IBM Tivoli Storage Manager for Mail
Version 6.3

Data Protection for Lotus Domino UNIX and Linux

Installation and User's Guide

SC27-4021-00

IBM Tivoli Storage Manager for Mail
Version 6.3

Data Protection for Lotus Domino UNIX and Linux

Installation and User's Guide

SC27-4021-00

Note:

Before using this information and the product it supports, read the information in “Notices” on page 205.

This edition applies to Version 6.3 of IBM Tivoli Storage Manager for Mail Data Protection for Lotus Domino (product number 5608-E06), and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters. This edition replaces SC32-9057-04

Contents

Tables v

About this publication vii

Who should read this guide vii
Publications vii
  Tivoli Storage Manager publications viii
  Tivoli Storage FlashCopy Manager publications. . x
Support information x
  Getting technical training x
  Searching knowledge bases xi
  Contacting IBM Software Support xiii
Conventions used in this book. xiv
Reading syntax diagrams. xv

New for IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino Version 6.3 xix

Chapter 1. Overview of Data Protection for Domino 1

Features 1
Backup (NSF databases) 2
  Domino NSF database backup and transaction log archive 2
  Expiration of NSF archived transaction log files. . 3
  NSF backup strategy considerations 4
Backup (DB2 enabled Notes databases) 6
  DB2 enabled Notes database backup 6
  Expiration of DB2 backups and transaction log objects 8
  DB2 enabled Notes database backup strategy considerations 8
Restore (NSF databases) 10
  Domino database restore and activation 10
  Restore of archived transaction logs 11
  Restore at document level 11
Restore (DB2 enabled Notes databases) 11
  Domino DB2 enabled Notes database restore, rollforward, and activation 11
Security 13
Performance 13

Chapter 2. Installing Data Protection for Domino 17

Prerequisites 17
Procedures 18
  Installing on AIX 18
  Installing on Linux 20
  Quick install 21

Chapter 3. Configuring Data Protection for Domino 23

Configure the Domino Server environment with dominstall 23
  Performing a manual dominstall configuration . 23
  Performing a silent dominstall configuration . . 27
  Dominstall considerations 29
Set environment variables 31
  Data Protection for Domino environment variables 31
  Tivoli Storage Manager environment variables. . 32
  Bourne and Korn Shell environment variables . . 32
  C Shell environment variables 33
Communication 33
Register 33
Create policy 34
Options and preferences 35
  Required options 36
  Preferred options 36
  Additional options 38
  Option precedence 40
DB2 enabled Notes Configuration 40
Graphical User Interface 44
  Getting started 45
  Backing up Domino NSF databases 48
  Backing up Domino DB2 enabled Notes databases and DB2 logs 48
  Restoring Domino NSF databases 49
  Restoring, rollforward, and activating Domino DB2 enabled Notes databases 50
  Activating NSF databases. 51
  Backing up (archiving) NSF transaction logs . . 52
  Restoring NSF transaction logs 52
  Inactivating archived NSF transaction logs . . . 53
Command-line interface 53
  NSF Commands 53
  DB2 Commands 129

Chapter 4. Protecting Lotus Domino Server data 169

Automating backups 169
  Scenario 169
  Scheduler considerations 172
  Setting up other schedules 173
  Sample command files 174
Recovery from loss of Domino transaction logs for NSF databases 176
Alternate server and alternate partition restores for NSF databases 177
  How to perform an alternate server restore for NSF databases 178
  How to perform an alternate partition restore for NSF databases 180
Include and exclude processing 182
Multiple Domino server partitions 185
Multiple Tivoli Storage Manager servers 186
Problem determination 187

Migration 188
  Migration in a replicated server environment 188
  Migration in a nonreplicated server environment 189
Using Data Protection for Domino to back up and restore Lotus Domino databases with DAOS . . . 189
  Overview. 189
  Using Data Protection for Domino to back up a Lotus Domino database with DAOS 191
  Using Data Protection for Domino to restore a Lotus Domino database with DAOS 193
  Disaster recovery for a Lotus Domino database with DAOS 195

Chapter 5. Reference information . . . 197
Frequently asked questions 197
Best practices 201

Appendix. Accessibility features for the Tivoli Storage Manager product family. 203

Notices 205
Trademarks 207

Glossary 209

Index 239

Tables

1. Tivoli Storage Manager server publications viii
2. Tivoli Storage Manager storage agent publications viii
3. Tivoli Storage Manager client publications ix
4. Tivoli Storage Manager data protection publications ix
5. IBM Tivoli Storage Manager troubleshooting and tuning publications ix
6. Tivoli Storage FlashCopy Manager publications x

About this publication

IBM® Tivoli® Storage Manager for Mail Data Protection for Domino® is a storage management software product that provides storage management services in a multiplatform environment. This publication explains how to install, configure, and administrate Data Protection for Domino.

Who should read this guide

The target audience for this publication are system installers, system users, Tivoli Storage Manager administrators, database administrators, Domino administrators, and system administrators. It explains the procedures needed to install and customize Data Protection for Domino.

In this publication, it is assumed that you have an understanding of the following applications:

- IBM DB2® UDB for UNIX or Linux
- Lotus® Domino Server
- Tivoli Storage Manager server
- Tivoli Storage Manager backup-archive client
- Tivoli Storage Manager Application Program Interface

It is also assumed that you have an understanding of one of the following operating systems:

- AIX®
- Linux

Publications

Publications for the IBM Tivoli Storage Manager family of products are available online. The IBM Tivoli Storage Manager product family includes IBM Tivoli Storage FlashCopy® Manager, IBM Tivoli Storage Manager for Space Management, IBM Tivoli Storage Manager for Databases, and several other storage management products from IBM Tivoli.

To search all publications, go to the Tivoli Storage Manager information center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.

You can download PDF versions of publications from the Tivoli Storage Manager information center or from the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Go to Tivoli Documentation Central to find information centers that contain official product documentation for current and previous versions of Tivoli products, including the Tivoli Storage Manager product family. You can find Tivoli Documentation Central at https://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home.

You can also order some related publications from the IBM Publications Center website. The website provides information about ordering publications from countries other than the United States. In the United States, you can order publications by calling 1-800-879-2755.

Tivoli Storage Manager publications

The following tables list the publications that make up the Tivoli Storage Manager library.

Table 1. Tivoli Storage Manager server publications

Publication title	**Order number**
IBM Tivoli Storage Manager for AIX Installation Guide	GC23-9781
IBM Tivoli Storage Manager for AIX Administrator's Guide	SC23-9769
IBM Tivoli Storage Manager for AIX Administrator's Reference	SC23-9775
IBM Tivoli Storage Manager for HP-UX Installation Guide	GC23-9782
IBM Tivoli Storage Manager for HP-UX Administrator's Guide	SC23-9770
IBM Tivoli Storage Manager for HP-UX Administrator's Reference	SC23-9776
IBM Tivoli Storage Manager for Linux Installation Guide	GC23-9783
IBM Tivoli Storage Manager for Linux Administrator's Guide	SC23-9771
IBM Tivoli Storage Manager for Linux Administrator's Reference	SC23-9777
IBM Tivoli Storage Manager for Oracle Solaris Installation Guide	GC23-9784
IBM Tivoli Storage Manager for Oracle Solaris Administrator's Guide	SC23-9772
IBM Tivoli Storage Manager for Oracle Solaris Administrator's Reference	SC23-9778
IBM Tivoli Storage Manager for Windows Installation Guide	GC23-9785
IBM Tivoli Storage Manager for Windows Administrator's Guide	SC23-9773
IBM Tivoli Storage Manager for Windows Administrator's Reference	SC23-9779
IBM Tivoli Storage Manager for z/OS Media Installation and User's Guide	SC27-4018
IBM Tivoli Storage Manager Upgrade and Migration Guide for V5 Servers	GC27-4017
IBM Tivoli Storage Manager Integration Guide for Tivoli Storage Manager FastBack®	SC27-2828

Table 2. Tivoli Storage Manager storage agent publications

Publication title	**Order number**
IBM Tivoli Storage Manager for SAN for AIX Storage Agent User's Guide	SC23-9797
IBM Tivoli Storage Manager for SAN for HP-UX Storage Agent User's Guide	SC23-9798
IBM Tivoli Storage Manager for SAN for Linux Storage Agent User's Guide	SC23-9799
IBM Tivoli Storage Manager for SAN for Oracle Solaris Storage Agent User's Guide	SC23-9800
IBM Tivoli Storage Manager for SAN for Windows Storage Agent User's Guide	SC23-9553

Table 3. Tivoli Storage Manager client publications

Publication title	Order number
IBM Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide	SC23-9791
IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and User's Guide	SC23-9792
IBM Tivoli Storage Manager Using the Application Programming Interface	SC23-9793
IBM Tivoli Storage Manager for Space Management for UNIX and Linux: User's Guide	SC23-9794
IBM Tivoli Storage Manager HSM for Windows Administration Guide	SC23-9795

Table 4. Tivoli Storage Manager data protection publications

Publication title	Order number
IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide	GC27-4010
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for UNIX and Linux Installation and User's Guide	SC27-4019
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for Windows Installation and User's Guide	SC27-4020
IBM Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server Installation and User's Guide	GC27-4009
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino UNIX and Linux Installation and User's Guide	SC27-4021
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino for Windows Installation and User's Guide	SC27-4022
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for DB2	SC33-6341
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for Oracle	SC33-6340
IBM Tivoli Storage Manager for Virtual Environments Installation and User's Guide	SC27-2898
IBM Tivoli Storage Manager for Microsoft SharePoint Guide	N/A

Table 5. IBM Tivoli Storage Manager troubleshooting and tuning publications

Publication title	Order number
IBM Tivoli Storage Manager Problem Determination Guide	GC23-9789
IBM Tivoli Storage Manager Performance Tuning Guide	GC23-9788
IBM Tivoli Storage Manager Client Messages and Application Programming Interface Return Codes	SC27-2878
IBM Tivoli Storage Manager Server Messages and Error Codes	SC27-2877
IBM Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server Messages	GC27-4011
IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Messages	GC27-4012
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle Messages	SC27-4014

Table 5. IBM Tivoli Storage Manager troubleshooting and tuning publications (continued)

Publication title	Order number
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino Messages	SC27-4015
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Messages	SC27-4016

Note: You can find information about IBM System Storage® Archive Manager at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3/c_complydataretention_ovr.html.

Tivoli Storage FlashCopy Manager publications

The following table lists the publications that make up the Tivoli Storage FlashCopy Manager library.

Table 6. Tivoli Storage FlashCopy Manager publications

Publication title	Order number
IBM Tivoli Storage FlashCopy Manager for UNIX and Linux Installation and User's Guide	SC27-4005
IBM Tivoli Storage FlashCopy Manager for Windows Installation and User's Guide	SC27-4006
IBM Tivoli Storage FlashCopy Manager for VMware Installation and User's Guide	SC27-4007
IBM Tivoli Storage FlashCopy Manager Messages	GC27-4008

Support information

You can find support information for IBM products from various sources.

Start at the IBM Support Portal: http://www.ibm.com/support/entry/portal/. You can select the products that you are interested in and search for a wide variety of relevant information.

Getting technical training

Information about Tivoli technical training courses is available online.

Go to the following websites to sign up for training, ask questions, and interact with others who use IBM storage products.

Tivoli software training and certification
Choose from instructor led, online classroom training, self-paced Web classes, Tivoli certification preparation, and other training options at http://www.ibm.com/software/tivoli/education/

Tivoli Support Technical Exchange
Technical experts share their knowledge and answer your questions in webcasts at http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html.

Storage Management community
Interact with others who use IBM storage management products at http://www.ibm.com/developerworks/servicemanagement/sm/index.html

Global Tivoli User Community
Share information and learn from other Tivoli users throughout the world at http://www.tivoli-ug.org/.

IBM Education Assistant
View short "how to" recordings designed to help you use IBM software products more effectively at http://publib.boulder.ibm.com/infocenter/ieduasst/tivv1r0/index.jsp

Searching knowledge bases

If you have a problem with your Tivoli Storage Manager family product, there are several knowledge bases that you can search.

Begin by searching the Tivoli Storage Manager Information Center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3. From this website, you can search the current Tivoli Storage Manager documentation.

Searching the Internet

If you cannot find an answer to your question in the IBM Tivoli Storage Manager information center, search the Internet for the information that might help you resolve your problem.

To search multiple Internet resources, go to the IBM support website at http://www.ibm.com/support/entry/portal/.

You can search for information without signing in. Sign in using your IBM ID and password if you want to customize the site based on your product usage and information needs. If you do not already have an IBM ID and password, click **Sign in** at the top of the page and follow the instructions to register.

From the support website, you can search various resources including:
- IBM technotes
- IBM downloads
- IBM Redbooks® publications
- IBM Authorized Program Analysis Reports (APARs)

Select the product and click **Downloads** to search the APAR list.

If you still cannot find a solution to the problem, you can search forums and newsgroups on the Internet for the latest information that might help you find problem resolution.

An independent user discussion list, ADSM-L, is hosted by Marist College. You can subscribe by sending an email to listserv@vm.marist.edu. The body of the message must contain the following text: `SUBSCRIBE ADSM-L` *your_first_name your_family_name*.

To share your experiences and learn from others in the Tivoli Storage Manager and Tivoli Storage FlashCopy Manager user communities, go to the following wikis:

Tivoli Storage Manager wiki
http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager

Tivoli Storage FlashCopy Manager wiki
https://www.ibm.com/developerworks/mydeveloperworks/wikis/home/wiki/Tivoli Storage FlashCopy Manager

Using IBM Support Assistant

IBM Support Assistant is a complimentary software product that can help you with problem determination. It is available for some Tivoli Storage Manager and Tivoli Storage FlashCopy Manager products.

To learn about which products are supported, go to the IBM Support Assistant download web page at http://www.ibm.com/software/support/isa/download.html.

IBM Support Assistant helps you gather support information when you must open a problem management record (PMR), which you can then use to track the problem. The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

You can find more information at the IBM Support Assistant website:

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

You can also install the stand-alone IBM Support Assistant application on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use. Find add-ons for specific products at http://www.ibm.com/support/docview.wss?uid=swg27012689.

Finding product fixes

A product fix to resolve your problem might be available from the IBM software support website.

You can determine what fixes are available by checking the IBM software support website at http://www.ibm.com/support/entry/portal/.

- If you previously customized the site based on your product usage:
  1. Click the link for your product, or a component for which you want to find a fix.
  2. Click **Downloads**, and then click **Fixes by version**.
- If you have not customized the site based on your product usage, click **Downloads** and search for your product.

Receiving notification of product fixes

You can receive notifications about fixes, flashes, upgrades, and other news about IBM products.

To sign up to receive notifications about IBM products, follow these steps:

1. From the support page at http://www.ibm.com/support/entry/portal/, click **Sign in to create, manage, or view your subscriptions** in the **Notifications** pane.
2. Sign in using your IBM ID and password. If you do not have an ID and password, click **register now** and complete the registration process.
3. Click **Manage all my subscriptions** in the **Notifications** pane.
4. Click the **Subscribe** tab and then click **Tivoli**.
5. Select the products for which you want to receive notifications and click **Continue**.

6. Specify your notification preferences and click **Submit**.

Contacting IBM Software Support

You can contact IBM Software Support if you have an active IBM subscription and support contract and if you are authorized to submit problems to IBM.

To obtain help from IBM Software Support, complete the following steps:

1. Ensure that you have completed the following prerequisites:
    a. Set up a subscription and support contract.
    b. Determine the business impact of your problem.
    c. Describe your problem and gather background information.
2. Follow the instructions in "Submitting the problem to IBM Software Support" on page xiv.

Setting up a subscription and support contract

Set up a subscription and support contract. The type of contract that you need depends on the type of product you have.

For IBM distributed software products (including, but not limited to, IBM Tivoli, Lotus, and Rational® products, as well as IBM DB2 and IBM WebSphere® products that run on Microsoft Windows or on operating systems such as AIX or Linux), enroll in IBM Passport Advantage® in one of the following ways:

- **Online:** Go to the Passport Advantage website at http://www.ibm.com/software/lotus/passportadvantage/, click **How to enroll**, and follow the instructions.
- **By telephone:** You can call 1-800-IBMSERV (1-800-426-7378) in the United States. For the telephone number to call in your country, go to the IBM Software Support Handbook web page at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you must understand and assess the business impact of the problem you are reporting.

Severity 1	**Critical** business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	**Significant** business impact: The program is usable but is severely limited.
Severity 3	**Some** business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	**Minimal** business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describing the problem and gathering background information

When explaining a problem to IBM, it is helpful to be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently.

To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? For example, hardware, operating system, networking software, and so on.
- Are you using a workaround for this problem? If so, be prepared to explain it when you report the problem.

Submitting the problem to IBM Software Support

You can submit the problem to IBM Software Support online or by telephone.

Online

Go to the IBM Software Support website at http://www.ibm.com/support/entry/portal/Open_service_request/Software/Software_support_(general). Sign in to access IBM Service Requests and enter your information into the problem submission tool.

By telephone

For the telephone number to call in your country, go to the IBM Software Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.

Conventions used in this book

This guide uses several conventions for special terms and actions, operating system-dependent commands and paths.

This guide uses the following typeface conventions:

Bold

- Commands, keywords, authorization roles, or other information that you must use.
- Example: Log on to the server as **root** user.

italics

- Values or variables that you must provide.
- Emphasized words and phrases.
- Example: The node name of the *production node* and *backup node* must not be the same.

bold italics

- Options and parameters.
- Example: Specify the value for the ***compression*** option.

`monospace`

- Directories, parameters, URLs, and output examples.
- Example: The product is installed in the `/usr/tivoli/tsm/client/ba/bin` directory.

UPPER CASE

- Environment variables associated with Tivoli Storage Manager, operating systems, or Domino server.
- Example: Make sure the DSM_DIR environment variable is set correctly.

Reading syntax diagrams

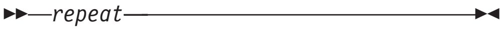
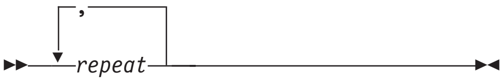
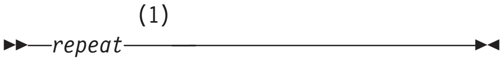
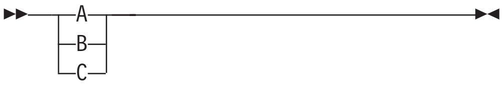
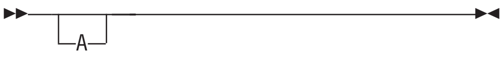
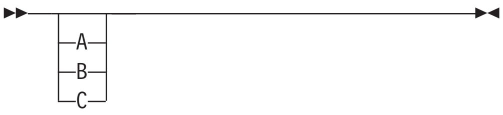
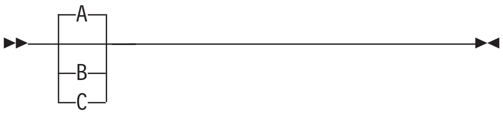
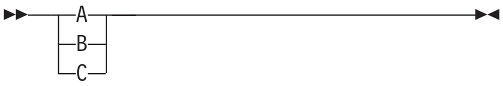
This section describes how to read the syntax diagrams used in this book. To read a syntax diagram, follow the path of the line. Read from left to right, and top to bottom.

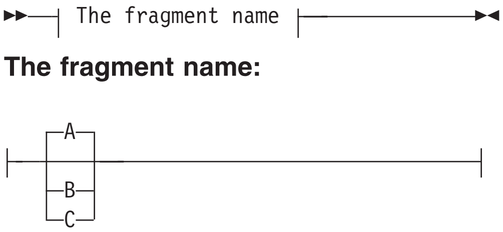
- The ►►── symbol indicates the beginning of a syntax diagram.
- The ───► symbol at the end of a line indicates the syntax diagram continues on the next line.
- The ►── symbol at the beginning of a line indicates a syntax diagram continues from the previous line.
- The ──►◄ symbol indicates the end of a syntax diagram.

Syntax items, such as a keyword or variable, can be:

- On the line (required element)
- Above the line (default element)
- Below the line (optional element).

Syntax Diagram Description	Example
Abbreviations: Uppercase letters denote the shortest acceptable truncation. If an item appears entirely in uppercase letters, it cannot be truncated. You can type the item in any combination of uppercase or lowercase letters. In this example, you can enter KEYWO, KEYWORD, or KEYWOrd.	`►►──KEYWOrd──────────────────────────►◄`
Symbols: Enter these symbols exactly as they appear in the syntax diagram.	* Asterisk { } Braces : Colon , Comma = Equal Sign - Hyphen () Parentheses . Period Space
Variables: Italicized lowercase items (*var_name*) denote variables. In this example, you can specify a *var_name* when you enter the KEYWORD command.	`►►──KEYWOrd──`*`var_name`*`──────────────►◄`

Syntax Diagram Description	Example
Repetition: An arrow returning to the left means you can repeat the item. A character or space within the arrow means you must separate repeated items with that character or space. A footnote by the arrow references the number of times you can repeat the item.	   **Notes:** 1 Specify *repeat* as many as 5 times.
Required Choices: When two or more items are in a stack and one of them is on the line, you *must* specify one item. In this example, you *must* choose A, B, or C.	
Optional Choice: When an item is below the line, that item is optional. In the first example, you can choose A or nothing at all. When two or more items are in a stack below the line, all of them are optional. In the second example, you can choose A, B, C, or nothing at all.	 
Defaults: Defaults are above the line. The default is selected unless you override it. You can override the default by including an option from the stack below the line. In this example, A is the default. You can override A by choosing B or C. You can also specify the default explicitly.	
Repeatable Choices: A stack of items followed by an arrow returning to the left means you can select more than one item or, in some cases, repeat a single item. In this example, you can choose any combination of A, B, or C.	

Syntax Diagram Description	Example
Syntax Fragments: Some diagrams, because of their length, must fragment the syntax. The fragment name appears between vertical bars in the diagram. The expanded fragment appears between vertical bars in the diagram after a heading with the same fragment name.	

New for IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino Version 6.3

Read about the new features and other changes in Data Protection for Lotus Domino Version 6.3.

Enhanced Statistics

Data Protection for Lotus Domino now indicates whether a backup or a restore is encrypted, compressed, LAN-free, or deduplicated.

The final statistics for backup operations provide deduplication, LAN-free, and compression information about the backup. The final statistics for restore provide LAN-free information about the restore. There is no information about encryption in the final statistics for either backup or restore.

When viewing the backups that are available to be restored, you can see if the backup was encrypted, deduplicated, or compressed. There is no information about LAN-free for the available backups as this information is only available in the final statistics.

This new functionality does not apply to DB2 operations.

Client Scalability

Memory has been enhanced for in-memory lists that contain large numbers of objects.

Communication Resiliency

Data Protection for Lotus Domino has been modified to tolerate most types of connectivity failures.

Cancel Session Support

Verifies whether the session was canceled by the Tivoli Storage Manager operator. Data Protection for Domino exits without processing any additional databases.

UTF-8 is added for the language locales that are already supported by Data Protection for Domino

The Data Protection for Domino version 6.3 message catalogs are encoded in UTF-8. If you are installing the Data Protection for Domino message catalogs for languages other than English, and you are not running in a UTF-8 locale, you must also have the appropriate iconv UTF-8 to the local locale converters installed on your system. If the appropriate iconv UTF-8 converters are not installed, all **Data Protection for Domino** messages are displayed in English.

Chapter 1. Overview of Data Protection for Domino

An overview of the features and capabilities of Tivoli Storage Manager Data Protection for Lotus Domino.

Features

An overview of Data Protection for Domino features is presented.

Data Protection for Domino for AIX, Linux, UNIX and System Services UNIX. is an application that backs up and restores Lotus Domino databases and transaction logs. When archival logging is used on the Domino server, it archives transaction log files and retrieves them as required for a database recovery. Database backups and archived transaction log files are stored on Tivoli Storage Manager server.

Data Protection for Domino communicates with a Tivoli Storage Manager server using the Tivoli Storage Manager application programming interface (API). Data Protection for Domino communicates with a Domino server using the Lotus Domino API.

Tasks

Data Protection for Domino helps protect and manage Lotus Domino server data by allowing you to perform the following actions:

- Back up Lotus Domino NSF databases.
- Back up DB2 enabled Notes® databases when a DB2-enabled Domino server is available.
- Restore DB2 enabled Notes databases when a DB2-enabled Domino server is available.
- Maintain multiple backup versions of Domino databases.
- Archive Lotus Domino transaction log files when archival logging is in effect.
- Restore backup versions of a Lotus Domino database and apply changes since the last backup from the transaction log.
- Restore Domino databases to a specific point in time.
- Restore one or more archived transaction log files.
- Expire database backups automatically based on version limit and retention period.
- Expire archived transaction log files when no longer needed.
- Automate scheduled backups.
- Restore Domino databases to an alternate server or partition.
- Access Data Protection for Domino remotely using the Tivoli Storage Manager Web client.
- Access Data Protection for Domino using the client GUI based on Oracle Java™.
- Access Data Protection for Domino using the command-line interface.

Backup (NSF databases)

This section describes the types of Domino NSF backups available with Data Protection for Domino.

Domino NSF database backup and transaction log archive

Concepts associated with Data Protection for Domino back ups of Domino databases and transaction logs.

The backup and recovery API in Domino provides the capability to perform these tasks

- Online full backups of individual databases
- Archives of the transaction log when archival logging is in effect.

Domino server transaction log

Updates to a logged database are recorded in the Domino server transaction log so full database backups are not required as frequently. Changes to a database since the last full backup can be applied from the transaction log after the backup is restored from the last full backup. Enabling transaction logging for all databases on a Domino server is not required, so the backup process must handle both logged and non-logged databases. Domino allows the active transaction log to be backed up as well.

Transactions recorded in the transaction log are keyed by a Database Instance Identifier (DBIID), which is unique for each database on a Domino server. The DBIID must match that of a restored database for transactions in the log to be applied to the database. The most common reason for a DBIID to change is compaction of the database to reduce file size. Therefore, whenever the DBIID of a database changes, a full backup must be taken so that subsequent updates (which are recorded in the transaction log) can be applied to a restored backup of that database. Transactions recorded since the DBIID change cannot be applied to prior backups of that database because the DBIID will not match. See your Domino server documentation for more information about the DBIID and when it can change.

Types of NSF backup and archive logs

Data Protection for Domino provides two types of database backups and an archive log function:

Incremental Backup

An incremental backup provides a conditional backup function that performs a full online backup of Domino databases under the following conditions:

- The database is not excluded in the Tivoli Storage Manager include-exclude options file (standard include and exclude processing is supported).
- The database is not logged and was modified since the last active backup image for that database. Both data and non-data modification dates are checked. If either is different from that of the active backup, the database is backed up.
- Archival logging is in effect and the DBIID of a logged database changed. If the DBIID has not changed, then logged databases are not backed up (the changes are captured in the transaction log backups). In

this case, periodic selective backups of all logged databases should be done to refresh the active backup images. This reduces the number of transaction logs to be applied during a recovery.

Note: When circular logging is used on the Domino server or when logging is disabled on the Domino server, transaction log files are not archived.

- The database is new or newly included in the backup and an active backup image does not exist on the Tivoli Storage Manager server.

The **incremental** command includes a function that determines if active backup database copies exist on the Tivoli Storage Manager server that are deleted from the Domino server or excluded from backup. If so, they are marked inactive so that automatic expiration of these backup copies can occur according to defined Tivoli Storage Manager management class parameters for backup files.

Selective Backup

A selective backup unconditionally performs a full online backup of the specified Domino databases, unless they are excluded from backup through exclude statements within the Data Protection for Domino options file (dsm.opt).

Archive Log

An archive log stores filled transaction log files on the Tivoli Storage Manager server so that space allocated to these files can be reused by the Domino logger. The **`archivelog`** command is available when transaction logging on the Domino server is enabled in archival mode. Filled transaction log files must be archived frequently enough to ensure the transaction log never fills completely and stops the Domino server.

Transaction log files stored on the Tivoli Storage Manager server are automatically restored as needed for a database recovery.

Archived transaction log files are retained on the Tivoli Storage Manager server as long as a database backup exists that needs these log files for a complete recovery. See “Expiration of NSF archived transaction log files” for further details.

Note: When circular or linear loop logging is used on the Domino server (or when logging is disabled on the Domino Server), transaction log files are not archived. See “NSF backup strategy considerations” on page 4 for more information.

Expiration of NSF archived transaction log files

This section describes concepts associated with expiring archived transaction log files.

The **`inactivatelogs`** command expires transaction log files from backup storage. There is a single shared transaction log for all logged databases on a Domino server. Thus log files cannot be deactivated (and allowed to expire) until all databases that require that log file for recovery are inactive. This command queries the database backups on the Tivoli Storage Manager server to determine which log files are required by any active database backup. This command also deactivates log files that are no longer required (because the database backups were deactivated). Run the **`inactivatelogs`** command after a full database backup is completed to deactivate the transaction logs as the database backups requiring them are deactivated.

NSF backup strategy considerations

This section describes factors to consider when planning your backup strategy and provides sample strategies.

You can choose different backup strategies depending on your specific requirements regarding network traffic, backup window, and acceptable restore times. Your choice of strategy includes selecting the type of backup commands to use and the type of transaction logging to be done on the Domino server. Data Protection for Domino can only back up transaction logs from a Domino server that has archival logging in effect. Transaction logs cannot be backed up from a Domino server that has circular or linear loop logging in effect.

Archival logging allows transaction log data to be *archived* on the Tivoli Storage Manager server so that changes to logged databases can be stored on the Tivoli Storage Manager server without having to perform a full backup. This allows a strategy with less frequent full database backups because changes to logged databases are available for restore in the archived transaction log files.

The **`archivelog`** command backs up Domino transaction log files when archival logging is in effect on the Domino server. The command queries the Domino server to determine if any log extents are ready for archiving. If so, the log files are backed up to Tivoli Storage Manager server storage, and the Domino server is notified of their availability for reuse.

In addition, high and low threshold values can be specified as a percentage of the log capacity to control whether log files should be archived when the command is run. This allows the command to be scheduled regularly to protect against a log full condition but to actually do the archive only if the log is getting close to being full.

Consider the following information when choosing a backup strategy:

- When using archival transaction logging, the frequency of **`archivelog`** command use depends on the size of your log and the rate of change for logged databases. Perform archival transaction logging several times per day if you generate a large volume of changes at a rapid rate.
- When a DBIID for a logged database changes, the database cannot be recovered until another backup of that database is performed. The **`incremental`** command detects the changed DBIID. Any changes recorded in the log between the DBIID change and backup are not restored if the original database is lost. The Domino server sends a message to the server console when a DBIID change occurs. It is useful to monitor the server console and perform a backup when a DBIID change occurs.
- When restoring a group of logged databases for which transactions need to be applied, activate them together when possible. This avoids restoring the same transaction log files multiple times. Restored transaction log files are deleted during a database recover by the Domino server. Activating and applying logs to the database separately requires retransmitting log files for each database.
- Data Protection for Domino provides backup and restore functions for the Domino databases (including template files) and associated transaction logs. However, Data Protection for Domino does not provide a complete disaster recovery solution for a Domino server by itself. There are many other files that are part of the Domino server installation, such as executable files and configuration files. For example, database link files have an `nsf` extension but are not considered databases and are not backed up by Data Protection for

Domino. These files must be recovered in a disaster recovery situation. A comprehensive disaster recovery plan can be achieved using the normal Tivoli Storage Manager backup-archive client for your server platform together with Data Protection for Domino.

- Personal copies (replicas) of Domino databases that are stored on Notes clients (not on the Domino server) are not protected by Data Protection for Domino. You can use the Tivoli Storage Manager backup-archive client on the Notes client platform to back up and restore these files or rely on Domino server replication if you need to recover them.
- To restore an individual Notes document, you must restore the entire database to an alternate name. Choose a time when the document existed for both the **restore /*pit*** and **activate /*applylogs*** commands but before the document was deleted, and then copy the desired document using the Notes client.
- The Tivoli Storage Manager encryption, deduplication and compression functions can be used with Data Protection for Domino. For more information read the Using the Application Programming Interface documentation on the Tivoli Storage Manager information center.

Sample strategies

Some strategies you can employ are described here.

Full backups only

The following backup option can be implemented if your network capacity and backup window support regular full database backups:

- Select circular transaction logging.
- Perform regular Selective backups.
- Perform occasional Incremental backups to deactivate backup copies of databases that have been deleted from the Domino server.

Each backup takes longer to perform, but the restore process is most efficient because only the most recent (or other appropriate) full backup needs to be restored.

Note: You can apply updates to the restored database from the transaction log if the log has not wrapped since the backup was performed. If the log has wrapped, the attempt to apply logs fails.

Full backup plus transaction log archives

It is often not practical to back up entire databases with each regular backup for large Domino installations. Archival logging captures changes to all logged databases in the archived transaction log files. This enables you to perform full database backups less frequently and reduce burdens on network and storage resources. To implement this strategy:

- Select archival transaction logging.
- Perform regular log archives using the `archivelog` command. This ensures the log does not fill and captures changes to logged databases.
- Perform regular Incremental backups. This does not back up logged databases unless the DBIID has changed.
- Perform occasional Selective backups of all logged databases. This reduces the number of transaction log files to be processed during a restore.
- Issue the `archivelog` command (following Selective backups) to allow nonessential transaction log files to expire.

The **archivelog** command captures changes to all logged databases in between full backups of selected databases. To restore a database to its most recent state, restore the most recent database backup and specify ***/applylogs*** when activating the restored database. This automatically restores the necessary archived transaction log files so that updates for the database can be applied.

In addition to the strategies described previously, see these sections for additional information that can help with strategy planning:
- "Best practices" on page 201
- "The sessions option" on page 15

Backup (DB2 enabled Notes databases)

This section describes the types of DB2 enabled Notes database backups available with Data Protection for Domino.

DB2 enabled Notes database backup

This section describes the concepts associated with Data Protection for Domino backups of Domino DB2 enabled Notes databases.

The following list provides a brief overview of key DB2 enabled Notes database backup features:
- The entire Domino DB2 database or separate DB2 Groups can be backed up.
- The backup can be restored to an alternate database.
- In a disaster recovery situation, the backup can be restored to the original Domino DB2 database.
- Individual DB2 enabled Notes databases are copied from the alternate DB2 database to the Domino DB2 database.

DB2 enabled Notes databases are stored in a DB2 database and managed by a DB2 server. Data Protection for Domino provides the ability to back up the Domino 8 DB2 database and DB2 Groups (table space). Online and DB2 Group backups are only available when the Domino DB2 database is enabled for roll-forward recovery. When roll-forward recovery is not enabled, the backup is performed offline.

Note that a DB2 enabled Notes backup is significantly different than an NSF backup. An NSF database is backed up directly. A DB2 enabled Notes database is backed up indirectly as a DB2 Group. A DB2 Group (or DB2 table space) is really a collection of one or more DB2 enabled Notes databases.

The table space is the smallest entity that can be backed up in DB2 applications. Since it is possible for a table space (DB2 Group) to contain more than one DB2 enabled Notes database, it is not possible to back up and restore a single DB2 enabled Notes database unless there is only one DB2 enabled Notes database in a table space (DB2 Group). A single DB2 enabled Notes database can be copied (from a restored table space) to the original table space or a new table space with the Domino FastCopy feature. FastCopy can only be used to restore a single DB2 enabled Notes database when a DB2 redirected restore is used. Note that a DB2 redirected restore and Domino FastCopy are only possible when DB2 is configured with federation enabled.

DB2 enabled Notes databases (NSF databases created and stored in DB2 databases) are represented in the Domino Data directory as regular files and are similar to

Domino database link and directory link files. They contain the `{DB2}` text string to identify that the database is stored in a DB2 database. The DB2 enabled Notes link files are not backed up by Data Protection for Domino. Only the full DB2 database or the DB2 Groups (that contain DB2 enabled Notes databases) are backed up by Data Protection for Domino.

DB2 Tivoli Storage Manager Agent

DB2 provides a Tivoli Storage Manager Agent and a utility program (db2adutl) that interfaces with the DB2 Recovery API in order to manage Tivoli Storage Manager objects created on the DB2 server. Data Protection for Domino uses the DB2 Tivoli Storage Manager Agent through the DB2 Recovery API to back up and restore the Domino DB2 database and DB2 Groups (table space). These Tivoli Storage Manager objects associated with DB2 backups are unique in that there is only one Tivoli Storage Manager object created for each backup operation per session. The db2adutl program, for example, can be used to expire these objects.

