini file in homedirectory LNSU.
# 8.  check if variable NSD_LOGDIR is set in the environment of the LNSU,
#     this is needed for the shutdown process.
# 9.  check to see if the notes.ini file is in DOS/Windows format and set
#     variable DOSFILE.
# 10.  check to see if there is a ServerKeyFileName setting in notes.ini
#     of the LNSU.
# 11. create temporary file to start the servers.
#
# The variable: $1 in this function always refers to the Lotus-Notes-User
# which runs this Domino-Server, whether it is partitioned or not.
################################################################################

chkenv()
{
  UNIXHOME='awk -F: '/^'$1'/ {print $6}' /etc/passwd'



  NOTESDATA_TRUE='su - $1 -c "env | grep -c NOTESDATA_DIR"'
    if [ $NOTESDATA_TRUE -eq 0 ]; then
      echo $ERSTR >>/tmp/run.$1.$$
      MESSAGE="No NOTESDATA_DIR variable in .profile of user: $1"
      echo "\n$MESSAGE\n" >>/tmp/run.$1.$$
    NOTESHOME="NOT SET FOR THIS USER!"
    else
   NOTESHOME='su - $1 -c "env | grep NOTESDATA_DIR" | awk -F= '{print $2}''
   fi

  ERSTR="====================== ERROR ======================"
  for i in home notesdata unique shell hush profile notes.ini
  do
    case $i in
     home)MESSAGE="no homedirectory at all for user: $1"
      TEST="! -d $UNIXHOME" ;;
     notesdata)MESSAGE="no notesdata directory at all for user: $1"
                  TEST="! -d $NOTESHOME";;
     unique)HOMECHECK='grep -c "/$1" /etc/passwd'
      MESSAGE="no unique homedirectory for user: $1"
      TEST="$HOMECHECK -ne 1" ;;
     shell)SHCHECK='sed -n -e "s-^$1:.*:--p" /etc/passwd'
      MESSAGE="user: $1 does not use a Bourne Shell"
      TEST="$SHCHECK != /bin/sh" ;;
     hush)MESSAGE="no .hushlogin file in homedirectory of user: $1"
      TEST="! -f $UNIXHOME/.hushlogin" ;;
     profile)MESSAGE="no .profile file in homedirectory of user: $1"
      TEST="! -f $UNIXHOME/.profile" ;;
     notes.ini)MESSAGE="no notes.ini file in notesdata directory of user: $1"
      TEST="! -f $NOTESHOME/notes.ini" ;;
     esac
    if [ $TEST ]; then
      echo $ERSTR >>/tmp/run.$1.$$
      echo "\n$MESSAGE\n" >>/tmp/run.$1.$$
      VALID=false
    fi
  done
  if [ $VALID = true ]; then
    NSD_TRUE='su - $1 -c "env | grep -c NSD_LOGDIR"'
    if [ $NSD_TRUE -eq 0 ]; then
      echo $ERSTR >>/tmp/run.$1.$$
      MESSAGE="No NSD_LOGDIR variable in .profile of user: $1"
      echo "\n$MESSAGE\n" >>/tmp/run.$1.$$
    fi
    DATA="$NOTESHOME/notes.ini"
    check_dosfile $DATA
    CHECKSTR='grep -c ServerKeyFileName $NOTESHOME/notes.ini'
    if [ $CHECKSTR -eq 0 ]; then
      echo $ERSTR >>/tmp/run.$1.$$
      MESSAGE="no string: ServerKeyFileName in notes.ini of user: $1"
      echo "\n$MESSAGE\n" >>/tmp/run.$1.$$
    fi
  fi
  if [ -f /tmp/run.$1.$$ ]; then
    echo " FAILED see /tmp/run.$1.$$"
  else
      echo " -- Okay to run Domino."
      echo "$1" >>/tmp/start_stop_server
  fi
}

################################################################################
# function chkrun() checks if a Domino Partition Server is already running,
# and sets a variable if it is not running.
# This function is needed to avoid starting a partitioned server twice.
# It is only called when using the script without any notesx-commandline-option
################################################################################

chkrun()
{

  ISRUN='ps -fU ${1} | awk '/server/ && $3==1 { print $2 }''
  if [ $ISRUN ]; then

    echo "Domino Partition Server for user: ${1} already runs on PID: $ISRUN"
    START=NO
  else
    START=YES

  fi
}
```

```
###############################################################################
# function id_wrapper() sets the SERVER variable and forces it to lower case
# letters. The notes.ini could also be MS-DOS/Windows style file-format because
# function check_dosfile() is called inside
###############################################################################

id_wrapper()
{
NOTESHOME='su - $1 -c "env | grep NOTESDATA_DIR" | awk -F= '{print $2}''
DATA="$NOTESHOME/notes.ini"

check_dosfile $DATA

CHECKSTR='grep -c ServerKeyFileName $NOTESHOME/notes.ini'

NSD_DIR='su - $1 -c "env | grep NSD_LOGDIR" | awk -F= '{print $2}''
cd $NOTESHOME
STR=ServerKeyFileName
SRV='nawk -F= '/^'$STR'/{sub(".id","");sub(".ID","");print tolower($2)}' $DATA'
SERVER=$SRV
}

###############################################################################
#
# loop():
# The function loop() is used to check the environment and to set
# variables. The variable LOTUSSERVERS is built at the startup of program.
# The for loop evaluates all the LNSU's which are found in the system password
# database and checks for their consistency via function: chkenv().
###############################################################################
#
loop()
{
  if [ $CHECK = true ]; then
    for i in $LOTUSSERVERS
    do
      echo "Checking environment for Domino-User: \c"
      echo "$i\c"
      chkenv $i

    done

  else
    echo "$LOTUSSERVERS" >>/tmp/start_stop_server
  fi
}

###############################################################################
#
```

```
# kill_server():
# The function kill_server() is used to check that a Domino server went
# down gracefully. If the server went down and did not leave any remaining
# procesess nothing happens; if not the switch-user command is executed and all
# remaining processes are killed with the standard domino script:
# /opt/lotus/bin/tools/diag/nsd.sh as the given LNSU user.
#
# Note:
# -----
# The LNSU is variable $2 in this function.

kill_server()
{

  PROCS='ptree $2 | awk 'END{print NR}''
  if [ "$PROCS" -gt 0 ]; then
    echo "Server: $SERVER did not go down gracefully"
    echo "Please check the log-files in $NSD_DIR/*"
    var=NOTES_USER_${count}_LOTUSBIN_DIR
    cmd='echo "\$ ${var}"|sed 's/ //''
    lotusbin_dir='eval "echo ${cmd}"'
    su - $2 -c "cd "$NOTESHOME"; "${lotusbin_dir}"/tools/diag/nsd.sh -user $2
-batch -kill"
  fi
}

###############################################################################
#
# look how much Lotus-Notes-Partition-Servers are installed,
# they have to be in the systems passwd table to be useable.
# Remark: If you use NIS, you may have to change the appropriate files...


users()
{
  LOTUSSERVERS='cat ${DOMSUN_CFG}|sed 's/#.*//g'|grep "^NOTES_USER_._NAME="|awk
-F'=' '{print $2}''
}

###############################################################################
#


###############################################################################
#

# remove temporary old start/stop file could be left somehow.
[ -f /tmp/start_stop_server ] && rm -f /tmp/start_stop_server
```

```
###############################################################################
#
#
# Start/stop Lotus partition servers. All in one, or one by one.
#
###############################################################################
#
count=0

case "$1" in
start)# check if a single instance should be started
if [ $2 ]; then
  # get the Domino-Servername via function id_wrapper()
  id_wrapper ${2}
  chkrun ${2}
  count='expr ${count} + 1'
  if [ $START = YES ]; then
    echo "Starting Lotus Partition Server: $SERVER in background"
    # ensure that the input/output-files are cleared when restarting
    su - $2 -c "cd "$NOTESHOME"; cat /dev/null > cinput; cat /dev/null >
coutput"
    # now issue the start-command
      var=NOTES_USER_${count}_LOTUSBIN_DIR
      cmd='echo "\$ ${var}"|sed 's/ //''
      lotusbin_dir='eval "echo ${cmd}"'
      su - $2 -c "cd "$NOTESHOME"; "${lotusbin_dir}"/server <cinput>coutput"
>/dev/null 2>&1 &
  fi
else
  # get the Domino-server-names via functions:
  # users(), loop() and check their environment via chkenv().
  # Note: function loop() only calls function chkenv() if variable
  # CHECK has the value "true" in it.
  CHECK=true
  echo "General Domino Server/Servers Startup."
  echo "Looking for Domino-Server(s): \c"
  # call function users to let /etc/passwd be examined for notes-users
  users
  echo $LOTUSSERVERS

  # if no LNSU user(s) are already setup, just give a message and exit.
  if [ "X" = "X$LOTUSSERVERS" ]; then
    echo "none found, please check settings ${DOMSUN_CFG}."
    exit 0
  fi

  VALID=true
  loop
  # start every domino-server which is set by function: chkenv().
  if [ -f /tmp/start_stop_server ]; then
    for i in 'cat /tmp/start_stop_server'
    do
      count='expr ${count} + 1'
      chkrun ${i}

      if [ $START = YES ]; then
        echo "Starting Lotus Partition Server: \c"
        id_wrapper ${i}
        echo "$SERVER in background\c"
        # ensure that the input/output-files are cleared prior to restarting
        su - ${i} -c "cd "$NOTESHOME"; cat /dev/null > cinput; cat /dev/null >
coutput"
        # now, do the actual starting of the server
        var=NOTES_USER_${count}_LOTUSBIN_DIR
        cmd='echo "\$ ${var}"|sed 's/ //''
        lotusbin_dir='eval "echo ${cmd}"'
        su - ${i} -c "cd "$NOTESHOME"; "${lotusbin_dir}"/server
<cinput>coutput" >/dev/null 2>&1 &
        echo " - Done."
      fi

    done
    rm -f /tmp/start_stop_server
  fi
fi ;;
stop)# get the Domino-Servername via function id_wrapper()
if [ $2 ]; then
  id_wrapper ${2}
  PROCS='ptree $2 | awk 'END{print NR}''
  count='expr ${count} + 1'
  if [ $PROCS -gt 0 ]; then
    var=NOTES_USER_${count}_LOTUSBIN_DIR
    cmd='echo "\$ ${var}"|sed 's/ //''
    lotusbin_dir='eval "echo ${cmd}"'
    echo "\nStopping Lotus Partition Server: $SERVER\c"
    su - $2 -c "cd "$NOTESHOME"; "${lotusbin_dir}"/server -q" >/dev/null 2>&1 &
    chkpid $2
    kill_server $SERVER ${2}
  else
    echo "Partition Server: $SERVER was not running !"
  fi
else
  # get the Domino-Servername names via function loop().
  CHECK=false
  users
  loop
  for i in 'cat /tmp/start_stop_server'
  do
    id_wrapper ${i}
    count='expr ${count} + 1'
    PROCS='ptree ${i} | awk 'END{print NR}''
    if [ $PROCS -gt 0 ]; then
      var=NOTES_USER_${count}_LOTUSBIN_DIR
      cmd='echo "\$ ${var}"|sed 's/ //''
      lotusbin_dir='eval "echo ${cmd}"'
      echo "Stopping Lotus Partition Server: $SERVER\c"
      su - $i -c "cd "$NOTESHOME"; "${lotusbin_dir}"/server -q" >/dev/null 2>&1
&
      echo " "
      chkpid $i
      kill_server $SERVER $i
    else
      echo "Partition Server: $SERVER was not running !"
    fi
  done
  [ -f /tmp/start_stop_server ] && rm -f /tmp/start_stop_server
  echo "Lotus Partition Server shutdown complete !"
fi ;;
*)
echo "Usage: /etc/init.d/lotusdomino { start | stop }\n"
echo "If you want to start/stop a single lotus instance:\n"
echo "Usage: /etc/init.d/lotusdomino { start [dominounxisuser] | stop
[dominounxisuser] }\n" ;;
esac
```

D

Removing a password from a server ID file

Automatically starting your IBM Lotus Domino server, if your server ID file is password-protected, requires a programmatic solution to accommodate the server’s password-entry requirement in the scripts that automate Domino server startup. This chapter shows how to remove a password from the server ID file.

It is not possible to automatically restart your Domino server if your server ID file is password-protected. If it does contain a password, you will be prompted for a password each time you start your Domino server.

> **Note:** The following method will work as long as a password policy has not been set on the ID file.

The following steps describe how to remove a password from a server ID file:

1. Make sure you are logged in as the UNIX user you created for running the Domino server.
2. Shut down your Domino server.
3. Change to the Domino data directory.
4. Use FTP to transfer the server.id file to your local machine. Use binary mode for file transfer.

© Copyright IBM Corp. 2006. All rights reserved.

5. Open the Domino Administrator client and click the **Configuration** tab.
6. Select **Certification** → **ID Properties** (Figure D-1).

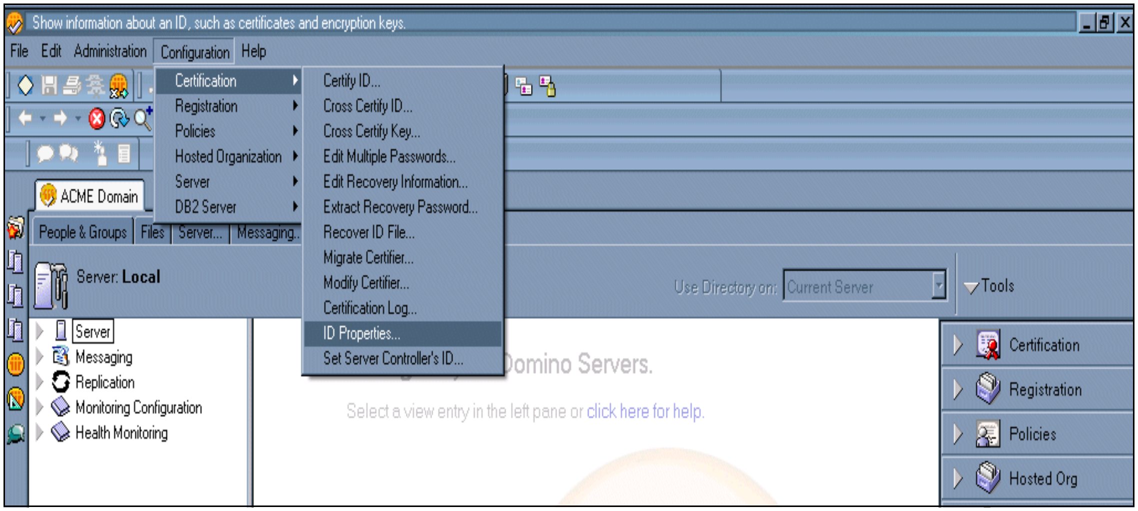
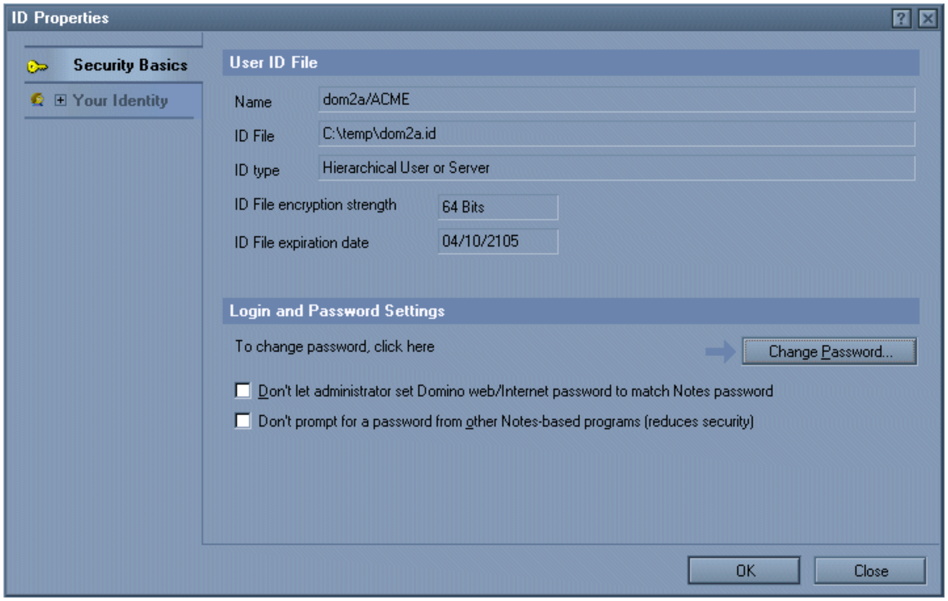


Figure D-1 Selecting the Certification ID properties

7. Open the server.id file from the local drive. Enter the password for the ID file.
8. ID Properties appears. Click **Change Password** (Figure D-2).



ID Properties

Security Basics

Your Identity

User ID File

Name: dom2a/ACME

ID File: C:\temp\dom2a.id

ID type: Hierarchical User or Server

ID File encryption strength: 64 Bits

ID File expiration date: 04/10/2105

Login and Password Settings

To change password, click here [Change Password...]

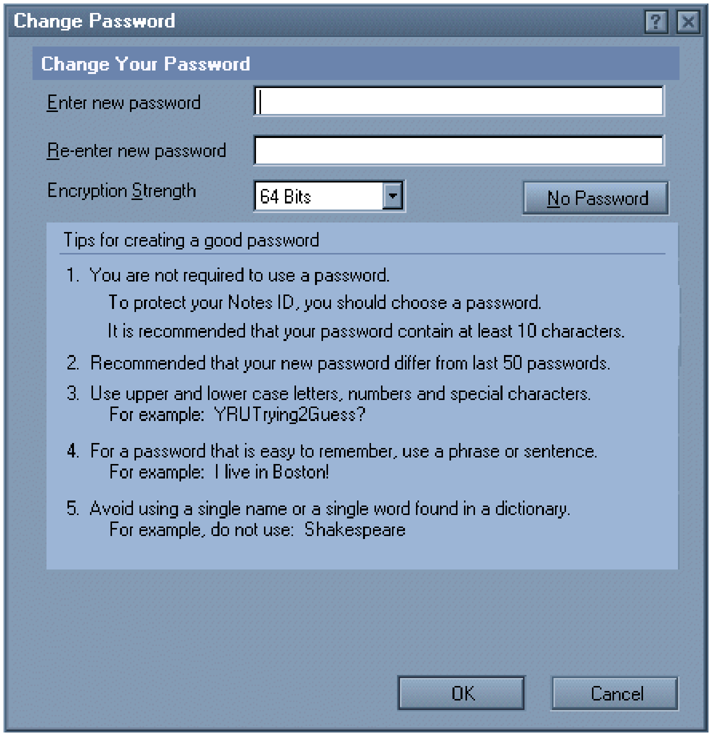
☐ Don't let administrator set Domino web/Internet password to match Notes password

☐ Don't prompt for a password from other Notes-based programs (reduces security)

[OK] [Close]

Figure D-2 ID properties information

9. At the ID Properties dialog box, click **No Password** (Figure D-3).

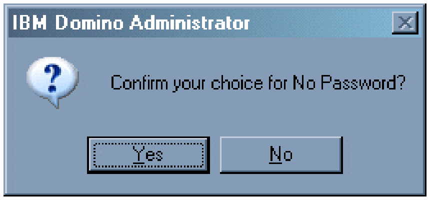


Tips for creating a good password

1. You are not required to use a password.
   To protect your Notes ID, you should choose a password.
   It is recommended that your password contain at least 10 characters.
2. Recommended that your new password differ from last 50 passwords.
3. Use upper and lower case letters, numbers and special characters.
   For example: YRUTrying2Guess?
4. For a password that is easy to remember, use a phrase or sentence.
   For example: I live in Boston!
5. Avoid using a single name or a single word found in a dictionary.
   For example, do not use: Shakespeare

Figure D-3 Clearing the password from a Domino server ID

10. Click **Yes** to confirm (Figure D-4).



Confirm your choice for No Password?

Figure D-4 Confirm password clear

11. A confirmation alert box displays `Password change succeeded`. Click **OK** to return to the ID Properties dialog box.
12. Click **OK** to close the ID Properties dialog box.
13. Use FTP with binary mode to transfer the server.id file back to the server.
14. Make sure that the server.id file has the correct owner and group., and start the Domino server. You will not be prompted for a password.

E

IBM Lotus Domino and syslog

This appendix describes the process of configuring your system to monitor for specific event occurrences in your Domino environment. Occurrences of such events then trigger a notification method (one of several that Domino provides) that logs the incident to a log file you specify in the Solaris file system via the Solaris syslogd daemon.

The syslogd daemon reads and forwards system messages to the appropriate Solaris log files, users, or both, depending on the priority of a message and the system facility from which it originates. As mentioned above, it can be configured to receive messages from external applications, such as the Domino server.

© Copyright IBM Corp. 2006. All rights reserved.

This is a procedure you can use to implement this capability in your organization.

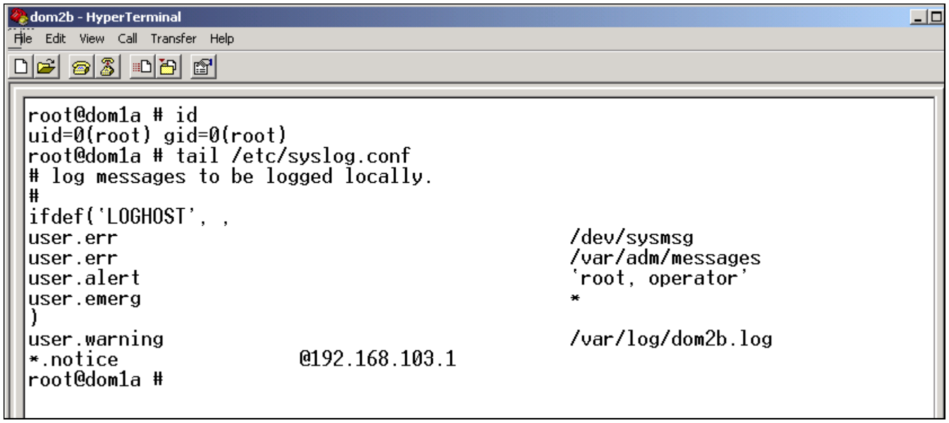
1. Change the syslogd configuration file to control output from the daemon. In our example we logged in as `root` and, in the /etc/syslog.conf file, we added the following line (Figure E-1 shows the updated file):

   ```
   user.warning/var/log/dom2b.log
   ```

   You can also specify **`user.*`** to include all event severities.

   > **Tip:** Be sure to use a tab as a separator; otherwise it will not work.

   > **Important:** The new `user.warning` line must *not* be placed within this construct:
   >
   > ```
   > ifdef('LOGHOST', ,
   > )
   > ```
   >
   > Ensure that your new user.warning line follows *after* the right parenthesis ")" that closes the ifdef statement as shown in Figure E-1.
   >
   > Failure to do so will result in monitored Domino event occurrences not being written to the Solaris log.