Data Protection for Domino and the DB2 API

Data Protection for Domino uses the DB2 Recovery API to communicate with the DB2 Tivoli Storage Manager Agent to back up DB2 data to the Tivoli Storage Manager server. Configure the DB2 Tivoli Storage Manager Agent to use the same Tivoli Storage Manager nodename and to access the same Tivoli Storage Manager server as Data Protection for Domino. This enables the Tivoli Storage Manager objects (created by the DB2 Recovery API) to belong to the same Tivoli Storage Manager node as the objects created by Data Protection for Domino for NSF databases. Specify the desired options file with the DSMI_CONFIG environment variable.

Types of DB2 backups

Data Protection for Domino provides three types of database backups:

DB2 Database Backup

Data Protection for Domino DB2 database backups create a selective backup image that can be used for disaster recovery of the Domino 8 DB2 database or for restoring individual DB2 enabled Notes databases. Only selective backup (db2selective) is provided for DB2 enabled Notes databases.

DB2 Group (table space) Backup

Data Protection for Domino DB2 Group backups create a selective table space backup image. This type of backup can only be performed after the DB2 database is enabled for roll-forward recovery.

Full DB2 Database and NSF Database Backup

Data Protection for Domino can perform a selective NSF database backup and a full Domino DB2 database backup in a single operation.

Expiration of DB2 backups and transaction log objects

This section describes concepts associated with expiring DB2 backup objects and DB2 transaction log files.

Data Protection for Domino uses the DB2 Recovery API to access the DB2 Tivoli Storage Manager Agent. When Data Protection for Domino performs a backup, it informs the DB2 Tivoli Storage Manager Agent to back up the DB2 data to the Tivoli Storage Manager server. During backup processing, Data Protection for Domino creates a group of Tivoli Storage Manager objects that describes the contents of each Tivoli Storage Manager object created by the DB2 Tivoli Storage Manager Agent. Each object describes the type of backup performed and the name of the DB2 enabled Notes databases contained in the backup. The Tivoli Storage Manager group object has a reference to the object created by the DB2 Tivoli Storage Manager Agent. Policy settings are applied to the Tivoli Storage Manager group object. As a result, when a backup version is no longer needed, the objects that are referenced by the Tivoli Storage Manager group object must also be inactivated.

These Tivoli Storage Manager group objects can be inactivated by using the **db2inactivateobjs** command. This command displays how to issue the DB2 Tivoli Storage Manager Agent db2adutl utility to inactivate these objects. The db2adutl utility ensures that information on the DB2 server remains consistent after objects have been inactivated.

The Domino DB2 database transaction logs are archived automatically by the DB2 server (using the DB2 Tivoli Storage Manager Agent) to the Tivoli Storage Manager server. The **db2archivelog** command forces a backup of the Domino DB2 database transaction log file. This command can be used to guarantee that the latest updates are available during an alternate DB2 database rollforward to the current time operation.

Note: Because transaction log file names are unique, they will not expire because of version limit.

Archived transaction log files are retained on the Tivoli Storage Manager server as long as a database backup exists that needs these log files for a complete recovery.

DB2 enabled Notes database backup strategy considerations

This section describes factors to consider when planning your DB2 enabled Notes database backup strategy and provides sample strategies.

You can choose different backup strategies depending on your specific requirements regarding network traffic, backup window, and acceptable restore times. Your choice of strategy will include selecting the type of DB2 backup commands to use.

Note: The DB2 commands do not return information on whether a backup to a Tivoli Storage Manager server was compressed, encrypted, sent LAN-free or de-duplicated

Sample strategies

Some strategies you can employ are described below.

Full DB2 database backups only

This backup strategy can be followed when the Domino DB2 database is enabled for rollforward recovery:

- Perform full DB2 database backups on a regular basis.
- Routinely inactivate (and delete) DB2 objects from the Tivoli Storage Manager server that are no longer needed.

A full DB2 database backup completes quicker and requires less storage space than DB2 Group backups. However, DB2 enabled Notes databases cannot be restored to a specific point-in-time since the database is not enabled for rollforward recovery and requires less storage space than backing up all the DB2 Groups individually.

Full DB2 database backups plus DB2 Group backups

This backup strategy can be followed when the Domino DB2 database is enabled for rollforward recovery:

- Perform full DB2 database backups on a regular basis.
- Perform DB2 Group backups on a regular basis in between full DB2 database backups. Note that only those DB2 Groups with the strictest restore time requirements should be backed up.
- Maintain a complete set of transaction log files to a specified point-in-time. DB2 automatically archives the transaction logs when the DB2 database is enabled for rollforward recovery.
- Routinely inactivate (and delete) DB2 objects from the Tivoli Storage Manager server that are no longer needed.

In order to restore a DB2 enabled Notes database to its most recent time, first select the most recent backup from a DB2 Group backup or from a full DB2 database backup that contains the DB2 enabled Notes database (if available). If the most recent DB2 Group backup is not available, restore the DB2 Group from the most recent full DB2 database backup. Note that this type of restore is to an alternate DB2 database. Rollforward the DB2 Group (or full DB2 database backup) and activate (copy) the desired DB2 enabled Notes database to the alternate Domino DB2 database.

Environments that contain both NSF and DB2 enabled Notes databases

Domino 8 environments that contain both NSF and DB2 enabled Notes databases can implement the following backup strategy:

- Perform full DB2 database backups and NSF selective backups on a regular basis.
- Perform routine incremental backups of NSF databases to inactivate backup copies that have been deleted from the Domino server.
- Perform regular DB2 Group backups if the DB2 database is enabled for rollforward recovery.
- Perform routine archiving of the transaction log files if archival transaction logging is enabled on the Domino server.
- Routinely inactivate the Domino server log file and routinely inactivate (and delete) DB2 objects from the Tivoli Storage Manager server.

Restore (NSF databases)

This section describes concepts associated with restoring and activating Domino databases and archived transaction logs.

A Domino database recovery can involve restoring several transaction log files in addition to the database backup file from the Tivoli Storage Manager server, depending on the backup strategy you choose. The function to restore database files is separate from the function that applies updates from the transaction log. This allows you to restore database files separately while transaction logs are processed for all restored databases. This avoids restoring the same transaction log files multiple times. Restoring and updating a database with current changes from the transaction log is a two-step process implemented by the **restore** and **activatedbs** commands.

See “NSF backup strategy considerations” on page 4 for additional information on backup and restore strategies.

Domino database restore and activation

This section describes the concepts associated with restoring a Domino database and activating the archived transaction logs.

Restore

Restore is the first step of a two-stage recovery process. This function restores a single database or group of databases from Tivoli Storage Manager storage to the Domino server. You can restore the database to a different database file name or to a different Domino server. You can also restore a group of databases to a different directory and preserve existing file names. In addition, if you specify a point in time on the **restore** command, the most recent backup version prior to that time is restored. To restore a database without applying updates from the transaction log, the two steps can be combined into one step by specifying ***/activate***=*yes* during the **restore** command.

Activation

This is the second step of the two stage recovery process. This function brings restored databases online for use by the Domino server. You can optionally apply transactions from the transaction log to update the database. Transactions can be applied up to a specific point in time or up through the most recent changes recorded in the transaction log. If archival logging is in effect, Data Protection for Domino automatically restores archived transaction log files as needed.

The Domino server provides an alternate restore path feature that allows you to specify the directory where transaction logs are restored. You can use this feature with the **activatedbs** command. See “Domdsmc Activatedbs” on page 53 for details on performing this procedure.

The **query pendingdbs** command retrieves a list of restored databases not yet activated. Databases pending activation are assigned a temporary file name to avoid recognition as database files on the Domino Server.

Restore of archived transaction logs

This section describes the concepts associated with restoring archived transaction logs.

This function allows a single, archived transaction log file to be restored independently of a routine database restore. Restoring a single, archived transaction log file assists with disaster recovery operations. By retrieving the most recent archived log file, it is possible to rebuild the Domino transaction log control file. This allows archived transaction log files to be used to recover restored database backups to a more current state, even after a loss of the active transaction log. Note that more than one archived transaction log file can be restored at a time.

See "Recovery from loss of Domino transaction logs for NSF databases" on page 176 for more information about disaster recovery procedures using an archived transaction log.

Restore at document level

This sections describes the concepts associated with restoring a Domino database at the document level.

Data Protection for Domino restores Domino databases at the database level. To restore a document in a database, the entire database must first be restored and the document copied.

A database can be restored to the production server under a temporary name and the desired document can be copied to the appropriate database. If for performance reasons, the production server cannot be used in the restore process, the database can be restored to an alternate server and copied to the production server. You should perform alternate server restores when possible to reduce demands on the production Domino server. Alternate server restores can be performed to an alternate partition or to a separate Domino server. See "Alternate server and alternate partition restores for NSF databases" on page 177 for details on performing this procedure.

Restore (DB2 enabled Notes databases)

This section describes concepts associated with restoring and activating Domino DB2 enabled Notes databases.

See "DB2 enabled Notes database backup strategy considerations" on page 8 for additional information on backup and restore strategies.

Domino DB2 enabled Notes database restore, rollforward, and activation

Concepts associated with a Domino DB2 enabled Notes database restore, rollforward, and activation are provided.

Restore

Data Protection for Domino provides the ability to restore a single DB2 enabled Notes database or a group of DB2 enabled Notes databases. A Domino 8 DB2 Group (table space) can be restored from either a full DB2 database backup image or a DB2 table space backup image. Only one DB2 Group can be restored at a time if the DB2 Group is being restored from a DB2 Group backup. The DB2 Group is restored to an alternate DB2 database within the same DB2 instance. If more than one DB2 Group is restored, each DB2 Group must be restored to a different DB2 database. Otherwise, restoring more than one DB2 Group to the same alternate DB2 database will overwrite the previously restored DB2 Group. If the DB2 Group is being restored from a full DB2 backup image, then more than one DB2 Group can be restored to the same alternate DB2 database.

A Domino 8 DB2 database can be restored from a full DB2 database backup image to an alternate DB2 database. This makes the individual DB2 enabled Notes databases available for restore. The DB2 database can also be restored directly to the Domino DB2 database. This type of "in-place" restore operation is useful for disaster recovery purposes.

Rollforward

Rollforward is an intermediate step that is required when the Domino DB2 database is enabled for rollforward recovery. This task rolls the Domino DB2 database forward to the specified point in time and marks the rollforward as complete. The DB2 database can be an alternate DB2 database or the Domino DB2 database.

The **"Domdsmc Query DB2rollforward" on page 163** command displays a list of DB2 databases available to rollforward.

Activation

This is the last step of the three stage recovery process. This function brings DB2 enabled Notes databases online for use by the Domino server. DB2 enabled Notes databases that are restored from a DB2 table space backup image can be activated after first rolling the alternate DB2 database forward to the desired point-in-time. The DB2 enabled Notes database can be restored to a time later than the backup time by applying necessary transaction log files by specifying the ***/applylogs*** parameter during the rollforward operation. The logs are then applied to the alternate DB2 database or to the Domino DB2 database if it is an "in-place" restore. Although the DB2 application automatically archives transaction log files when they become full, the active transaction log files should be archived before starting the rollforward operation to ensure that the latest transactions are available. The necessary logs (from those archived) are automatically restored during the rollforward operation. The DB2 enabled Notes databases are then copied into the Domino 8 DB2 database to their original filename location or to a new filename location.

DB2 enabled Notes databases that are restored from a full DB2 database backup image are activated in the same manner as described for activating DB2 enabled Notes databases restored from a DB2 table space backup image. However, DB2 enabled Notes databases that reside on different table spaces can be rolled forward simultaneously if more than one table space is restored from the full backup image.

The **"Domdsmc Query DB2pendingdbs" on page 161** command displays a list of restored DB2 enabled Notes databases that are available for activation.

Security

This section describes concepts associated with security issues and Data Protection for Domino.

Data Protection for Domino must be registered to the Tivoli Storage Manager server and use the appropriate node name and password when connecting to the Tivoli Storage Manager server.

Data Protection for Domino must run from the same system user ID the Domino server is running under.

The Tivoli Storage Manager API ***enableclientencryptkey*** option provides 128-bit transparent encryption of Domino databases during Data Protection for Domino backup and restore processing. Note that transparent encryption is only available on Tivoli Storage Manager server Version 5.3 (or later). See "Additional options" on page 38 for details.

Note: You can see if an NSF backup has been encrypted by issuing the **`query DBBackup`** command or by using the Web or Java GUI.

Performance

Many factors can affect the performance of Data Protection for Domino. Performance can be improved by implementing some changes.

Many factors can affect the backup and restore performance of your Domino Server databases. Some of these, such as hardware configuration, network type, and capacity are beyond the control of Data Protection for Domino. However, some parameters that are related to Data Protection for Domino can be tuned for optimum performance.

Data Protection for Domino uses multiple data buffers when transferring data between the Domino and Tivoli Storage Manager servers. The number and size of the buffers can be specified using the ***/buffers*** parameter. The number and size of buffers that are allocated by default can be configured through the **set** command. The default number of buffers is 3 and the default buffer size is 1024 KB.

To improve throughput for backup and restore operations, run multiple sessions in parallel. This is most effective when work is partitioned by physical volume. For example, one Data Protection for Domino session backs up all databases on one physical volume while a second Data Protection for Domino session backs up all databases on another volume.

To improve throughput for backup operations, run multiple sessions in parallel.

On UNIX and Linux systems there are two ways to accomplish this:
- When the databases are cleanly partitioned by physical volume, you can start one Data Protection for Domino instance to back up the databases on one physical volume and a second Data Protection for Domino instance to back up the databases on another volume.
- If the databases are not cleanly partitioned, you can start one Data Protection for Domino instance to back up all databases and use the sessions parameter to create multiple independent threads and sessions with the Tivoli Storage Manager server . This is equivalent to starting multiple independent Data

Protection for Domino instances. The difference is independent threads are used instead of independent instances. When using independent threads, you do not have explicit control of which databases are backed by the individual threads.

You can also specify `tcpnodelay yes` in the dsm.sys file to improve backup and restore performance. Instead of buffering the data, this option sends the data as successive small packets across the network without delay.

The *statistics* option

The ***statistics*** option logs performance information about an individual database at the backup or restore level. Data Protection for Domino processing is performed under two threads: a producer process (which reads the data) and a consumer process (which sends the data). During a backup, the producer reads the database and the consumer sends this data to the Tivoli Storage Manager server. During a restore, the producer receives the data from the Tivoli Storage Manager server and the consumer writes the restored database. The ***statistics*** option logs this information to assist in tuning Data Protection for Domino for optimal performance.

Example of the *statistics* option

In the example display output below, the consumer send rate is greater than the producer file read rate. Because the consumer completes sending the data before the producer completes filling the next buffer, the consumer waits an average of 25 milliseconds for each read buffer being filled by the producer. The best method for improving throughput would be to modify the input/output (I/O) subsystem. If the send/receive rate was lower than the read/write rate, the best method for improving throughput would be to modify the TCP/IP subsystem. If both the producer and the consumer have significant average wait times and the send/receive and read/write rates are similar, then the best method for improving throughput would be to modify the processor. The standard Long Wait value is *0*. A Long Wait value other than *0* is most likely caused by tape mounts being loaded during processing. As a result, the consumer send/receive time will be artificially increased and not representative of the standard data transfer time.

```
==========================================================================
Request : SELECTIVE
Database Input List : Sample.db1.nsf
Number of Buffers : 2
Buffer Size : 1024
Logged Databases Only? : No
Wait for Tape Mounts? : No
Process Subdirectories? : No
TSM Options File : c:\Program Files\Tivoli\TSM\domino\dsm.opt
TSM Nodename Override :
--------------------------------------------------------------------------
Performance statistics for database Sample.db1.nsf
Section Total Time Wait Time Average Time Long Waits
(msec) (msec) (msec)
----------------------------------------------------------------------
Producer 231 1 0 0
Consumer 393 75 25 0
----------------------------------------------------------------------
Sub Section Total Time Bytes Transferred Transfer Rate
(msec) (bytes) (Kb/sec)
----------------------------------------------------------------------
ReadWrite 160 458752 2867
SendRecv 70 458752 6553
Domino Server 1 0 0
----------------------------------------------------------------------
```

```
Total Elapsed Time Total Bytes Transferred Rate
(msec) (bytes) (Kb/sec)
----------------------------------------------------------------------
1493 458752 307
Total Domino databases inspected: 1
Total Domino databases backed up: 1
Total Domino databases excluded: 0
Total Domino databases deduplicated: 0

Throughput rate: 300.07 Kb/Sec
Total byes inspected: 458,752
Total bytes transferred: 458,752
Total LanFree bytes transferred: 0
Total bytes before deduplication: 0
Total bytes after deduplication: 0
Data compressed by: 0.00%
Deduplication reduction: 0.00%
Total data reduction ratio: 0.00%
Elapsed processing time: 1.49 Secs
```

You can find more information about the `statistics` option in the description of “Domdsmc Set” on page 123.

The *sessions* option

The ***sessions*** option allows a specified number of TCP/IP sessions to be made available for communication with the Tivoli Storage Manager server when backing up Domino NSF databases. Since more than one TCP/IP session is made available for backup processing, improvements in performance are possible. For example, the ***sessions*** option should be specified when simultaneously backing up NSF data to multiple tape drives. You can specify from *1* to *64* sessions. The default value is *1*. However, be aware that since network and hardware capabilities of the production environment can also impact the overall performance enhancements of the ***sessions*** option, environment conditions should be considered when using the ***sessions*** option.

In addition, be aware that each session requests a mount point from the Tivoli Storage Manager server when backup processing begins. If a mount point is in use (unavailable), then the mount point is not released for use by a new session until the backup (on that mount point) is complete. Because of this behavior, it is possible that a session (waiting for an available mount point) may timeout, causing the backup attempt to fail. This situation can occur when the number of specified backup sessions exceeds the number of available mount points. To avoid this situation, make sure that the number of available mount points (from the Tivoli Storage Manager server) is equal to the number of sessions specified with the ***sessions*** option. Note that it is the responsibility of the user to determine the number of available mount points as Data Protection for Domino does not determine this information. Also, the Tivoli Storage Manager Administrator must set the `maxnummp` option in order to specify the maximum number of mount points to use (for the Domino Server ID) on the Tivoli Storage Manager server.

The ***sessions*** option is available with the following commands:

- “Domdsmc Incremental” on page 77
- “Domdsmc Selective” on page 118
- “Domdsmc Fullselective” on page 137
- “Domdsmc Set” on page 123

The *DOMTXNBYTELIMIT* option

The ***DOMTXNBYTELIMIT***=*number* option specifies the number of bytes sent between Data Protection for Domino and the Tivoli Storage Manager server in a single transaction. The default value is *0*, which indicates no limit, and the maximum value is *2097152*. This number is multiplied by 1024 to calculate the limit in bytes.

This parameter is useful when backing up NSF databases to tape storage for these reasons:

- Processing for each transaction causes the tape to stop and start. Considerable time can be lost during this stop and start when using high speed tapes. This is true in a LAN free environment.
- Errors that occur during backup processing are automatically retried when `domtxnbytelimit` is set.

When a failure occurs during a backup, all of the backups in the transaction are retried, not just the NSF database in error. Each backup is retried in a separate transaction. After all backups are retried, the `domtxnbytelimit` parameter is used to control the number of bytes per transaction.

The *DOMTXNGROUPmax* option

The ***DOMTXNGROUPmax***=*number* option specifies the number of individual objects sent to the Tivoli Storage Manager server in a single transaction.

Two objects are sent to the Tivoli Storage Manager server for each database backup so the default value of this option is 2. The maximum value is *65000*.

The `DOMTXNGROUPmax` option can be overridden by the Tivoli Storage Manager server `TXNGRPMAX` option. However, when `domtxngroupmax` is set, the minimum of the two values is used.

This parameter is useful when backing up NSF databases to tape storage for these reasons:

- Processing for each transaction causes the tape to stop and start. Considerable time can be lost during this stop and start when using high speed tapes. This is true in a LAN free environment.
- Errors that occur during backup processing are automatically retried once `domtxngroupmax` is set.

When a failure occurs during a backup, all of the backups in the transaction are retried, not just the NSF database in error. Each backup is retried in a separate transaction. After all backups are retried, the `domtxngroupmax` parameter is used to control the number of individual objects per transaction. Consider using the `domtxngroupmax` parameter when backing up small NSF databases.

Chapter 2. Installing Data Protection for Domino

Describes the prerequisites and procedures involved when installing Data Protection for Domino.

Prerequisites

This section provides information on the client environment that must exist before you install Data Protection for Domino.

Before you begin

Before you install Tivoli Storage Manager for Mail: Data Protection for Lotus Domino in a UNIX or Linux environment, make sure your system meets the minimum hardware, software and operating system requirements.

The following sections provide an overview of the minimum hardware and software requirements defined for the 6.3 release of Tivoli Storage Manager for Mail: Data Protection for Lotus Domino at the time of this guide's creation. Additional details and functional requirements are available via the Hardware and Software Requirements tech note associated with this release.

Details of the hardware and software requirements for Tivoli Storage Manager for Mail: Data Protection for Lotus Domino can evolve over time via maintenance updates and the addition of operating system, application, and other software currency support. For the most up-to-date requirements, visit the Hardware and Software Requirements tech note associated your level of code via the http://www.ibm.com/support/docview.wss?uid=swg21219345

Once the page is displayed, follow the link to the requirements tech note for your specific release or update level.

Minimum hardware requirements

The following information describes the minimum hardware requirements for operating Tivoli Storage Manager for Mail: Data Protection for Lotus Domino in a UNIX or Linux environment.

The following hardware is supported for the AIX platform.

- IBM System p®
- IBM System i®
- Compatible hardware supported by the operating system and the application At least 8 MB of disk space and 128 MB of RAM

The following hardware is supported for the Linux on System z® platform.

- Any System z machine that is supported by the operating system and the application

Minimum software and operating system requirements

The following information describes the minimum software requirements for operating Tivoli Storage Manager for Mail: Data Protection for Lotus Domino in a UNIX or Linux environment.

The following operating systems are supported for the AIX platform.

- 64-bit AIX 6.1
- 64-bit AIX 7.1

The following operating systems are supported for the Linux on System z platform.

- 64-bit Red Hat Enterprise Linux (RHEL) 5.0, and later mod levels and fix packs
- 64-bit Red Hat Enterprise Linux (RHEL) 6.0, and later mod levels and fix packs
- 64-bit SUSE Enterprise Linux (SLES) 10.0, and later mod levels and fix packs
- 64-bit SUSE Enterprise Linux (SLES) 11.0, and later mod levels and fix packs

The following Lotus Domino Server levels are supported.

- Lotus Domino 8.0.1 Server, and later levels of 8.0.x
- Domino Server 8.5.x Server, and later levels of 8.5.x

The following DB2 database levels are supported as defined by the Lotus Domino Server's own hardware and software requirements documentation

- Any version of DB2 supported by the level of Lotus Domino Server in use and supported by Tivoli Storage Manager for Mail: Data Protection for Lotus Domino

Virtualization Support

Information regarding the virtualization environments supported by Tivoli Storage Manager for Mail: Data Protection for Lotus Domino is available at the following URL http://www.ibm.com/support/docview.wss?uid=swg21239546.

Procedures

This section provides detailed instructions for installing Data Protection for Domino on AIX and zLinux machines.

Installing on AIX

This section provides step by step instructions for installing Data Protection for Domino on an AIX machine.

These instructions guide you through the installation of Data Protection for Domino and assume that AIX Version 6.1 (or later) is the operating system on the Domino Server machine.

- The Data Protection for Domino Version 6.3 64-bit and Tivoli Storage Manager API Version 6.3 packages are available on the installation media in the `/usr/sys/inst.images` directory.

Note: The Java GUI (dsmj) requires Java version 1.6.0 to connect to the Domino 8.5 server.

If you are not installing from a CD, run the following command from the AIX command line:

```
/usr/sbin/inutoc <dir>
```

where `<dir>` is the directory where the installation image resides. A .toc file is created in the directory and used during installation.

The following steps show a sample installation using the **smitty** command:

1. Log in as the **root** user.
2. Insert the Data Protection for Domino CD into the CD reader.
3. From the AIX command line, type **smitty install** and press **Enter**.
4. Select **Install and Update Software** and press **Enter**.
5. Select **Install and Update from ALL Available Software** and press **Enter**.
6. At the **INPUT device/directory for software** prompt, press the **F4** key and select the CD device that contains the installation CD, and press **Enter**.
7. At the **SOFTWARE to Install** prompt, select the file sets you want to install, press the **F7** key, and press **Enter**.
8. Highlight the Electronic License Agreement (`tivoli.tsm.loc.client.domino.ela`) and press **F7**.
    a. Make sure you set **ACCEPT new license agreements?** to **Yes**. (The default is **No**). You can also specify the *-Y* option with the **installp** command.
    b. Set **Preview new license agreements?** to **No** (the default value) for the installation to proceed.
    c. If **Preview new license agreements?** is set to **Yes**, the installation will enter preview mode but Data Protection for Domino does not install. **Preview new license agreements?** must be set to **No** for Data Protection for Domino to install.
9. Select any options and press **Enter** to begin the installation.

See the Domdsmfiles.txt file for a list of files copied to your machine during installation. After successfully installing Data Protection for Domino, run the **dominstall** program. See “Performing a manual dominstall configuration” on page 23 for detailed information.

Uninstalling on AIX

This section describes how to uninstall Data Protection for Domino from an AIX machine.

Follow these steps to uninstall Data Protection for Domino and the Tivoli Storage Manager API:

1. Log in as the **root** user.
2. From the AIX command line, enter this command and follow the instructions displayed on the screen: `smitty remove`
3. At the SOFTWARE name prompt, press the **F4** key to select the filesets to uninstall.
4. Press the **F7** key and press **Enter**.

Installing on Linux

This section provides step by step instructions for installing Data Protection for Domino on a Linux machine.

These instructions guide you through the installation of Data Protection for Domino on a Linux on System z machine. Simply refer to your Linux platform throughout the procedure.

The following Linux on System z installable files and package are available on the installation media:

- `TIVsm-API64.s390x.rpm`

  This file installs the Tivoli Storage Manager API Version 6.3.
- `TDP-Domino.s390x.bin`

  This file installs Data Protection for Domino
- `6.3.0.0-TIV-TSMDOM_xx_XX-s390x.bin`

  This file installs the Data Protection for Domino language catalog.

  Note: In the file name, xx_XX represents the country code for the language contents of the package.

This installation procedure is designed to install directly from the Data Protection for Domino CD:

1. Log in as the **root** user.
2. Mount the Data Protection for Domino CD to `/cdrom:mount <device name> /cdrom`
3. Change to the directory where the installable files and package reside on the CD. For Linux on System z, change to the `/cdrom/domino/linux390` directory.
4. Install the Tivoli Storage Manager API. For Linux on System z, enter the `rpm -ivh TIVsm-API64.s390x.rpm` command.
5. Install Data Protection for Domino using one of these methods:
   - Enter the name of the installable file `TDP-Domino.s390x.bin` on the command line and press **Enter** to install Data Protection for Domino.
   - To install in console mode, enter the **`TDP-Domino.s390x.bin -i console`** command and press **Enter**.
   - To install in silent mode, enter the **`TDP-Domino.s390x.bin -i silent`** command and press **Enter**.
   - To install in GUI mode, enter the **`TDP-Domino.s390x.bin -i gui`** command and press **Enter**.
   - To install Data Protection for Domino in a language other than English, enter the name of the Data Protection for Domino installable file for the desired language (`TDP-Domino.msg.xx_XX.s390x.bin`) on the command line and press **Enter**. Make sure the Tivoli Storage Manager API language package for the desired language (`TIVsm-API64.s390x.rpm`) is also installed.

   Note: If the installable file was downloaded from the FTP site, the filename might be different than `TDP-Domino.s390x.bin`.

After successfully installing Data Protection for Domino, run the **dominstall** program. See "Performing a manual dominstall configuration" on page 23 for detailed information.

Uninstalling on Linux

How to uninstall Data Protection for Domino from a Linux machine.

1. Change to the following directory: `/opt/tivoli/tsm/client/domino/_uninstall`
2. Uninstall Data Protection for Domino using one of these methods:
   - Enter the **`./uninstall`** command and press **Enter** to uninstall Data Protection for Domino using the method it was installed with.
   - Enter the **`./uninstall -i silent`** command and press **Enter** to uninstall Data Protection for Domino in silent mode.
   - Enter the **`./uninstall -i console`** command and press **Enter** to uninstall Data Protection for Domino in console mode.
   - Enter the **`./uninstall -i gui`** command and press **Enter** to uninstall Data Protection for Domino in GUI mode.
3. Enter this command to uninstall the Tivoli Storage Manager API: `rpm -e TIVsm-API64`

To uninstall any additional language packs:

1. Change to the directory `/opt/tivoli/tsm/client/domino/_uninstall_xx` (where xx is the language pack you want to uninstall).
2. Uninstall the Data Protection for Domino language pack using one of these methods:
   - Enter the **`./uninstall`** command and press **Enter** to uninstall the language pack using the method with which it was installed.
   - Enter the **`./uninstall -i silent`** command and press **Enter** to silently uninstall the language pack.
   - Enter the **`./uninstall -i console`** command and press **Enter** to uninstall the language pack in console mode.

   Enter the **`./uninstall -i gui`** command and press **Enter** to uninstall the language pack in GUI mode.

Quick install

Instructions on how to perform a quick configuration of Data Protection for Domino on an AIX machine.

This procedure uses default settings and requires minimal configuration tasks. It minimizes set up time and allows you to proceed quickly to a state where you can begin backing up your Domino databases. You must change the installation paths and library extensions documented in this procedure if you are using an operating system other than AIX. Detailed instructions on how to customize Data Protection for Domino for your environment and processing needs are available in the configuration section.

Consider the following additional quick installation steps required for DB2 enabled Notes databases:

- Make sure the Tivoli Storage Manager API settings are defined for the DB2 environment.
- Set the level of access a user has to the DB2 environment by issuing this command:

  ```
  domdsmc set db2user=<DB2 user name>
  ```

1. Install Data Protection for Domino. Detailed installation instructions are available in the installation section.

2. Change to the `/usr/tivoli/tsm/client/domino/bin64` directory and create a `dsm.opt` file. Edit the `dsm.opt` file to include the following `servername` entry: `SErvername dpdom`The `dpdom` entry specifies a server stanza in the dsm.sys file. More information about this option and the dsm.opt file is available on page “Options and preferences” on page 35.
3. Change to the `/usr/tivoli/tsm/client/api/bin64` directory and create a symbolic link to `/usr/tivoli/tsm/client/ba/bin64/dsm.sys`. Edit the dsm.sys file to create the server stanza (referenced in Step 2) with the following options:

   ```
   SErvername dpdom
   COMMMethod TCPip
   TCPServeraddress x.x.x.x
   PASSWORDAccess generate
   PASSWORDDIR /usr/tivoli/tsm/client/domino/bin64/domdsmc_notes
   NODename hostname_notes
   ```

   Replace *x.x.x.x* with the IP address of the Tivoli Storage Manager server to which Data Protection for Domino backs up data.
   a. If the Tivoli Storage Manager backup-archive client is not installed, do not create a symbolic link.
   b. More information about the dsm.sys file, these options, and their relationship with Data Protection for Domino is available on page “Options and preferences” on page 35.
4. Register the node (specified in step 3) to the Tivoli Storage Manager server with the following command: `REG NODE hostname_notes password` Where `hostname_notes` is the name of the machine where Data Protection for Domino is installed and `password` is the password for this node. All other options use default settings. If your Tivoli Storage Manager policy settings for Data Protection for Domino backups are different from the default settings, make sure that you register the node to the DOMAIN that contains your Data Protection for Domino information.
5. Change to the `/usr/tivoli/tsm/client/domino/bin64` directory and run the **`dominstall`** program. This program helps configure your Data Protection for Domino environment. See “Performing a manual dominstall configuration” on page 23 for detailed instructions.
6. If a password file for the Domino user ID does not exist, create one with the following command: `domdsmc query adsm -adsmpwd=password` A password file is required to access the Domino Server and partitions with the Web client GUI.
7. Verify that you can communicate with the Domino Server by running the **`domdsmc query domino`** command.
8. Verify that you can communicate with the Tivoli Storage Manager server by running the **`domdsmc query adsm`** command.
9. Data Protection for Domino is now ready for backup and restore processing. For example, to perform an incremental backup of your databases from the Data Protection for Domino command-line interface, enter the following command: `domdsmc incr "*"`

Chapter 3. Configuring Data Protection for Domino

How to configure Data Protection for Domino to protect Lotus Domino databases.

Configure the Domino Server environment with dominstall

After successfully installing Data Protection for Domino, you must configure the Domino environment by running the **dominstall** program for each Domino server partition.

The **dominstall** program utilizes user-specified input to configure the Domino Server to operate within your desired Data Protection for Domino and Domino Server single partition or multiple partition environment. You can run the **dominstall** program multiple times in order to set up additional partitions or to reconfigure your Data Protection for Domino installation configuration. The input can be entered manually for each partition (referred to as a manual dominstall configuration) or the input can be captured in a dominstall configuration file in order to perform a configuration on other partitions without user interaction (referred to as a silent dominstall configuration).

The following configuration tasks are performed by the **dominstall** program:

- Determines the Data Protection for Domino installation directory.
- Determines the Domino executables directory.
- Determines the Tivoli Storage Manager API installation directory.
- Determines the Domino data directory (single Domino server partition).
- Determines each partition Domino data directory (multiple Domino server partitions).
- Configures Data Protection for Domino and creates the symbolic link to the Domino `/bin64` directory.
- Creates a Domino partition user profile to set up the Data Protection for Domino environment.
- Configures Data Protection for Domino for access to the Web client GUI.
- Automates configuration by using a silent configuration file that captures the user input from a previous configuration task. "Performing a silent dominstall configuration" on page 27 provides complete instructions for this task.

Performing a manual dominstall configuration

A manual dominstall configuration utilizes user-specified input to configure the Domino Server to operate within your desired Data Protection for Domino and Domino Server single partition or multiple partition environment.

This procedure reflects a Data Protection for Domino installation on a Linux operating system. Directory structures and file names will differ among UNIX, and Linux systems.

1. Log in with the user ID set up to run the Domino server.
2. Use the **su root** command to switch to the root user ID.
3. Change to the Data Protection for Domino installation directory:
```
# cd /opt/tivoli/tsm/client/domino/bin64
```

4. Run the dominstall program by entering the **./dominstall** command If you need to run the dominstall configuration again using the current Domino server setup, you can record your responses to a dominstall configuration file for subsequent use in a silent dominstall configuration by entering the **./dominstall dominstall.response** command.

   Note:
   - When the dominstall program is invoked and *dominstall.response* exists, the contents of that file is used to perform a silent dominstall configuration.
   - When the dominstall program is invoked and *dominstall.response* does not exist, your responses are recorded to *dominstall.response* and that file can be used to run the dominstall program on other partitions without user interaction.

   See "Performing a silent dominstall configuration" on page 27 for additional information.
5. Verify the directory location of the Data Protection for Domino executable:
   ```
   Using the Data Protection for Lotus Domino client, domdsmc, installed
   in /opt/tivoli/tsm/client/domino/bin. Is that correct?.  (Yes (Y)/No
   (N))
   ```
   - Enter `Y` if the directory listed is correct.
   - Enter `N` if the directory listed is not correct. You are prompted for the directory where domdsmc is installed. Specify the correct directory and press `Enter`.
6. Verify the location of the Domino executable directory:
   ```
   Using the Domino, libnotes.so, installed in /opt/lotus/notes/latest/
   linux. Is that correct?.  (Yes (Y)/No (N))
   ```
   - Enter `Y` if the directory listed is correct.
   - Enter `N` if the directory listed is not correct. You are prompted for the directory where the Domino executable is installed. Specify the correct directory and press `Enter`.

   Note that if multiple releases of the Domino server are installed on the system, then run the dominstall program multiple times and specify the appropriate Domino executable directory during each invocation of dominstall.
7. Specify the directory where the notes.ini file resides and press `Enter`:
8. Verify the directory location where the Tivoli Storage Manager API resides:
   ```
   Using the Tivoli Storage Manager Api, libApiDS.so, installed in
   /usr/tivoli/tsm/client/api/bin64/libApiTSM64.a. Is that correct?.  (Yes
   (Y)/No (N))
   ```
   - Enter `Y` if the directory listed is correct.
   - Enter `N` if the directory listed is not correct. You are prompted for the directory where the Tivoli Storage Manager API is installed. Specify the correct directory and press `Enter`.
9. Dominstall sets notes as the owner for the Data Protection for Domino executables:
   ```
   Setting notes as owner for the Data Protection for Domino executables.
   ```
10. (Optional) You are prompted to configure the Tivoli Storage Manager Web client for backup and restore processing:
    ```
    Do you want to configure the Tivoli Storage Manager Web Client? (Yes
    (Y)/No (N))
    ```

- If you do not plan to use the Tivoli Storage Manager Web client GUI, enter `N` and proceed to Step 11.
- If you plan to use the Tivoli Storage Manager Web client GUI, enter `Y` and perform Step a. through Step c. below.

a. Verify the directory where the Tivoli Storage Manager client system options file (dsm.sys) resides:

```
Using the Tivoli Storage Manager client system options file, dsm.sys,
installed in /opt/tivoli/tsm/client/ba/bin64. Is that correct?.
(Yes (Y)/No (N))
```

Enter `Y` if the displayed location is correct. Enter `N` if the displayed location is not correct. You are prompted for the directory where dsm.sys is installed. Specify the correct directory and press `Enter`.

b. Select the Tivoli Storage Manager server to be used by the Web client:

```
Choose the server entry used by the Tivoli Storage Manager Web client.
0 serverA
1 serverB
2 serverC
```

c. Specify a server and press `Enter`. Information about the selected server (serverA) displays:

```
SERVERNAME  serverA
TCPSERV serverA.xyzcompany.com
COMMMETH tcpip
TCPPORT 1500
NODENAME CADlinux
PASSWORDACCESS generate
PASSWORDDIR /opt/tivoli/tsm/client/ba/bin/CADpasswords
MANAGEDSERVICES webclient

Is that correct?
 (Yes (Y)/No (N))
```

Enter `Y` to select this server entry. Enter `N` to select a different server entry. You are prompted to select another Tivoli Storage Manager server. Specify a server and press `Enter`. Information about the selected server (serverB) displays:

```
SERVERNAME  serverB
TCPSERV serverB.xyzcompany.com
COMMMETH tcpip
TCPPORT 1500
NODENAME linuxps
PASSWORDACCESS generate

Is that correct?
 (Yes (Y)/No (N))
```

Enter `Y` to select this server entry. Enter `N` to select a different server entry.

11. The dominstall program creates these symbolic links:

```
Created symbolic link /opt/lotus/notes/latest/linux/domdsmc to
/opt/tivoli/tsm/client/domino/bin/domdsmc.

Created symbolic link /opt/lotus/notes/latest/linux/domdsmp to
/opt/tivoli/tsm/client/domino/bin/domdsmp.

Created symbolic link /opt/lotus/bin/domdsmc to tools/startup.
```

The dominstall program continues to set notes as owner and create symbolic links:

```
Setting notes as owner for the Data Protection for Domino executable
/opt/tivoli/tsm/client/domino/bin/domdsmc_notes/domdsmc.

Created symbolic link /opt/lotus/notes/latest/linux/domdsmc_notes to
/opt/tivoli/tsm/client/domino/bin/domdsmc_notes/domdsmc.

Created symbolic link /opt/lotus/bin/domdsmc_notes to tools/startup.
************************************************
* Make the suggested changes to the dsm.sys file
/opt/tivoli/tsm/client/ba/bin/dsm.sys.
*
* Register the node notes to the Tivoli Storage Managemer server.
*
* Then issue the following command to complete the setup for this
Domino server

domdsmc query adsm -configfile=/opt/tivoli/tsm/client/domino/bin/
domdsmc_notes/domdsm.cfg2
-adsmpwd=
******************************************************************
```

12. Verify whether the Domino server enabled for DB2:

    ```
    Is the Domino server DB2 enabled?
    (Yes (Y)/No (N))
    ```

    Enter `Y` if the Domino server is enabled for DB2 and enter the DB2 user name. Enter `N` if the Domino server is not enabled for DB2 and proceed to the next step.

13. You are prompted to specify the directory where you want to place your profile:

    ```
    Installing profile in directory /opt/tivoli/tsm/client/domino/bin

    Is that correct?.
     (Yes (Y)/No (N))
    ```

    Enter `Y` if the directory listed is where you want to place your profile. Enter `N` if the directory listed is not where you want to place your profile. You are prompted for the directory where you want to place your profile. Specify the directory and press `Enter`. The dominstall program continues to set notes as owner and create symbolic links:

    ```
    Setting notes as owner for the Data Protection for Domino executable
    /opt/tivoli/tsm/client/domino/bin/domdsmc_notes/domdsmc.

    Created symbolic link /opt/lotus/notes/latest/linux/domdsmc_notes to
    /opt/tivoli/tsm/client/domino/bin/domdsmc_notes/domdsmc.

    Created symbolic link /opt/lotus/bin/domdsmc_notes to tools/startup.
    ************************************************
    * Make the suggested changes to the dsm.sys file
    /opt/tivoli/tsm/client/ba/bin/dsm.sys.
    *
    * Register the node notes to the Tivoli Storage Managemer server.
    *
    * Then issue the following command to complete the setup for this
    Domino server

    domdsmc query adsm -configfile=/opt/tivoli/tsm/client/domino/bin/
    domdsmc_notes/domdsm.cfg2
    -adsmpwd=
    ******************************************************************
    ```

14. At this stage your Data Protection for Domino environment is configured and you are prompted to configure another Domino server partition:

```
Reply with the next notesdata partition or a NULL line (enter key)
```

To configure another Domino server partition, specify the Domino data directory where the notes.ini file is installed for that partition. Proceed to Step 7 of this procedure and follow the instructions. Then complete steps 12, 13 and 14. To exit the dominstall program, press `Enter`. This message displays:

```
Data Protection for Domino installation process has successfully completed.
```

Performing a silent dominstall configuration

A silent dominstall configuration uses a file to configure the Domino Server to operate within your desired Data Protection for Domino and Domino Server single partition or multiple partition environment without user interaction.

The dominstall program provides an option (*filename*) that records all user input (through key strokes) to a file during a manual dominstall configuration. This file can be used to run the dominstall program on other partitions without user interaction. This type of dominstall operation is called a silent dominstall configuration.

A dominstall configuration file is required in order to perform a silent dominstall configuration. This file is created by entering the following command:

```
./dominstall filename
```

Once the manual dominstall configuration is completed, copy the dominstall configuration file to the machine where a silent configuration is desired. When the dominstall program is invoked with the name of an existing dominstall configuration file, the contents of that file is used to perform the silent dominstall configuration.

Be aware that when a change occurs to the Domino environment for which a dominstall configuration file was created, the silent dominstall configuration will not function. A manual dominstall configuration must be performed for that environment to create a current dominstall configuration file.

The dominstall configuration file (*filename*) contains the user input recorded during a manual dominstall configuration. For example:

```
N
/opt/tivoli/tsm/client/domino/bin
N
/opt/ibm/lotus/notes/latest/linux
N
/opt/ibm/lotus/notesdata
y
n
y
db2inst1
y
n
```

The previous *filename* example was created from the manual dominstall configuration shown here. Note that the key strokes that were captured to the dominstall configuration file are shown in ***bold italic***.

```
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino Version
5, Release 6, Level 3.0 (C) Copyright IBM Corporation 1999, 2011. All rights
reserved.

Using the Data Protection for Lotus Domino client, domdsmc, installed
```

```
 in /opt/tivoli/tsm/client/domino/bin. Is that correct?.  (Yes (Y)/No (N))
N
Unable to locate Data Protection for Lotus Domino client. Please specify the
directory where domdsmc is installed.
The default is /opt/tivoli/tsm/client/domino/bin.

/opt/tivoli/tsm/client/domino/bin

Using the Domino, libnotes.so, installed in /opt/ibm/lotus/notes/latest/linux.
Is that correct?.
(Yes (Y)/No (N))
N
Unable to locate Domino. Please specify the directory where libnotes.so is
installed. The default is /opt/ibm/lotus/notes/latest/linux.

/opt/ibm/lotus/notes/latest/linux
Using the Domino file, notes.ini, installed in /opt/ibm/lotus/notesdata.
Is that correct?.
(Yes (Y)/No (N))
N
Unable to locate Domino file. Please specify the directory where notes.ini
is installed. The default is (null).

/opt/ibm/lotus/notesdata

Using the Tivoli Storage Manager Api, libApiDS.so, installed in /usr/lib.
Is that correct?.
(Yes (Y)/No (N))
y
Setting notes1 as owner for the Data Protection for Domino executables.
Do you want to continue with the Tivoli Storage Manager Web
client configuration?.
(Yes (Y)/No (N))
n
ACD6008I Symbolic link /opt/ibm/lotus/notes/latest/linux/domdsmc to
/opt/tivoli/tsm/client/domino/bin/domdsmc already exists.
ACD6008I Symbolic link /opt/ibm/lotus/notes/latest/linux/dsmdomp to
/opt/tivoli/tsm/client/domino/bin/dsmdomp already exists.
ACD6008I Symbolic link /opt/ibm/lotus/bin/domdsmc to tools/startup
 already exists.
ACD6008I Symbolic link /opt/ibm/lotus/bin/dsmdomp to tools/startup
already exists.
Is the Domino server DB2 enabled?
(Yes (Y)/No (N))
y
Enter the DB2 user name.

db2inst1
Installing notes1.profile profile in directory
 /opt/tivoli/tsm/client/domino/bin.
Is that correct?.
(Yes (Y)/No (N))
y

The file domdsm.cfg exists. Reply Yes to overwrite this file, or No to
create the  file domdsm.cfg2.
(Yes (Y)/No (N))
n
ACD6008I Symbolic link /opt/ibm/lotus/notes/latest/linux/domdsmc_notes1 to
/opt/tivoli/tsm/client/domino/bin/domdsmc_notes1/domdsmc already exists.
ACD6008I Symbolic link /opt/ibm/lotus/bin/domdsmc_notes1 to tools/startup
already exists.
Reply with the next notesdata partition or a NULL line (enter key).
```

This procedure reflects a Data Protection for Domino installation on a Linux 86 operating system. Directory structures and file names will differ among UNIX, and Linux systems.

1. Log in with the user ID set up to run the Domino server.
2. Use the **su root** command to switch to the root user ID.
3. Change to the Data Protection for Domino installation directory:
   ```
   # cd /opt/tivoli/tsm/client/domino/bin
   ```
   - If the dominstall configuration file contains input from a manual dominstall configuration, enter this command to perform a silent dominstall configuration:
     ```
     ./dominstall filename
     ```
   - If the dominstall configuration file does *not* exist (and therefore does not contain input data), enter this command to create a file and perform a manual dominstall configuration:
     ```
     ./dominstall filename
     ```
     Go to Step 5 in "Performing a manual dominstall configuration" on page 23 and enter a response to all of the dominstall prompts.
   1. After responding to all of the dominstall prompts, copy the dominstall configuration file (*filename*) to the machine where a silent configuration is desired.
   2. Perform Step 1 through Step 4 above. Note that the contents of the dominstall configuration file (*filename*) performs the configuration without any further user input. The silent configuration file can be used repeatedly to silently configure additional partitions.

Dominstall considerations

Issues to consider when using the **`dominstall`** command.

For each Domino partition that you configure, the dominstall program creates the following files in the Data Protection for Domino installation directory:

```
domdsmc_<notes_user>
domdsmc_<notes_user>/domdsmc
domdsmc_<notes_user>/<notes_user>.profile

domdsmc_<notes_user>/domdsm.cfg
domdsmc_<notes_user>/dsm.opt
domdsmc_<notes_user>/dsm.sys.additions
domdsmc_<notes_user>/dsm.sys.changes
```

The following links are also created in the Domino `/bin` and executable directories:

```
/opt/lotus/bin/domdsmc_<notes_user> -> tools/startup

/opt/lotus/notes/latest/ibmpow/domdsmc_<notes_user> ->
/opt/tivoli/tsm/client/domino/bin/domdsmc_<notes_user>/domdsmc

/opt/lotus/bin/domdsmc -> tools/startup

/opt/lotus/notes/latest/ibmpow/domdsmc ->
/opt/tivoli/tsm/client/domino/bin/domdsmc

/opt/lotus/bin/dsmdomp -> tools/startup ->
/opt/tivoli/tsm/client/domino/bin/dsmdomp
```

Note: As demonstrated in the previous example:

1. Data Protection for Domino is set up to be launched by the Domino startup script (`tools/startup`).
2. `dsmdomp` is the Data Protection for Domino plug-in executable for the Web client GUI.

After running the dominstall program, the Notes user ID that runs Data Protection for Domino should include the environment variables shown in the profile file. This profile file sets the environment so that for each partition the command **domdsmc** resolves to `/opt/lotus/bin/domdsmc_<notes_user>`. The profile file also sets the environment so that each partition uses its own Data Protection for Domino preferences files.

Once the alias is defined in the profile file, you can run Data Protection for Domino by issuing the command:

```
domdsmc
```

If the alias is *not* set in the profile file, run Data Protection for Domino by issuing the command:

```
/opt/lotus/bin/domdsmc_<notes_user>
```

If Data Protection for Domino is installed over a previous version, the dominstall program creates the following links so that changes to the existing environment are not required:

```
/opt/lotus/bin/domdsmc -> /opt/lotus/notes/latest/ibmpow/domdsmc
```

```
/opt/lotus/notes/latest/ibmpow/domdsmc ->
/usr/tivoli/tsm/client/domino/bin64/domdsmc
```

You can remove these symbolic links if Data Protection for Domino is *not* installed over a previous version.

Dominstall sets the ownership of all the files in the Data Protection for Domino installation directory to the Notes user. If multiple partitions with unique UNIX and Linux user IDs are configured, verify that each note user has appropriate access to its configuration files. To ensure appropriate access, specify the ***passworddir*** option for each Notes user. Make sure the directory specified by the ***passworddir*** option is different for each Notes user. You should not specify the installation directory for the ***passworddir*** option because that would prevent other users from having write access to the password file (TSM.PWD). If a Notes user does not have read/write permission to the password file, the ***passwordaccess***=*generate* setting will fail for that partition. In order for the Web client to be able to access its partitions, the password must be generated for all of the partitions. Carry out these actions to address this issue:

- Define a separate server stanza in dsm.sys for each partition. For example, on the server stanza in dsm.sys for the Notes user ID *notes*, specify

  ```
  passworddir /opt/tivoli/tsm/client/domino/bin/domdsmc_notes/
  ```

  On the server stanza in dsm.sys for the Notes user ID *notes1*, specify

  ```
  passworddir /opt/tivoli/tsm/client/domino/bin/domdsmc_notes1/
  ```
- The values for DSMI_LOG, DOMI_LOG, and DOMI_CONFIG can specify the same directory for a Notes user. However, the directory specified by these environment variables cannot be specified for a separate Notes user. For example, set the environment for a Domino server with two partitions identified with Notes user IDs *notes* and *notes1*, as follows:

  notes

  ```
  DSMI_LOG=/opt/tivoli/tsm/client/domino/bin64/domdsmc_notes
  DOMI_LOG=/opt/tivoli/tsm/client/domino/bin64/domdsmc_notes
  DOMI_CONFIG=/opt/tivoli/tsm/client/domino/bin64/domdsmc_notes/domdsm.cfg
  ```

  notes1

```
DSMI_LOG=/opt/tivoli/tsm/client/domino/bin64/domdsmc_notes1
DOMI_LOG=/opt/tivoli/tsm/client/domino/bin64/domdsmc_notes1
DOMI_CONFIG=/opt/tivoli/tsm/client/domino/bin64/domdsmc_notes1/domdsm.cfg
```

The key objective of these requirements is that these values must specify a location where the Notes user has read/write permission.

See "Multiple Domino server partitions" on page 185 for more information about using Data Protection for Domino in multiple Domino server partitions.

Set environment variables

Required and optional environment variable settings are provided.

The **`dominstall`** program automatically sets the following Data Protection for Domino and Tivoli Storage Manager environment variables:

- DOMI_DIR
- DOMI_LOG
- DOMI_CONFIG
- DSMI_DIR
- DSMI_LOG
- DSMI_CONFIG

These settings are contained in a `<notesuser>`.profile file generated by the **`dominstall`** program. See the descriptions in this section if you would like to change your Data Protection for Domino or Tivoli Storage Manager environment variable settings. You must, however, set the shell environment variables described in this section.

See *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide* for additional information on these environment variables.

Data Protection for Domino environment variables

How to set the Data Protection for Domino environment variables.

These environment variables can be set by executing the profile generated by the dominstall program. For example

```
. ./notes.profile
```

The following environment variables are used to point to files and directories that Data Protection for Domino uses:

1. Set the **DOMI_DIR** environment variable to point to the directory where Data Protection for Domino is installed. The default installation directory is
   - AIX (64-bit): `/usr/tivoli/tsm/client/domino/bin64`
   - Linux: `/opt/tivoli/tsm/client/domino/bin64`
2. Set the **DOMI_LOG** environment variable to point to the directory where the Data Protection for Domino log file (domdsm.log) will be stored. The default is the directory where Data Protection for Domino was installed. Specify this environment variable to change the default setting.
3. Set the **DOMI_CONFIG** environment variable. Points to the file name of the Data Protection for Domino preferences file. The default is domdsm.cfg in the directory where Data Protection for Domino is installed. Specify this

environment variable to change the default setting. The file name can include a fully-qualified path or a relative path. A relative path is relative to the current directory where Data Protection for Domino is run.

Tivoli Storage Manager environment variables

This section describes how to set the Tivoli Storage Manager environment variables.

The following Tivoli Storage Manager API environment variables are used to point to files that the API uses:

1. Set the **DSMI_DIR** environment variable. Points to the directory where the Tivoli Storage Manager API is installed. The default value is the default installation directory for the Tivoli Storage Manager API.
2. Set the **DSMI_LOG** environment variable. Points to the directory where the Tivoli Storage Manager API error log file (dsierror.log) will be stored. The default directory is the Data Protection for Domino install directory. Specify this environment variable to change the default setting.
3. Set the **DSMI_CONFIG** environment variable. Points to the Tivoli Storage Manager API options file name. The default is the dsm.opt file in the directory where Data Protection for Domino is installed. Specify this environment variable to change the default setting. The file name can include a fully-qualified path or a relative path. A relative path is relative to the current directory where Data Protection for Domino is run.

Bourne and Korn Shell environment variables

This section describes how to set the Bourne and Korn Shell environment variables.

1. Make sure these environment variables are set in the user profile of the partition directory for the Bourne or Korn shell.

   ```
   DOMI_DIR=/usr/tivoli/tsm/client/domino/bin64
   DOMI_LOG=/usr/tivoli/tsm/client/domino/bin64/domdsmc_notes
   DOMI_CONFIG=/usr/tivoli/tsm/client/domino/bin64/domdsmc_notes/domdsm.cfg
   DSMI_LOG=/usr/tivoli/tsm/client/domino/bin64/domdsmc_notes
   DSMI_CONFIG=/usr/tivoli/tsm/client/domino/bin64/domdsmc_notes/dsm.opt
   PATH=/opt/lotus/bin:/local/notesdata:$PATH
   export DOMI_DIR DOMI_CONFIG DOMI_LOG DSMI_CONFIG DSMI_LOG PATH
   ```

   The `domdsmc_notes` value is relative to the Domino user profile and partition directory.

   Note: These environment variables must be set. The shell script generate by `dominstall` in the DP for Domino directory (`/usr/tivoli/tsm/client/domino/bin64/domino_notes/notes.profile`) for each partition can be used to set these environment variables.
2. Make sure that the PATH statement specifies the Domino executable directory (`.../lotus/bin`) and the Domino data directory.
3. For AIX, the following environment variable must be set as shown:`AIXTHREAD_MNRATIO=1:1`

C Shell environment variables

This section describes how to set the C Shell environment variables.

1. Make sure these environment variables are set for the C shell in the .cshrc file of the user ID that runs the Domino server:

   ```
   setenv DOMI_DIR /usr/tivoli/tsm/client/domino/bin64
   setenv DOMI_LOG /usr/tivoli/tsm/client/domino/bin64/domdsmc_notes
   setenv DOMI_CONFIG /usr/tivoli/tsm/client/domino/bin64/domdsmc_notes/domdsm.cfg
   setenv DSMI_LOG /usr/tivoli/tsm/client/domino/bin64/domdsmc_notes
   setenv DSMI_CONFIG /usr/tivoli/tsm/client/domino/bin64/domdsmc_notes/dsm.opt
   setenv PATH /opt/lotus/bin:/local/notesdata:$PATH
   ```

2. Make sure that the PATH statement specifies the Domino executable directory (`.../lotus/bin`) and the Domino data directory.
3. For AIX, the following environment variable must be set as shown:`AIXTHREAD_MNRATIO=1:1`

Communication

This section describes the communication concepts between Data Protection for Domino and the Tivoli Storage Manager server.

Data Protection for Domino communicates with several product APIs in order to complete various functions. The Tivoli Storage Manager API is accessed in order for Data Protection for Domino to communicate with the Tivoli Storage Manager server. The Domino API is accessed in order to communicate with the Domino server during database operations, and DB2 enabled Notes data is accessed by communicating with the DB2 Recovery API. The option parameters are specified in the dsm.syssystem options file. See *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide* for additional information on specifying the communication method.

You can end a Data Protection for Domino client session by issuing the **Cancel Session** command from a Tivoli Storage Manager Admin client. Do not press Ctrl-C as this can lead to unexpected results.

Register

The registration concepts between Data Protection for Domino and the Tivoli Storage Manager server.

Before backing up to and recovering from a Tivoli Storage Manager server, you must have a Tivoli Storage Manager registered node name and a password. The process of setting up a node name and password is called *registration*. Once Data Protection for Domino is registered with a Tivoli Storage Manager server, you can begin using Data Protection for Domino to back up and restore your Domino databases and transaction logs.

If your system has a node name assigned to the Tivoli Storage Manager backup-archive client, you should have a different node name and define a separate stanza in the dsm.sys system options file for Data Protection for Domino.

For information about performing the registration process, see *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide*.

Create policy

Concepts associated with Tivoli Storage Manager policies and provides information about settings.

Although Data Protection for Domino operates in ways similar to other Tivoli Storage Manager clients, it is unlike regular Tivoli Storage Manager clients in that it does not always store complete replacements for objects on the Tivoli Storage Manager server. When a database file is backed up, it is a complete backup of the entire database and becomes a new backup version of that database. However, if archival logging is being used on the Domino server, then each archived transaction log file contains changes to one or more logged databases over a period of time. Each of these transaction log files has a unique name so there will never be multiple versions of the same transaction log file. Because of this difference, Data Protection for Domino requires special Tivoli Storage Manager policy settings.

How Data Protection for Domino affects policy (NSF databases)

Data Protection for Domino affects Tivoli Storage Manager backup policy for NSF databases in these ways:

- Regular use of the **`Domdsmc Inactivatelogs`** command inactivates the archived transaction log files when all NSF databases that would require that file for a complete recovery are inactive. Therefore, be sure to set the retention period for inactive transaction log files to be equal to or greater than that of the database backup objects. This ensures the files are available as long as any inactive database file that may need them is available so that a point in time recovery of an inactive database backup version can be accomplished. This can be done by using the same management class for the transaction log files that is used for the database files.
- It is possible to have multiple versions of the same transaction log file under certain circumstances. Data Protection for Domino and the Domino Server provide the capability to archive the currently filling transaction log. Thus, the same transaction log file can be backed up multiple times (while it is filling and again when it is full). Also, if the Domino server is stopped abnormally after transaction log files have been archived but not yet reused by the Domino server, those transaction log files can be archived again (even though they are unchanged). As a result, version limit parameters for the management class used for transaction log files should be set to ensure that extra versions of a transaction log file are purged from the backup storage pools.
- To optimize the recovery process, use collocation for the file space containing the transaction log files if they are stored on sequential media on the Tivoli Storage Manager server. The transaction log files are stored in a separate file space from the database files on the Tivoli Storage Manager server.

How Data Protection for Domino affects policy (DB2 enabled Notes databases)

Data Protection for Domino affects Tivoli Storage Manager backup policy for DB2 enabled Notes databases in these ways:

- Regular use of the **`Domdsmc DB2INActivateobjs`** command shows how to inactivate the archived transaction log files and backup objects when all DB2 enabled Notes databases that would require those files for a complete recovery are inactive. Therefore, be sure to set the retention period for inactive transaction log files to be equal to or greater than that of the database backup objects. This ensures the files are available as long as any inactive database file that may need them is available so that a point in time recovery of an inactive database backup version can be accomplished. This can be done by using the same management class for the transaction log files and backup objects that is used for the database files.

- To optimize the recovery process, use collocation for the file space containing the transaction log files if they are stored on sequential media on the Tivoli Storage Manager server. The transaction log files are stored in a separate file space from the database files on the Tivoli Storage Manager server.

Policy settings

You should use default values for the following Backup Copy Group parameters because they are not applicable to Data Protection for Domino:

- ***frequency***
- ***mode***
- ***serialization***

You should define a separate policy domain where the default management class has the settings required for your Domino backup data and then just register all DominoTivoli Storage Manager nodes to that domain. If you choose to define a new management class within an existing policy domain (which is not the default management class for that domain), then you must add an ***include*** statement to the Data Protection for Dominoinclude-exclude options file to bind all objects to that management class. For example: `include * mcname` .

See your Tivoli Storage Manager administrator or the appropriate Tivoli Storage Manager Administrator's Guide for your server platform for more information on defining or updating policy domains and copy groups.

Data Protection for Domino stores all objects as backup objects on Tivoli Storage Manager so an Archive Copy Group is not required, although it can exist.

All database backup objects are complete file backups so normal version controls available through Tivoli Storage Manager server policies apply. Set the ***verdeleted***, ***verexists***, ***retonly*** and ***retextra*** parameters of the Backup Copy Group according to your needs for the number of backup versions to be kept and the retention period of these backup versions.

Options and preferences

This section describes the files where options and preferences must be set.

Data Protection for Domino uses these files to store configuration information.

If you have a Tivoli Storage Manager backup-archive client, on the same system with Data Protection for Domino, you must use different node names for the two clients.

domdsm.cfg

The domdsm.cfg preferences file contains options specific to Data Protection for Domino. Use the **set** command to set values for these options. Do not use a text editor to edit this file.You can display the current values in domdsm.cfg by issuing the **query preferences** command. If the preferences file is corrupt and contains invalid values, the default values for the preferences are used. See "Domdsmc Set" on page 123 on page 123 for parameters stored in this file.

dsm.opt

The options file, dsm.opt, identifies the Tivoli Storage Manager server to contact by specifying the ***servername*** option.Use the sample options file, dsm.opt.smp, to create the dsm.opt file. The dsm.opt.smp file is located in the Data Protection for Domino installation directory.

dsm.sys

The Tivoli Storage Manager system options file. The client system options file, dsm.sys, contains stanzas that identify the Tivoli Storage Manager server to access and the node name by which Data Protection for Domino is known to the Tivoli Storage Manager server. These stanzas also specify communication parameters, backup and restore processing options, authorization options and select scheduling options. If you are using the Tivoli Storage Manager backup-archive client together with Data Protection for Domino, you should define separate stanzas in the dsm.sys system options file for the two clients. Only the root user can edit the dsm.sys file.

Required options

This section describes required options.

After Data Protection for Domino is registered to a Tivoli Storage Manager server, the following Tivoli Storage Manager options must be specified in the system options file in the Tivoli Storage Manager API installation directory in order to communicate with the Tivoli Storage Manager server:

- ***nodename***
- ***password***
- ***tcpserveraddress***

The default system options file name is dsm.sys. The Tivoli Storage Manager administrator should provide you with the node name, password, and the communications method for connecting to the Tivoli Storage Manager server.

Preferred options

Preferred options to use when configuring Data Protection for Domino.

You can specify these options to customize your Data Protection for Domino environment in the system options file in the Tivoli Storage Manager API installation directory.

passwordaccess

When ***passwordaccess*** is set to *prompt*, you are prompted for your password. When ***passwordaccess*** is set to *generate*, the Tivoli Storage Manager API saves the current password (encrypted) and automatically generates a new one when the current one expires. This method of password management is useful when running scheduled, unattended backups. This ensures that the backup never fails due to an expired password.

Specify this option in the client system options file.

passworddir

The `passwordddir` option specifies the directory to store an encrypted password file, `TSM.PWD`. The default location of the `passworddir` on AIX is `/etc/security/adsm`. This default location can only be accessed by the root user. Therefore when defining the Data Protection for Domino options, you must specify a directory that can be accessed by the notes user, such as `/usr/tivoli/tsm/client/domino/bin64/domdsmc_notes`.

compression

Specifying ***compression*** *yes* causes Data Protection for Domino to compress data before sending it to the Tivoli Storage Manager server. If you enable compression, it affects performance in two ways:

- CPU utilization is higher on the machine on which Data Protection for Domino is running
- Network bandwidth utilization is lower because fewer bytes are transmitted.

If the computer running Data Protection for Domino has a CPU overload, specify ***compression*** *no* because additional CPU usage can impact other applications including the Domino server. It is better to specify ***compression*** *yes* when any of the following conditions exist:

- The network adapter has a data overload
- Communications between Data Protection for Domino and the Tivoli Storage Manager server are over a low bandwidth connection
- There is heavy network traffic

Specifying ***compression*** *yes* results in reduced storage usage on the Tivoli Storage Manager server.

The Tivoli Storage Manager administrator can restrict use of the compression option by specifying, on the Tivoli Storage Manager server side, that a particular node:

- Always uses compression
- Never uses compression
- Leaves the decision up to the node to decide

The value of the compression option for Data Protection for Domino is honored only if the Tivoli Storage Manager administrator leaves the compression decision to the node. The default is to let the node decide.

Specify this option in the client system options file.

Exclude databases that increase in size during compression (***compression*** *yes*) by using the client option, ***exclude.compression***. See *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide* for information about this option. See “Include and exclude processing” on page 182 for examples of include/exclude statements.

The compression status of an NSF backup can be seen by issuing a query command or in the GUI.

tapeprompt

This option controls whether Data Protection for Domino waits for tape mount requests to be resolved on the Tivoli Storage Manager server or terminates the current operation when the Tivoli Storage Manager server indicates it is waiting for a tape mount. During a backup operation, Tivoli Storage Manager might issue a prompt to place a tape volume in a drive. Also, during a restore operation, the data you want to recover might be on a tape not currently mounted by the server. In either case, a Tivoli Storage Manager operator or autochanger must take time to mount the particular tape. During that time, Data Protection for Domino continues to show activity and wait for a Tivoli Storage Manager server operation to complete. If this option is selected (***tapeprompt****yes*), Data Protection for Domino waits for a tape to be mounted before it continues. If this option is not selected (***tapeprompt****no*), the operation ends.

Specify this option in the client system options file.

Additional options

This section describes additional options that you can specify.

You can specify these additional options to customize your Data Protection for Domino environment.

Note: Information on how to configure Tivoli Storage Manager compression, encryption and deduplication is available in the Using the Application Programming Interface guide in the Tivoli Storage Manager Information Center.

COMMRESTARTDURATION

This option allows you to specify the total number of minutes that the server will attempt to restart a session after a communication failure. The range of values is one through 9999 and the default is *60*. This option should be set high on a network that is unreliable.

You can specify this option in the Data Protection for Domino preferences file.

COMMRESTARTINTERVAL

This option allows you to specify how many seconds the server will wait before attempting to restart a session after a communication failure. The range of values is one through 9999 and the default is *15*. This means you can avoid overloading the network with restart requests. The ***COMMRESTARTINTERVAL*** time should always be less than or equal to the ***COMMRESTARTDURATION*** time.

You can specify this option in the Data Protection for Domino preferences file.

deduplication

This option allows you to specify whether data deduplication is used. The option can be set to `deduplication yes` or `deduplication no` depending you your requirements. You can specify this option in the Data Protection for Domino preferences file.

domnode

This option allows you to use the Web client GUI to back up and restore Domino server data. It provides the Web client GUI with the Tivoli Storage Manager node name and respective Domino server to access for processing. It also provides important configuration information for the specified node. Specify the full path and name of the Data Protection for Domino preferences file. For example: `domnode /usr/tivoli/tsm/client/domino/bin64/domdsmc_notes/domdsm.cfg`

Consider the following when specifying the ***domnode*** option:

- It must be specified to access the Web client GUI.
- It can be specified multiple times for as many Domino servers or Domino Partitioned Servers as are available.
- It can be used in short form (***domno***) and is not case sensitive.
- Specify this option in the dsm.sys file that is used by the backup-archive client.

domnode example

In this example, the backup-archive client can access Domino server A, Domino server B, and Domino server C:

- Contents of the dsm.sys file:

```
SERVERNAME serverA_notes
DOMNODE /opt/tivoli/tsm/client/domino/bin/domdsmc_notesA/serverA.cfg
SERVERNAME serverB_notes
DOMNODE /opt/tivoli/tsm/client/domino/bin/domdsmc_notesB/serverB.cfg
SERVERNAME serverC_notes
DOMNODE /opt/tivoli/tsm/client/domino/bin/domdsmc_notesC/serverC.cfg
```

- Contents of dsm1.opt: `SERVERNAME domservA`
- Contents of dsm2.opt: `SERVERNAME domservB`
- Contents of dsm3.opt: `SERVERNAME domservC`
- Contents of serverA.cfg: `NOTESInipath /home/notes1/notesdata DOMINstallpath /opt/lotus/bin ADSMLOGDIR=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes1 ADSMOPTFILE=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes1/dsm.opt LOGFILE=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes1/domdsm.log DOMI_DIR=/opt/tivoli/tsm/client/domino/bin`
- Contents of serverB.cfg: `NOTESInipath /home/notes2/notesdata DOMINstallpath /opt/lotus/bin ADSMLOGDIR=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes2 ADSMOPTFILE=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes2/dsm.opt LOGFILE=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes2/domdsm.log DOMI_DIR=/opt/tivoli/tsm/client/domino/bin`
- Contents of serverC.cfg: `NOTESInipath /home/notes/notesdata DOMINstallpath /opt/domino6/lotus/bin ADSMLOGDIR=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes ADSMOPTFILE=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes/dsm.opt LOGFILE=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes/domdsm.log DOMI_DIR=/opt/tivoli/tsm/client/domino/bin`

enableclientencryptkey

When ***enableclientencryptkey*** is set to *yes*, Data Protection for Domino provides 128-bit transparent encryption of Domino databases during backup and restore processing. One random encryption key is generated per session and is stored on the Tivoli Storage Manager server with the object in the server database. Although Tivoli Storage Manager manages the key, a valid database must be available in order to restore an encrypted object. You can specify the databases you want encrypted by adding an include statement with the ***include.encrypt*** option in the dsm.sys file. See “Include and exclude processing” on page 182 for an example of an ***include.encrypt*** statement. Note that transparent encryption is only available on Tivoli Storage Manager server Version 5.3 (or later). See *IBM Tivoli Storage Manager Using the Application Program Interface* for more details regarding the ***enableclientencryptkey*** option.

Information on the encryption status of a backup can be seen during the backup or restore process by using the /DEtail command.

asnodename

When ***asnodename*** is specified, Data Protection for Domino backs up or restores databases on *multiple* clients under the single Tivoli Storage Manager node name specified by this option. Unlike the ***nodename*** option which requires you to enter the password for the node name you specify, the ***asnodename*** option requires that you enter the password for your client node in order to access data that you own. Specify this option in the dsm.sys file. See *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide* for more details regarding the ***asnodename*** option.

Option precedence

This section describes the sequence in which options values are prioritized.

The same option can derive from more than one configuration source. When this happens, the source with the highest priority takes precedence, in the sequence shown as follows:

1. Data Protection for Domino command line option.
2. Data Protection for Domino preferences file, domdsm.cfg.
3. Tivoli Storage Manager client system options file, dsm.sys (highest precedence).
4. Data Protection for Domino options file, dsm.opt.

DB2 enabled Notes Configuration

This section provides configuration information required for DB2 enabled Notes operations.

Before performing standard Data Protection for Domino configuration tasks as described in the configuration section, DB2 enabled Notes operations require additional configuration tasks as described in this section.

Domino Server settings

In addition to DB2 enabled Notes configuration requirements specified in your Domino server documentation, the Domino Server must also be enabled for DB2. This can be performed by running the DB2 Enablement tool. See your Domino Server documentation for details regarding this DB2 tool.