```
root@dom1a # id
uid=0(root) gid=0(root)
root@dom1a # tail /etc/syslog.conf
# log messages to be logged locally.
#
ifdef('LOGHOST', ,
user.err                                        /dev/sysmsg
user.err                                        /var/adm/messages
user.alert                                      'root, operator'
user.emerg                                      *
)
user.warning                                    /var/log/dom2b.log
*.notice                @192.168.103.1
root@dom1a #
```

Figure E-1 Solaris - updated /etc/syslog.conf

2. Specify a file name and location for Domino event output. In our example, we used /var/log/dom2b.log.

Note: Normally on Solaris systems, all log files are located in the /var/log file system.

In our example, although we used a Domino partition-specific (dom2b) log file name, this log file can collect any kind of event information that you want Domino to monitor. This means that events on *any* server in your Domino domain can trigger an update to the Solaris log file. Consequently, you can specify a more generically named log file, such as `/var/log/domino.log`.

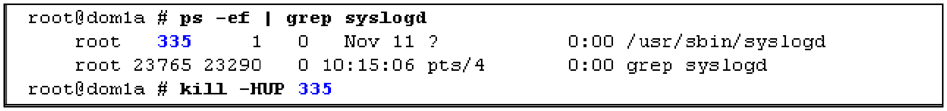
3. Create the new log file and instruct syslogd to reload its configuration file.

   a. Use the UNIX command **`touch`** to create a new empty file:

   ```
   touch /var/log/dom2b.log
   ```

   b. Send the SIGHUP signal to syslogd using the **`kill`** command. For example (Figure E-2), if the syslogd daemon has the pid=335, then type:

   ```
   kill -HUP 335
   ```



```
root@dom1a # ps -ef | grep syslogd
    root   335     1   0   Nov 11 ?         0:00 /usr/sbin/syslogd
    root 23765 23290   0 10:15:06 pts/4     0:00 grep syslogd
root@dom1a # kill -HUP 335
```

Figure E-2 Solaris - reload syslogd configuration

4. Switch user to the Solaris user account that owns the Domino server partition:

   ```
   su - sol2b
   ```

   At the Domino server console (in our example we're using server dom2b), enter the **`show task`** command to see whether the Event task is already running. If not, then load the Event task by typing:

   ```
   > load event
   ```

   Going forward, to load the Event task when you start your Domino servers, add it to the `ServerTasks=` line in notes.ini.

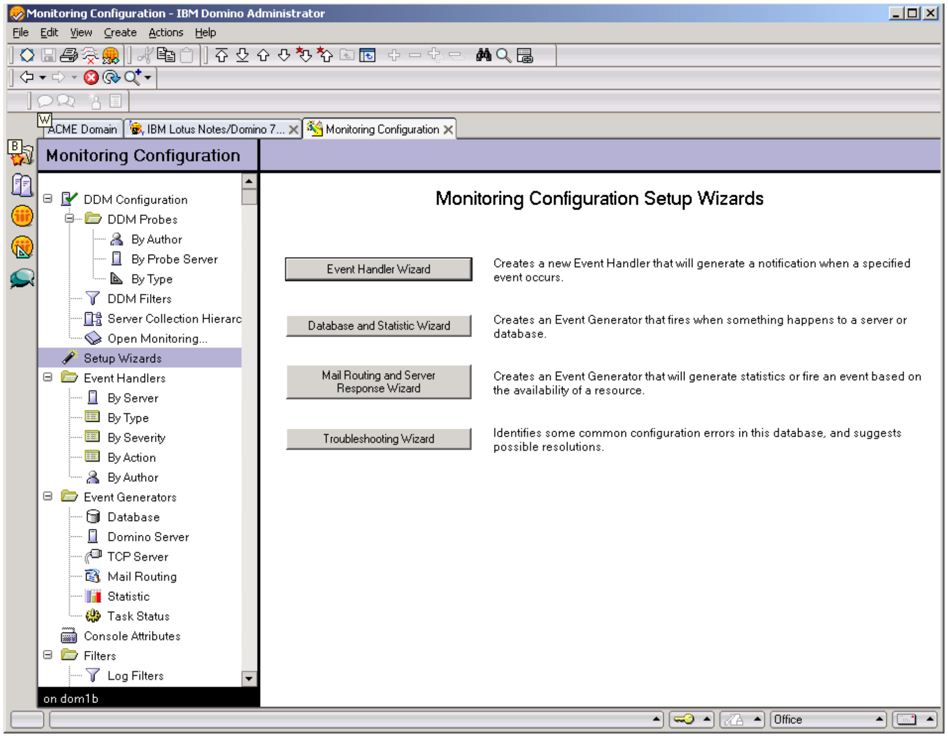
Note: The first time you load the Event task, it creates a Monitoring Configuration database (events4.nsf). In previous releases of Notes and Domino, this was called the *Statistics & Events* database.

Tip: If the Event task is already running, you should restart the task to make it work with the restarted syslogd on Solaris.

5. Go to the Domino Administrator client, open the Monitoring Configuration database, and set up your Database monitors, Event monitors, and so forth.

6. The following procedure is an example of the steps you would follow to monitor the ACL changes in the Domino Directory database, names.nsf

   a. Open the Monitoring Configuration database (events4.nsf) from the Files tab in the Domino Administrator (Figure E-3).



Monitoring Configuration Setup Wizards

Event Handler Wizard — Creates a new Event Handler that will generate a notification when a specified event occurs.

Database and Statistic Wizard — Creates an Event Generator that fires when something happens to a server or database.

Mail Routing and Server Response Wizard — Creates an Event Generator that will generate statistics or fire an event based on the availability of a resource.

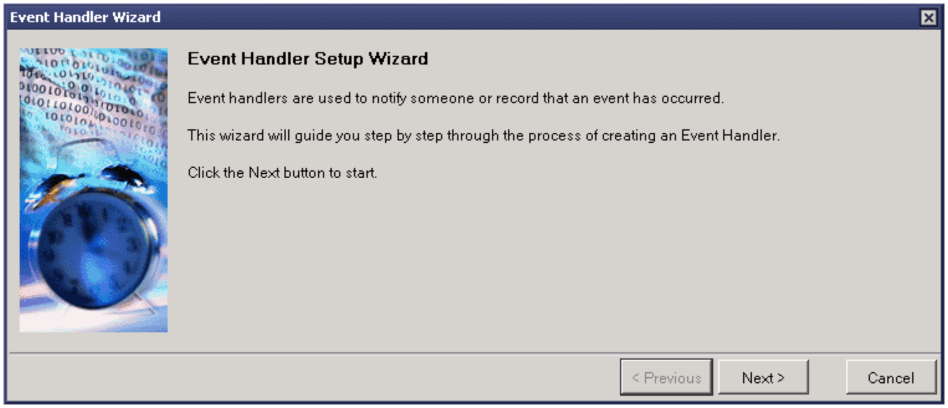
Troubleshooting Wizard — Identifies some common configuration errors in this database, and suggests possible resolutions.

Figure E-3 Admin Client - open the Monitoring configuration database

   b. The first time you open the database, you see the About this Database Help information. Press Esc to display the main view and the Monitoring Configuration navigator pane.

   c. Click **Setup Wizards** to display the Monitoring Configuration Setup Wizards screen.

d. Click **Event Handler Wizard** to open the Event Handler Setup Wizard (Figure E-4).



Event Handler Setup Wizard

Event handlers are used to notify someone or record that an event has occurred.

This wizard will guide you step by step through the process of creating an Event Handler.

Click the Next button to start.

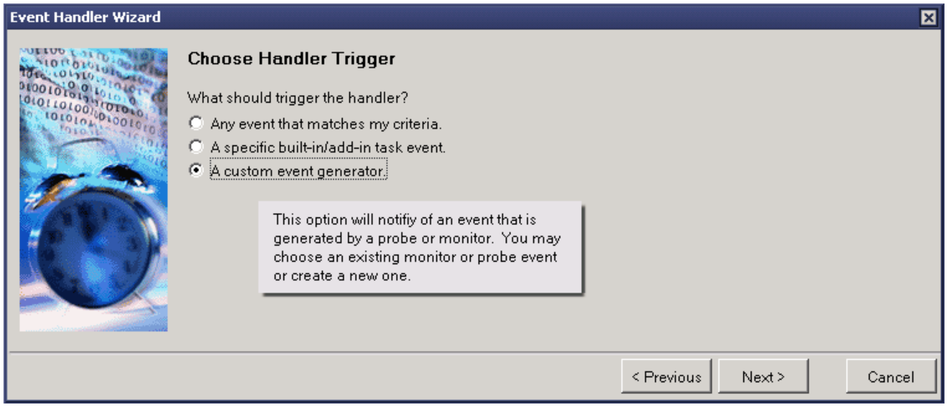
Figure E-4 Admin Client - Event Handler Setup Wizard

e. Click **Next** to continue.

f. There are three Event Handler Trigger types available to us in Figure E-5:

   i. Any event that matches certain criteria
   ii. A specific built-in or add-in task event