DB2 settings

In addition to DB2 enabled Notes configuration requirements specified in your DB2 documentation, the following settings must also be implemented for the DB2 instance:

- For best results, use a DB2 instance that will manage DB2 enabled Notes databases only.
- Configure the DB2 instance to use Tivoli Storage Manager:
  1. Set the system environment variables.
     - DSMI_DIR: Specify the installation directory for the Tivoli Storage Manager API. There are specific settings that must be used. See "32-bit and 64-bit settings" on page 42 for details.
     - DSMI_LOG: Specify the directory where the Tivoli Storage Manager API error log file (dsierror.log) is located.
     - DSMI_CONFIG: Specify the directory where the Tivoli Storage Manager API options file (dsm.opt) is located. This should be the same dsm.opt file used by Data Protection for Domino.
  2. Make sure the DB2 instance and Data Protection for Domino use the same Tivoli Storage Manager server, node name, and password file. To ensure that the same information is shared, make sure the dsm.opt file used by DB2 points to the same Tivoli Storage Manager server stanza (to be used for DB2 enabled Notes backups) in the dsm.opt file used by Data Protection for Domino. See "How to configure DB2 and Data Protection for Domino to use the same password file" on page 43 for detailed information about sharing the password file.

     Set the password by issuing this command as the note user: `domdsmc query adsm –adsmpwd=<password_value>` This command must be issued because the **dominstall** program performs initial Data Protection for Domino configuration tasks as the root user and therefore, cannot set the Tivoli Storage Manager password. In addition, the value of the ***passworddir*** option (specified in the appropriate server stanza in the dsm.sys) must specify a directory that is accessible to the Notes user.
  3. Restart the DB2 instance so that the environment variable settings are updated. This can be done by issuing **db2stop** from a DB2 command window. Make sure that the Domino server is stopped and that no other application can connect to it before issuing **db2start** to restart the instance.
  4. Make sure that the password file has been initialized by Data Protection for Domino and that the DB2 instance user has permission to access the file.
  5. Verify the configuration by backing up the Domino database by logging in as the DB2 instance user and issuing this command from a DB2 command window:

     ```
     db2 backup db DOMINO use tsm
     ```

  If the DB2 database does not reside on the same machine as the Domino server, the following requirements must be met:
  - Data Protection for Domino and the DB2 Tivoli Storage Manager Agent cannot share the same dsm.opt file. The ***nodename*** specified in both dsm.opt files must be the same.
  - The Tivoli Storage Manager node password must be updated manually on both machines when it expires.
  - Generate the Tivoli Storage Manager password file using the DB2 Tivoli Storage Manager Agent utility, **dsmapipw**, located in DB2 installation directory.
- Enable the Domino DB2 database for rollforward recovery:
  1. Stop the Domino server.
  2. Issue the following command to enable rollforward recovery: `db2 update database configuration using logarchmeth1 tsm`

3. Back up the database by issuing this command: `db2 backup database domino use tsm` Backing up the database allows applications to connect to the database and also verifies whether the DB2 Tivoli Storage Manager Agent is configured correctly.
4. Start the Domino server.

- Data Protection for Domino must use the DB2 instance user ID and password to back up and restore the Domino DB2 database. The DBUSER preference option stores the DB2 instance user ID and is set with the **domdsmc set db2user** command. For example:

  ```
  domdsmc set db2user=db2admin
  ```
- If you are using DB2 Server 9.1.2 on an AIX or Linux x86 machine, the AIX LIBPATH or Linux LD_LIBRARY_PATH environment variable must be set to include the DB2 instance directory (`sqllib/lib32`) before launching the Web client GUI. These examples display the correct setting with DB2 instance name *db2inst1*:

  ```
  LIBPATH=/usr/lib:/lib:/home/db2inst1/sqllib/lib32
  ```

  or

  ```
  LD_LIBRARY_PATH=/usr/lib:/lib:/home/db2inst1/sqllib/lib32
  ```
- Make sure to refer to your Lotus Domino documentation for information regarding Domino DB2 Enablement Requirements.

Data Protection for Domino settings

Data Protection for Domino provides the following new preference options for use when backing up and restoring DB2 enabled Notes databases:

- ***db2altdbname***
- ***db2containerpath***
- ***db2logpath***
- ***db2logtarget***
- ***db2replace***
- ***db2restoreintopath***
- ***db2sessions***
- ***db2user***

See the description of the "Domdsmc Set" on page 123 command for details regarding these options.

After completing the DB2 enabled Notes configuration tasks described in this section, perform the standard Data Protection for Domino configuration tasks as described in the configuration section.

32-bit and 64-bit settings

Be aware that since DB2 is a 64-bit application and Data Protection for Domino is a 32-bit application, the DSMI_DIR environment variable requires the settings described in this section. The DSMI_DIR environment variable is used to set the Tivoli Storage Manager API path. DB2 (64-bit) requires the Tivoli Storage Manager

64-bit library, libApiTSM64.a. However, Data Protection for Domino (32-bit) requires the Tivoli Storage Manager 32-bit library, libApiDS.a. Therefore, make sure the following settings are specified:

- **DB2 (64-bit)**: The DSMI_DIR environment variable (used by the DB2 instance) must specify the path to the Tivoli Storage Manager 64-bit library, libApiTSM64.a, located in the AIX `/usr/tivoli/tsm/client/api/bin64` or Linux `/opt/tivoli/tsm/client/api/bin64` directory. For example:

  ```
  AIX: DSMI_DIR /usr/tivoli/tsm/client/api/bin64
  ```

  or

  ```
  Linux: DSMI_DIR /opt/tivoli/tsm/client/api/bin64
  ```

  Note that if the DSMI_DIR environment variable (used by the DB2 instance) is not set to the Tivoli Storage Manager 64-bit API path *before* the DB2 **db2start** command is issued, the Tivoli Storage Manager 32-bit API will be used (by default). The DSMI_DIR environment variable (used by the DB2 instance) must specify the Tivoli Storage Manager 64-bit API path in order to function properly.

  Note:
  The Tivoli Storage Manager 64-bit API directory also contains the Tivoli Storage Manager dsm.sys file. Although it is possible that multiple dsm.sys files can reside in both the Tivoli Storage Manager 64-bit API directory and the Tivoli Storage Manager 32-bit API directory, you should use only one dsm.sys file in the Tivoli Storage Manager 32-bit API directory and create a symbolic link to it from the Tivoli Storage Manager 64-bit API directory.
- **Data Protection for Domino (32-bit)**: The DSMI_DIR environment variable (used by Data Protection for Domino) must specify the path to the Tivoli Storage Manager 32-bit library, libApiDS.a, located in the AIX `/usr/tivoli/tsm/client/api/bin` directory or Linux `/opt/tivoli/tsm/client/api/bin` directory. For example:

  ```
  AIX: DSMI_DIR /usr/tivoli/tsm/client/api/bin
  ```

  or

  ```
  Linux: DSMI_DIR /opt/tivoli/tsm/client/api/bin
  ```

How to configure DB2 and Data Protection for Domino to use the same password file

Follow these steps to configure DB2 and Data Protection for Domino to use the same password file:

1. Log in to the Data Protection for Domino node with the Domino User ID.
   a. Configure the dsm.opt file (used by Data Protection for Domino) with desired settings.
   b. Generate the password file (TSM.PWD).
   c. If TSM.PWD is first generated by the DB2 Tivoli Storage Manager Agent, change the access values of the password file (TSM.PWD) to include read and write access for the DB2 User ID. For example:

```
chmod o+rw TSM.PWD
```

If TSM.PWD is first generated by Data Protection for Domino, do not change the access values of the password file (TSM.PWD).

   d. Issue the **"Domdsmc Query Adsmserver" on page 82** command to verify that the Domino user (Data Protection for Domino node) can access the Tivoli Storage Manager server.

2. Log in as the DB2 instance user.
   a. Add the following variable settings to the .profile file (`/home/db2inst1`) and the db2profile file (`/home/db2inst1/sqllib/`):

```
export DSMI_DIR=/usr/tivoli/tsm/client/api/bin64
export DSMI_CONFIG=/home/db2inst1/dsm.opt
export DSMI_LOG=/home/db2inst1
```

   Note that DSMI_DIR is an AIX example. The DSMI_DIR setting on Linux is `DSMI_DIR=/opt/tivoli/tsm/client/api/bin64`.

   b. Symbolically link the dsm.opt file (located in `/home/db2inst1`) to the dsm.opt file used by the Domino user (Data Protection for Domino node). For example:

```
$db2inst1@/home/db2inst1/>ln -s
/usr/tivoli/tsm/client/domino/bin64/domdsmc_polardp1/dsm.opt dsm.opt
```

3. (Optional) This step is necessary in a remote DB2 configuration. Log in as the root user.
   a. Change to the `/home/db2inst1/sqllib/adsm/` directory.
   b. Make sure the root environment has the DSMI_DIR, DSMI_CONFIG, and DSMI_LOG environment variables set. If the root environment does*not* have these environment variables set, then set the following:

```
export DSMI_DIR=/usr/tivoli/tsm/client/api/bin64
export DSMI_CONFIG=/home/db2inst1/dsm.opt
export DSMI_LOG=/home/db2inst1
```

   Note that DSMI_DIR is an AIX example. The DSMI_DIR setting on Linux is `DSMI_DIR=/opt/tivoli/tsm/client/api/bin64`.

   c. Issue the **dsmapipw** utility to generate the password.
   d. Issue the **db2adutl query** command to verify the password was set successfully.

Graphical User Interface

Requirements and procedures on how to access, start, and use the various GUIs to backup and restore your Domino databases and transaction log files.

The Tivoli Storage Manager Web client GUI is available only when the Tivoli Storage Manager Backup-Archive client is installed. The Tivoli Storage Manager Web client GUI allows you to back up and restore Domino server data from a remote machine via a Web browser. It is useful for monitoring multiple servers.

For information about performing these tasks with the command line interface, see "Command-line interface" on page 53.

Getting started

This section describes the requirements needed to use the Tivoli Storage Manager Web client GUI.

Make sure that the following requirements are satisfied before attempting to use the Web client GUI.

Software requirements

Tivoli Storage Manager backup-archive client Version 6.3 (or later)

The Tivoli Storage Manager Backup-Archive Client 6.3 (or later) is required in order to perform Data Protection for Domino NSF or DB2 enabled Notes operations using the Tivoli Storage Manager Web client GUI. The backup-archive client must be installed on the same machine as Data Protection for Domino.

Data Protection for Domino Version 6.3 plug-in

The backup-archive client must reside on the same machine as Data Protection for Domino in order to use the Web client GUI.

You can verify that the Data Protection for Domino plug-in is installed by entering the **`dsmc show plugins`** command. When `Tivoli Storage Manager Domino Utility` displays, the plug-in is installed. For example:

```
<<< Installed plug-ins: >>>
******************************************************
Tivoli Storage Manager Domino Utility
******************************************************
******************************************************
Tivoli Storage Manager Domino Utility
******************************************************
plug-in name            : PIDOM
library name            : libPiDOM.a
library path            : /usr/tivoli/tsm/client/ba/bin64/plugins/libPiDOM.a
function map            : 0x10099e28
plug-in type            : Domino
plug-in ver.            : 6.3.0.0
plug-in info.           : NONE
plug-in lic.            : /usr/tivoli/tsm/client/ba/bin64/plugins/pidomclient.lic
<<< Plug-in table information >>>
Plug-in directory search path       : /usr/lpp/Tivoli/tsm/client/ba/bin/plugins
Plug-in name criteria               : libPi*
Plug-in load member name            : n/a
Return code from piTable creation   : 00000000
```

Microsoft Internet Explorer 5.0 (or later) with Java Runtime Environment (JRE) 1.6 (or later)

This browser is required. When running Data Protection for Domino on AIX or Linux environments, you can also use Mozilla 1.4 (or later).

Tivoli Storage Manager server Version 5.5.0 (or later)

The Tivoli Storage Manager server can reside on a different machine than Data Protection for Domino.

To use deduplication on Tivoli Storage Manager server, Tivoli Storage Manager server version 6.1.0 and above version is required. To use deduplication on the Tivoli Storage Manager Backup Archive client , Tivoli Storage Manager server version 6.2.0 and above is required.

Environment requirements

The following environment must exist before attempting to use the Web client GUI.

The Web client is installed and configured.

Important: If you are using DB2 Server 9.1.2 on an AIX or Linux x86 machine, the AIX LIBPATH or Linux LD_LIBRARY_PATH environment variable must be set to include the DB2 instance directory (`sqllib/lib32`) before launching the Web client GUI. These examples display the correct setting with DB2 instance name db2inst1:

```
LIBPATH=/usr/lib:/lib:/home/db2inst1/sqllib/lib32
```

or

```
LD_LIBRARY_PATH=/usr/lib:/lib:/home/db2inst1/sqllib/lib32
```

Use the backup-archive client command line to configure the Web client:

1. Generate the Tivoli Storage Manager password by starting the backup-archive client session with the following command:
   ```
   dsmc query session
   ```
2. Enter the following command to start the client acceptor daemon (CAD):
   ```
   dsmcad
   ```

Data Protection for Domino is installed and configured.

Make sure that you have followed the instructions provided in the configuration section so that your system is ready to back up and restore Domino data.

The **`dominstall`** program assists you in automatically configuring the Tivoli Storage Manager Web client to operate within your Domino environment. If you have not already done so, run the **`dominstall`** program for your Domino server partition and configure the Tivoli Storage Manager Web client when prompted. See “Performing a manual dominstall configuration” on page 23.

Example files and settings used by the Tivoli Storage Manager Web client

The following files are created in the profile directory by the **`dominstall`** program for use by the Web client. They contain settings used specifically by the Web client.

domdsm.cfg

The Data Protection for Domino preferences file:

```
ADSMLOGDIR=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes
ADSMOPTFILE=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes
 /dsm.opt
LOGFILE=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes/domdsm.cfg
DOMI_DIR=/opt/tivoli/tsm/client/domino/bin
NOTESINIPATH=/notesdata
DOMINSTALLPATH=/opt/lotus/bin
```

dsm.opt

The Data Protection for Domino options file:

```
SERVERNAME serverA_notes
```

dsm.sys.changes

The Tivoli Storage Manager system options file. This file contains the server stanza settings (serverA) of the original dsm.sys file:

```
SERVERNAME       serverA
TCPSERV          serverA.storage.sanjose.ibm.com
COMMMETH         tcpip
TCPPORT          1500
NODENAME         CADlinux
PASSWORDACCESS   generate
DOMNODE          /usr/tivoli/tsm/client/domino/bin64/
domdsmc_notes/domdsm.cfg
```

dsm.sys.additions

The Tivoli Storage Manager system options file. This file contains the server stanza settings (serverA) of the original dsm.sys file with the addition of the updated server name:

```
SERVERNAME       serverA_notes
TCPSERV          serverA.storage.sanjose.ibm.com
COMMMETH         tcpip
TCPPORT          1500
NODENAME         notes
PASSWORDACCESS   generate
PASSWORDDIR      /opt/tivoli/tsm/client/domino/bin/domdsmc_notes
```

notes.profile

The Domino server notes profile:

```
export DSMI_LOG=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes
export DSMI_CONFIG=/opt/tivoli/tsm/client/domino/bin/
domdsmc_notes/dsm.opt
export DOMI_DIR=/opt/tivoli/tsm/client/domino/bin
export DOMI_LOG=/opt/tivoli/tsm/client/domino/bin/domdsmc_notes
export DOMI_CONFIG=/opt/tivoli/tsm/client/domino/bin/
domdsmc_notes/domdsm.cfg
alias domdsmc=domdsmc_notes
export PATH=/opt/lotus/bin:/notesdata:$PATH
```

Starting the Web client GUI

1. Make sure that the software and environment requirements are met.
2. Specify the URL of the client workstation running the Web client in your Web browser. You also need to specify the `httpport` number defined on the client workstation. The default value is 1581. For example: `http://myhost.mycompany.com:1581` Tivoli Storage Manager logs information (such as the httpport number, CAD activity, and errors) to the dsmwebcl.log file. By default, this file is located in the directory where the Tivoli Storage Manager backup-archive client is installed.
3. To launch the Java client GUI, run the **dsm** command. The Java client GUI is only available for zLinux.

For more information

See the *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide* for detailed instructions regarding how to configure the Web client GUI.

Backing up Domino NSF databases

How to configure Data Protection for Domino to backup Domino NSF databases.

Back up Domino NSF databases by performing these steps:

1. Click the Backup button in the Tivoli Storage Manager Web client window. If you have not logged in to the server, the TSM Login Window appears. Fill in the TSM Login window. Then click the **Login** button. The Backup window appears.
2. In the View drop-down list at the top of the directory tree, select **Domino NSF**.
3. Expand the directory tree under Data Protection for Domino to reveal your Data Protection for Domino node. Note that this is the node name specified in the Tivoli Storage Manager options file.
4. Expand the directory tree next to the Domino Server to view the Domino Data Directory.
5. Expand the directory tree next to the Domino Data Directory.
6. Click the selection box next to the objects that you want to back up.
7. In the drop-down list near the top of the Backup window, click the type of backup you want to perform:

   Always backup
   This performs an unconditional (selective) backup of the database.

   Incremental (complete)
   This performs a conditional full backup of the database.

   Backup Domino
   This performs a selective backup of NSF databases and a backup of the Domino DB2 database. This selection is only valid when the Domino Server node is selected.
8. Click the **Backup** button. After the backup completes, the Domino Backup Report window displays processing details, including the actual size of the backup.

To display information about a Domino object (from the Backup window), select the Domino object, click the View menu and then File Details. You can then view detailed information about the backup, including whether it is compressed, encrypted, or deduplicated.

In a multiple Domino server partition environment, only one partition can be backed up at a time.

Backing up Domino DB2 enabled Notes databases and DB2 logs

In order to back up DB2 enabled Notes databases, the DB2 Group (that contains the DB2 enabled Notes databases) or the entire Domino DB2 database must be backed up. See “DB2 enabled Notes database backup” on page 6 for more backup information.

Back up Domino DB2 Groups, DB2 databases, and DB2 database logs by performing the following steps:

1. Click the Backup button in the Tivoli Storage Manager Web client window. If you have not logged in to the server, the TSM Login Window appears. Fill in the TSM Login window. Then click the **Login** button. The Backup window appears.

2. In the View drop-down list at the top of the directory tree, select **Domino DB2**.
3. Expand the directory tree under Data Protection for Domino to reveal your Data Protection for Domino node. Note that this is the node name specified in the Tivoli Storage Manager options file.
4. Expand the directory tree next to the Domino Server and perform one of the following backup operations:

   To perform a full DB2 database backup and back up all the DB2 enabled Notes databases:

   a. Click the selection box next to the Domino Server.
   b. Select **DB2 database** in the drop-down list near the top of the Backup window.
   c. Click the **Backup** button.

   To back up (archive) a DB2 database log file:

   a. Click the selection box next to the Domino Server.
   b. Click the **Archive Log** button.

   To back up all the DB2 enabled Notes databases in a DB2 Group:

   a. Expand the directory tree next to the DB2 Groups to view the Class Names.
   b. Expand the directory tree next to the Class Names to view the individual DB2 Groups.
   c. Click the selection box next to the DB2 Group(s) you want to back up.
   d. Select **DB2 Group** in the drop-down list near the top of the Backup window.
   e. Click the **Backup** button.

   To back up the Domino DB2 enabled Notes database and all the NSF databases on the Domino Server:

   a. Click the selection box next to the Domino Server.
   b. Select **Backup Domino** in the drop-down list near the top of the Backup window.
   c. Click the **Backup** button.

After the backup completes, the Domino Backup Report window displays processing details, including the actual size of the backup.

To display information about a Domino object (from the Backup window), select the Domino object, click the View menu and then File Details.

In a multiple Domino server partition environment, only one partition can be backed up at a time.

Restoring Domino NSF databases

Restore is the first step in the two-step recovery process (activation is the second step). Domino databases need to be restored after a device failure or after a database has been corrupted. Domino databases are restored by reloading a database backup and optionally applying updates (from the transaction logs) that occurred after the backup was taken. Database backups can be restored over corrupted databases or to a different database file. When you restore a database to an existing file, that existing database is overwritten with the information from the restored version.

Perform these tasks to restore a Domino NSF database:

1. Click the **Restore** button in the Data Protection for Domino Web client window. If you have not logged in to the server, the Data Protection for Domino Login Window appears. Enter the required details and click the **Login** button. The Restore window appears.
2. In the View drop-down list at the top of the directory tree, select **Domino NSF**.
3. Expand the directory tree under Data Protection for Domino to reveal your Data Protection for Domino node. This is the node name specified in the Data Protection for Domino options file.
4. Expand the directory tree next to your Data Protection for Domino node to reveal available Domino servers.
5. Expand the directory tree next to the Domino server that contains the databases to restore.
6. Expand the directory tree next to **Databases to Restore**.
7. Click the selection box next to the databases that you want to restore.
8. (Optional) If you want to perform a point in time restore, click the **Point In Time** button and specify the date and time.
9. (Optional) If you want to activate the databases, click the **Options** button and check the box next to Activate Databases on a Restore operation.
10. Click the **Restore** button. In a multiple Domino server partition environment, only one Domino server can be restored at a time.

    Note: To display information about a Domino object (from the Restore window), select the Domino object, click the View menu and then File Details. Information about whether the restore has been compressed, deduplicated, or encrypted is available.

Restoring, rollforward, and activating Domino DB2 enabled Notes databases

How to restore, rollforward, and activate DominoDB2 enabled Notes databases

Domino databases might need to be restored after a device failure or after a database has been corrupted. Remember that in order to restore DB2 enabled Notes databases, the DB2 Group backup (that contains the DB2 enabled Notes databases) or the entire Domino DB2 database backup must be restored. Domino databases are restored by reloading a database backup and optionally applying updates (from the transaction logs) that occurred after the backup was taken. Database backups can be restored over corrupted databases or to a different database file. When you restore a database to an existing file, keep in mind that data which exists in the database is overwritten and replaced by the data in the backup version.

Perform these tasks to restore a DB2 enabled Notes database:

1. Click the Restore button in the Tivoli Storage Manager Web client window or Java client window. If you have not logged in to the server, the TSM Login Window appears. Fill in the TSM Login window. Then click the **Login** button. The Restore window appears.
2. In the View drop-down list at the top of the directory tree, select **Domino DB2**.
3. Expand the directory tree under Data Protection for Domino to reveal your Data Protection for Domino node. Note that this is the node name specified in the Tivoli Storage Manager options file.

4. Expand the directory tree next to your Data Protection for Domino node to reveal available Domino Servers.
5. Expand the directory tree next to the Domino Server that contains the data to restore.
   - To restore a DB2 Group that contains the DB2 enabled Notes database, expand the directory tree next to *Groups to Restore*, find the DB2 enabled Notes database, then click the selection box next to the DB2 Group where it resides.
   - To restore a full DB2 database backup, expand the directory tree next to *Databases to Restore* and click the selection box next to the database that you want to restore.
   - To restore a set of DB2 Groups, expand the directory tree next to *Databases to Restore* and click the selection box next to the DB2 Groups that you want to restore.
   - To rollforward a DB2 database that has been previously restored, expand the directory tree next to *Databases to Rollfoward* and click the selection box next to the database to rollforward. Use the **Rollforward options** to roll the database forward to a specific point in time. The transaction logs are applied to the DB2 database where the DB2 enabled Notes database resides.
   - To activate a DB2 database, expand the directory tree next to *Databases to Activate* and click the selection box next to the database to activate.
6. Perform one of these actions:
   - Click the **Restore** button to restore a full DB2 database or a DB2 Group.
   - Click the **Rollforward** button to rollforward a DB2 database.
   - Click the **Activate** button to activate DB2 NSF databases.

Activating NSF databases

This section provides information on how to use the Tivoli Storage Manager Web client GUI or Java client GUI to activate Domino databases and apply the archived transaction logs.

Activation brings the restored databases online for use by the Domino server. In a multiple Domino server partition environment, databases from only one Domino partition can be activated at a time.

Perform these steps to activate a Domino database.

1. Click the Restore button in the Tivoli Storage Manager Web client window or the Java client window. If you have not logged in to the server, the TSM Login Window appears. Fill in the TSM Login window. Then click the **Login** button. The Restore window appears.
2. Expand the directory tree under Data Protection for Domino to reveal your Data Protection for Domino node. Note that this is the node name and Domino server specified by the *domnode* option.
3. Expand the directory tree next to the Domino server that contains the databases to activate.
4. Expand the directory tree next to *Databases to Activate*.
   - The databases under *Domino Data Directory* are databases that have been restored to their original location.
   - The databases under *Other Databases* are databases that have been restored to an alternate location.
5. Click the selection box next to the databases that you want to activate.

6. (Optional) If you want to activate databases to a time other than the current time, click on the Point In Time button and then use the Apply Logs option.
7. (Optional) If you want to activate to the current time, click the Options button and check the box next to Apply Logs.
8. Click the **Activate** button.

Backing up (archiving) NSF transaction logs

The Tivoli Storage Manager Web client GUI or Java client GUI can be used to back up (archive) Domino transaction log files.

You can back up (archive) Domino transaction log files when archival logging is in effect on the Domino server. This option stores filled transaction log files on the Tivoli Storage Manager server so that space allocated to these files can be reused by the Domino logger.

Perform these steps to back up Domino transaction log files.

1. Click the **Backup** button in the Tivoli Storage Manager Web client or the Java client window. If you have not logged in to the server, the Tivoli Storage Manager Login window appears. Enter the required details and click the **Login** button. The Backup window appears.
2. Expand the directory tree under Data Protection for Domino to reveal your Data Protection for Domino node. This is the node name specified in the Tivoli Storage Manager options file.
3. Select the Domino server that contains the transaction log files to back up. In a multiple Domino server partition environment, only one Domino server can be archived at a time.
4. Click the **Archive Log** button. After processing completes, the Domino Backup Report window displays processing details, including the actual size of the backup

   Note: Information on the status of backup is also displayed in this window. This indicates whether the backup is compressed or deduplicated, along with information about how many LAN free bytes were transferred.

Restoring NSF transaction logs

This section provides information on how to use the Tivoli Storage Manager Web client GUI and Java client GUI to restore Domino transaction log files.

Be aware that necessary Domino transaction log files are restored automatically during database restore processing. You should only restore these log files manually (as shown below) in special circumstances. Note that in a multiple Domino server partition environment, only one transaction log file can be restored at a time.

Perform these steps to restore a Domino transaction log file from the Tivoli Storage Manager server.

1. Click the Restore button in the Tivoli Storage Manager Web client window. If you have not logged in to the server, the TSM Login Window appears. Fill in the TSM Login window. Then click the **Login** button. The Restore window appears.
2. Expand the directory tree under Data Protection for Domino to reveal your Data Protection for Domino node. Note that this is the node name specified in the Tivoli Storage Manager options file.

3. Expand the Domino server that contains the transaction log files to restore.
4. If you want to restore all available transaction log files, click the selection box next to *Restore Log Archive* and then click the **Restore** button.
5. If you want to restore individual transaction log files, expand the directory tree next to *Restore Log Archive* and then click the selection box next to the transaction log files you want to restore. Click the **Restore** button.

   Note: The restore progress report shows details of how many LAN free bytes were transferred. Click on the Details button for detailed information about the backup. Details of encryption, deduplication. and compression are shown, and information about the LanFree bytes transferred. To display information about a Domino object (from the Restore window), select the Domino object, click the View menu and then File Details. Information about whether the restore has been compressed, deduplicated, or encrypted is available.

Inactivating archived NSF transaction logs

This section provides information on how to use the Tivoli Storage Manager Web client GUI to inactivate archived Domino transaction log files.

Perform these steps to inactivate archived Domino transaction log files.

1. Click the Restore button in the Tivoli Storage Manager Web client window. If you have not logged in to the server, the TSM Login Window appears. Fill in the TSM Login window. Then click the **Login** button. The Restore window appears.
2. Expand the directory tree under Data Protection for Domino to reveal your Data Protection for Domino node. Note that this is the node name specified in the Tivoli Storage Manager options file.
3. Click the selection box next *Restore Log Archive*.
4. Click the **Inactivate Log Archives** button. Note that in a multiple Domino server partition environment, only one Domino Server at a time is available for Inactivate Log Archives.

Command-line interface

This section describes how to use the Data Protection for Domino command line interface to perform tasks with Domino NSF and DB2 databases.

NSF Commands

How to use the Data Protection for Domino command line interface with Domino NSF databases.

Domdsmc Activatedbs

The **Domdsmc activatedbs** command brings restored database backups online.

Purpose

The **Domdsmc activatedbs** command allows you to bring restored database backups online. If the database is logged, you can apply all applicable transactions from the transaction logs or apply transactions up to a specific point in time to update the database.

You can put databases in a corrupt state if you press **CTRL-C** (or cancel the job) in the middle of an activate. This prevents the databases from being activated. Also, any databases activated before the **CTRL-C** (or cancel) was pressed, can be corrupted, and must be restored and activated again.

This command acts on restored database backups that are pending activation (that is, they have been restored with the **`/activate=no`** parameter). The Tivoli Storage Manager server is not contacted unless archived transaction logs are needed when using the **`/applylogs`** parameter.

If you receive the Domino message `Recovery Manager: Database is not latest copy.` when you issue the **`domdsmc activatedbs`** command with the **`/applylogs`** parameter, a problem may exist with your Domino Logger ID. Consult your Domino documentation to determine why you received this error message. You can also run the **`domdsmc query logarchive`** command to view archived transaction log extents for more information. If two Logger IDs display as in the following example:

```
Domino Server: restroan01
--------------

Logger Id: OF88256BC1:005F8602-ON00000365:0136DCCF
----------
                          Transaction

Log Archive Date       Log Filename    A/I      Size
---------------------    ------------    ---     ------
05/22/2004 10:27:26      S0000000.TXN     A     64.00MB


Domino Server: restroan01
--------------

Logger Id: OF88256BC1:005EDBA5-ON00000365:0136DCCF
----------
             Transaction

Log Archive Date       Log Filename    A/I      Size
---------------------    ------------    ---     ------
05/22/2004 10:20:23      S0000000.TXN     A     64.00MB
```

Data Protection for Domino uses an alternate restore path for the transaction logs on a Domino 6 or later environment when the *TRANSLOG_RECOVER_PATH* variable is specified in the `NOTES.INI` file. If the alternate log restore path specified in the `NOTES.INI` file is not a fully qualified path, Data Protection for Domino does not use the alternate restore path. Contact Lotus support to determine why your Logger ID has changed.

You can use any of the displayed Logger IDs to restore logged databases. In order to use any of the Logger IDs other than the current one, you need to use an alternate server to restore logged databases. See "Alternate server and alternate partition restores for NSF databases" on page 177 for detailed instructions on how to perform this procedure.

```
►►──DOMDSMC──ACTIVatedbs──┬──────────────────────────┬────────────────────────────────►
                          └─/ADSMNODe=──nodename─┘

►─┬─────────────────────────────────────┬─┬──────────────────────────┬──────────────────►
  │                 ┌─dsm.opt──────┐    │ └─/ADSMPWD=──password─┘
  └─/ADSMOPTFile=───┴─optionsfile──┴────┘
```

```
►──┬───────────────────────────────────────────────┬────────────────────────────────────────►
   │                             ┌─,00:00:00─┐     │
   └─/APPLYLogs=──┬──────────┬───┴─,time─────┴─────┘
                  └─date─────┘

►──┬────────────────────────────────────────────────────────┬───────────────────────────────►
   │              ┌─3──────────┐      ┌─,1024───────┐       │
   └─/BUFFers=────┴─numbuffers─┴──────┴─,buffersize─┴───────┘

►──┬──────────────────────────────────────────┬──┬──────────────────────────────────────┬───►
   │                  ┌─domdsm.cfg───┐        │  │              ┌─domdsm.log───┐        │
   └─/CONFIGfile=─────┴─cfgfilename──┴────────┘  └─/LOGFile=────┴─logfilename──┴────────┘

►──┬──────────────────────────────┬──┬──────────────────────────────┬──┬──────────┬──┬───────────┬──►◄
   │                 ┌─60─┐       │  │                  ┌─Yes─┐     │  └─/PICk────┘  └─/Quiet────┘
   └─/LOGPRUne=──────┼─n──┼───────┘  └─/MOUNTWait=──────┴─No──┴─────┘
                     └─No─┘
```

Parameters

/ADSMNODe=*nodename*
Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile= *optionsfile*
Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means that the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **`dominstall`** program, a relative path means that the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- It is recommended that you specify the **`adsmoptfile`** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD= *password*
Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess****generate* in the Tivoli Storage Managersystem options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/APPLYLogs *=date,time*

Specifies that transaction log recovery for the restored databases is performed if they are logged. The *date* and *time* values must be specified in the same date and time format defined in the Data Protection for Domino preferences file. The transaction logs are applied to a specified point in time or to the current date and time if no *date* and *time* values are specified.

date Specify a date string in the active date format. When specified, transactions that are completed and committed before the specified date are applied to the restored database. The date specified should be after the backup date of the backup image that is being restored. The ***/pit*** option can be used with the **restore** command to automatically restore the most recent full backup image that is performed before the desired point in time.

Because there is one transaction log for all logged databases, all the databases should be activated together (in one command). This situation applies when restoring multiple databases that need to have transactions applied from the log. This prevents the fetching of the same transaction logs multiple times from the Tivoli Storage Manager server. The databases can be restored separately (if necessary) with the ***/activate****=no* parameter and then activated together with a single **activatedbs** command.

If you are restoring a database that is backed up from a different Domino server, logged transactions cannot be applied. In this case, you can only activate a full backup image. You must also use the Notes *fixup* utility to reset the internal sequence numbers of the restored and activated database.

Note: If circular logging is in effect, it might not be possible to properly apply transactions if the log has wrapped. If an attempt to apply transaction logs fails, the database or databases being processed are marked as corrupted. The database or databases will have to be restored again.

The date must be specified using the same date format defined in the Data Protection for Domino preferences file. See "Domdsmc Set" on page 123 for a list of available date formats.

time Specify a time string in the active time format. If you specify a date without the time, 00:00:00 on a 24-hour clock is used.

The time must be specified using the same time format defined in the Data Protection for Domino preferences file. See "Domdsmc Set" on page 123 for a list of available time formats.

/BUFFers= *numbuffers,buffersize*

Specifies the number and size of data buffers that transfer data between the Domino server and the Tivoli Storage Manager API. Increasing the number or size (or both) of the data buffers can improve throughput.

You can specify from 2 to 8 buffers, the default value is *3*. The size of the buffers can be from 64 to 8192 kilobytes, the default value is *1024*.

If the ***/buffers*** parameter is not specified on the command line or defined in the preferences file, Data Protection for Domino uses the default values.

/CONFIGfile= *cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile= *logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne= *60*|*n*|*No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.
No	Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/MOUNTWait= *Yes*|*No*

If the Tivoli Storage Manager server is configured to store transaction log backup data on removable media, then the Tivoli Storage Manager server can indicate to Data Protection for Domino that it is waiting for a required storage volume to be mounted. If this occurs, this option allows you to specify whether Data Protection for Domino waits for the media mount or stops the current operation. Removable media is media such as tapes.

You can specify:

Yes Wait for tape mounts. This is the default.

No Do not wait for tape mounts.

/PICk

Displays a list of the restored databases that are waiting for activation. The databases listed are those that match the *dbname* pattern specified. Databases to be activated can be selected from the list.

The *pick list* is presented as a scrollable list with the same manipulation functions as offered in the base Tivoli Storage Manager client PICK function.

Quiet

Specifies that status information does not display. However, the information is written to the activity log.

Examples

Example 1: The following example brings all the restored database backups online and applies transactions from the transaction log to update the database to the date specified:

```
domdsmc activatedbs /applylogs=02/23/2007
```

Output example:

```
Starting Domino database activation...

Initializing Domino connection...
Logging on to the Tivoli Storage Manager server, please wait...

Starting archivelog recovery...

Media Recovery Replay: 100%
02/22/07 04:32:25 PM  Recovery Manager: Media Recovery complete for
/local/notesdata/datadir3/yyyy.nsf.dad, last update applied 02/22/07
03:51:12 PM.

Archivelog recovery completed successfully.

Activating database datadir3/yyyy.nsf, 1 of 1,
Activate of datadir3/yyyy.nsf completed successfully.


Total pending databases inspected:                1
Total pending databases requested for activation:  1
Total pending databases activated:                1

Throughput rate:                                  0.00 Kb/Sec
Total bytes transferred:                          0
Elapsed processing time:                          0.00 Secs
```

Example 2: The following example brings all the restored database backups online:

```
domdsmc activatedbs
```

Output example:

```
Starting Domino database activation...

Initializing Domino connection...
Logging on to the Tivoli Storage Manager server, please wait...

Activating database testdb2.nsf, 1 of 1,
Activate of testdb2.nsf completed successfully.


Total pending databases inspected: 1
Total pending databases requested for activation: 1
Total pending databases activated: 1
```

Domdsmc Archivelog

`Domdsmc archivelog` backs up Domino transaction log files when archival logging is in effect on the Domino server.

Purpose

This command queries the Domino server to determine if any log extents are ready for archiving. If so, the log files are backed up to Tivoli Storage Manager server storage, and the Domino server is notified of their availability for reuse. In addition, high and low threshold values can be specified as a percentage of the log capacity to control whether or not log files should be archived when the command is run. This allows the command to be scheduled regularly to protect against a log full condition but to actually do the archive only if the log is getting close to being full. Thus, if enough log space is allocated to contain an average day's worth of updates, it is possible to establish a strategy where log files are normally archived daily during low usage time (e.g. a daily schedule without threshold values) but unusually high volumes of change can also be handled on an exception basis. For example, an hourly schedule of the `archivelog` command with appropriate specified threshold values performs the archive only if necessary.

You should run this command frequently to ensure that allocated transaction log space is freed.

The active transaction log is also backed up with Domino Server 8.5.x (or higher).

```
>>--DOMDSMC--ARCHivelog--+------------------------+--------------------------->
                         '-/ADSMNODe=--nodename-'

>--+---------------------------------+--+------------------------+------------>
   |                 .-dsm.opt-----. |  '-/ADSMPWD=--password-'
   '-/ADSMOPTFile=---+-optionsfile-+-'

>--+----------------------------------------------------+--------------------->
   |              .-3----------.  .-,1024-------.        |
   '-/BUFFers=----+-numbuffers-+--+-,buffersize-+--------'

>--+----------------------------------+--+-------------------------------+---->
   |                .-domdsm.cfg--.   |  |             .-domdsm.log--.   |
   '-/CONFIGfile=---+-cfgfilename-+---'  '-/LOGFile=---+-logfilename-+---'
```

```
►──┬────────────────────────┬──┬──────────────────────────┬──┬─────────┬──────────────►
   │               ┌─60─┐   │  │               ┌─Yes─┐    │  └─/Quiet─┘
   └─/LOGPRUne=────┼─n──┼───┘  └─/MOUNTWait=───┴─No──┴────┘
                   └─No─┘
```

```
►──┬──────────────────────────────────────────┬──────────────────────────────────►◄
   │                          ┌─,0────────┐   │
   └─/THRESHold=──highvalue───┴─,lowvalue─┴───┘
```

Parameters

/ADSMNODe=nodename

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=optionsfile

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the **adsmoptfile** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=password

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify **passwordaccess generate** in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If **passwordaccess** is set to **generate** and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If **passwordaccess** is set to **prompt** and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If **passwordaccess** is set to **prompt** and you do not specify a password on the command line, then you are prompted for a password.

/BUFFers=*numbuffers,buffersize*

Specifies the number and size of data buffers that transfer data between the Domino server and the Tivoli Storage Manager API. Increasing the number or size (or both) of the data buffers can improve throughput.

You can specify from 2 to 8 buffers, the default value is *3*. The size of the buffers can be from 64 to 8192 kilobytes, the default value is *1024*.

If the ***/buffers*** parameter is not specified on the command line or defined in the preferences file, Data Protection for Domino uses the default values.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60***|***n***|***No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/MOUNTWait=*Yes***|***No*

If the Tivoli Storage Manager server is configured to store transaction log backup data on removable media, then the Tivoli Storage Manager server can indicate to Data Protection for Domino that it is waiting for a required storage volume to be mounted. If this occurs, this option allows you to specify whether Data Protection for Domino waits for the media mount or stops the current operation. Removable media is media such as tapes.

You can specify:

Yes Wait for tape mounts. This is the default.

No Do not wait for tape mounts.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

/THRESHold=*highvalue***,** *lowvalue*

Use this option to specify when the **archivelog** command should start and stop archiving eligible transaction log files. The *highvalue*, specified as a percentage of the transaction log capacity, identifies the point at which log archiving should begin. If the current occupancy of the transaction log equals or exceeds the value for this parameter, eligible log files are archived until the occupancy falls to or below the *lowvalue* which is also specified as a percentage of the log capacity.

The *highvalue* variable is an integer in the range from 1 to 99.

The *lowvalue* variable is an integer in the range from 0 to 98 but it must be less than the high value. The default is 0 which means that all log files eligible for archive will be archived. Specify a low threshold value (greater than 0) to prevent the active transaction log from being backed up.

If the ***/threshold*** option is not specified, then all eligible transaction log files are archived. The active transaction log is an eligible transaction log file.

For example, specifying the following command will cause transaction log files to be archived only after the log is at or more than 90% full and the archive process will stop once sufficient space has been reclaimed to make the log less than or equal to 50% full:

```
/threshold=90,50
```

It is important to note that the ***/threshold*** option is impacted by the total size of the transaction log. The total size of the transaction log is determined on the Domino server by the value of the TRANSLOG_UseAll and TRANSLOG_MaxSize options in the notes.ini file.

Example

The following example backs up the current archive log:

```
domdsmc archivelog
```

Output example:

```
Starting Domino transaction log archive...
Initializing Domino connection...
Logging on to the Tivoli Storage Manager server, please wait...

Archiving transaction log file /local/notesdata/domlogs/S0000002.TXN
Full: 0   Read: 67,109,888  Written: 67,109,888  Rate: 9,616.58 Kb/Sec
Archive of /local/notesdata/domlogs/S0000002.TXN completed successfully.

Total Domino transaction log files ready for archive: 1
Total Domino transaction log files archived:          1
Total Domino transaction log files deduplicated:      0

Throughput rate:                                      9,615.17 Kb/Sec
Total bytes inspected:                                67,109,888
Total bytes transferred:                              67,109,888
Total LanFree bytes transferred:                      0
Total bytes before deduplication:                     0
Total bytes after deduplication:                      0
Data compressed by:                                   0%
Deduplication reduction:                              0.00%
Total data reduction ratio:                           0.00%
Elapsed processing time:                              6.82 Secs
```

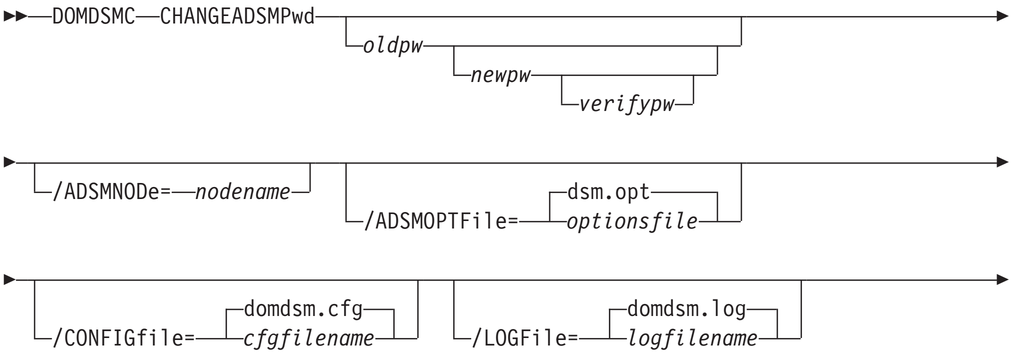
Domdsmc Changeadsmpwd

This section describes how to use the **domdsmc changeadsmpwd** command.

Purpose

Domdsmc changeadsmpwd changes the Tivoli Storage Manager password that is used by Data Protection for Domino. If you do not enter the old and new passwords on the command, you are prompted for them. When Data Protection for Domino prompts you for the passwords, the password is not displayed on the screen.

You must run as the Domino server ID, which must be the same as the Tivoli Storage Manager Authorized user ID, to change the Tivoli Storage Manager password.



```
►─┬──────────────────────┬──────────────────────────────────────────────►◄
  │             ┌─60─┐   │
  └─/LOGPRUne=──┼─n──┼───┘
                └─No─┘
```

Parameters

oldpw The current password to change. You are prompted for this value if omitted.

newpw The new password. You are prompted for this value if omitted. When choosing a new password, you can use from 1 to 64 characters.

Valid password characters are as follows:

A-Z	Any letter, A through Z, uppercase or lowercase
0–9	Any number, 0 through 9
+	Plus
.	Period
_	Underscore
-	Hyphen
&	Ampersand

A password is not case-sensitive.

verifypw
The verify password is used to validate the password entered for newpw. You are prompted for this value if omitted.

/ADSMNODe=*nodename*
Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*
Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/CONFIGfile=*cfgfilename*
Specifies the name of the Data Protection for Domino preferences file. The

file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60 | n | No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

Example

The following example changes the Tivoli Storage Manager password to **secret**:

```
domdsmc changeadsmpwd oldpassword secret secret
```

Output example:

```
ACD0260I Password successfully changed.
```

Domdsmc Help

This section describes how to use the **`domdsmc help`** command.

Purpose

`Domdsmc help` provides online help for the **`domdsmc`** commands. This command lists one or more commands and their parameters.

```
                         ┌"*"─────────┐ ┌"*"────────┐
►►──DOMDSMC──┬─?────┬────┴────────────┴─┴───────────┴──────────────────────►◄
             └─HELP─┘    └─cmdname─┘     └─subcmd─┘
```

Parameters

`"*"|cmdname`

Identifies the specific Data Protection for Domino command that is to be displayed. If the wildcard character * is used, help for all Data Protection for Domino commands is displayed. If you do not specify a command name, asterisk (*) is the default.

The valid command names are shown here:

```
ACTIVatedbs
ARCHivelog
CHANGEADSMPwd
DB2ACTivatedbs
DB2ARCHivelog
DB2DELetealternate
DB2INActivateobjs
DB2RESTore
DB2ROLLforward
DB2Selective
FULLSelective
HELP
INACTivatelogs
Incremental
Query
RESETdatabase
RESTore
RESTORELOGArchive
SELective
SET
UPDATEDB2Pwd
```

`"*"|subcmd`

Help can be displayed for commands that have several subcommands, for example, the **`query`** commands. If you do not specify a subcommand or the wildcard character asterisk (*), then help for all Data Protection for Domino **`query`** commands is displayed.

The valid subcommand names for the **`query`** commands are shown here:

```
Adsmserver
DBBackup
DB2Backup
DB2Pendingdbs
DB2ROLLforward
DOMino
LOGArchive
PENDingdbs
PREFerences
```

Examples

Example 1: The command **`domdsmc`** or **`domdsmc help "*"`** provides information about the syntax of all the commands.

Output example:

```
Choose from the following commands:

DOMDSMC ACTIVatedbs
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/APPLYLogs=date[,time]] (default: currentdate,currenttime)
  [/BUFFers=numbuffers[,buffersize]] (default: 3,1024)
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/MOUNTWait=Yes|No] (default: Yes)
  [/PICk]
  [/Quiet]

DOMDSMC ARCHivelog
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/BUFFers=numbuffers[,buffersize]] (default: 3,1024)
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/MOUNTWait=Yes|No] (default: Yes)
  [/Quiet]
  [/THRESHold=highvalue[,lowvalue]]

DOMDSMC CHANGEADSMPwd [oldpw [newpw [verifypw]]]
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)

DOMDSMC DB2ACTivatedbs dbname[dbname,...]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/DB2ALtdbnames=db2database] (default: DOM_ALT)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/INTO=filename]
  [/ISOLATE]
  [/LOCKGroup]
  [/LOGPRUne=60|n|No] (default: 60)
  [/PICk=[SHOWAl]]
  [/REPlace=Yes|No] (default: Yes)
  [/Quiet]

DOMDSMC DB2ARCHivelog
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/Quiet]

DOMDSMC DB2DELetealternate db2database
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)

DOMDSMC DB2INActivateobjs
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/Quiet]
  [/SERVer=currentserver|servername]

DOMDSMC DB2RESTore db2group[,db2group,...]
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/DB2ALtdbname=db2datbase] (default: DOM_ALT)
  [/DB2DATAbase=db2database]
  [/DB2CONTainerpath=path]
  [/DB2LOGPath=path]
  [/DB2REPlace=Yes|No] (default;Yes)
  [/DB2RESTIntopath=path]
  [/DB2SESSIONS=numsessions] (default: 1)
  [/FULL]
  [/INPlace]
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/PICk=SHOWACtive|SHOWAll] (default: SHOWACtive)
  [/PIT=date[,time]] (default: currentdate,currenttime)
  [/Quiet]
  [/SERVer=currentserver|servername]

DOMDSMC DB2ROLLforward db2database
  [/APPLYLogs=date[,time]]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/PICk=[SHOWAll]]
  [/Quiet]

DOMDSMC DB2Selective db2group[,db2group,...]
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/DB2SESSIONS=numsessions] (default: 1)
  [/FULL]
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/Quiet]

DOMDSMC FULLSelective
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/BUFFers=numbuffers[,buffersize]] (default: 3,1024)
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/DB2SESSions=numsessions (default: 1)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/MOUNTWait=Yes|No] (default: Yes)
  [/Quiet]
  [/SESSions=numsessions (default: 1)

DOMDSMC HELP|? [*|command] [*|subcmd]
Valid command names :       Valid subcmds :
   ACTIVatedbs                 Adsmserver
   ARCHivelog                  DBBackup
   CHANGEADSMPwd               DB2Backup
   DB2ACTivatedbs              DB2Pendingdbs
   DB2ARCHivelog               DB2ROLLforward
   DB2DELetealternate          DOMino
   DB2INActivateobjs           LOGArchive
   DB2RESTore                  PENDingdbs
   DB2ROLLforward              PREFerences
   DB2Selective
   FULLSelective
   HELP
   INACTivatelogs
   Incremental
   Query
   RESETdatabase
   RESTore
   RESTORELOGArchive
   Selective
   SET

DOMDSMC INACTivatelogs
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/Quiet]
  [/SERVer=currentserver|servername]

DOMDSMC Incremental dbname[,dbname,...]
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/BUFFers=numbuffers[,buffersize]] (default: 3,1024)
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/MOUNTWait=Yes|No] (default: Yes)
  [/Quiet]
  [/SUBDir=No|Yes] (default: No)
  [/SESSions=numsessions (default: 1)

DOMDSMC Query Adsmserver
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)

DOMDSMC Query DBBackup *|dbname
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/DEtail]
  [/INACTive]
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/SERVer=currentserver|servername]
  [/SUBDir=No|Yes]  (default: No)

DOMDSMC Query DB2Backup *|db2group
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/DB2DATAbase=db2database]
  [/DEtail]
  [/FULL]
  [/INACTive]
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/SERVer=currentserver|servername]

DOMDSMC Query DB2Pendingdbs
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)

DOMDSMC Query DB2ROLLforward
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)

DOMDSMC Query DOMino [*|dbname]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/SUBDir=No|Yes] (default: No)
  [/TYpe=All|Nsf|Db2] (default: All)

DOMDSMC Query LOGArchive
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/DEtail]
  [/INACTive]
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/SERVer=currentserver|servername]
  [/FROMDate=date]
  [/TODate=date]

DOMDSMC Query PENDingdbs
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)

DOMDSMC Query PREFerences
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)

DOMDSMC RESETdatabase [dbname|dbname,...]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)

DOMDSMC RESTore dbname[,dbname,...]
  [/ACTIVate=No|Yes] (default: No)
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/BUFFers=numbuffers[,buffersize]] (default: 3,1024)
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/INTO=filename]
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/MOUNTWait=Yes|No] (default: Yes)
  [/PICk=SHOWACtive|SHOWALl] (default: SHOWACtive)
  [/PIT=date[,time]] (default: currentdate,currenttime)
  [/Quiet]
  [/REPlace=Yes|No]  (default: Yes)
  [/SERVer=currentserver|servername]
  [/SUBDir=No|Yes] (default: No)

DOMDSMC RESTORELOGArchive [logname[,logname,...]] (default: 'last')
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/BUFFers=numbuffers[,buffersize]] (default: 3,1024)
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/INTOPath=pathname]
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)
  [/MOUNTWait=Yes|No] (default: Yes)
  [/PICk=SHOWACtive|SHOWALl] (default: SHOWACtive)
  [/Quiet]
  [/REPlace=Yes|No]  (default: Yes)
  [/SERVer=currentserver|servername]
  [/FROMDate=date]
  [/TODate=date]

DOMDSMC Selective dbname[,dbname,...]
  [/ADSMNODe=nodename]
  [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
  [/ADSMPWD=password]
  [/BUFFers=numbuffers[,buffersize]] (default: 3,1024)
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGGedonly]
  [/LOGPRUne=60|n|No] (default: 60)
  [/MOUNTWait=Yes|No] (default: Yes)
  [/Quiet]
  [/SESSions=numsessions (default: 1)
  [/SUBDir=No|Yes] (default:No)

DOMDSMC SET PARMname=value
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)

  where PARMname and default values are:
     ADSMLOGDir=
     ADSMOPTFile=
     BUFFers=3  (2..8)
     BUFFERSIze=1024  (64..8192)
     DATEformat=
       0    locale-specified
       1    MM/DD/YYYY
       2    DD-MM-YYYY
       3    YYYY-MM-DD
       4    DD.MM.YYYY
       5    YYYY.MM.DD
     DB2ALtdbname=DOM_ALT
     DB2CONTainerpath=
     DB2LOGPath=
     DB2LOGTarget=
     DB2REPlace=Yes (Yes|No)
     DB2RESTIntopath=
     DB2SESSions=1 (1..64)
     DB2USER=
     DOMI_DIR=
     DOMINstallpath=
     LOGFile=domdsm.log
     LOGPRUne=60  (0..9999 | No)
     MOUNTWait=Yes  (Yes|No)
     NOTESInipath=
     NUMberformat=
       0    locale-specified
       1    n,nnn.dd
       2    n,nnn,dd
       3    n nnn,dd
       4    n nnn.dd
       5    n.nnn,dd
       6    n'nnn,dd
     REPlace=Yes  (Yes|No)
     SESSions=1 (1..64)
     STATistics=No (No|Yes)
     SUBDir=No  (No|Yes)
     TIMEformat=
       0    locale-specified
       1    HH:MM:SS
       2    HH,MM,SS
       3    HH.MM.SS
       4    HH:MM:SSA/P
     DOMTXNBYTElimit=0 (0...2097152)
     DOMTXNGROUPmax=2 (2,65000)
     COMMRESTARTDuration=60(1,9999)
     COMMRESTARTInterval=15(1,9999)

DOMDSMC UPDATEDB2Pwd [oldpw [newpw [verifypw]]]
  [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
  [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
  [/LOGPRUne=60|n|No] (default: 60)

EXAMPLES:

  DOMDSMC Selective adb.nsf
  DOMDSMC Query Domino
```

Example 2: To display help for all the **query** commands, enter the following:

```
domdsmc help query "*" or domdsmc help query
```

Output example:

```
DOMDSMC Query Adsmserver
[/ADSMNODe=nodename]
[/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
[/ADSMPWD=password]
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)

DOMDSMC Query DBBackup *|dbname
[/ADSMNODe=nodename]
[/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
[/ADSMPWD=password]
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/DEtail]
[/INACTive]
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)
[/SERVer=currentserver|servername]
[/SUBDir=No|Yes] (default: No)

DOMDSMC Query DB2Backup *|db2group
[/ADSMNODe=nodename]
[/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
[/ADSMPWD=password]
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/DB2DATAbase=db2database]
[/DEtail]
[/FULL]
[/INACTive]
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)
[/SERVer=currentserver|servername]

DOMDSMC Query DB2Pendingdbs
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)

DOMDSMC Query DB2ROLLforward
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)

DOMDSMC Query DOMino [*|dbname]
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)
[/SUBDir=No|Yes] (default: No)
[/TYpe=All|Nsf|Db2] (default: All)

DOMDSMC Query LOGArchive
[/ADSMNODe=nodename]
[/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
[/ADSMPWD=password]
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/DEtail]
[/INACTive]
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)
[/SERVer=currentserver|servername]
[/FROMDate=date]
[/TODate=date]

DOMDSMC Query PENDingdbs
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)

DOMDSMC Query PREFerences
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)
```

Example 3: To display help for the **`query domino`** command, enter the following:

```
domdsmc help query domino
```

Output example:

```
DOMDSMC Query DOMino [*|dbname]
[/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
[/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
[/LOGPRUne=60|n|No] (default: 60)
[/SUBDir=No|Yes] (default: No)
[/TYpe=All|Nsf|Db2] (default: All)
```

Example 4: To display help for the **`db2selective`** command, enter the following:

```
domdsmc help db2selective
```

Output example:

```
DOMDSMC DB2Selective db2group[,db2group,...]
 [/ADSMNODe=nodename]
 [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
 [/ADSMPWD=password]
 [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
 [/DB2SESSIONS=numsessions] (default: 1)
 [/FULL]
 [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
 [/LOGPRUne=60|n|No] (default: 60)
 [/Quiet]
```

Example 5: To display help for the **`query db2backup`** command, enter the following:

```
domdsmc help query db2backup
```

Output example:

```
DOMDSMC Query DB2Backup *|db2group
 [/ADSMNODe=nodename]
 [/ADSMOPTFile=dsm.opt|filename] (default: dsm.opt)
 [/ADSMPWD=password]
 [/CONFIGfile=domdsm.cfg|filename] (default: domdsm.cfg)
 [/DB2DATAbase=db2database]
 [/DEtail]
 [/FULL]
 [/INACTive]
 [/LOGFile=domdsm.log|logfilename] (default: domdsm.log)
 [/LOGPRUne=60|n|No] (default: 60)
 [/SERVer=currentserver|servername]
```

Domdsmc Inactivatelogs

This section describes how to use the **domdsmc inactivatelogs** command.

Purpose

Domdsmc inactivatelogs expires transaction log files from backup storage. Because there is a single shared transaction log for all logged databases on a Domino server, log files cannot be inactivated (and allowed to expire) until all databases that require that log file for recovery are inactive. This command queries the database backups on the Tivoli Storage Manager server to determine which log files are required by any active database backup. This command also inactivates log files that are no longer required (because the database backups were inactivated). This command should be run after full database backups are completed, to inactivate the transaction logs at the same time the database backups requiring them are inactivated.

```
►►──DOMDSMC──INACTivatelogs──┬───────────────────────┬──────────────────────────►
                             └─/ADSMNODe=──nodename─┘

►──┬──────────────────────────────────┬──┬──────────────────────────┬───────────►
   │                ┌─dsm.opt──────┐  │  └─/ADSMPWD=──password─┘
   └─/ADSMOPTFile=──┴─optionsfile──┴──┘

►──┬──────────────────────────────────┬──┬──────────────────────────────┬──────►
   │               ┌─domdsm.cfg───┐   │  │           ┌─domdsm.log───┐   │
   └─/CONFIGfile=──┴─cfgfilename──┴───┘  └─/LOGFile=──┴─logfilename──┴───┘

►──┬─────────────────────────┬──┬──────────┬──┬─────────────────────────────────┬──►◄
   │              ┌─60─┐     │  └─/Quiet─┘  │            ┌─currentserver─┐   │
   └─/LOGPRUne=──┼─n──┼─────┘              └─/SERVer=──┴─servername────┴───┘
                  └─No─┘
```

Parameters

/ADSMNODe=*nodename*
: Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*
: Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*
: Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

Note: Using a colon (:) as the filename for the preferences file will result in unnecessary output.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* **|** *n* **|** *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of

values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

/SERVer=*currentserver* | *servername*

Specifies the Domino server name. If not specified, Data Protection for Domino uses the current Domino server.

Example

This example causes the archive log extents that are no longer needed to expire:

```
domdsmc inactivatelogs
```

Output example:

```
Number of Logs Inactivated: 1
```

Domdsmc Incremental

This section describes how to use the **domdsmc incremental** command.

Purpose

Domdsmc incremental performs the following functions:

- Backs up new databases since the last backup (or newly included ones)
- Backs up any non-logged databases that changed since the last backup (based on modification dates of both data and metadata)
- Backs up any logged databases with a DBIID that changed (if archival logging is in effect)
- Inactivates any active database backups on the Tivoli Storage Manager server that are excluded from backup or no longer exist on the Domino server

A query of the current backup objects from the Tivoli Storage Manager server is required before any actions take place.

This command backs up a database by matching the *dbname* pattern with the following conditions:

- The database is not excluded in the Tivoli Storage Manager include-exclude options file (standard include and exclude processing is supported).
- The database is not logged, and was modified since the last active backup image for that database. Both data and non-data modification dates are checked. If either is different from that of the active backup, the database is backed up.
- Archival logging is in effect, and the DBIID of a logged database changed. If the DBIID has not changed, then logged databases are not backed up (the changes are captured in the transaction log backups). In this case, periodic selective

backups of all logged databases should be done to refresh the active backup images. This reduces the number of transaction logs to be applied during a recovery.

Note: When circular logging is used on the Domino server (or when logging is disabled on the Domino server), transaction log files are not archived. See "NSF backup strategy considerations" on page 4 for more information.

- The database is new or newly included in the backup (an active backup image does not exist on the Tivoli Storage Manager server).

The incremental command can also inactivate active backup images for databases that are deleted from the Domino server or excluded from backup. Backups can automatically be expired according to the retention parameters that are defined in the Tivoli Storage Manager management class.

Use the incremental command to back up a single directory or all databases within the Notes data path by specifying an appropriate *dbname* pattern.

```
►►──DOMDSMC──Incremental───┬─"*"───────────┬──┬──────────────────────────┬──────────────────►
                           │ ┌─,───────┐   │  └─/ADSMNODe=──nodename─────┘
                           │ ▼         │   │
                           └───dbname──┴───┘

►──┬────────────────────────────────────────┬──┬────────────────────────┬──────────────────►
   │                 ┌─dsm.opt──────┐       │  └─/ADSMPWD=──password────┘
   └─/ADSMOPTFile=───┴─optionsfile──┴───────┘

►──┬─────────────────────────────────────────────────────┬─────────────────────────────────►
   │           ┌─3────────────┐   ┌─,1024────────┐       │
   └─/BUFFers=─┴─numbuffers───┴───┴─,buffersize──┴───────┘

►──┬──────────────────────────────────┬──┬────────────────────────────────┬────────────────►
   │              ┌─domdsm.cfg──┐     │  │            ┌─domdsm.log──┐     │
   └─/CONFIGfile=─┴─cfgfilename─┴─────┘  └─/LOGFile=───┴─logfilename─┴─────┘

►──┬──────────────────────┬──┬────────────────────────┬──┬──────────┬──────────────────────►
   │             ┌─60─┐   │  │              ┌─Yes─┐   │  └─/Quiet───┘
   └─/LOGPRUne=──┼─n──┼───┘  └─/MOUNTWait=───┴─No──┴───┘
                 └─No─┘

►──┬──────────────────────────────────┬──┬──────────────────────┬─────────────────────────►◄
   │            ┌─1────────────┐      │  │           ┌─No──┐    │
   └─/SESSIONS=─┴─numsessions──┴──────┘  └─/SUBDir=──┴─Yes─┴────┘
```

Parameters

"*" | *dbname,dbname,...,*

Specifies the file path of a database or file path pattern for a group of databases. The file path pattern can represent a group of databases to be conditionally backed up. The wildcard character asterisk (*) is used to specify a group of databases when used in the *dbname*. Multiple *dbnames* can be specified as long as they are separated with commas.

If you specify the wildcard character in the *dbname*, you must use double or single quotes, for example, "abc*" or 'abc*'.

The file path must be relative to the Notes data directory.

Symbolic links are referred to by their symbolic names. To reference a database in a directory outside of the Notes data directory and any subsequent directories pointed to by a directory link in the data path, use the directory link name as the directory name. For example, if database `xyz.nsf` is in a directory, and pointed to by the link `vol1.dir`, refer to it as `vol1/xyz.nsf`. If a symbolic directory link is created with the same name as a physical directory in the Notes data path, only the physical directory is searched.

The wildcard character (*) is used to represent any number of any characters when used in the file name portion of the file path. The wildcard character is not supported within directory names. The following example backs up all databases within the dir_A directory beginning with the characters **ter**:

```
domdsmc incremental "dir_A/ter*"
```

The following example backs up all databases on the server that meet the criteria of the incremental back up:

```
domdsmc incremental "*" /subdir=yes
```

The following example backs up all databases whose file name ends in **acct**:

```
domdsmc incremental "*acct.n*" /subdir=yes
```

Note: Standard include and exclude processing applies to Domino database names. Wildcards can be used on the backup command, and specific databases can be excluded from the backup with the include-exclude list in the Tivoli Storage Manager include-exclude options file. For example, to exclude all databases on a volume pointed to by the symbolic directory link *temp.dir*, use the following statement:

```
exclude /temp/*
```

Note that the exclude statement refers to the relative file name including symbolics and not the physical file path. For additional information on include and exclude options, see “Include and exclude processing” on page 182 and *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide*.

***/ADSMNODe=**nodename*

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

***/ADSMOPTFile=**optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.

- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/BUFFers=*numbuffers****,****buffersize*

Specifies the number and size of data buffers that transfer data between the Domino server and the Tivoli Storage Manager API. Increasing the number or size (or both) of the data buffers can improve throughput.

You can specify from 2 to 8 buffers, the default value is *3*. The size of the buffers can be from 64 to 8192 kilobytes, the default value is *1024*.

If the ***/buffers*** parameter is not specified on the command line or defined in the preferences file, Data Protection for Domino uses the default values.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* | *n* | *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/MOUNTWait=*Yes* | *No*

If the Tivoli Storage Manager server is configured to store transaction log backup data on removable media, then the Tivoli Storage Manager server can indicate to Data Protection for Domino that it is waiting for a required storage volume to be mounted. If this occurs, this option allows you to specify whether Data Protection for Domino waits for the media mount or stops the current operation. Removable media is media such as tapes.

You can specify:

Yes Wait for tape mounts. This is the default.

No Do not wait for tape mounts.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

/SESSions=*numsessions* | **1**

Specifies the number of Tivoli Storage Manager server sessions to be used by Data Protection for Domino. You can specify from *1* to *64* sessions. The default value is *1*.

/SUBDir=*No* | *Yes*

Specifies whether subdirectories within the specified file path are searched for databases that match the file pattern. If this option is not specified, Data Protection for Domino uses the value of the ***/subdir*** parameter in the Data Protection for Domino preferences file.

You can specify:

No	Do not search the subdirectories within the specified file path for databases that match the file pattern. This is the default unless reset in the Data Protection for Domino preferences file.
Yes	Search the subdirectories within the specified file path for databases that match the file pattern.

Example

The following example backs up all databases that need to be backed up using the conditions outlined at the beginning of this section (any database ID changed for logged databases or data changed for non-logged databases). This inactivates any database backups that refer to databases that no longer exist on the Domino server or is specifically excluded.

```
domdsmc incremental "*" /subdir=yes
```

Output example:

```
Starting Domino database backup...
Initializing Domino connection...
Querying Domino for a list of databases, please wait...
Querying Tivoli Storage Manager server for a list of database backups, please wait...


Backing up database a_dir/b_dir/clienttest2.nsf, 1 of 1.
Full: 0   Read: 41,418,752   Written: 41,418,752   Rate: 18,310.55 Kb/Sec
Backup of a_dir/b_dir/clienttest2.nsf completed successfully.


Total Domino databases inspected:       120
Total Domino databases backed up:       1
Total Domino databases excluded:        0
Total Domino backup objects expired:   0
Total Domino databases deduplicated:    0

Throughput rate:                        17,779.34 Kb/Sec
Total bytes inspected:                  41,418,752
Total bytes transferred:                41,418,752
Total LanFree bytes transferred:       0
Total bytes before deduplication:    0
Total bytes after deduplication:     0
Data compressed by:          0%
Deduplication reduction:        0.00%
Total data reduction ratio:       0.00%
Elapsed processing time:        2.27 Secs
```

Domdsmc Query Adsmserver

This section describes how to use the **domdsmc query adsmserver** command.

Purpose

Use this command to provide the following information about the Tivoli Storage Manager server:

- Tivoli Storage Manager server name
- Tivoli Storage Manager server level
- Tivoli Storage Manager server platform

- Tivoli Storage Manager nodename of the server
- NetWork Host name of the server
- Options in effect at the server that affects this node (for example, management class information)

```
►►──DOMDSMC──Query──Adsmserver──┬─────────────────────────┬──────────────────►
                                └─/ADSMNODe=──nodename──┘

►──┬──────────────────────────────────────┬──┬─────────────────────────┬──────►
   │                  ┌─dsm.opt──────┐   │  └─/ADSMPWD=──password──┘
   └─/ADSMOPTFile=───┴─optionsfile──┴───┘

►──┬────────────────────────────────────┬──┬────────────────────────────────┬─►
   │                ┌─domdsm.cfg──┐   │  │              ┌─domdsm.log──┐   │
   └─/CONFIGfile=───┴─cfgfilename─┴───┘  └─/LOGFile=───┴─logfilename─┴───┘

►──┬──────────────────────────┬─────────────────────────────────────────────►◄
   │              ┌─60─┐     │
   └─/LOGPRUne=───┼─n──┼─────┘
                  └─No─┘
```

Parameters

/ADSMNODe=*nodename*

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* **|** *n* **|** *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of

values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

Example

The following example queries your Tivoli Storage Manager server:

```
domdsmc query adsmserver
```

Output example:

```
Starting Domino database activation...

Initializing Domino connection...
Logging on to the Tivoli Storage Manager server, please wait...

Activating database testdb2.nsf, 1 of 1,
Activate of testdb2.nsf completed successfully.


Total pending databases inspected: 1
Total pending databases requested for activation: 1
Total pending databases activated: 1
```

Domdsmc Query Dbbackup

This section describes how to use the **domdsmc query dbbackup** command.

Purpose

This command displays a list of database backups that are stored on the Tivoli Storage Manager server that match the *dbname* pattern. Active and inactive objects can be displayed. By default, only the active backup objects are displayed. To include inactive backup versions in the list, use the ***/inactive*** parameter.

The following information is provided:

- Database title
- Database relative path name
- Database size
- Database backup date and time
- Domino server name
- Whether the backup is active or inactive
- Whether the database is logged or not
- Whether the database is encrytped
- Whether the database is compressed
- Whether the database is deduplicated

```
►►──DOMDSMC──Query──DBBackup──┬─"*"────┬──┬──────────────────────┬──────────────────►
                              └─dbname─┘  └─/ADSMNODe=──nodename─┘

►──┬───────────────────────────────────┬──┬──────────────────────┬──────────────────►
   │               ┌─dsm.opt─────┐     │  └─/ADSMPWD=──password─┘
   └─/ADSMOPTFile=─┴─optionsfile─┴─────┘

►──┬────────────────────────────────────┬──┬─────────┬──┬────────────┬──────────────►
   │              ┌─domdsm.cfg───┐      │  └─/DEtail─┘  └─/INACTive──┘
   └─/CONFIGfile=─┴─cfgfilename──┴──────┘

►──┬───────────────────────────────┬──┬────────────────────────┬────────────────────►
   │           ┌─domdsm.log───┐    │  │              ┌─60─┐    │
   └─/LOGFile=─┴─logfilename──┴────┘  └─/LOGPRUne=───┼─n──┼────┘
                                                     └─No─┘

►──┬──────────────────────────────────┬──┬───────────────────────┬─────────────────►◄
   │          ┌─currentserver─┐       │  │            ┌─No──┐    │
   └─/SERVer=─┴─servername────┴───────┘  └─/SUBDir=───┴─Yes─┴────┘
```

Parameters

"*" | *dbname*

Specifies the file path of a database or file path pattern. The file path pattern can represent a group of databases. You can also specify a group of databases by using the wildcard character asterisk (*).

If you specify the wildcard character in the *dbname*, you must use double or single quotes, for example, "abc*" or 'abc*'.

The file path must be relative to the Notes data directory.

Symbolic links are referred to by their symbolic names. To reference a database in a directory pointed to by a directory link in the data path, use the directory link name as the directory name. For example, if database `xyz.nsf` is in a directory, pointed to by the link `vol1.dir`, refer to it as `vol1/xyz.nsf`. If a symbolic directory link is created with the same name as a physical directory in the Notes data path, only the physical directory is searched.

The wildcard character (*) is used to represent any number of any characters. For example:

```
domdsmc query dbbackup "abc*"
```

This example lists all databases that begin with the characters *abc*. When used with the ***/subdir*** parameter, all databases within all subdirectories are listed.