   iii. **A custom event generator** (this is what we chose for our example)

g. Click **Next** to continue.



Choose Handler Trigger

What should trigger the handler?

○ Any event that matches my criteria.
○ A specific built-in/add-in task event.
● A custom event generator.

This option will notifiy of an event that is generated by a probe or monitor. You may choose an existing monitor or probe event or create a new one.

Figure E-5 Admin Client - choose Handler Trigger

h. The Custom Event dialog box (Figure E-6) prompts you to select your custom event. Click the small drop-down list button.

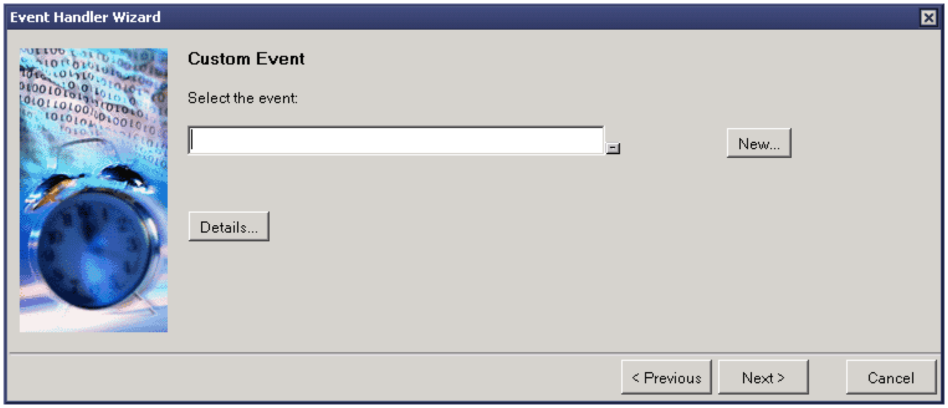
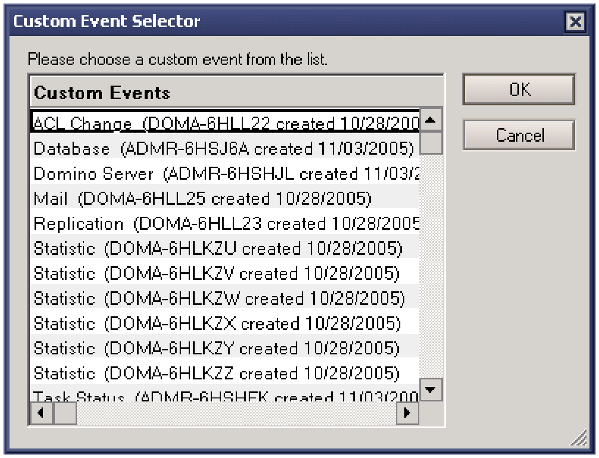


Figure E-6 Admin Client - choose the Custom Event

i. This displays the Custom Event Selector pop-up box (Figure E-7). In our example we chose the ACL Change event. Click **OK**.



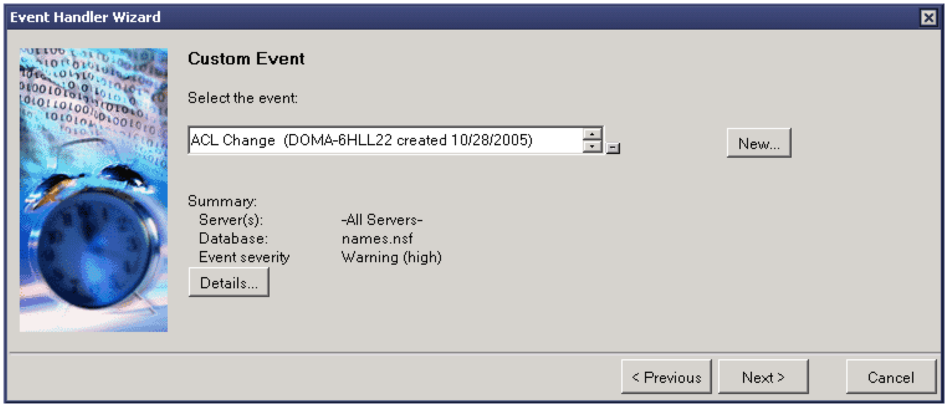
Please choose a custom event from the list.

Custom Events

ACL Change (DOMA-6HLL22 created 10/28/200
Database (ADMR-6HSJ6A created 11/03/2005)
Domino Server (ADMR-6HSHJL created 11/03/2
Mail (DOMA-6HLL25 created 10/28/2005)
Replication (DOMA-6HLL23 created 10/28/2005
Statistic (DOMA-6HLKZU created 10/28/2005)
Statistic (DOMA-6HLKZV created 10/28/2005)
Statistic (DOMA-6HLKZW created 10/28/2005)
Statistic (DOMA-6HLKZX created 10/28/2005)
Statistic (DOMA-6HLKZY created 10/28/2005)
Statistic (DOMA-6HLKZZ created 10/28/2005)
Task Status (ADMR-6HSHEK created 11/03/200

Figure E-7 Admin Client - Custom Event Selector

j. This returns you to the Custom Event dialog box (Figure E-8).



Event Handler Wizard

Custom Event

Select the event:

ACL Change (DOMA-6HLL22 created 10/28/2005)

Summary:

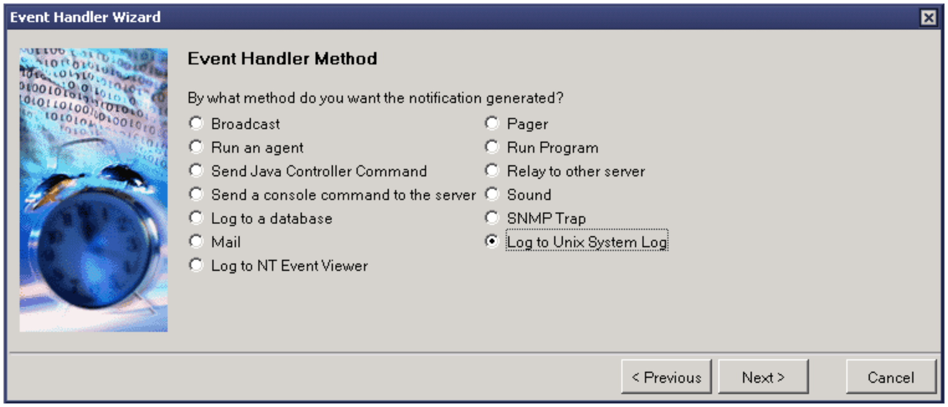
Server(s):	-All Servers-
Database:	names.nsf
Event severity	Warning (high)

Figure E-8 Admin Client - Custom Event specified

k. Now that we've chosen our custom event, the next step is to specify the notification method that this event will trigger.

> **Note:** If you do not have Events to select from, then click **New** to create a new Event.

Click **Next** to continue.



Event Handler Wizard

Event Handler Method

By what method do you want the notification generated?

○ Broadcast	○ Pager
○ Run an agent	○ Run Program
○ Send Java Controller Command	○ Relay to other server
○ Send a console command to the server	○ Sound
○ Log to a database	○ SNMP Trap
○ Mail	● Log to Unix System Log
○ Log to NT Event Viewer	

Figure E-9 Admin Client - Event Handler Method options

l. The Event Handler Method window appears (Figure E-9 on page 555). Because the goal of our example is to log a specific event occurrence to a Solaris log file, we select **Log to Unix System Log** and click **Next** to continue.

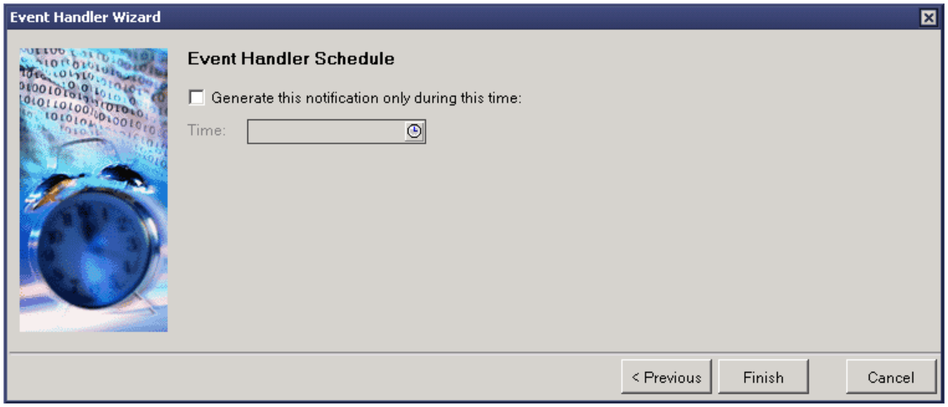


Figure E-10 Admin Client - Event Handler Schedule

m. Using the display in Figure E-10, we can specify a schedule that this Event Handler will observe, if required. In our example we have no need to specify a schedule, so we left this unchanged.

n. Click **Finish**.

7. Restart the Event task with the Domino server console command:

```
> tell event restart
```

8. Perform an ACL change by adding a new user to the ACL list for names.nsf. If everything is configured correctly, an entry will appear in the `/var/log/dom2b.log` file that looks like this:

```
Nov 15 18:04:46 dom1a event[13296]: [ID 875527 user.warning] dom2b/ACME:
The ACL in database names.nsf has been changed by Administrator/ACME.
[ADMR-6J6T6Z]
```

F

IBM Lotus Domino IP resolve process

This appendix discusses the Domino server name to IP address resolve process and how the Notes name service can assist the process.

© Copyright IBM Corp. 2006. All rights reserved.

F.1 The resolve process

When a new workstation is set up for the first time with Notes, the protocol's Name to Address resolve process is used exclusively where the server's common name is expected to be resolvable. In most cases the client and the server are located within the same IP domain and IP domain level and can access a DNS server.

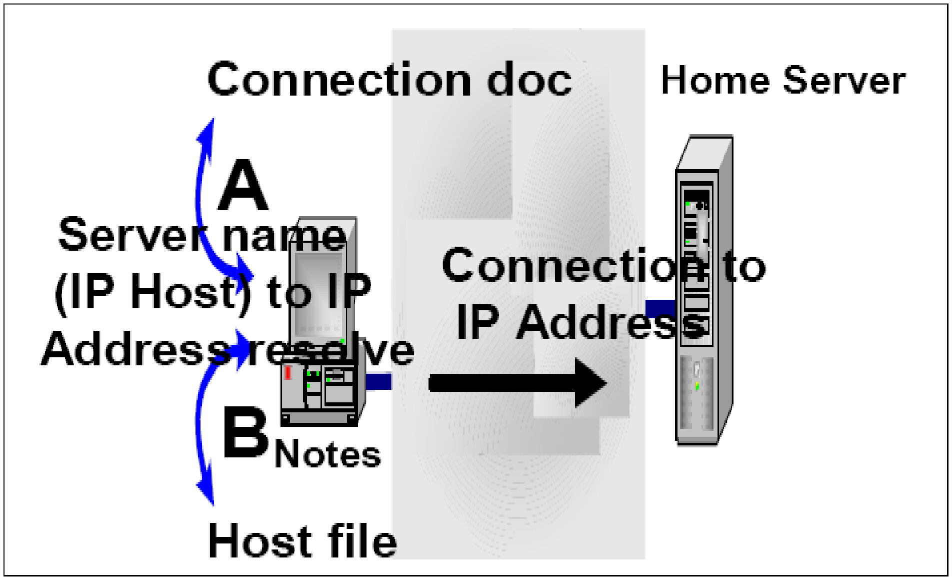


Figure F-1 Local protocol resolve

In some cases a DNS is not available or the Domino server is not listed in the DNS. In other cases the IP domain level where the Domino server is located is deeper than the client's IP domain level. In all of these cases, you can leverage a local host file or (if prepopulated in the user's personal address book via the personal NAB template) connection documents to guide the workstation to the Domino server. This approach must be used if there is no DNS server or the Domino server is not listed in the DNS (as you are likely to do with Internet-based resources). There are a few alternatives with hierarchical DNS resolve problems that require less effort, which we cover later on.

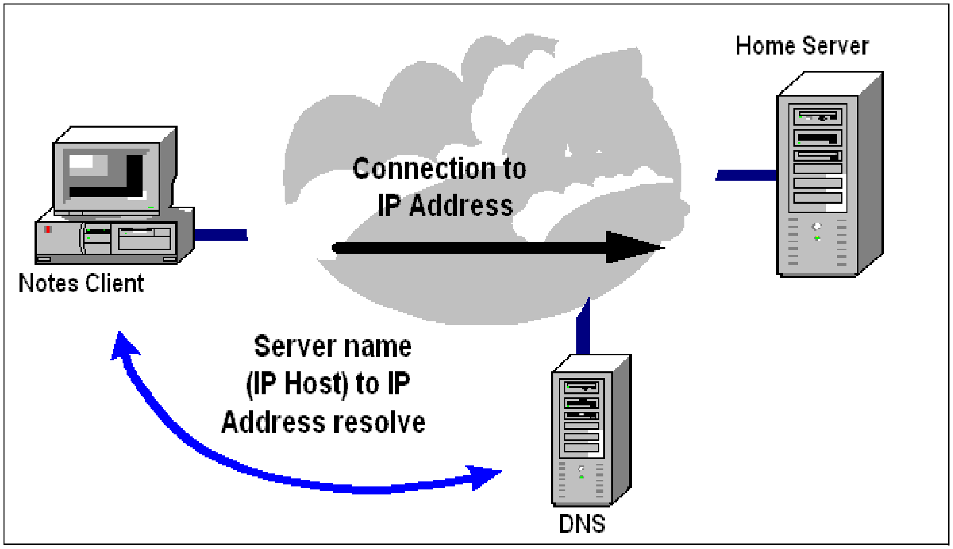


Figure F-2 Centralized protocol resolve

The order of resolve sometimes becomes important when you have multiple listings. A connection document is always used first, then the workstation's host file (default per the IETF RFCs). Because connection documents can be biased to a given location document, this enables you to have multiple listings for the same Domino server by different connection document or host file entries. As an example: a user's laptop needs to access the same Domino server from the Internet as well as from the internal network, but the Domino server is known by different IP addresses either because there is a network address translation (NAT) router in the pathway or the Domino server is multi-homed with two interfaces.

Either directly placing the IP addresses in the connection documents, or placing two different host names that are only known within the connection documents to query either a host file or DNS, enables the Admin to leverage either Notes setup profiles or user policies or replication of connection documents. Or, by using OS replication services to maintain the host file entries directly.

So far our discussion has been how the native IP name resolve process works. If you have a UNIX, AS/400, or S/390® server, this is what you would expect. With Windows NT/2000/XP systems, you may have a second or third name service present (for example, NetBIOS), which could confuse things. Ideally, the server's name should not be the same as the system's name, so name ghosting between the name spaces does not take place. Many connection failures or strange access reactions can be traced to NetBIOS name services getting in the way.

F.2 Leveraging the Notes name services

So far we have talked exclusively about how the Notes client uses the protocol's name services directly to gain access to the user's home server. Once there, the user's home server can offer assistance leveraging the Notes name service within the same Domino domain. For the Notes name service (NNS) to be effective, the given server's Server document must have a resolvable name within the protocol's name service. Depending on what your needs are you may require a Hard versus Soft resolve. A *Hard* resolve implies the full DNS hierarchy is listed out (i.e. red.boston.acme.com). A *Soft* resolve is when only the IP host name is listed (i.e. red). In most cases the Domino server's common name should be used as the simple host name in either case (i.e. 'red' and in the case of the Domino server called Red/Bos/Acme). One problem you can encounter with Hard resolve is when you have multiple IP addresses (multi-homed system), unless you have a means to isolate the resolve from the different directions using different resolvers (host file or parallel DNS offer, as in the case of a shadow DNS).

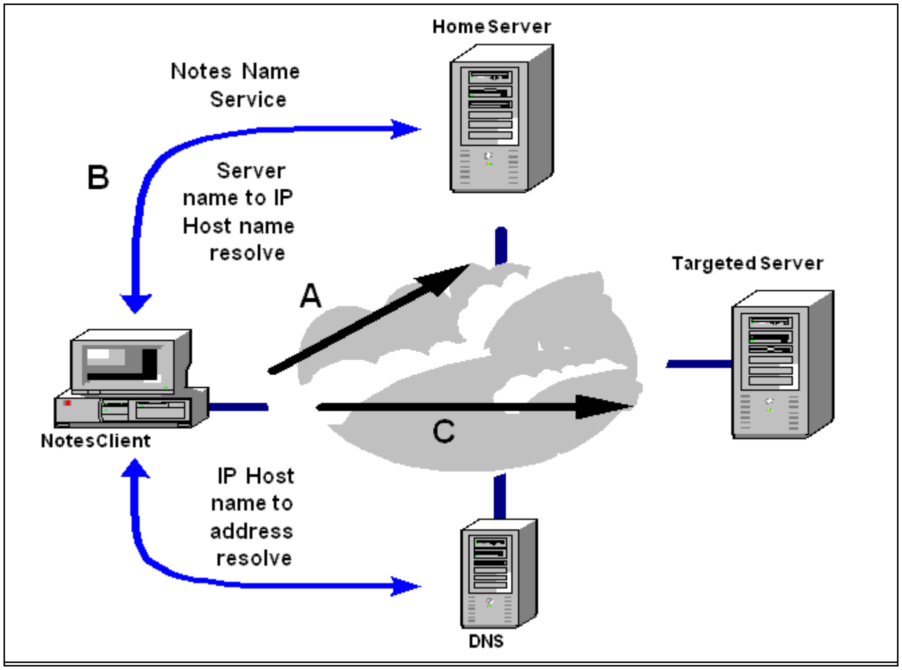

Home Server
Notes Name Service
B
Server name to IP Host name resolve
A
Targeted Server
NotesClient
C
IP Host name to address resolve
DNS

Figure F-3 Notes name service to central resolve

In Figure F-3, we can see how the user's home server (Home Server) can offer an alternative host name or the fully qualified host name of the targeted server. So, looking at the example, we can see how the Home Server is able to supply the Notes client with the protocol's name (targetedserver.chicago.acme.com, for example), and if the user's workstation's name lookup scope was based in boston.acme.com, the workstation is able to get to the correct subdomain level within the DNS offerings to locate the server in the chicago.acme.com subdomain.

F.3 Leveraging a common secondary Notes name server

So far we have assumed that the user's workstation was within the same DNS subdomain as the user's home server, so simple IP host name resolve was possible for the server's common name (for example, HomeServer). In larger enterprise networks this is not possible, or the user's workstation may be accessing different DNS domains due to DHCP leases when they move about from site to site. While having a connection document for the user's home server can be very useful in making sure the Notes client can locate the home server, there are many good reasons not to do this with a large number of client installs. A better means is to leverage a single Domino server as the secondary name server. As long as the clients can locate this server by its simple IP host name (because it is located within the root level of the DNS domain), this enables a single management point to maintain the lookup offers by the Notes name service.

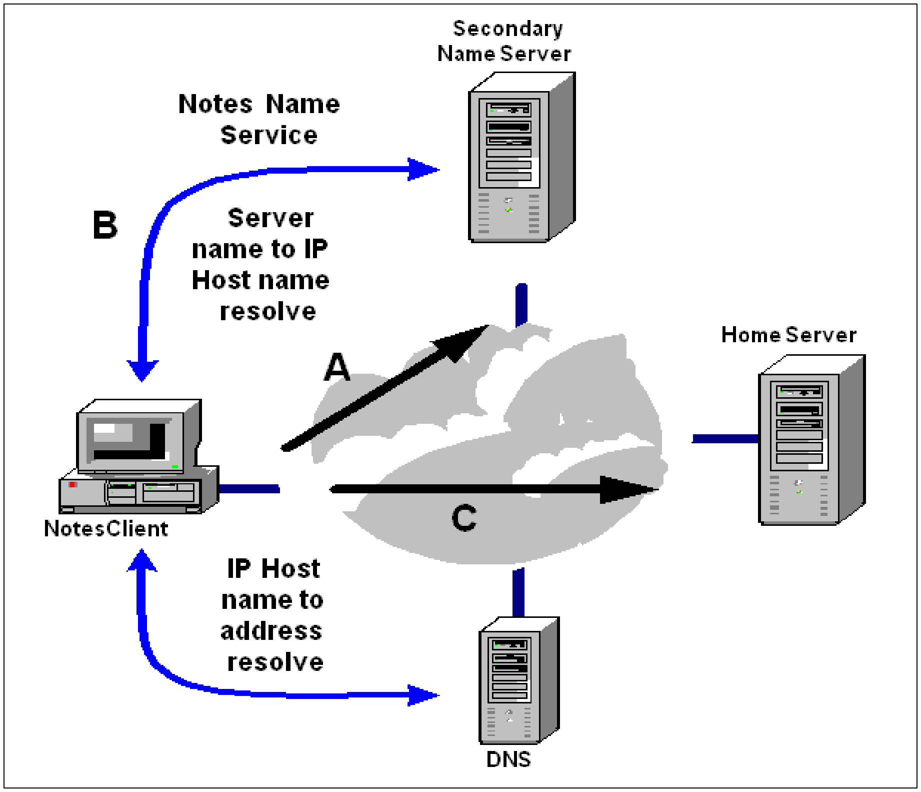


Figure F-4 Notes name service secondary server to central resolve

Here we can see how the Secondary Name Server (we can call it *venus* for simplicity's sake), which is located within the root level of the acme IP domain (venus.acme.com), is accessible from any subdomain location within the acme domain, as long as each of the Server document's Net Address field offers the fully qualified host name of each Domino server Notes name. The name to address resolve is then a matter of the Domino Directory and DNS servers having accurate entries. Sometimes there is no network pathway to this secondary server from one location or another. This is where multiple listings of different servers by the same IP host name can fill the gap. Additionally, having a single server can be thought to be risky, and this is where a Notes cluster can be useful. In the case of multilisting of the same IP host name within the DNS, this requires a DNS based on BIND 9.xx to be functional. It has the advantage of *not* requiring a sustained network connection between the Domino servers, but requiring only that the DNS tables are held in synch between the remote sites and the master DNS server system for the root and subdomains, and that the Domino Directory is replicated as well.

F.4 Using secondary name servers to back up the user's home server

One more use for secondary name servers is when the user's home server goes down or for some other reason is not accessible. This could be because the user is not at a location to gain access to his home server but can access other Domino servers within the Domino domain. As Figure F-5 shows, the user can still locate the targeted server even though his home server cannot be reached for Notes name service resolve assistance.