/ADSMNODe=*nodename*

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/DEtail

Shows detailed information on the backup. This includes information on whether the backup in encrypted, compressed or deduplicated.

/INACTive

Specifies that both active and inactive backup objects are displayed. The default is to display only the active backup objects.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file

name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* | *n* | *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/SERVer=*currentserver* | *servername*

Specifies the Domino server name. If not specified, Data Protection for Domino uses the current Domino server.

/SUBDir=*No* | *Yes*

Specifies whether subdirectories within the specified file path are searched for databases that match the file pattern. If this option is not specified, Data Protection for Domino uses the value of the ***/subdir*** parameter in the Data Protection for Domino preferences file.

You can specify:

No Do not search the subdirectories within the specified file path for databases that match the file pattern. This is the default unless reset in the Data Protection for Domino preferences file.

Yes Search the subdirectories within the specified file path for databases that match the file pattern.

Examples

Example 1: This example displays information for all the active database backups that are stored on the local Tivoli Storage Manager server.

```
domdsmc query dbbackup "*"
```

Output example (only a portion of the actual output is shown):

```
                             Database Backup List
                             --------------------

      Domino Server: chilly
      --------------------

   DB Backup Date     Size    A/I Logged Database Title  Database File
------------------- --------- --- ------ -------------- -------------
01/22/2008 14:29:42 819.00KB  A   Yes    Administration  admin4.nsf
01/22/2008 14:29:44 501.50KB  A   No     Administration  admin4.ntf
01/22/2008 14:29:46 384.00KB  A   Yes    Ja AgentRunne   AgeRunner.nsf
01/22/2008 14:29:47 153.50KB  A   No     Agent Log       alog4.ntf
01/22/2008 14:29:48 246.50KB  A   No     Archive Log     archlg80.ntf
01/22/2008 14:29:49 226.00KB  A   No     Billing         billing.ntf
01/22/2008 14:29:54 1226.50KB A   No     Bookmarks       bookmark.ntf
01/22/2008 14:29:56 320.00KB  A   Yes    Local free time busytime.nsf
01/22/2008 14:29:58 143.00KB  A   No     Local free time busytime.ntf
01/22/2008 14:29:58 140.50KB  A   No     Local Document  cache.ntf
01/22/2008 14:29:59 1170.00KB A   Yes    Catalog         catalog.nsf
01/22/2008 14:30:02 799.00KB  A   No     Catalog         catalog.ntf
01/22/2008 14:30:04 1896.00KB A   No     Domino    Certi cca80.ntf
01/22/2008 14:30:08 159.00KB  A   No     Certification L certlog.ntf
```

Example 2: This example displays information for all the database backups that are stored on the local Tivoli Storage Manager server. The information includes inactive backup objects and subdirectories within the file path.

```
domdsmc query dbbackup "*" /inactive /subdir=yes
```

Output example (only a portion of the actual output is shown):

```
                             Database Backup List
                             --------------------

   Domino Server: chilly
   --------------------

  DB Backup Date     Size     A/I Logged Database Title Database File
------------------- --------- --- ------ -------------- -------------
01/22/2008 14:29:42  819.00KB A   Yes    Administration admin4.nsf
01/07/2008 12:11:07  729.00KB I   Yes    Administration admin4.nsf
01/07/2008 12:29:04  729.00KB I   Yes    Administration admin4.nsf
01/07/2008 12:46:21  729.00KB I   Yes    Administration admin4.nsf
01/19/2008 13:50:27  819.00KB I   Yes    Administration admin4.nsf
01/22/2008 14:29:44  501.50KB A   No     Administration admin4.ntf
01/07/2008 12:29:06  389.50KB I   No     Administration admin4.ntf
01/07/2008 12:46:23  389.50KB I   No     Administration admin4.ntf
01/19/2008 13:50:33  501.50KB I   No     Administration admin4.ntf
01/19/2008 13:56:48  501.50KB I   No     Administration admin4.ntf
01/22/2008 14:30:24  300.75MB A   Yes    A new database data2/db1.nsf
01/07/2008 11:51:39  300.75MB I   Yes    A new database data2/db1.nsf
01/01/2008 12:11:42  300.75MB I   Yes    A new database data2/db1.nsf
01/07/2008 12:29:42  300.75MB I   Yes    A new database data2/db1.nsf
01/07/2008 12:47:04  300.75MB I   Yes    A new database data2/db1.nsf
```

Example 3: The following example queried the Tivoli Storage Manager server and included the ***/adsmpwd*** parameter:

```
domdsmc q dbb "*" /adsmpwd=notes
```

Output example:

```
                             Database Backup List
                             --------------------

   Domino Server: Server1
   --------------------

  DB Backup Date     Size     A/I Logged Database Title Database File
------------------- --------- --- ------ -------------- -------------
01/16/2008 11:14:19 1019.50KB A   Yes    db1             db1.nsf
01/16/2008 10:56:28 1019.50KB A   Yes    db2             db2.nsf
01/16/2008 10:56:29 1019.50KB A   Yes    db3             db3.nsf
01/16/2008 10:56:30 1170.00KB A   Yes    newdb           dblink.nsf
01/16/2008 10:56:31 1019.50KB A   Yes    SERVER1 Mailbox mail.box
```

Example 4: This example displays detailed information for a specific data base that is stored on the local Tivoli Storage Manager server.

```
domdsmc query dbbackup mynotes1.nsf /detail
```

Output example:

```
Database Backup List
--------------------


Backup Object Information
-------------------------

Domino Server Name ..................... DOMINOTESTSERVER
Database Title ......................... mynotes1
Database File .......................... mail\mynotes1.nsf
Database Backup Date ................... 07/22/2011 12:56:24
Database Size .......................... 24.50MB
Database Backup State .................. Active
Database Logged ........................ Yes
Database Compressed .................... Yes
Database Encryption Type ............... None
Database Client-deduplicated ........... Yes
```

Domdsmc Query Domino

This section describes how to use the **domdsmc query domino** command.

Purpose

This command displays general information and an optional list of databases on the local Domino server. If you do not specify a *dbname* pattern, then only general server information is displayed. If you specify a *dbname* pattern, then a list of databases on the Domino server that match the *dbname* pattern is displayed.

The information provided includes the following:

- Domino server name
- Domino server level
- Domino server build
- Logging type in effect
- When the Domino server is enabled for DB2, the DB2 enabled status and the name of the Domino DB2 database are provided.
- Optionally lists current databases with their specific details (for example: database title and relative path name)

```
►►──DOMDSMC──Query──DOMino──┬───────┬──┬──────────────────────────────────┬──────►
                            ├─"*"───┤  │               ┌─domdsm.cfg───┐   │
                            └─dbname┘  └─/CONFIGfile=──┴─cfgfilename──┴───┘

►──┬────────────────────────────────┬──┬─────────────────────────┬────────────────►
   │            ┌─domdsm.log───┐    │  │                ┌─60─┐   │
   └─/LOGFile=──┴─logfilename──┴────┘  └─/LOGPRUne=─────┼─n──┼───┘
                                                        └─No─┘

►──┬─────────────────────┬──┬──────────────────┬─────────────────────────────────►◄
   │           ┌─No──┐   │  │         ┌─All─┐  │
   └─/SUBDir=──┴─Yes─┴───┘  └─/TYpe=──┼─Nsf─┼──┘
                                      └─Db2─┘
```

Parameters

"*" | *dbname*

Specifies the file path of a database or file path pattern. The file path pattern can represent a group of databases. Use the wildcard (*) character to specify a group of databases. If you specify the wildcard character in the *dbname*, you must use double or single quotes, for example, "abc*" or 'abc*'. If the *dbname* or wildcard character is not used, only general server information will be displayed.

The file path must be relative to the Notes data directory.

Symbolic links are referred to by their symbolic names. To reference a database in a directory pointed to by a directory link in the data path, use the directory link name as the directory name. For example, if database `xyz.nsf` is in a directory, pointed to by the link `vol1.dir`, refer to it as `vol1/xyz.nsf`. If a symbolic directory link is created with the same name as a physical directory in the Notes data path, only the physical directory is searched.

The wildcard character (*) is used to represent any number of any characters. For example:

```
domdsmc query domino "abc*"
```

This command lists all databases that begin with the characters *abc* in the Notes data directory. When used with the **query dbbackup** command, this can provide a list of all database backups that are stored on the Tivoli Storage Manager server. When used with the ***/subdir*** parameter, all databases within all subdirectories are listed.

Note: "All" databases on a Domino server are defined to mean all databases within the Notes data directory or symbolically linked to the Notes data directory. This means that databases with nonstandard file extensions are not included. (Databases with a file extension of .nsf are standard file extensions. Templates have a standard file extension of .ntf and are included.)

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* | *n* | *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.
No	Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/SUBDir=*No* | *Yes*

Specifies whether subdirectories within the specified file path are searched for databases that match the file pattern. If this option is not specified, Data Protection for Domino uses the value of the ***/subdir*** parameter in the Data Protection for Domino preferences file.

You can specify:

No Do not search the subdirectories within the specified file path for databases that match the file pattern. This is the default unless reset in the Data Protection for Domino preferences file.

Yes Search the subdirectories within the specified file path for databases that match the file pattern.

/TYpe=*All* **|** *Nsf* **|** *Db2*

Specifies the type of database to display.

You can specify:

All Specifies that both Domino NSF and Domino DB2 enabled Notes databases are displayed. This is the default.

Nsf Specifies that only Domino NSF databases are displayed.

Db2 Specifies that only Domino DB2 enabled Notes databases are displayed.

Examples

Example 1: The command below shows how to list all the databases in the Notes data directory on the Domino server that match the *dbname* pattern *xyz*.

```
domdsmc query domino "xyz*"
```

Example 2: The following example queried the Tivoli Storage Manager server and listed databases on the Domino server with the wildcard character *:

```
domdsmc q dom "*"
```

Output example (only a portion of the actual output is shown):

```
Domino Server Information
-------------------------

  Domino Server Name:  chilly
  Domino Server Level: 7.0
  Domino Server Build: 166
  Logging:             Archival

Domino Database Information
---------------------------

Last Modified Date    Size   Logged   Database Title        Database
------------------    ----   ------   --------------        --------
01/16/2008 02:00:21  819.00KB  Yes  Administration Reque  admin4.nsf
01/16/2008 05:00:24  503.00KB  No   Administration Reque  admin4.ntf
01/16/2008 05:00:26  153.00KB  No   Agent Log             alog4.ntf
01/16/2008 05:00:27  246.00KB  No   Archive Log           archlg70.ntf
01/16/2008 05:00:29  226.00KB  No   Billing               billing.ntf
01/16/2008 05:00:34  1226.00KB No   Bookmarks             bookmark.ntf
01/16/2008 02:00:26  320.00KB  Yes  Local free time info  busytime.nsf
```

Example 3: The following example queries (and displays) the DB2 enabled Notes databases available on the Domino server with the wildcard character *:

```
domdsmc query domino "*" /type=db2
```

Output example:

```
Domino Server Information
-------------------------

  Domino Server Name:  domino7
  Domino Server Level: 7.0.0.0
  Domino Server Build: 259
  Logging:             Archival
  DB2 Enabled:         Yes
  DB2 Database Name:   DOMINO7


Domino NSF DB2 Database Information
-----------------------------------

  Class Name: class0
  -----------

  Last Modified Date         Size     Database Title Group    Database
  ------------------         ----     -------------- -------- --------
  01/20/2008 02:00:19       111.00KB  db2 nsf 1      GRP4     cb2nsf1.nsf
  01/21/2008 02:00:25       110.00KB  db2 nsf 1      GRP4     db2f.nsf
  01/20/2008 02:00:36       114.00KB  db2 nsf 2      GRP4     pb2nsf2.nsf

  Class Name: class1
  -----------

  Last Modified Date         Size     Database Title Group    Database
  ------------------         ----     -------------- -------- --------
  01/21/2008 02:00:24       107.00KB  db2 nsf 1      GRP1     db1.nsf
  01/21/2008 02:00:24       107.00KB  db2 nsf 2      GRP1     db2a.nsf
  01/21/2008 02:00:24       110.00KB  db2 nsf 1      GRP1     db2c.nsf
  01/21/2008 02:00:25       107.00KB  db2 nsf 1      GRP1     db2e.nsf
  01/20/2008 02:00:17       112.00KB  db2 nsf 1      GRP2     ab2nsf1.nsf
  01/21/2008 02:00:24       107.00KB  db2 nsf 2      GRP2     db2b.nsf
  01/21/2008 02:00:25       107.00KB  db2 nsf 1      GRP2     db2g.nsf
  01/20/2008 02:00:37       113.00KB  db2 nsf 1      GRP2     xb2nsf1.nsf

  Class Name: class2
  -----------

  Last Modified Date         Size     Database Title Group    Database
  ------------------         ----     -------------- -------- --------
  01/20/2008 02:00:18       112.00KB  db2 nsf 2      GRP3     bb2nsf2.nsf
  01/21/2008 02:00:25       107.00KB  db2 nsf 1      GRP3     db2d.nsf
  01/21/2008 02:00:26       107.00KB  db2 nsf 1      GRP3     dbi.nsf
  01/20/2008 02:00:36       114.00KB  db2 nsf 1      GRP3     ob2nsf1.nsf
```

Domdsmc Query Logarchive

This section describes how to use the **domdsmc query logarchive** command.

Purpose

This command displays a list of the archived transaction log extents that are stored on the Tivoli Storage Manager server. By default, only the active log extents are listed. To display inactive extents, use the ***/inactive*** parameter.

```
►►──DOMDSMC──Query──LOGArchive──┬─────────────────────┬──────────────────────►
                                └─/ADSMNODe=──nodename─┘

►──┬──────────────────────────────────┬──┬──────────────────────┬────────────►
   │                ┌─dsm.opt──────┐  │  └─/ADSMPWD=──password─┘
   └─/ADSMOPTFile=──┴─optionsfile──┴──┘
```

```
►──┬────────────────────────────────────┬──┬───────────┬──┬─────────────┬──────►
   │              ┌─domdsm.cfg───┐      │  └─/DEtail───┘  └─/INACTive───┘
   └─/CONFIGfile=─┴─cfgfilename──┴──────┘

►──┬──────────────────────────────────┬──┬────────────────────────┬────────────►
   │           ┌─domdsm.log───┐       │  │              ┌─60─┐    │
   └─/LOGFile=─┴─logfilename──┴───────┘  └─/LOGPRUne=───┼─n──┼────┘
                                                        └─No─┘

►──┬──────────────────────────────────┬────────────────────────────────────────►◄
   │          ┌─currentserver─┐       │
   └─/SERVer=─┴─servername────┴───────┘
```

Parameters

/ADSMNODe=*nodename*

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- It is recommended that you specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/DEtail

Displays information about the backup, such as whether it is encrypted, compressed or deduplicated.

/INACTive

Specifies that both active and inactive backup objects are displayed. The default is to display only the active backup objects.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* | *n* | *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.
No	Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/SERVer=*currentserver***|***servername*

Specifies the Domino server name. If not specified, Data Protection for Domino uses the current Domino server.

Examples

Example 1: The following example displays the list of archived log extents that are stored on the Tivoli Storage Manager server.

```
domdsmc query logarchive
```

Output example:

```
Domino Server: Donatello
--------------

Logger Id: OF50E90638:EDC0ED8E-ON00000395:231EEEA9
----------

Transaction
Log Archive Date Log Filename A/I Size
--------------------- ------------ --- ------
08/21/2011 12:40:53 S0000002.TXN A 64.00MB
08/21/2011 11:37:52 S0000001.TXN A 64.00MB
08/21/2011 11:37:43 S0000000.TXN A 64.00MB


Domino Server: Donatello
--------------

Logger Id: OF94C6A275:5DCDD692-ON00000344:69A3C2C3
----------

Transaction
Log Archive Date Log Filename A/I Size
--------------------- ------------ --- ------
05/08/2011 09:49:55 S0000005.TXN A 64.00MB
05/08/2011 09:49:53 S0000004.TXN A 64.00MB
```

```
With Detail:
domdsmc query logarchive /detail

IBM Tivoli Storage Manager for Mail:
Data Protection for Lotus Domino
Version 6, Release 3, Level 0.0
(C) Copyright IBM Corporation 1999, 2011. All rights reserved.


Backup Object Information
-------------------------

Domino Server Name ................. Donatello
Logger Id .......................... OF50E90638:EDC0ED8E-ON00000395:231EEEA9
```

```
Log Archive File .................... S0000002.TXN
Log Archive Date .................... 08/21/2011 12:40:53
Log Archive Size .................... 64.00MB
Log Archive State ................... Active
Log Archive Compressed .............. No
Log Archive Encryption Type ......... None
Log Archive Client-deduplicated ..... No

Backup Object Information
-------------------------

Domino Server Name .................. Donatello
Logger Id ........................... OF50E90638:EDC0ED8E-ON00000395:231EEEA9
Log Archive File .................... S0000001.TXN
Log Archive Date .................... 08/21/2011 11:37:52
Log Archive Size .................... 64.00MB
Log Archive State ................... Active
Log Archive Compressed .............. No
Log Archive Encryption Type ......... None
Log Archive Client-deduplicated ..... No

Backup Object Information
-------------------------

Domino Server Name .................. Donatello
Logger Id ........................... OF50E90638:EDC0ED8E-ON00000395:231EEEA9
Log Archive File .................... S0000000.TXN
Log Archive Date .................... 08/21/2011 11:37:43
Log Archive Size .................... 64.00MB
Log Archive State ................... Active
Log Archive Compressed .............. No
Log Archive Encryption Type ......... None
Log Archive Client-deduplicated ..... No



Backup Object Information
-------------------------

Domino Server Name .................. Donatello
Logger Id ........................... OF94C6A275:5DCDD692-ON00000344:69A3C2C3
Log Archive File .................... S0000005.TXN
Log Archive Date .................... 05/08/2011 09:49:55
Log Archive Size .................... 64.00MB
Log Archive State ................... Active
Log Archive Compressed .............. No
Log Archive Encryption Type ......... None
Log Archive Client-deduplicated ..... No

Backup Object Information
-------------------------

Domino Server Name .................. Donatello
Logger Id ........................... OF94C6A275:5DCDD692-ON00000344:69A3C2C3
Log Archive File .................... S0000004.TXN
Log Archive Date .................... 05/08/2011 09:49:53
Log Archive Size .................... 64.00MB
Log Archive State ................... Active
Log Archive Compressed .............. No
Log Archive Encryption Type ......... None
Log Archive Client-deduplicated ..... No
```

Example 2: The following example displays the list of archived log extents that are stored on the Tivoli Storage Manager server, including inactive backup objects. This example uses a Tivoli Storage Manager client options file named aserver.opt.

```
domdsmc query logarchive /inactive /adsmoptfile=aserver.opt
```

Output example:

```
   Domino Server: /chilly
   --------------

   Logger Id: OF8525679F:004266F1-ON000003EC:BD9D27DB
   ----------

                         Transaction
  Log Archive Date       Log Filename    A/I     Size
---------------------    ------------    ---    ------
01/23/2008 09:43:16      S0000003.TXN     A       64MB
01/23/2008 09:41:22      S0000002.TXN     A       64MB
01/22/2008 16:52:15      S0000001.TXN     I       64MB
```

Example 3: The following example queried the Tivoli Storage Manager server and included the ***/adsmpwd*** parameter:

`domdsmc q loga /adsmpwd=3n1`

Output example:

```
ACD5819I There are no archived logs for the server named SnailTrail.
```

Example 4: The example below displays detailed information for the list of archived log extents that are stored on the Tivoli Storage Manager server:

`domdsmc query logarchive /detail`

Output example:

```
Backup Object Information
-------------------------

Domino Server Name .................. DOMINOTESTSERVER
Logger Id ........................... OF09A666BF:AACF9914-ON00000302:A048A61F
Log Archive File .................... S0000035.TXN
Log Archive Date .................... 07/22/2011 12:52:37
Log Archive Size .................... 64.00MB
Log Archive State ................... Active
Log Archive Compressed .............. Yes
Log Archive Encryption Type ......... None
Log Archive Client-deduplicated ..... Yes
```

Domdsmc Query Pendingdbs

This section describes how to use the **domdsmc query pendingdbs** command.

Purpose

This command displays a list of all the databases that have been restored but not yet activated.

```
►►──DOMDSMC──Query──PENDingdbs──┬──────────────────────────────────┬──────────►
                                 │               ┌─domdsm.cfg───┐  │
                                 └─/CONFIGfile=──┴─cfgfilename──┴──┘

►──┬────────────────────────────────┬──┬──────────────────────┬──────────────►◄
   │           ┌─domdsm.log──┐      │  │              ┌─60─┐  │
   └─/LOGFile=─┴─logfilename─┴──────┘  └─/LOGPRUne=───┼─n──┼──┘
                                                      └─No─┘
```

Parameters

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60 | n | No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.
No	Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

Example

The command below shows how to list all the pending databases on the Domino server.

```
domdsmc query pendingdbs
```

Output example:

```
                              Pending Database List
                              ---------------------

     Domino Server: chilly
     --------------

  Backup Time Stamp  Size     A/I Logged Database Title Database File
 ------------------- -------- --- ------ -------------- -------------
 01/22/2008 14:36:50 896.00KB A   No     Vacation Planne datadir3/db8.nsf
```

Domdsmc Query Preferences

The **`domdsmc query preferences`** command displays a list of the current values set in the preferences file for Data Protection for Domino.

Purpose

You can view a list of the current values set in the preferences file for Data Protection for Domino by running the **`domdsmc query preferences`** command

```
►►──DOMDSMC──Query──PREFerences──┬──────────────────────────────────┬─────────►
                                 │                ┌─domdsm.cfg───┐  │
                                 └─/CONFIGfile=───┴─cfgfilename──┴──┘

►──┬─────────────────────────────┬──┬──────────────────────┬──────────────────►◄
   │           ┌─domdsm.log───┐  │  │             ┌─60─┐   │
   └─/LOGFile=─┴─logfilename──┴──┘  └─/LOGPRUne=──┼─n──┼───┘
                                                  └─No─┘
```

Parameters

`/CONFIGfile=cfgfilename`

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the *DOMI_CONFIG* environment variable.

The default preferences file is domdsm.cfg.

`/LOGFile=logfilename`

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **`set`** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=60|n|No

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the `/logprune` option to override these defaults for one command run. When the value of **/logprune** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

Example

This command shows the current values stored in the default preferences file for Data Protection for Domino.

```
domdsmc query preferences
```

Output example:

```
ACD5023W The configuration file cannot be found, using default settings.

 ACD5221I The /usr/tivoli/tsm/client/domino/bin64/domdsmc_notes1/domdsm.log
 log file has been pruned
 successfully.

 Data Protection for Domino Preferences
--------------------------------

ADSMLOGDir .....................
ADSMOPTFile ....................
BUFFers ........................ 3
BUFFERSIze ..................... 1024
DATEformat ..................... 0
DOMI_DIR .......................
DOMINstallpath ................. /opt/ibm/lotus/bin
LOGFile ........................ domdsm.log
LOGPRUne ....................... 60
MOUNTWait ...................... Yes
NOTESInipath ...................
NUMberformat ................... 0
REPlace ........................ Yes
SESSions ....................... 1
STATistics ..................... No
SUBDir ......................... No
TIMEformat ..................... 0
DOMTXNBYTElimit................. 0
DOMTXNGROUPmaX.................. 2
COMMRESTARTDuration ............ 60
COMMRESTARTInterval ............ 15

DB2ALTDBname ................... DOM_ALT
DB2CONTainerpath ...............
DB2LOGPath .....................
DB2LOGTarget ...................
DB2REPlace ..................... Yes
DB2RESTIntopath ................
DB2SESSions .................... 1
DB2USER ........................
```

Domdsmc Resetdatabase

This section describes how to use the **domdsmc resetdatabase** command.

Purpose

Domdsmc resetdatabase resets a Domino server database that is in an incomplete state as a result of an unexpected termination occurring during a Data Protection for Domino backup. An unexpected termination during a Data Protection for Domino backup can be caused by the following:

- A program check or segment violation.
- A **kill** command.
- Exiting a debugging program.

Subsequent attempts to back up such a database will fail until the **resetdatabase** command is issued.

You can specify one or more Domino databases to be reset. You must specify the database name. The **resetdatabase** command does not accept wildcard characters.

For more information on disaster recovery procedures, see “Recovery from loss of Domino transaction logs for NSF databases” on page 176.

```
►►──DOMDSMC──RESETdatabase──┬─dbname──────┬──┬─────────────────────────────────┬──────►
                            │ ┌─,──────┐  │  │               ┌─domdsm.cfg───┐  │
                            │ ▼        │  │  └─/CONFIGfile=──┴─cfgfilename──┴──┘
                            └───dbname─┴──┘

►──┬───────────────────────────────┬──┬──────────────────────┬──────────────────────►◄
   │           ┌─domdsm.log────┐   │  │             ┌─60─┐   │
   └─/LOGFile=─┴─logfilename───┴───┘  └─/LOGPRUne=──┼─n──┼───┘
                                                    └─No─┘
```

Parameters

dbname *dbname,dbname,...,*

Specifies the database to be reset. Multiple *dbnames* can be specified as long as they are separated with commas.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60|n|No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.
No	Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

Example

The following example resets the database *testdata.nsf*:

```
domdsmc resetdatabase 'testdata.nsf'
```

Output Example:

```
Database testdata.nsf successfully reset.
```

Domdsmc Restore

This section describes how to use the **domdsmc restore** command.

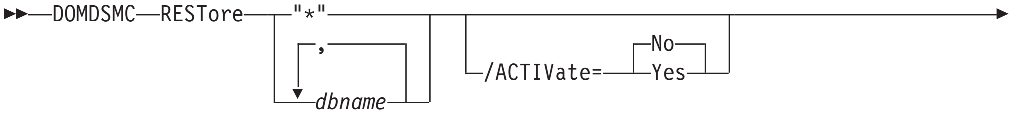
Purpose

Domdsmc restore restores a single database or a group of databases from Tivoli Storage Manager storage to the Domino server. If you are planning to apply transaction logs to the restored database or databases to get a more current state, then use the ***/activate**=no* parameter. This allows you to apply transaction logs once using the **activatedbs** command.

Note: If you receive the error message ACD5223E, you must check the permissions of the directory where the *<name of the Tivoli Storage Manager server>.pdb* file will be created.

The .pdb file is created according to the following rules:

1. If the DOMI_CONFIG environment variable is set, the .pdb file is created in the directory where the preferences file is located.
2. If the DOMI_DIR environment variable is set, the .pdb file is created in the directory specified by this environment variable.
3. The .pdb file is created in the default installation directory.



```
►─┬──────────────────────┬─┬──────────────────────────────────┬──────────────────►
  └─/ADSMNODe=──nodename─┘ │                  ┌─dsm.opt─────┐  │
                           └─/ADSMOPTFile=────┴─optionsfile─┴──┘

►─┬─────────────────────┬─┬─────────────────────────────────────────────────┬────►
  └─/ADSMPWD=──password─┘ │             ┌─3───────────┐   ┌─,1024───────┐  │
                          └─/BUFFers=───┴─numbuffers──┴───┴─,buffersize─┴──┘

►─┬────────────────────────────────────┬─┬──────────────────────┬────────────────►
  │                ┌─domdsm.cfg───┐    │ └─/INTO=──filename─────┘
  └─/CONFIGfile=───┴─cfgfilename──┴────┘

►─┬──────────────────────────────────┬─┬─────────────────────┬───────────────────►
  │             ┌─domdsm.log───┐     │ │               ┌─60─┐│
  └─/LOGFile=───┴─logfilename──┴─────┘ └─/LOGPRUne=────┼─n──┼┘
                                                       └─No─┘

►─┬─────────────────────────┬─┬───────────────────────────┬──────────────────────►
  │              ┌─Yes─┐    │ │         ┌─SHOWACtive─┐    │
  └─/MOUNTWait=──┴─No──┴────┘ └─/PICk=──┴─SHOWALl────┴────┘

►─┬───────────────────────────────────┬─┬──────────┬─┬────────────────────────┬──►
  │                 ┌─,00:00:00─┐     │ └─/Quiet───┘ │             ┌─Yes─┐    │
  └─/PIT=──date─────┴─,time─────┴─────┘              └─/REPlace=───┴─No──┴────┘

►─┬───────────────────────────────────┬─┬──────────────────────┬────────────────►◄
  │           ┌─currentserver─┐       │ │             ┌─No──┐  │
  └─/SERVer=──┴─servername────┴───────┘ └─/SUBDir=────┴─Yes─┴──┘
```

Parameters

"*" | *dbname,...,dbname*

Specifies the file path of a database or file path pattern for a group of databases. The file path pattern can represent a group of databases to be restored from the Tivoli Storage Manager server. The wildcard character asterisk (*) is used to specify a group of databases when used in the *dbname*. Multiple *dbnames* can be specified as long as they are separated with commas.

If you specify the wildcard character in the *dbname*, you must use double or single quotes, for example, "abc*" or 'abc*'.

The file path must be relative to the Notes data directory.

Symbolic links are referred to by their symbolic names. For example, if `mydata.dir` is a directory link in the Notes data directory that points to `/data`, database `mydb.nsf` in the `/data` directory would be named `mydata/mydb.nsf`. The physical file path for the relative name is resolved according to the symbolic values at the time of the restore.

If a symbolic link used in the name of a database backup image does not exist, the restore must be done using the ***/into*** parameter. This parameter specifies where the database should be placed.

The wildcard character (*) can be used in the file name portion of the file path. The wildcard character is not supported within directory names. The * is used to represent any number of any characters. For example, the following command restores the active backup of all databases beginning with the characters *ter*:

```
domdsmc restore "ter*"
```

For example, the following command lists all active database backups on the Tivoli Storage Manager server so that the desired ones can be selected for restore:

```
domdsmc restore "*" /pick
```

Note: The value of the **`/subdir`** parameter determines whether only the specified directory or all subdirectories are searched for databases that match the file pattern.

There is no default for **`dbname`**.

/ACTIVate=*No* **|** *Yes*
Specifies whether the databases being restored are to be brought online. If the restored database is to be rolled forward to a more current state by applying transaction logs, then ***/activate****=no* should be specified so that transaction logs can be applied with the **activatedbs** command.

Because there is a single transaction log for all logged databases, all databases should be activated together (in one command). This prevents the fetching of the same transaction logs multiple times from the Tivoli Storage Manager server. The databases can be restored separately (if necessary) by specifying ***/activate****=no*. Then the databases can be activated together with a single **activatedbs** command.

If the ***/activate*** parameter is not specified, ***/activate****=no* is the default value.

No	Do not activate the database. This is the default.
Yes	Activate the database.

/ADSMNODe=*nodename*
Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*
Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*
Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/BUFFers=*numbuffers***,***buffersize*

Specifies the number and size of data buffers that transfer data between the Domino server and the Tivoli Storage Manager API. Increasing the number or size (or both) of the data buffers can improve throughput.

You can specify from 2 to 8 buffers, the default value is *3*. The size of the buffers can be from 64 to 8192 kilobytes, the default value is *1024*.

If the ***/buffers*** parameter is not specified on the command line or defined in the preferences file, Data Protection for Domino uses the default values.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/INTO=*filepath*

Specifies the file path and file name to be used for the restored database. The file path specified must be relative to the Notes data directory or can be a fully qualified physical path. If a relative file path is specified, symbolic names can be included as long as the symbolic links exist to resolve the names. The specified path is considered a physical file path if it begins with a directory delimiter. A leading directory delimiter indicates a physical file path.

If multiple databases are being restored at once, the file name must be specified as a pattern with a single equal sign, **=**, represents the entire file name and extension of the database backup. For example, the following command restores all backups from the **vola** directory into the **tempvol** directory using the same file names:

```
domdsmc restore "vola/*" /into=tempvol/=
```

For example, the following command restores all backups from the **vola** directory into the **vola** directory using the file names from the backup version prefixed with a **t**:

```
domdsmc restore "vola/*" /into=vola/t=
```

If you entered **domdsmc restore "vola/*" /into=vola/=xyz /activate=yes**, **xyz** is appended to the database suffix. For example, a database called **abc.nsf** is restored as **abc.nsfxyz**.

If you perform a restore without doing an **activatedbs**, **.dad** is appended to the suffix of the database name. When you perform an **activatedbs** from the command line, the **.dad** append is removed from the suffix of the database name.

If multiple databases in a subdirectory branch are being restored and you need to preserve the directory structure, the file name must be specified as a pattern with two equal signs, **==**, representing the filepath of the database backup. For example, the following command restores all backups from the **vola** directory and its subdirectories into the **tempvol** directory using the same file names and directory structure. The **==** is replaced by the full relative path for each database file restored, including the **vola** directory:

```
domdsmc restore "vola/*" /subdir=yes /into=tempvol/==
```

Note:

- When the **/into** parameter is used on the **restore** command, replication will be disabled for the restored database(s).
- If the **/into** parameter is not used, replication settings will remain as they were in the backup version that is restored.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* | *n* | *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/MOUNTWait=*Yes* | *No*

If the Tivoli Storage Manager server is configured to store transaction log backup data on removable media, then the Tivoli Storage Manager server can indicate to Data Protection for Domino that it is waiting for a required storage volume to be mounted. If this occurs, this option allows you to specify whether Data Protection for Domino waits for the media mount or stops the current operation. Removable media is media such as tapes.

You can specify:

Yes Wait for tape mounts. This is the default.

No Do not wait for tape mounts.

/PICk=*SHOWACtive* | *SHOWALl*

Displays a list of database backups matching the *dbname* pattern that can be selected for restore. The pick list is displayed as a scrollable list from which you can select the database backups for restore.

You can specify:

SHOWACtive

Displays a list of active database backup versions. This is the default.

SHOWALl

Displays a list of both active and inactive database backup versions. This shows all the backup versions that match the *dbname* pattern.

/PIT=*currentdate,currenttime* | *date,time*

Specifies a point in time when the specified databases are restored. The *date* and *time* values must be specified in the same date and time format defined in the Data Protection for Domino preferences file. The most recent database backup images taken before the specified point in time are restored. Deleted backup images are not restored. Logged databases can then be rolled forward to that point by specifying the same date and time values on the ***/applylogs*** option of the **activatedbs** command.

date Specify a date string in the active date format. If you do not specify a date, the specified databases are restored unless the ***/pick*** parameter was used to select inactive backup versions.

The date must be specified using the same date format defined in the Data Protection for Domino preferences file. See “Domdsmc Set” on page 123 for a list of available date formats.

time Specify a time string in the active time format. If you specify a date without the time, HH:MM:SS on a 24-hour clock is used.

The time must be specified using the same time format defined in the Data Protection for Domino preferences file. See "Domdsmc Set" on page 123 for a list of available time formats.

Note: If this parameter is used with the ***/pick*** parameter, the *showactive* and *showall* variables for the ***/pick*** parameter are ignored. The pick list will contain the database backup images that meet the ***/pit*** criteria.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

/REPlace=*Yes***|***No*

Specifies whether to replace existing databases on the target machine.

You can specify:

Yes Allows an existing database on the target machine to be replaced during the restore process. This is the default.

No Prevents an existing database on the target machine from being overwritten during the restore process.

/SERVer=*currentserver***|***servername*

Specifies the Domino server name. If not specified, Data Protection for Domino uses the current Domino server.

/SUBDir=*No***|***Yes*

Specifies whether subdirectories within the specified file path are searched for databases that match the file pattern. If this option is not specified, Data Protection for Domino uses the value of the ***/subdir*** parameter in the Data Protection for Domino preferences file.

You can specify:

No Do not search the subdirectories within the specified file path for databases that match the file pattern. This is the default unless reset in the Data Protection for Domino preferences file.

Yes Search the subdirectories within the specified file path for databases that match the file pattern.