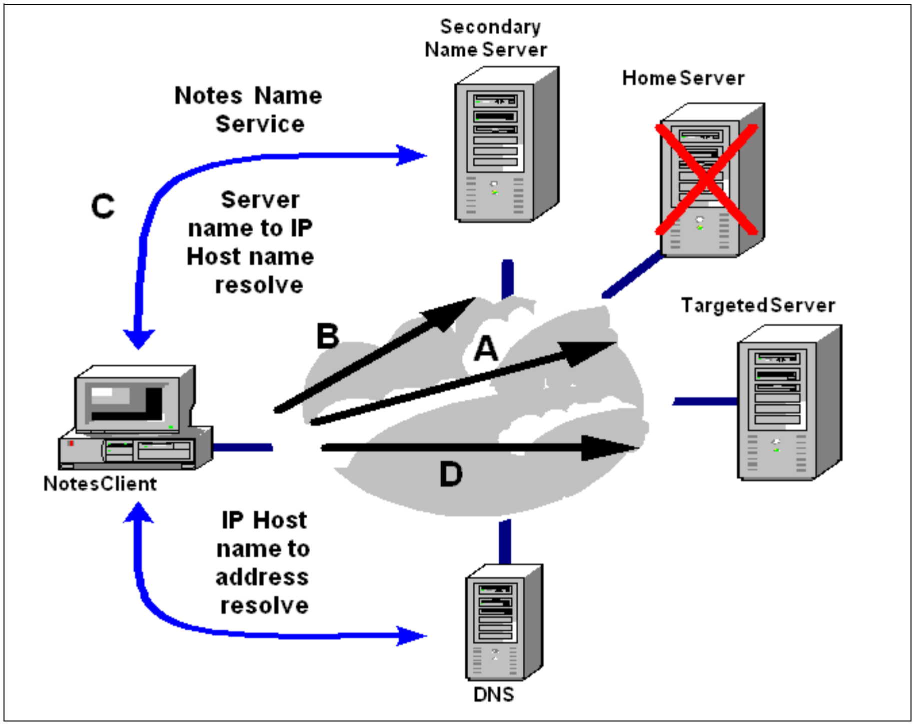


Figure F-5 Secondary name service failover

F.5 Using a pass-through server

Unlike with direct connections, you can encounter network requirements that can be confusing from a resolve process perspective when using a pass-through server because you quite often have to pass through to a different Domino domain. If the pass-through server has no means to query the inner domain's Domino Directory, or the protocol's name-to-address resolve is likewise restricted (both common practices within a DMZ designs), either the connecting Notes client has to tell the pass-through server the targeted system's IP address or the pass-through server has to have connection documents to leverage on behalf of the connecting Notes client as a the resolving proxy. Although our focus is on Notes clients here, Domino servers from other Domino domains likewise can use the same processes. Of course, authentication, certification, and ACL controls also play a part here, securing your Domino servers and their data.

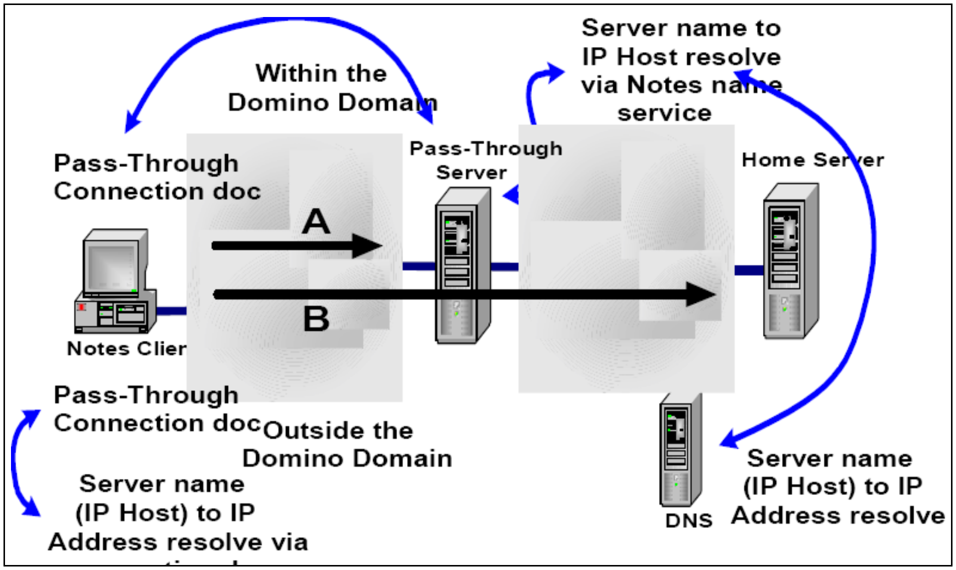


Figure F-6 NRPC pass-through

When using a pass-through server, the user's location document should point to the pass-through server as its secondary Notes name server. In our example we used a discrete server. Ideally, you should have a Notes cluster and point to the cluster's name. Then either using a reverse proxy (Internet) or discrete connection documents for each of the clustered servers gives the remote system the ability to access any one of the servers in the cluster as its pass-through server.

F.6 Conclusions

In all of the configurations we have described here, the given server's Server document Net Address fields carry a fully qualified host name (FQHN), and if there is more than one NRPC TCP port, each offers the same name reference with the expectation that either the remote system's access by name resolve aims them to the correct interface's IP address, or, they have connection documents within Notes that bypass the protocol's name services. This is where the overall design of your Domino and IP networks has to be reviewed carefully to use the best methods given the imposed requirements. Your aim should be to minimize the creation of connection documents in the user's address book. At least limit the connection documents for the user's home server and, if required, the pass-through server, if you do not have a root-level secondary notes name server within your IP domain that all of your Notes clients can leverage if you have a hierarchical IP domain.

G

Moving to IBM Lotus Notes and Domino 7

A new Help database was posted on the IBM Lotus Web site on November 16, 2005, and it merits a mention here in the appendix. No doubt, there are many customers with Domino 5.x and 6.x running on Solaris, and these customers will be interested in upgrading their current Notes and Domino infrastructures to ND7.

It is beyond the scope of this book to address upgrading to ND7 or migrating to ND7 with the detail such topics require. However, to help you structure your upgrade process and rollout, or your migration, visit:

http://www.lotus.com/ldd/notesua.nsf/0/de2da7b609c6cb038525703b005e2f59?OpenDocument

© Copyright IBM Corp. 2006. All rights reserved.

G.1 Upgrading to Lotus Notes/Lotus Domino 7

Most organizations do not move to Lotus Notes/Domino 7 all at once; rather, they phase in Lotus Notes/Domino 7. There is a period of time when the old systems (including earlier releases and other mail and groupware products) coexist with Lotus Notes/Domino 7.

Lotus created Lotus Notes/Domino 7 with this coexistence phase in mind: Key system databases, such as the Domino Directory and the Administration Requests database, were designed for backward compatibility. In addition, features such as native Simple Message Transfer Protocol (SMTP) and Multipurpose Internet Mail Extensions (MIME) support in the Domino router do not require infrastructure changes. Existing routing paths and addressing work as they did in Domino R5 and Domino 6.

G.2 Migrating to Notes and Domino 7 via Domino Upgrade Services

The address books, message stores, and archives of a messaging system contain a great deal of information. When migrating users from another system to Domino and Notes or to Domino Web Access, it is important to maintain both reliable messaging services with minimal disruption and access to the information on the old system by converting that information so that users can access it from a Notes client or Domino Web Access client.

Migration is the process of moving user directory information, mailboxes, mail, and addresses from one system to another. Migration includes importing data from a legacy messaging system and converting it to Notes mail and Domino Directory format. Importing refers to the task of moving data from an external directory, post office, or mailbox and making it available for processing into Domino or Notes format. Converting refers to the task of processing imported information and changing it to Domino or Notes format.

Lotus Domino Upgrade Services include the migration tools for administrators and the upgrade wizards for users. Depending on your environment, and the type of migration you are performing, you may use one or both of these tools.

G.3 ODS issues migrating to Lotus Notes and Domino 7

ODS 41 is the database on-disk structure (ODS) for Domino 5. ODS 43 is the database disk structure for Domino 6.x and 7.x.

Upgrading to Domino 6 or 7 does not require that each database be upgraded to ODS 43. However, if a customer maintains ODS 41 beyond the upgrade to Domino 6 or 7 they should be aware of the impact of this on system loads. Domino 5 uses a different view index engine than Domino 6 and 7; as a result, if ODS41 is maintained, the Domino 5 indexes for each view must be, to, so that the database is usable on a Domino 5 server.

While running on Domino 6 or Domino 7, the server will build new indexes using the new Index engine for Domino 6/7. The result is duplicate indexes for each view. It should also be noted that the index creation will happen on first database access. This will cause higher-than-normal CPU use and memory use as the new indexes are built.

Indexes can consume a large amount of database storage. The amount used can be seen from the Files tab of the Domino 6 Administrator client; select the desired file, then in the right pane select **Manage Views**.

The total amount of storage increase will vary, but is based on database content and view complexity. Customers using database quotas should be wary of exceeding quota limits as a result of creating new indexes.

The ODS 41 indexes will be maintained even after conversion to ODS 43. Customers wishing to reclaim this storage must run a COMPACT - D on the database. The indexes for both Domino 5.x and Domino 6.x/7.x will be deleted.

H

Additional material

This book refers to additional material that can be downloaded from the Internet as described below.

Locating the Web material

The Web material associated with this book is available in softcopy from the IBM Redbooks Web server. Point your Web browser to:

ftp://www.redbooks.ibm.com/redbooks/SG247162

Alternatively, you can go to the IBM Redbooks Web site at:

http://ibm.com/redbooks

Select **Additional materials** and open the directory that corresponds with the redbook form number, SG247162.

Using the Web material

The additional Web material that accompanies this book includes the following file:

File name	*Description*
SG247162.zip	Start and stop scripts

© Copyright IBM Corp. 2006. All rights reserved.

System requirements for downloading the Web material

The following system configuration is recommended:

Hard disk space:	1 MB minimum
Operating System:	Solaris/Windows/Linux/AIX/UNIX

How to use the Web material

Create a subdirectory (folder) on your workstation, and unzip the contents of the Web material zip file into this folder.

The Solaris command to unzip this file is:

```
unzip SG247162.zip
```

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

For information about ordering these publications, see "How to get IBM Redbooks" on page 574. Note that some of the documents referenced here may be available in softcopy only.

- *Getting the Most From Your Domino Directory,* SG24-5986
- *Lotus Domino 6 spam Survival Guide for IBM eServer*, SG24-6930
- *Lotus Domino R5 for Sun Solaris 8,* SG24-5969
- *Lotus Notes and Domino Security Infrastructure Revealed*, SG24-5341

Other publications

These publications are also relevant as further information sources:

- *Sun Performance and Tuning: Java and the Internet* by Adrian Cockcroft and Richard Pettit, ISBN 0-13-095249-4.The book is now rather dated; computers have become much larger and faster in the seven years since its publication. Nonetheless the approaches and insights it offers remain valuable, and the volume belongs on every Solaris administrator's bookshelf.

Online resources

These Web sites and URLs are also relevant as further information sources:

- Sun's Web site for information about the Sun and Lotus alliance:

  `http://www.sun.com/lotus/`

- *Domino on Solaris: Common Tuning Tips* is updated from time to time with the latest information on tuning both Domino and Solaris for best performance. Look for it in the Technical Documentation section at Sun's Lotus information page:

  `http://www.sun.com/lotus/`

© Copyright IBM Corp. 2006. All rights reserved.

- Sun’s Web site for Solaris system administrator resources:

  `http://www.sun.com/bigadmin`

- Sun’s Web site for documentation:

  `http://www.sun.com/docs`

- Sun’s Web site for patches:

  `http://www.sun.com/sunsolve`

- Upgrading to IBM Lotus Notes/Domino 7:

  `http://www-10.lotus.com/ldd/notesua.nsf/0/de2da7b609c6cb038525703b005e2f59?OpenDocument`

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

© Copyright IBM Corp. 2006. All rights reserved.

IBM

Redbooks

Domino 7 for Sun Solaris 10

(1.0” spine)
0.875”<->1.498”
460 <-> 788 pages

Domino 7 for Sun Solaris 10

Installation, configuration, and administration

Tuning IBM Lotus Domino 7 and Sun Solaris 10

Domino 7 and Solaris 10 security overview

Although the IBM Lotus Domino server is platform independent, each platform it runs on requires some additional platform-specific knowledge and configuration to ensure that it operates efficiently and at maximum capability. This IBM Redbook explains how to run Domino 7 on the Sun Solaris 10 Operating Environment.

The primary focus is to explain the installation, configuration, and performance tuning of Domino 7 in this environment. We take you through all of the steps that are required to run a Domino 7 server on Solaris 10, from choosing the right hardware, installing Solaris and Domino, tuning the OS and the Domino server, security for the OS and Domino, and performing administrative tasks, through to problem determination and troubleshooting.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7162-00 ISBN 0738496065