Examples

Example 1: This example restores all your databases and subdirectories.

```
domdsmc restore "*" /subdir=yes
```

Example 2: The following example restores a database to the specified date and time.

```
domdsmc restore datadir3/yyyy.nsf /subdir=yes /pit=01/11/2004,10:00:00
```

Output example:

```
Starting Domino database restore...

Initializing Domino connection...
Logging on to the Tivoli Storage Manager server, please wait...
Querying Tivoli Storage Manager server for a list of database backups, please wait...


Restoring database userlicenses.ntf, 1 of 1,
to /data/testdata1/notes1/notesdata/userlicenses.ntf.dad
Full: 0 Read: 663,552 Written: 663,552 Rate: 3,600.00 Kb/Sec
Restore of userlicenses.ntf completed successfully.


Total database backups inspected: 1
Total database backups requested for restore: 1
Total database backups restored: 1
Total database activated: 0

Throughput rate: 3,600.00 Kb/Sec
Total bytes transferred: 663,552
Total LanFree bytes transferred: 0
Elapsed processing time: 0.18 Secs
```

Example 3: The following example restores a database into the same directory but with a different name.

```
domdsmc restore a_dir/db1.nsf /into=a_dir/db8.nsf
```

Output example:

```
Starting Domino database restore...

Initializing Domino connection...
Logging on to the Tivoli Storage Manager server, please wait...
Querying Tivoli Storage Manager server for a list of database backups, please wa
it...


Restoring database a_dir/test.nsf, 1 of 1,
to /local/notesdata/a_dir/db8.nsf.dad

Full: 0 Read: 16,252,928 Written: 16,252,928 Rate: 10,666.67 Kb/Sec
Restore of a_dir/test.nsf completed successfully.


Total database backups inspected: 1
Total database backups requested for restore: 1
Total database backups restored: 1
Total database activated: 0

Throughput rate: 10,659.50 Kb/Sec
Total bytes transferred: 16,252,928
Total LanFree bytes transferred: 0
Elapsed processing time: 1.49 Secs
```

Domdsmc Restorelogarchive

This section describes how to use the **domdsmc restorelogarchive** command.

Purpose

Domdsmc restorelogarchive restores archived transaction logs from Tivoli Storage Manager storage to the Domino server. This command assists with disaster recovery operations. By retrieving the most recent archived log file, it is possible to rebuild the Domino transaction log control file. This allows archived transaction log files to be used to recover restored database backups to a more current state, even after a loss of the active transaction log.

When restoring a transaction log file from an old Logger ID during an alternate server or alternate partition restore procedure, you must specify the ***/pick*** parameter with the **restorelogarchive** command in order to choose the desired log extent. See “Alternate server and alternate partition restores for NSF databases” on page 177 for detailed information.

For more information on disaster recovery procedures, see “Recovery from loss of Domino transaction logs for NSF databases” on page 176.

```
                               ┌─lastarchivedlogfile─┐
►►──DOMDSMC──RESTORELOGArchive─┼─────────────────────┴──────────────────────────►
                               │ ┌─,───────┐         │
                               │ ▼         │         │
                               └──logname──┴─────────┘

►─┬──────────────────────┬──┬──────────────────────────────────┬─────────────────►
  └─/ADSMNODe=──nodename─┘  │                ┌─dsm.opt─────┐   │
                            └─/ADSMOPTFile=──┴─optionsfile─┴───┘

►─┬─────────────────────┬──┬──────────────────────────────────────────────┬──────►
  └─/ADSMPWD=──password─┘  │            ┌─3──────────┐  ┌─,1024───────┐  │
                           └─/BUFFers=──┴─numbuffers─┴──┴─,buffersize─┴──┘

►─┬───────────────────────────────────┬──┬──────────────────────────────────┬────►
  │               ┌─domdsm.cfg──┐     │  │             ┌─translogpath─┐     │
  └─/CONFIGfile=──┴─cfgfilename─┴─────┘  └─/INTOPath=──┴─pathname─────┴─────┘

►─┬───────────────────────────────┬──┬────────────────────────┬──────────────────►
  │            ┌─domdsm.log───┐   │  │              ┌─60─┐    │
  └─/LOGFile=──┴─logfilename──┴───┘  └─/LOGPRUne=───┼─n──┼────┘
                                                    └─No─┘

►─┬─────────────────────┬──┬──────────────────────────┬──┬─────────┬─────────────►
  │             ┌─Yes─┐ │  │          ┌─SHOWACtive─┐  │  └─/Quiet──┘
  └─/MOUNTWait=─┴─No──┴─┘  └─/PICk=───┴─SHOWALl────┴──┘
```

```
►──┬──────────────────────┬──┬──────────────────────────────────┬──────────────────►◄
   │            ┌─Yes─┐   │  │            ┌─currentserver─┐     │
   └─/REPlace=──┴─No──┴───┘  └─/SERVer=───┴─servername────┴─────┘
```

Parameters

logname,...,logname
The *logname* variable is an optional parameter that specifies the logname of the archived transaction log to be restored. Multiple *lognames* can be specified as long as they are separated with commas. Use the wildcard character (*) to specify a group of files when used in *logname*. Make sure the wildcard character (*) is enclosed in single or double quotes (for example, "abc*" or 'abc*').

When a logname is not specified with the **restorelogarchive** command, the last transaction log archived to the Tivoli Storage Manager server (that is still active on the Tivoli Storage Manager server) is restored. The *lastarchivedlogfile* variable shown in the syntax diagram represents the default behavior and is not a keyword that can be specified on the command line.

To restore an inactive transaction log file from the Tivoli Storage Manager server, use the ***/pick***=*showall* parameter and select the desired file from the list.

/ADSMNODe=*nodename*
Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*
Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*
Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/BUFFers=*numbuffers****,****buffersize*

Specifies the number and size of data buffers that transfer data between the Domino server and the Tivoli Storage Manager API. Increasing the number or size (or both) of the data buffers can improve throughput.

You can specify from 2 to 8 buffers, the default value is *3*. The size of the buffers can be from 64 to 8192 kilobytes, the default value is *1024*.

If the ***/buffers*** parameter is not specified on the command line or defined in the preferences file, Data Protection for Domino uses the default values.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/INTOPath=*translogpath* **|** *pathname*

Specifies the file path used for the restored transaction log(s). The file path must be a fully qualified physical path. The *translogpath* variable shown in the syntax diagram represents the default location of the Domino server transaction log files and is not a keyword that can be specified on the command line. The default location of the Domino server transaction log files is defined by the TRANSLOG_Path variable in the notes.ini file.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* | *n* | *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/MOUNTWait=*Yes* | *No*

If the Tivoli Storage Manager server is configured to store transaction log backup data on removable media, then the Tivoli Storage Manager server can indicate to Data Protection for Domino that it is waiting for a required storage volume to be mounted. If this occurs, this option allows you to specify whether Data Protection for Domino waits for the media mount or stops the current operation. Removable media is media such as tapes.

You can specify:

Yes Wait for tape mounts. This is the default.

No Do not wait for tape mounts.

/PICk=*SHOWACtive* | *SHOWALl*

Displays a list of transaction log backups matching the *logname* pattern that can be selected for restore. The pick list is displayed as a scrollable list from which you can select the transaction log backups for restore.

You can specify:

SHOWACtive

Displays a list of active transaction log backup versions. This is the default.

SHOWALl

Displays a list of both active and inactive transaction log backup versions. This shows all the backup versions that match the *logname* pattern.

Note: When restoring a transaction log file from an old Logger ID during an alternate server or alternate partition restore procedure, you must specify the ***/pick*** parameter with the **restorelogarchive** command in order to choose the desired log extent. See "Alternate server and alternate partition restores for NSF databases" on page 177 for detailed information.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

/REPlace=*Yes*|*No*

Specifies whether to replace existing log files on the target machine. This parameter overrides the ***replace*** value in the preferences file.

If the target path name for a log file to be restored already exists, you can specify:

Yes A *Yes* value activates the restore procedure and replaces the existing log file on the target machine. This is the default.

No A *No* value will not allow the existing log file to be replaced so the restore of that log file will be skipped.

/SERVer=*currentserver*|*servername*

Specifies the Domino server name. If not specified, Data Protection for Domino uses the current Domino server.

Example

The following example restores the last transaction log archived to the Tivoli Storage Manager server.

```
domdsmc restorelogarchive /intopath=/testdata1/notes1/newlogdir
```

Output Example:

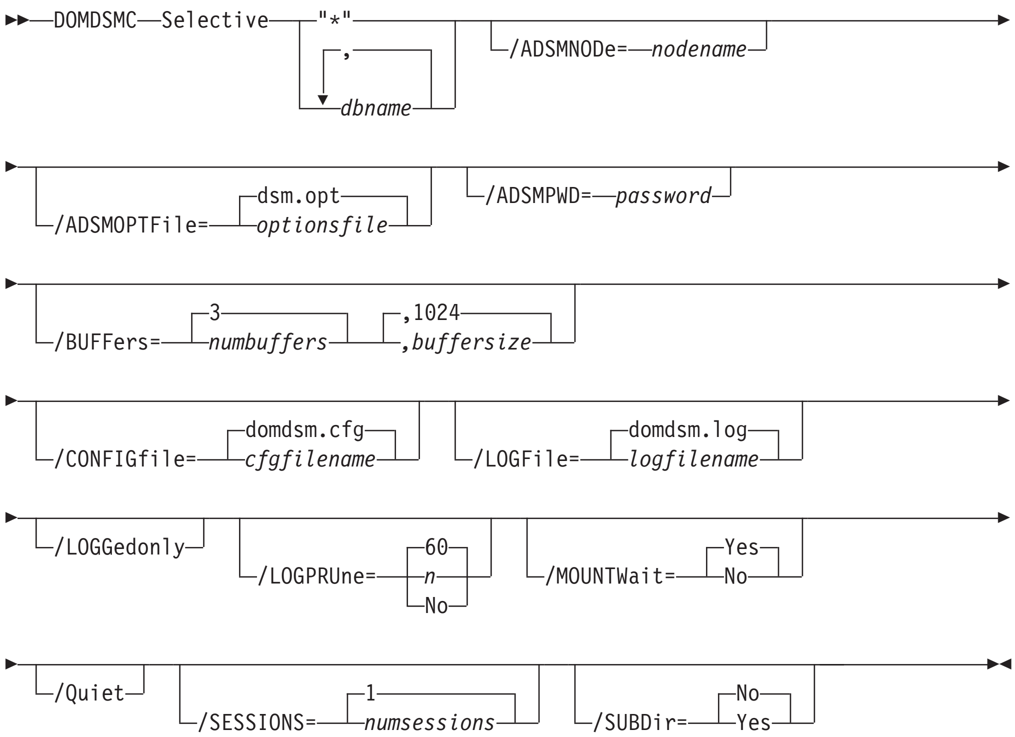
```
Starting transaction log file restore...

Initializing Domino connection...
Logging on to the Tivoli Storage Manager server, please wait...
Querying Tivoli Storage Manager server for a list of transaction log file archives,
please wait...


Restoring transaction log file S0000005.TXN
to /testdata1/notes1/newlogdir/S0000005.TXN
Full: 0 Read: 67,109,888 Written: 67,109,888 Rate: 10,353.40 Kb/Sec
Restore of S0000005.TXN completed successfully.


Total transaction log file archives inspected:                    2
Total transaction log file archives requested for restore:        1
Total transaction log file archives restored:                     1

Throughput rate:                                          10,351.76 Kb/Sec
Total bytes transferred:                                 67,109,888
Total LanFree bytes transferred:                                  0
Elapsed processing time:                                       6.33 Secs
```

Domdsmc Selective

How to use the **`domdsmc selective`** command.

Purpose

`Domdsmc selective` backs up the databases you specify. You can exclude databases from backup with the exclude statement in the include-exclude options file. This command does not do comparisons of attributes with the active backup images as does the incremental command. It simply backs up all databases that match the *dbname* pattern and passes the include-exclude filter.



Parameters

"*" | *dbname,dbname,...*

Specifies the file path of a database or file path pattern for a group of databases. The file path pattern can represent a group of databases to be restored from the Tivoli Storage Manager server. The wildcard character asterisk (*) is used to specify a group of databases when used in the *dbname*. Multiple *dbnames* can be specified as long as they are separated with commas.

If you specify the wildcard character in the *dbname*, you must use double or single quotes, for example, "abc*" or 'abc*'.

The file path must be relative to the Notes data directory.

Symbolic links are referred to by their symbolic names. To reference a database in a directory pointed to by a directory link in the data path, use the directory link name as the directory name. For example, if database `xyz.nsf` is in a directory, pointed to by the link `vol1.dir`, refer to it as `vol1/xyz.nsf`. If a symbolic directory link is created with the same name as a physical directory in the Notes data path, only the physical directory is searched.

The wildcard character (*) is used to represent any number of any characters when used in the file name portion of the file path. The wildcard character is not supported within directory names. The following example backs up all databases within the dir_A directory beginning with the characters *ter*:

```
domdsmc selective "dir_A/ter*"
```

The following example backs up all databases on the server:

```
domdsmc selective "*" /subdir=yes
```

The following example backs up all databases whose file name ends in *acct*:

```
domdsmc selective "*acct.n*" /subdir=yes
```

Note: Standard include and exclude processing applies to Domino database names. Wildcards can be used on the backup command, and specific databases can be excluded from the backup with the include-exclude list in the Tivoli Storage Manager include-exclude options file. For example, to exclude all databases on a volume pointed to by the symbolic directory link temp.dir, use the following statement:

```
exclude /temp/*
```

Note that the exclude statement refers to the relative file name including symbolics and not the physical file path. For additional information on include and exclude options, see "Include and exclude processing" on page 182 and *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide*.

/ADSMNODe=*nodename*

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/BUFFers=*numbuffers***,***buffersize*
Specifies the number and size of data buffers that transfer data between the Domino server and the Tivoli Storage Manager API. Increasing the number or size (or both) of the data buffers can improve throughput.

You can specify from 2 to 8 buffers, the default value is *3*. The size of the buffers can be from 64 to 8192 kilobytes, the default value is *1024*.

If the ***/buffers*** parameter is not specified on the command line or defined in the preferences file, Data Protection for Domino uses the default values.

/CONFIGfile=*cfgfilename*
Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*
Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGGedonly
Specifies that only logged databases matching the *dbname* pattern should be backed up. This option is used to force periodic refreshes of the backup

for logged databases. Without this refresh these databases are not backed up by the Incremental command on a Domino server when archival logging is in effect.

/LOGPRUne=*60* **|** *n* **|** *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/MOUNTWait=*Yes* **|** *No*

If the Tivoli Storage Manager server is configured to store transaction log backup data on removable media, then the Tivoli Storage Manager server can indicate to Data Protection for Domino that it is waiting for a required storage volume to be mounted. If this occurs, this option allows you to specify whether Data Protection for Domino waits for the media mount or stops the current operation. Removable media is media such as tapes.

You can specify:

Yes Wait for tape mounts. This is the default.

No Do not wait for tape mounts.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

/SESSions=*numsessions* **| 1**

Specifies the number of Tivoli Storage Manager server sessions to be used by Data Protection for Domino. You can specify from *1* to *64* sessions. The default value is *1*.

/SUBDir=*No* **|** *Yes*

Specifies whether subdirectories within the specified file path are searched for databases that match the file pattern. If this option is not specified, Data Protection for Domino uses the value of the ***/subdir*** parameter in the Data Protection for Domino preferences file.

You can specify:

No Do not search the subdirectories within the specified file path for databases that match the file pattern. This is the default unless reset in the Data Protection for Domino preferences file.

Yes Search the subdirectories within the specified file path for databases that match the file pattern.

Examples

Example 1: The following example backs up all databases contained in the `a_dir` directory and its subdirectories:

```
domdsmc selective "a_dir/*" /subdir=yes
```

Output example:

```
Starting Domino database backup...
Initializing Domino connection...
Querying Domino for a list of databases, please wait...

Backing up database a_dir/b_dir/clienttest2.nsf, 1 of 4.
Full: 0  Read: 41,418,752  Written: 41,418,752  Rate: 25,327.49 Kb/Sec
Backup of a_dir/b_dir/clienttest2.nsf completed successfully.

Backing up database a_dir/clienttest.nsf, 2 of 4.
Full: 0  Read: 41,418,752  Written: 41,418,752  Rate: 30,140.09 Kb/Sec
Backup of a_dir/clienttest.nsf completed successfully.

Backing up database a_dir/test.nsf, 3 of 4.
Full: 0  Read: 16,252,928  Written: 16,252,928  Rate: 26,765.60 Kb/Sec
Backup of a_dir/test.nsf completed successfully.

Backing up database a_dir/testdb2.nsf, 4 of 4.
Full: 0  Read: 29,622,272  Written: 29,622,272  Rate: 27,682.30 Kb/Sec
Backup of a_dir/testdb2.nsf completed successfully.


Total Domino databases inspected:      4
Total Domino databases backed up:      4
Total Domino databases excluded:       0
Total Domino databases deduplicated:     0

Throughput rate:              26,852.38 Kb/Sec
Total bytes inspected:           128,712,704
Total bytes transferred:          128,712,704
Total LanFree bytes transferred:       0
Total bytes before deduplication:      0
Total bytes after deduplication:       0
Data compressed by:            0%
Deduplication reduction:          0.00%
Total data reduction ratio:         0.00%
Elapsed processing time:          4.68 Secs
```

Example 2: The following example backs up all databases by including subdirectories:

```
domdsmc selective "*" /subdir=yes
```

Domdsmc Set

How to use the **domdsmc set** command.

Purpose

Domdsmc set sets the configuration options and values in the Data Protection for Domino preferences file. The value saved in the preferences file is used as the default value when a parameter is not specified on a command invocation that permits the use of the parameter.

```
►►──DOMDSMC──SET──parmname──=──value──┬─────────────────────────────────────┬──────────►◄
                                      │                ┌─domdsm.cfg───┐     │
                                      └─/CONFIGfile=───┴─cfgfilename──┴─────┘
```

Parameters

parmname=value

Specifies the parameter and value to save in the preferences file. You can only set one value per **domdsmc set** command run.

The ***parmname***=***value*** is one of the following:

ADSMLOGDir=*directory path*

Specify the full path name to where the Tivoli Storage Manager API error log file (dsierror.log) will be stored. The default directory is the Data Protection for Domino install directory. You should specify ***adsmlogdir*** in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI. This option functions in the same manner as the DSMI_LOG environment variable.

ADSMOPTFile=*optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

BUFFers=*numbuffers*

Specifies the number of data buffers that are used for moving data between the Domino server and the Tivoli Storage Manager API. Separate, asynchronous execution threads are used by Data Protection for Domino for communicating with the Domino server and the Tivoli Storage Manager API. Increasing the number or size (or both) of the data buffers can reduce the possibility of one thread having to wait for another thread. This can improve throughput.

You can specify from 2 to 8 buffers. The default is *3*.

BUFFERSIze=*size*
Specifies the size of the buffers. The size can be from 64 to 8192 kilobytes. The default is *1024*.

COMMRESTARTDURATION =*number*
Specifies the total number of minutes that the server will continue trying to restart a session. The valid range is from 1 to 9999 and the default is *60*.

COMMRESTARTINTERVAL=*number*
Specifies the number of seconds the server will wait between attempts to restart a session. The valid range is from 1 to 9999 and the default is *15*.

DATEformat=*formatnumber*
Specifies the format you want to use to display dates.

The default value depends on the language format.

The *formatnumber* variable displays the date in one of the formats listed below. Select the format number that corresponds to the format you want to use.

0	The format is the locale-specified format.
1	The format is MM/DD/YYYY.
2	The format is DD–MM–YYYY.
3	The format is YYYY–MM–DD.
4	The format is DD.MM.YYYY.
5	The format is YYYY.MM.DD.

Changes to the value of the **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file (tdpdom.log by default). You can avoid losing existing log file data by performing one of the following:

- After changing the value of the **dateformat** parameter, make a copy of the existing log file before running Data Protection for Domino.
- Specify a new log file with the **/logfile** parameter.

DB2ALtdbname=*name of alternate database*
Specifies the name of the alternate DB2 database. The default value is DOM_ALT.

DB2CONTainerpath=*directory path*
Specifies the default path for table space containers used on DB2 redirected restores. Redirected DB2 restores are selected automatically by Data Protection for Domino when performing an alternate DB2 database restore. If this option is not specified, the target path for the table space container is defined relative to the value of the ***db2restoreintopath*** option.

Attention: ***db2containerpath*** is required when the DB2DIRECTORY option is specified in the Domino server notes.ini file. Otherwise the restore will fail. That is because DB2 attempts to place the alternate DB2 database data in the directory specified by the DB2DIRECTORY option, which is already used by the Domino DB2 database.

DB2LOGPath=*directory path*
Specifies the absolute path name of a directory that will be used for active log files after a restore operation.

DB2LOGTarget=*directory path*
Specifies the location for the logs from the backup image during an inplace restore operation.

DB2REPlace=*Yes***|***No*
Specifies whether to replace the existing alternate DB2 database when performing a restore. This parameter defines the default behavior if the ***db2replace*** parameter is not specified during the **db2restore** command. The default value is *Yes*.

DB2RESTIntopath=*directory*
Specifies the target DB2 database directory when restoring to an alternate DB2 database. The specified drive and directory must be local. The default is the value of the DB2 instance default database path configuration option.

DB2SESSions=*number*
Specifies the number of sessions to be created between DB2 and the Tivoli Storage Manager server. This parameter is used by the Tivoli Storage Manager DB2 agent to back up DB2 data. You can specify from *1* to *64* sessions. The default is *1* session.

DB2USER=*user name*
Specifies the DB2 user name.

DOMI_DIR=*directory path*
Points to the directory where Data Protection for Domino is installed

DOMINstallpath=*directory path*
Specifies the full installation path of the Domino server. It must be specified in the Data Protection for Domino preferences file (domdsm.cfg) in order to access the Web client GUI. The value must be the server installation directory for the corresponding notes.ini file specified by the ***notesinipath*** option. Note that this option cannot be specified on the command line.

DOMTXNBYTElimit=*number*
Specifies the number of bytes sent between Data Protection for Domino and the Tivoli Storage Manager server in a single transaction. The default value is 0 (which indicates no limit) and the maximum value is 2097152. This number is multiplied by 1024 to calculate the limit in bytes. This parameter is useful when backing up NSF databases to tape storage for these reasons:

- Processing for each transaction causes the tape to stop and start. Considerable time can be lost during this stop and start when using high speed tapes. This is particularly true in a LAN free environment.

- Errors that occur during backup processing are automatically retried once when ***domtxnbytelimit*** is set.
- When a failure occurs during a backup, all of the backups in the transaction are retried, not just the NSF database in error. Each backup is retried in a separate transaction. After all backups are retried, the ***domtxnbytelimit*** parameter is used to control the number of bytes per transaction.

Considering that the overhead of stopping and starting tape storage for large NSF databases is small when compared to the data transfer time, the ***domtxnbytelimit*** parameter allows you to adjust the behavior for large database backups.

DOMTXNGROUPmax=*number*

Specifies the number of individual objects sent to the Tivoli Storage Manager server in a single transaction. Note that two objects are sent to the Tivoli Storage Manager server for each database backup. The default value of 2 specifies that there is one database per transaction and that each database is stored as two objects on the Tivoli Storage Manager server. The maximum value is 65000. This parameter can be overridden by the Tivoli Storage Manager server TXNGRPMAX option. However, when ***domtxngroupmax*** is set, the minimum of the two values is used. This parameter is useful when backing up NSF databases to tape storage for these reasons:

- Processing for each transaction causes the tape to stop and start. Considerable time can be lost during this stop and start when using high speed tapes. This is particularly true in a LAN free environment.
- Errors that occur during backup processing are automatically retried once when ***domtxngroupmax*** is set.
- When a failure occurs during a backup, all of the backups in the transaction are retried, not just the NSF database in error. Each backup is retried in a separate transaction. After all backups are retried, the ***domtxngroupmax*** parameter is used to control the number of individual objects per transaction.

The ***domtxngroupmax*** parameter should be used when backing up small NSF databases.

LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. If there are spaces in the name, then the name must be enclosed in double quotes (for example, "log file".) The file name can include a fully-qualified path. However, if you do not specify a path, the file is written to the current working directory. If your current working directory is read-only, the commands that you issue will fail. The default log file is `domdsm.log`.

LOGPRUne=*60***|***n***|***No*

Specifies whether to disable or request log pruning. By default, log pruning is enabled and performed once per day. You can specify the ***logprune*** parameter to do the following:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

When the value of ***logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999.

No Do not prune the log.

MOUNTWait=*Yes* | *No*

If the Tivoli Storage Manager server is configured to store transaction log backup data on removable media, then the Tivoli Storage Manager server can indicate to Data Protection for Domino that it is waiting for a required storage volume to be mounted. If this occurs, this option allows you to specify whether Data Protection for Domino waits for the media mount or stops the current operation. Removable media is media such as tapes.

You can specify:

Yes Wait for tape mounts. This is the default.

No Do not wait for tape mounts.

NOTESInipath=*dirpath*

Specifies the directory path where the notes.ini file resides for the target Domino server. In a multiple Domino server partition environment, the ***notesinipath*** parameter MUST be specified for each partition in order to identify the Domino server for Data Protection for Domino.

When specified for a non-partitioned Domino server, the Domino path setting in the registry takes precedence over this value.

NUMberformat=*fmtnum*

The ***numberformat*** parameter specifies the format you want to use to display numbers.

The default value depends on the language format.

The *fmtnum* variable displays numbers by using one of the formats listed below. Select the format number that corresponds to the format you want to use.

0 The format is the locale-specified format.

1 The format is *n,nnn.dd*.

2 The format is *n,nnn,dd*.

3 The format is *n nnn,dd*.

4 The format is *n nnn.dd*.

5 The format is *n.nnn,dd*.

6 The format is *n'nnn,dd*.

REPlace=*Yes* | *No*

Specifies whether to replace existing databases (or log files) on the target machine when performing a restore. This parameter defines the default behavior if the ***/replace*** parameter is not specified on the restore command.

If the target path name for a database (or log file) to be restored already exists, you can specify:

Yes A *Yes* value activates the restore procedure and replaces the existing database (or log file) on the target machine. This is the default.

No A *No* value will not allow the existing database (or log file) to be replaced so the restore of that database (or log file) will be skipped.

SESSions=*number*

Specifies the number of sessions to open to the Tivoli Storage Manager server. This option applies to NSF database backups only. You can specify from *1* to *64* sessions. The default value is *1*.

STATistics=*No* | *Yes*

Specifies whether to log backup and restore performance statistics about an individual database at the backup or restore level. Statistics are logged to the Data Protection for Domino log file (domdsm.log by default). These statistics contain information such as the database read/write time and transfer rate, the send/receive time and transfer rate, and the Domino server data transfer time and transfer rate. This information can assist in tuning Data Protection for Domino for optimal performance.

You can specify:

No A *No* value will not log backup and restore performance statistics about an individual database. This is the default.

Yes A *Yes* value will log backup and restore performance statistics about an individual database.

SUBDir=*No* | *Yes*

Specifies whether subdirectories within the specified file path are searched for databases that match the file pattern.

You can specify:

No Do not search the subdirectories within the specified file path for databases that match the file pattern. This is the default unless reset in the Data Protection for Domino preferences file.

Yes Search the subdirectories within the specified file path for databases that match the file pattern.

TIMEformat=*formatnumber*

Specifies the format in which you want system time displayed.

The default value depends on the language format.

The *formatnumber* variable displays time in one of the formats that are listed below. Select the format number that corresponds to the format you want to use.

0 The format is the locale-specified format.

1 The format is HH:MM:SS.

2	The format is HH,MM,SS.
3	The format is HH.MM.SS.
4	The format is HH:MM:SSA/P.

Changes to the value of the **timeformat** parameter can result in an undesired pruning of the log file (tdpdom.log by default). You can avoid losing existing log file data by performing one of the following:

- After changing the value of the **timeformat** parameter, make a copy of the existing log file before running Data Protection for Domino.
- Specify a new log file with the **/logfile** parameter.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

Example

Example: The following example sets the number of buffers to 8.

```
domdsmc set buffers=8
```

Output example:

```
ACD5217I The preference has been set successfully.
```

DB2 Commands

This section describes how to use the Data Protection for Domino command line interface with Domino DB2 enabled Notes databases.

Important: If you are using DB2 Server 9.1.2 on an AIX or Linux x86 machine, the AIX LIBPATH or Linux LD_LIBRARY_PATH environment variable must be set to include the DB2 instance directory (`sqllib/lib32`) before running any Data Protection for Domino DB2 commands. These examples display the correct setting with DB2 instance name *db2inst1*:

```
LIBPATH=/usr/lib:/lib:/home/db2inst1/sqllib/lib32
```

or

```
LD_LIBRARY_PATH=/usr/lib:/lib:/home/db2inst1/sqllib/lib32
```

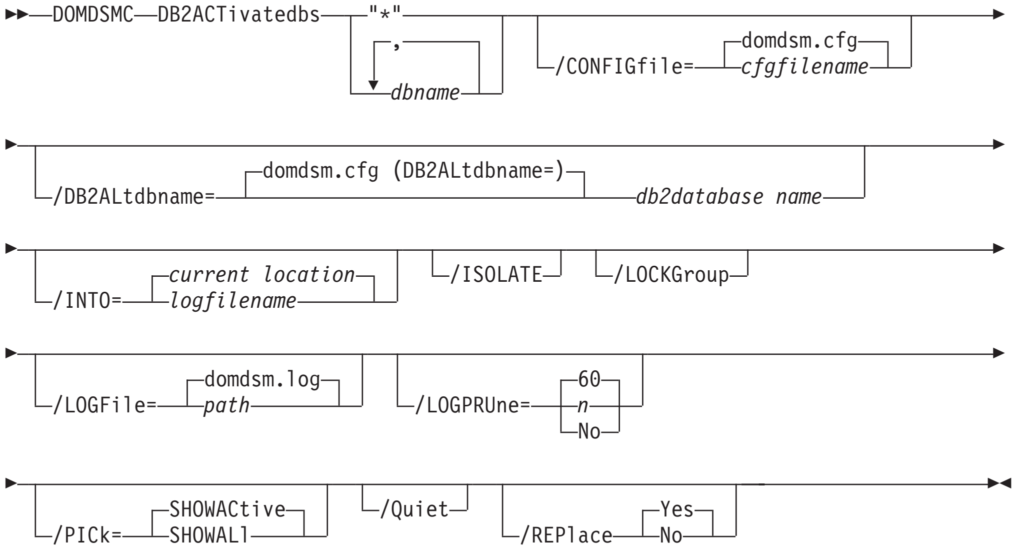
Domdsmc DB2activatedbs

This section describes how to use the **domdsmc db2activatedbs** command.

Purpose

Domdsmc db2activatedbs activates DB2 enabled Notes databases that have been restored to an alternate database. This command copies the specified DB2 enabled Notes database into the Domino DB2 database and brings the database online. Note that when a list of database is activated and the ***/isolate*** parameter is specified, each DB2 enabled Notes database is activated to a new DB2 Group.

Note that the DB2 enabled Notes databases located in the alternate DB2 database are available for restore as long the alternate DB2 database is available. The alternate DB2 database is considered available when it is not manually deleted through DB2 server interface, overwritten by another restore operation, or removed from the list of DB2 databases (that contain DB2 enabled Notes databases) available for activation. See the “Domdsmc DB2deletealternate” on page 135 command for information about how to remove a database from the activation list.



Parameters

"*" | *dbname,dbname,...*

Specifies the DB2 enabled Notes databases to activate. The DB2 enabled Notes databases are activated into the current DB2 Group.

If you specify the wildcard character in the *dbname*, you must use double or single quotes, for example, "abc*" or 'abc*'.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/DB2ALtdbname=*database name*

Specify the name of the alternate DB2 database to use for activation. If the ***/db2altdbname*** parameter is not specified, the value of the ***db2altdbname*** configuration option (defined in the Data Protection for Domino domdsm.cfg preferences file) is used. If ***db2altdbname*** is not defined in the preferences file, the alternate database name DOM_ALT is used.

/INTO=path

Specify the target path (relative to the Domino Data directory) where the DB2 enabled Notes database is activated. If the ***/into*** parameter is not specified, the DB2 enabled Notes database is activated in the same location. The ***/into*** parameter special characters "=" and "==" operate in the same manner as in the **domdsmc restore** command.

/ISOLATE

Specify this parameter to activate the database into a new DB2 Group.

/LOCKGroup

Specify whether to lock the DB2 Group after the DB2 enabled Notes database is activated.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60***|***n***|***No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of

values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/PICk=*SHOWACtive***|***SHOWALl*

Displays a list of database backups matching the *dbname* pattern that can be selected for restore. The pick list is displayed as a scrollable list from which you can select the database backups for restore.

You can specify:

SHOWACtive

Displays a list of active database backup versions. This is the default.

SHOWALl

Displays a list of both active and inactive database backup versions. This shows all the backup versions that match the *dbname* pattern.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

/REPlace=*Yes***|***No*

Specify whether to replace the existing DB2 enabled Notes database.

Example

The following example displays a list of DB2 enabled Notes databases that are ready to activate from specified alternate DB2 database:

```
domdsmc db2activatedbs "*" /pick=showall
```

Output example:

```
 #       Backup Time Stamp            Size   DB2 DB   GROUP  NSFDB2 Database
      ----------------------------------------------------------------------
    1. | 01/19/2008 13:55:33         0.00B  DOM_ALT  GRP1   db2nsf1.nsf
    2. | 01/19/2008 13:55:33         0.00B  DOM_ALT  GRP1   db2nsf2.nsf
    2. | 01/19/2008 13:55:33         0.00B  DOM_ALT  GRP1   db2nsf3.nsf
    3. | 01/20/2008 13:55:33         0.00B  DOMFULL1 GRP1   db2nsf1.nsf
    4. | 01/20/2008 13:55:33         0.00B  DOMFULL1 GRP1   db2nsf2.nsf
    4. | 01/20/2008 13:55:33         0.00B  DOMFULL1 GRP1   db2nsf3.nsf
    4. | 01/20/2008 13:55:33         0.00B  DOMFULL1 GRP2   db2nsf4.nsf
    4. | 01/20/2008 13:55:33         0.00B  DOMFULL1 GRP2   db2nsf5.nsf
    4. | 01/20/2008 13:55:33         0.00B  DOMFULL1 GRP2   db2nsf6.nsf
       |
       |
       |
       |
       |
       |
       |
       |
       0---------10--------20--------30--------40--------50--------60--------7
<U>=Up  <D>=Down  <T>=Top  <B>=Bottom  <R>=Right  <L>=Left <G#>=Goto Line #
<#>=Toggle Entry  <+>=Select All  <->=Deselect All <#:#+>=Select A Range
<#:#->=Deselect A Range  <O>=Ok  <C>=Cancel
```

Domdsmc DB2archivelog

This section describes how to use the **domdsmc db2archivelog** command.

Purpose

Domdsmc db2archivelog archives the Domino DB2 database log files. Although DB2 automatically archives the log file, it is possible to force an archive of the log so that the latest transactions are available when the alternate database is rolled forward.

An archive copy croup is required to archive the Domino DB2 database log file. If an archive copy group is not defined on the target management class, the **db2archivelog** command completes successfully but the log is not archived to the Tivoli Storage Manager server. The logs are archived to the path specified by the Domino DB2 database configuration option, FAILARCHPATH.

```
►►──DOMDSMC──DB2ARCHivelog──┬──────────────────────────────────┬──────────►
                            │              ┌─domdsm.cfg───┐    │
                            └─/CONFIGfile=─┴─cfgfilename──┴────┘

►──┬──────────────────────────────┬──┬───────────────────────┬──┬─────────┬──►◄
   │            ┌─domdsm.log───┐  │  │              ┌─60─┐   │  └─/Quiet──┘
   └─/LOGFile=──┴─logfilename──┴──┘  └─/LOGPRUne=───┼─n──┼───┘
                                                    └─No─┘
```

Parameters

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* | *n* | *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

Example

The following example archives the DB2 transaction log file:

```
domdsmc db2archivelog
```

Output example:

```
Starting Domino DB2 database transaction log archive...
Initializing Domino connection...
Initializing DB2 connection...

Archiving Domino DB2 transaction logs

Domino DB2 transaction log archive completed successfully.
```

Domdsmc DB2deletealternate

This section describes how to use the **domdsmc db2deletealternate** command.

Purpose

Domdsmc db2deletealternate deletes the specified alternate DB2 database from the pending DB2 file.

```
►►──DOMDSMC──DB2DELetealternate──database name──────────────────────────────►

►──┬─────────────────────────────────┬──┬──────────────────────────────┬────►
   │                 ┌─domdsm.cfg──┐ │  │              ┌─domdsm.log──┐ │
   └─/CONFIGfile=────┴─cfgfilename─┴─┘  └─/LOGFile=────┴─logfilename─┴─┘

►──┬────────────────────────┬───────────────────────────────────────────────►◄
   │              ┌─60─┐    │
   └─/LOGPRUne=───┼─n──┼────┘
                  └─No─┘
```

Parameters

dbname
: Specifies the alternate DB2 database to deleted. If not specified, the default alternate DB2 database (DB2ALTDBNAME) is used.

/CONFIGfile=*cfgfilename*
: Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

  You can also specify the preferences file using the DOMI_CONFIG environment variable.

  The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*
: Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file

name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60***|***n***|***No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

Example

The following example deletes the alternate DB2 database:

```
domdsmc db2deletealternate
```

Output example:

```
Starting Domino DB2 database transaction log archive...
Initializing Domino connection...
Initializing DB2 connection...

Archiving Domino DB2 transaction logs

Domino DB2 transaction log archive completed successfully.
```

Domdsmc Fullselective

The **Domdsmc fullselective** command is a method of backing up both NSF and DB2 enabled Notes databases.

Purpose

Domdsmc fullselective first backs up all of the Domino NSF databases and then performs a full back up of the Domino DB2 database in order to back up all of the DB2 enabled Notes databases. It differs from the `selective` command, which backs up NSF databases only. For non DB2 enabled servers, use the `selective` command.

```
►►──DOMDSMC──FULLSelective──┬─────────────────────┬──────────────────────────►
                            └─/ADSMNODe=──nodename─┘

►──┬─────────────────────────────────────┬──┬────────────────────────┬────────►
   │                 ┌─dsm.opt─────┐     │  └─/ADSMPWD=──password─┘
   └─/ADSMOPTFile=───┴─optionsfile─┴─────┘

►──┬──────────────────────────────────────────────────┬──────────────────────►
   │            ┌─3──────────┐   ┌─,1024───────┐      │
   └─/BUFFers=──┴─numbuffers─┴───┴─,buffersize─┴──────┘

►──┬────────────────────────────────────┬──┬──────────────────────────────────┬──►
   │                ┌─domdsm.cfg──┐     │  │                 ┌─1───────────┐  │
   └─/CONFIGfile=───┴─cfgfilename─┴─────┘  └─/DB2SESSIONS=───┴─numsessions─┴──┘

►──┬───────────────────────────────┬──┬──────────────────────┬────────────────►
   │            ┌─domdsm.log───┐   │  │              ┌─60─┐  │
   └─/LOGFile=──┴─logfilename──┴───┘  └─/LOGPRUne=───┼─n──┼──┘
                                                     └─No─┘

►──┬───────────────────────┬──┬─────────┬──┬──────────────────────────────┬────►◄
   │              ┌─Yes─┐  │  └─/Quiet──┘  │              ┌─1───────────┐  │
   └─/MOUNTWait=──┴─No──┴──┘               └─/SESSIONS=───┴─numsessions─┴──┘
```

Parameters

/ADSMNODe=*nodename*

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.

- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/BUFFers=*numbuffers,buffersize*

Specifies the number and size of data buffers that transfer data between the Domino server and the Tivoli Storage Manager API. Increasing the number or size (or both) of the data buffers can improve throughput.

You can specify from 2 to 8 buffers, the default value is *3*. The size of the buffers can be from 64 to 8192 kilobytes, the default value is *1024*.

If the ***/buffers*** parameter is not specified on the command line or defined in the preferences file, Data Protection for Domino uses the default values.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/DB2SESSIONS=*numsessions*

Specify the number of Tivoli Storage Manager sessions that the DB2 Tivoli Storage Manager agent uses. You can specify from *1* to *64* sessions. The default value is *1*.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file

name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

***/LOGPRUne**=60|n|No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/MOUNTWait=Yes|No

If the Tivoli Storage Manager server is configured to store transaction log backup data on removable media, then the Tivoli Storage Manager server can indicate to Data Protection for Domino that it is waiting for a required storage volume to be mounted. If this occurs, this option allows you to specify whether Data Protection for Domino waits for the media mount or stops the current operation. Removable media is media such as tapes.

You can specify:

Yes Wait for tape mounts. This is the default.

No Do not wait for tape mounts.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

/SESSions=*numsessions* **| 1**

Specifies the number of Tivoli Storage Manager server sessions to be used by Data Protection for Domino. You can specify from *1* to *64* sessions. The default value is *1*.

Example

The following example backs up both NSF and DB2 enabled Notes databases using two sessions for the DB2 Tivoli Storage Manager agent to access the Tivoli Storage Manager server: `domdsmc fullselective /db2session=2`

```
Starting Domino full backup...
Initializing Domino connection...
Querying Domino for a list of databases, please wait...

Restart Analysis (0 MB): 100%
09/28/2011 06:55:58 AM Recovery Manager: Restart Recovery complete.
(0/0 databases needed full/partial recovery)
09/28/2011 06:56:01 AM The map for DB2 errors was successfully created.


...

Backing up database statrep5.ntf, 114 of 122.
Full: 0 Read: 1,686,528 Written: 1,686,528 Rate: 4,844.12 Kb/Sec

Backup of statrep5.ntf completed successfully.

Backing up database teamrm7.ntf, 115 of 122.
Full: 0 Read: 2,883,584 Written: 2,883,584 Rate: 6,834.95 Kb/Sec

Backup of teamrm7.ntf completed successfully.

Backing up database toolbox.ntf, 116 of 122.
Full: 0 Read: 688,128 Written: 688,128 Rate: 5,209.30 Kb/Sec

Backup of toolbox.ntf completed successfully.

Backing up database updatesite.ntf, 117 of 122.
Full: 0 Read: 2,883,584 Written: 2,883,584 Rate: 8,233.92 Kb/Sec

Backup of updatesite.ntf completed successfully.

Backing up database userlicenses.ntf, 118 of 122.
Full: 0 Read: 663,552 Written: 663,552 Rate: 4,729.93 Kb/Sec

Backup of userlicenses.ntf completed successfully.

Backing up database userreg.ntf, 119 of 122.
Full: 0 Read: 458,752 Written: 458,752 Rate: 3,612.90 Kb/Sec

Backup of userreg.ntf completed successfully.

Backing up database webadmin.nsf, 120 of 122.
Full: 0 Read: 8,388,608 Written: 8,388,608 Rate: 11,457.34 Kb/Sec

Backup of webadmin.nsf completed successfully.

Backing up database webadmin.ntf, 121 of 122.
Full: 0 Read: 10,747,904 Written: 10,747,904 Rate: 11,371.61 Kb/Sec

Backup of webadmin.ntf completed successfully.

Backing up database xxx\busytime.ntf, 122 of 122.
Full: 0 Read: 248,832 Written: 248,832 Rate: 1,840.91 Kb/Sec
```

```
Backup of xxx\busytime.ntf completed successfully.

Backing up DB2 database DOMINO7.

Domino DB2 database backup completed successfully.


Total Domino NSF databases inspected: 122
Total Domino NSF backed up: 122
Total Domino NSF excluded: 0
Total Domino NSF deduplicated: 0
Total Domino NSF bytes inspected: 1,734,538,240
Total Domino NSF bytes transferred: 1,734,538,240
Total Domino NSF LanFree bytes transferred: 0
Total Domino NSF bytes before deduplication: 0
Total Domino NSF bytes after deduplication: 0
Total Domino NSF data compressed by: 0%
Total Domino NSF deduplication reduction: 0.00%
Total Domino NSF data reduction ratio: 0.00%

Domino DB2 database inspected: 1
Domino DB2 database backed up: 1

Throughput rate: 19,821.81 Kb/Sec
Total bytes transferred: 2,325,935,104
Elapsed processing time: 114.59 Secs
```

Domdsmc DB2INActivateobjs

This section describes how to use the **domdsmc db2inactivateobjs** command.

Purpose

Domdsmc db2inactivateobjs displays the db2adutl utility commands that are required to inactivate Tivoli Storage Manager objects that have been created by the DB2 API and are no longer referenced by any Data Protection for Domino Tivoli Storage Manager objects. The db2adutl utility is part of the DB2 Tivoli Storage Manager Agent and is used to manage Tivoli Storage Manager objects. The db2adutl commands (displayed by the **domdsmc db2inactivateobjs** command) must be issued from a DB2 command window and should be issued regularly after DB2 Group or full DB2 backups.

When Data Protection for Domino backs up a DB2 Group or a DB2 database, the backup objects is created by the DB2 API. These objects have a unique name and must be inactivated when they are no longer referenced by Tivoli Storage Manager objects that have been expired as a result of management policies. This command also inactivates table spaces, full DB2 database backups, and archived logs. This command should be run regularly after DB2 Group or full DB2 backups.

```
►►──DOMDSMC──DB2INActivateobjs──┬──────────────────────────┬───────────────────────►
                                └─/ADSMNODe=──nodename─────┘

►─┬──────────────────────────────────────┬──┬─────────────────────────┬───────────►
  │                 ┌─dsm.opt─────────┐  │  └─/ADSMPWD=──password─────┘
  └─/ADSMOPTFile=───┴─optionsfile─────┴──┘

►─┬────────────────────────────────────┬──┬─────────────────────────────────┬─────►
  │               ┌─domdsm.cfg────┐    │  │            ┌─domdsm.log────┐    │
  └─/CONFIGfile=──┴─cfgfilename───┴────┘  └─/LOGFile=──┴─logfilename───┴────┘
```

```
►─┬──────────────────────┬─┬──────────┬─┬──────────────────────────────────┬──────────────►◄
  │              ┌─60─┐  │ └─/Quiet─┘ │              ┌─currentserver─┐  │
  └─/LOGPRUne=───┼─n──┼──┘            └─/SERVer=─────┴─servername────┴──┘
                 └─No─┘
```

Parameters

/ADSMNODe=*nodename*

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.
- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

***/LOGFile=**logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

***/LOGPRUne=**60 | n | No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.
No	Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

***/SERVer=**currentserver | servername*

Specifies the Domino server name. If not specified, Data Protection for Domino uses the current Domino server.

Example

The following example displays the db2adutl utility commands that are required to inactivate Tivoli Storage Manager objects that have been created by the DB2 API and are no longer referenced by any Data Protection for Domino Tivoli Storage Manager objects:

```
domdsmc db2inactivateobjs
```

Output example:

```
Issue the following DB2 command to delete unneeded log archives:
db2adutl DELETE FULL OLDER THAN 20070925091903 DATABASE DOMINO

Issue the following DB2 command to delete unneeded tablespace backups:
db2adutl DELETE TABLESPACE OLDER THAN 20070925082543 DATABASE DOMINO

Issue the following DB2 command to delete unneeded full database backups:
db2adutl DELETE LOGS BETWEEN S0000000 AND S0000016 DATABASE DOMINO
```

Domdsmc DB2restore

This section describes how to use the **domdsmc db2restore** command.

Purpose

Domdsmc db2restore restores Domino DB2 enabled Notes databases from one of the following sources:

- a DB2 Group backup image.
- a set of DB2 Groups from a full DB2 database backup image
- a full DB2 database from a full DB2 database backup image

Note that all of the DB2 enabled Notes databases that reside in the DB2 Group, the set of DB2 Groups, or the full DB2 database backup image are restored.

The pending DB2 file is updated during a successful **db2restore** restore operation. Note that when performing an alternate database restore, the alternate database can exist as long as ***/db2replace***=*yes* is specified and the log directory must not be in use by another DB2 database during the first alternate database restore operation.

```
►►──DOMDSMC──DB2RESTore──┬─db2group───────┬──┬─────────────────────────┬──────────►
                         │ ┌─,────────┐   │  └─/ADSMNODe=──nodename────┘
                         │ ▼          │   │
                         └───db2group─┴───┘

►─┬──────────────────────────────────────┬──┬─────────────────────────┬────────────►
  │                   ┌─dsm.opt──────┐   │  └─/ADSMPWD=──password─────┘
  └─/ADSMOPTFile=─────┴─optionsfile──┴───┘

►─┬──────────────────────────────────────┬─────────────────────────────────────────►
  │                ┌─domdsm.cfg───┐      │
  └─/CONFIGfile=───┴─cfgfilename──┴──────┘

►─┬──────────────────────────────────────────────────────────────────────────┬─────►
  │                 ┌─domdsm.cfg (DB2ALtdbname=)─┐                           │
  └─/DB2ALtdbname=──┴────────────────────────────┴─────db2database name──────┘

►─┬───────────────────────────────────────┬────────────────────────────────────────►
  └─/DB2DATAbase=──db2database name───────┘
```

```
►──┬─────────────────────────────────────────────────────────────────┬──►
   │                    ┌─path relative to alternate database directory─┐ │
   └─/DB2CONTainerpath=─┴─path──────────────────────────────────────────┴─┘

►──┬──────────────────────────────────────────────────────────┬──►
   │             ┌─domdsm.cfg (DB2LOGPath=)─┐                  │
   └─/DB2LOGPath=─┴──────────────────────────┴──directory path─┘

►──┬──────────────────────────────────────────────────────────────┬──►
   │               ┌─domdsm.cfg (DB2LOGTarget=)─┐                  │
   └─/DB2LOGTarget=─┴────────────────────────────┴──directory path─┘

►──┬──────────────────────┬──►
   │              ┌─Yes─┐ │
   └─/DB2REPlace=─┴─No──┴─┘

►──┬──────────────────────────────────────────────────────────────────────┬──►
   │                   ┌─domdsm.cfg (DB2RESTIntopath=)─┐                   │
   └─/DB2RESTIntopath=─┴───────────────────────────────┴──directory path──┘

►──┬───────────────────────────────┬──┬─────────┬──┬────────────┬──►
   │                ┌─1───────────┐ │  └─/FULL─┘  └─/INPlace─┘
   └─/DB2SESSIONS=──┴─numsessions─┴─┘

►──┬─────────────────────────────┬──┬──────────────────────┬──┬──────────────────────────┬──►
   │            ┌─domdsm.log───┐ │  │             ┌─60─┐   │  │         ┌─SHOWACtive─┐   │
   └─/LOGFile=──┴─logfilename──┴─┘  └─/LOGPRUne=──┼─n──┼───┘  └─/PICk=──┴─SHOWAll────┴───┘
                                                  └─No─┘

►──┬────────────────────────────────┬──┬───────────┬──┬─────────┬──►
   │                 ┌─,00:00:00─┐  │  └─/PREPare─┘  └─/Quiet─┘
   └─/PIT=──date─────┴─,time─────┴──┘

►──┬──────────────────────────────────┬─────────────────────────────────►◄
   │             ┌─currentserver─┐    │
   └─/SERVer=────┴─servername────┴────┘
```

Parameters

db2group,...

Specifies the DB2 Group to restore from a table space backup image. Only one DB2 Group can be specified when restoring from a table space back up image. When restoring a full DB2 database backup image (**/full**=*yes*), you can specify multiple DB2 Groups by name or you can specify the wildcard character (*).

If you specify the wildcard character in the *db2group*, you must use double or single quotes, for example, "abc*" or 'abc*'.

/ADSMNODe=*nodename*

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.

- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution. Note that if the DB2 Tivoli Storage Manager Agent uses the same dsm.opt file as Data Protection for Domino, *generate* must be specified.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/DB2ALtdbname=*database name*

Specify the name of the alternate DB2 database to use for activation. If the ***/db2altdbname*** parameter is not specified, the value of the ***db2altdbname*** configuration option (defined in the Data Protection for Domino domdsm.cfg preferences file) is used. If ***db2altdbname*** is not defined in the preferences file, the alternate database name DOM_ALT is used.

/DB2DATAbase=*database name*

Specify the name of the DB2 database to restore. The name specified overrides the default name (which is the name of the Domino DB2 database used by the Domino server). If the ***db2database*** parameter is not specified, the current Domino DB2 database name is used.

/DB2CONTainerpath=*path*

Specify container path to be used for a redirected restore operation. A redirected restore operation is performed when restoring to an alternate database (***inplace=****no*) or when restoring in place and redefining the tablespace containers. If ***db2containerpath*** is not specified during an alternate restore operation, the tablespace containers are defined relative to the alternate database directory.

Attention: ***db2containerpath*** is required when the DB2DIRECTORY option is specified in the Domino server notes.ini file. Otherwise the restore will fail. That is because DB2 attempts to place the alternate DB2 database data in the directory specified by the DB2DIRECTORY option, which is already used by the Domino DB2 database.

/DB2LOGPath=*path*

Specify the base log directory for the alternate database. The directory must exist and must not contain any files before the **db2restore** command is executed. When the ***db2logpath*** parameter is not specified, the configuration option ***db2altdbname*** is used. Since the log path cannot be shared by more than one DB2 database, this option must be specified if one alternate database exists.

/DB2LOGTarget=*path*

Specify the target directory for extracting log files from a backup image during an inplace restore. If the ***/db2logtaget*** parameter is not specified, the value of the ***db2logtarget*** configuration option (defined in the Data Protection for Domino domdsm.cfg preferences file) is used.

/DB2REPlace=*Yes* **|** *No*

Specify whether to replace an alternate database (if it exists). The default value is *Yes*.

/DB2RESTIntopath=*directory*

Specify the base target DB2 database directory for the alternate database when restoring to an alternate DB2 database. The specified drive and directory must be local. If the ***db2restintopath*** parameter is not specified, the configuration option ***db2restintopath*** is used. If the ***db2restintopath*** configuration option is not specified, the DB2 database default database directory configuration setting is used.

/DB2SESSIONS=*numsessions*

Specify the number of Tivoli Storage Manager sessions that the DB2 Tivoli Storage Manager agent uses. You can specify from *1* to *64* sessions. The default value is *1*.

/FULL=*Yes* **|** *No*

Specify whether a full DB2 database is restored.

/INPlace

Specify an in place restore. An in place restore is allowed only when restoring a full DB2 database backup image.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* | *n* | *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/PICk=*SHOWACtive* | *SHOWALl*

Displays a list of database backups matching the *dbname* pattern that can be selected for restore. The pick list is displayed as a scrollable list from which you can select the database backups for restore.

You can specify:

SHOWACtive
Displays a list of active database backup versions. This is the default.

SHOWALl
Displays a list of both active and inactive database backup versions. This shows all the backup versions that match the *dbname* pattern.

/PIT=*currentdate,currenttime* | *date,time*

Specifies a point in time when the specified databases are restored. The *date* and *time* values must be specified in the same date and time format defined in the Data Protection for Domino preferences file. The most recent database backup images taken before the specified point in time are restored. Deleted backup images are not restored. Logged databases can then be rolled forward to that point by specifying the same date and time values on the ***/applylogs*** option of the **activatedbs** command.

date Specify a date string in the active date format. If you do not specify a date, the specified databases are restored unless the ***/pick*** parameter was used to select inactive backup versions.

The date must be specified using the same date format defined in the Data Protection for Domino preferences file. See "Domdsmc Set" on page 123 for a list of available date formats.

time Specify a time string in the active time format. If you specify a date without the time, HH:MM:SS on a 24-hour clock is used.

The time must be specified using the same time format defined in the Data Protection for Domino preferences file. See "Domdsmc Set" on page 123 for a list of available time formats.

Note: If this parameter is used with the ***/pick*** parameter, the *showactive* and *showall* variables for the ***/pick*** parameter are ignored. The pick list will contain the database backup images that meet the ***/pit*** criteria.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

/SERVer=*currentserver* | *servername*
Specifies the Domino server name. If not specified, Data Protection for Domino uses the current Domino server.

Examples

Example 1: The following example restores the full backup image of all DB2 Groups (created when originally backed up with the `db2selective /full=yes` command) into the existing database (inplace restore):

```
domdsmc db2restore /full /inplace
```

Output example:

```
Starting Domino DB2 database restore...
Restoring Domino DB2 Database DOMINO to DOMINO
Restore of DOMINO completed successfully.
```

Example 2: The following example restores a DB2 enabled Notes database from a full backup image of all DB2 Groups (created when originally backed up with the `db2selective /full=yes` command) into an alternate DB2 database:

```
domdsmc db2restore /full
```

Output example:

```
Starting Domino DB2 database restore...
Restoring Domino DB2 Database DOMINO to DOM_ALT
Restore of DOMINO completed successfully.
```

After the restore completes:

1. The DB2 Groups in the restored alternate DB2 database are updated with the changes in the DB2 transaction logs by issuing the "Domdsmc DB2rollforward" on page 150 command.

2. The DB2 enabled Notes databases (in the restored DB2 Groups) must be copied from the alternate restored DB2 database to their final DB2 enabled Notes location by issuing the "Domdsmc DB2activatedbs" on page 130 command.

Example 3: The following example restores a DB2 enabled Notes database from a backup image of DB2 Group `GRP1` (created when originally backed up with the `db2selective GRP1` command) into an alternate DB2 database:

```
domdsmc db2restore GRP1
```

Output example:

```
Starting Domino DB2 database restore...
Restoring Domino DB2 group GRP1 to DB2 Database DOM_ALT
Restore of GRP1 completed successfully.
```

After the restore completes:

1. The restored DB2 Group is updated with the changes in the DB2 transaction logs by issuing the "Domdsmc DB2rollforward" command.
2. The DB2 enabled Notes databases (in the restored DB2 Group) must be copied from the temporary restored DB2 Group to their final DB2 enabled Notes location by issuing the "Domdsmc DB2activatedbs" on page 130 command.

Domdsmc DB2rollforward

This section describes how to use the **domdsmc db2rollforward** command.

Purpose

The **domdsmc db2rollforward** command rolls a DB2 database forward to the specified point in time and marks the rollforward as complete. The DB2 database can be an alternate DB2 database or the Domino DB2 database. When the Domino DB2 database is enabled for rollforward recovery, the rollforward command must be executed after the restore. To recover a database to a time greater than the backup time, use the ***/applylogs*** parameter. The list of available DB2 databases to rollforward is obtained from the pending DB2 database file. To view the pending DB2 list, use the **domdsmc query db2rollforward** command. The **db2rollforward** command is only valid when the Domino DB2 database has been enabled for rollforward recovery.

When the ***/applylogs*** parameter is specified and the database is being rolled forward after an inplace restore, it is not necessary to manually extract the logs.

If the DB2 database is being rolled forward after an inplace restore or an alternate database restore, the archived logs (required to roll the database forward) are automatically restored.

DB2 automatically archives the transaction log files when they become full. However, the user can also initiate an archive of the log to archive active log files and have them available for alternate database rollforward command.

Transaction log files stored on the Tivoli Storage Manager server are automatically restored as needed for a database recovery.

Be aware that when a DB2 database is enabled for rollforward recovery and the database is used for an inplace restore, the Domino server cannot connect to the

DB2 database until after the rollforward operation completes. As a result, the command output displays this message text:

```
Starting Domino DB2 database rollforward...
Initializing Domino connection...
Restart Analysis (0 MB): 100%
04/21/2007 12:02:57 AM  A RM error occurred.: An error occurred accessing the db
2 datasource.

DB2 CONNECTION ERROR:  Domino unable to connect to DB2 database 'DOMDB2' as user
 'db2admin'...
[IBM][CLI Driver] SQL1117N  A connection to or activation of database "DOMDB2" c
annot be made because of ROLL-FORWARD PENDING.  SQLSTATE=57019

DB2 CONNECTION ERROR:  set DEBUG_DB2CONNECT=0 to suppress this message.
04/21/2007 12:02:57 AM  Unable to initialize DB2 services.  DB2-based nsfs will
be unusable.: An error occurred accessing the db2 datasource.
```

There is no DB2 connection error and therefore, this message text can be ignored.

```
>>--DOMDSMC--DB2ROLLforward--database name---------------------------------------->

>--+-----------------------------------------+--+-------------------------------------+-->
   |                        .-,00:00:00-.    |  |                  .-domdsm.cfg---.   |
   '-/APPLYLogs=--+------+--+-,time-----+----'  '-/CONFIGfile=-----+-cfgfilename--+---'
                  '-date-'

>--+-------------------------------------+--+------------------------+------------>
   |             .-domdsm.log---.        |  |              .-60-.    |
   '-/LOGFile=---+-logfilename--+--------'  '-/LOGPRUne=---+-n--+----'
                                                           '-No-'

>--+----------------------------------+--+----------+---------------------------><
   |          .-SHOWACtive-.          |  '-/Quiet---'
   '-/PICk=---+-SHOWALl----+----------'
```

Parameters

dbname

Specifies the DB2 database to rollforward. If not specified, the default alternate DB2 database (DB2ALTDBNAME) is used.

/APPLYLogs=*date,time*

Specifies that transaction log recovery for the restored databases is performed if they are logged. The *date* and *time* values must be specified in the same date and time format defined in the Data Protection for Domino preferences file. The transaction logs are applied to a specified point in time or to the current date and time if no *date* and *time* values are specified.

date Specify a date string in the active date format. When specified, transactions that are completed and committed before the specified date are applied to the restored database. The date specified should be after the backup date of the backup image that is being restored. The ***/pit*** option can be used with the **restore** command to automatically restore the most recent full backup image that is performed before the desired point in time.

The date must be specified using the same date format defined in the Data Protection for Domino preferences file. See "Domdsmc Set" on page 123 for a list of available date formats.

time Specify a time string in the active time format. If you specify a date without the time, 00:00:00 on a 24-hour clock is used.

The time must be specified using the same time format defined in the Data Protection for Domino preferences file. See "Domdsmc Set" on page 123 for a list of available time formats.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60* **|** *n* **|** *No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/PICk=*SHOWACtive* **|** *SHOWALl*
Displays a list of database backups matching the *dbname* pattern that can be selected for restore. The pick list is displayed as a scrollable list from which you can select the database backups for restore.

You can specify:

SHOWACtive
Displays a list of active database backup versions. This is the default.

SHOWALl
Displays a list of both active and inactive database backup versions. This shows all the backup versions that match the *dbname* pattern.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

Example

This command sequence shows rollforward processing for a full inplace DB2 database restore:

Command 1: `domdsmc query db2rollforward`

Output:

```
Backup Date        Size      Group     DB2 Database State
-----------       --------- ---------- -------
01/26/08   05:34:22   57.00MB   DOMINO     Pending
```

Command 2: `domdsmc db2rollforward DOMINO`

Output:

```
Starting Domino DB2 database rollforward...
Rollforward DB2 database DOMINO.
Rollforward of DOMINO completed successfully.
```

Domdsmc DB2selective

How to use the **domdsmc db2selective** command.

Purpose

Domdsmc db2selective backs up DB2 Groups and the Domino DB2 database.

- If the Domino DB2 database is enabled for rollforward recovery, an online backup is performed.
- If the Domino DB2 database is not enabled for rollforward recovery, Data Protection for Domino cannot back it up.

- DB2 Group backups are only available when the Domino DB2 database is enabled for rollforward recovery.

Tip: When backing up multiple DB2 groups, increase the value of the Tivoli Storage Manager server COMMTIMEOUT option to avoid a backup failure due to a session timeout.

```
►►──DOMDSMC──DB2Selective──┬─"*"──────────┬──┬────────────────────────┬──────►
                           │ ┌─,────────┐ │  └─/ADSMNODe=──nodename─┘
                           │ ▼          │ │
                           └───db2group─┴─┘

►──┬──────────────────────────────────────┬──┬──────────────────────┬────────►
   │                ┌─dsm.opt──────┐      │  └─/ADSMPWD=──password─┘
   └─/ADSMOPTFile=──┴─optionsfile──┴──────┘

►──┬──────────────────────────────────┬──┬──────────────────────────────────┬─►
   │              ┌─domdsm.cfg───┐    │  │                 ┌─1───────────┐  │
   └─/CONFIGfile=─┴─cfgfilename──┴────┘  └─/DB2SESSIONS=───┴─numsessions─┴──┘

►──┬─────────┬──┬──────────────────────────────┬──┬───────────────────────┬──►
   └─/FULL───┘  │            ┌─domdsm.log───┐  │  │              ┌─60─┐   │
                └─/LOGFile=──┴─logfilename──┴──┘  └─/LOGPRUne=────┼─n──┼───┘
                                                                  └─No─┘

►──┬──────────┬────────────────────────────────────────────────────────────►◄
   └─/Quiet───┘
```

Parameters

"*"|*db2group,db2group,...*

Specifies the DB2 Groups to back up. When a DB2 Group is not specified and the **/full** parameter is specified, a full DB2 database backup is performed. Otherwise, a table space backup is performed. The wildcard character asterisk (*) is used to specify a group of databases when used in the *db2group*. Multiple *db2group* can be specified as long as they are separated with commas.

If you specify the wildcard character in the *db2group*, you must use double or single quotes, for example, "abc*" or 'abc*'.

/ADSMNODe=*nodename*

Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*

Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.

- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution. Note that if the DB2 Tivoli Storage Manager Agent uses the same dsm.opt file as Data Protection for Domino, *generate* must be specified.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/DB2SESSIONS=*numsessions*

Specify the number of Tivoli Storage Manager sessions that the DB2 Tivoli Storage Manager agent uses. You can specify from *1* to *64* sessions. The default value is *1*.

/FULL Specify whether a full DB2 database is backed up.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60***|***n***|***No***

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/Quiet Specifies that status information does not display. However, the information is written to the activity log.

Examples

Example 1: The following example backs up the Domino DB2 database:

```
domdsmc db2selective /full
```

Output example:

```
Starting Domino DB2 database backup...
Backing up DB2 database DOMINO.
Domino DB2 database backup completed successfully.
```

Example 2: The following example backs up the DB2 Groups `GRP1` and `GRP2`:

```
domdsmc db2selective GRP1,GRP2
```

Output example:

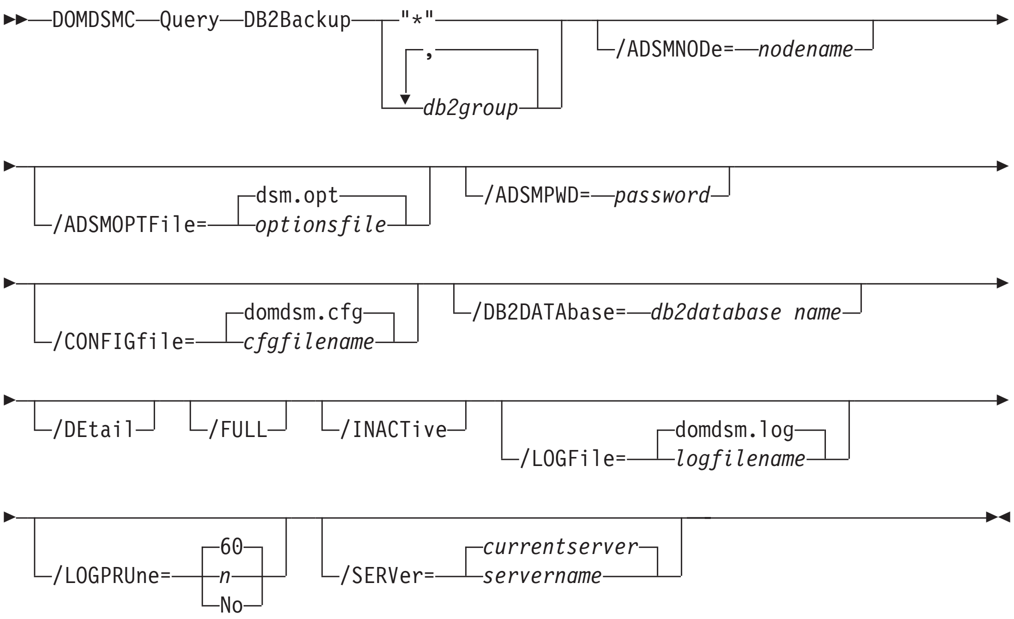
```
Starting Domino DB2 group backup...
Backing up DB2 group Default/GRP1, 1 of 2.
Backup of GRP1 completed successfully.

Backing up DB2 group Default/GRP2, 2 of 2.
Backup of GRP1 completed successfully
```

Domdsmc Query DB2backup

This section describes how to use the **domdsmc query db2backup** command.

Purpose

Domdsmc query db2backup lists DB2 backup objects.



Parameters

"*" | *db2group,db2group,...*
Specifies the DB2 Group to query.

If you specify the wildcard character in the *db2group*, you must use double or single quotes, for example, "abc*" or 'abc*'.

/ADSMNODe=*nodename*
Specifies the Tivoli Storage Manager node name Data Protection for Domino uses to logon to the Tivoli Storage Manager server. The command-line value overrides the value in the Tivoli Storage Manager system options file.

/ADSMOPTFile=*optionsfile*
Specifies the name of the options file used by the Tivoli Storage Manager API. The default file name is dsm.opt. The *optionsfile* variable can include a fully qualified path name or a relative path. A relative path means the path is relative to the directory from which Data Protection for Domino is currently run. Note the following considerations:

- When Data Protection for Domino is launched by a Domino startup script (`tools/startup`) that was configured by the **dominstall** program, a relative path means the path is relative to the Domino Data directory and NOT to the directory from which Data Protection for Domino is currently run.

- This parameter functions in the same manner as the DSMI_CONFIG environment variable. When the DSMI_CONFIG environment variable is set, the options file specified by this environment variable is recognized as the default options file.
- You should specify the ***adsmoptfile*** parameter in the Data Protection for Domino preferences file (domdsm.cfg) when using the Web client GUI.

/ADSMPWD=*password*

Specifies the Tivoli Storage Manager password Data Protection for Domino uses to logon to the Tivoli Storage Manager server. If you specify ***passwordaccess*** *generate* in the Tivoli Storage Manager system options file, then the password is not required. In this case, Data Protection for Domino uses the password that is stored by the Tivoli Storage Manager API.

If ***passwordaccess*** is set to *generate* and you specify a password, the value is ignored unless a password for this node has not been stored. In this case, the specified password is stored and used for the current command execution.

If ***passwordaccess*** is set to *prompt* and you specify a password on the command line, you are not prompted for a password. The command line value overrides the need to prompt.

If ***passwordaccess*** is set to *prompt* and you do not specify a password on the command line, then you are prompted for a password.

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/DB2DATAbase=*database name*

Specify the name of the alternate DB2 database to use for restore. If the ***db2altdbname*** parameter is not specified, the configuration option ***db2altdbname*** is used.

/DEtail

Specify whether to display a detailed output of the DB2 Groups and databases contained in the backup images.

/FULL Specify whether a full DB2 database backup image is queried.

/INACTive

Specify that both active and inactive backup objects are displayed. The default value is to display only the active backup objects.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne**=60|***n***|***No***

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60 Specifies that log entries are saved for 60 days before pruning. This is the default.

n Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.

No Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

/SERVer=*currentserver*|*servername*

Specifies the Domino server name. If not specified, Data Protection for Domino uses the current Domino server.

Examples

Example 1: The following example queries (and displays) a list of active and inactive DB2 Group backups:

```
domdsmc query db2backup "*" /inactive
```

Output example:

```
  Domino Server: domino7     DB2 Database Name: DOMINO
  --------------             ------------------

Group Backup Date          Size      A/I  Type   Class        Group(TID)
-----------------          ----      ---  ----   ---------    ----------
01.08.2008 14:46:40       162.00B     A    T     DEFAULT      GRP1(6)
01.08.2008 14:44:37       166.00B     A    T     DEFAULT      GRP2(8)
```

Example 2: The following example queries (and displays) a list of active DB2 Group backups and the DB2 enabled Notes databases contained within the DB2 Group backup:

`domdsmc query db2backup "*" /detail`

Output example:

```
  Domino Server: domino7     DB2 Database Name: DOMINO
  --------------             ------------------

Group Backup Date          Size      A/I  Type   DB2 Group    Group Name
-----------------          ----      ---  ----   ---------    ----------
01.08.2008 11:46:52       160.00B     A    T      DEFAULT      GRP2

                           Size      Database Title   Database File
                           ----      --------------   -------------
                          160.00B    db2 nsf 1        ab2nsf1.nsf
                          160.00B    db2 nsf 2        db2b.nsf
                          160.00B    db2 nsf 1        db2g.nsf
                          160.00B    db2 nsf 1        xb2nsf1.nsf
```

Example 3: The following example queries (and displays) a full DB2 database backup and the DB2 Groups and DB2 enabled Notes databases contained within the full DB2 database backup:

`domdsmc query db2backup "*" /detail /full`

Output example:

```
  Domino Server: domino7     DB2 Database Name: DOMINO
  --------------             ------------------

Group Backup Date          Size      A/I  Type   Class        Group(TID)
-----------------          ----      ---  ----   ---------    ----------
01.08.2008 14:46:40       162.00B     A    T     DEFAULT      GRP1(6)

                           Size      Database Title   Database File
                           ----      --------------   -------------
                          162.00B    db2 nsf 1        db1.nsf
                          162.00B    db2 nsf 2        db2a.nsf
                          162.00B    db2 nsf 1        db2c.nsf
                          162.00B    db2 nsf 1        db2e.nsf

Group Backup Date          Size      A/I  Type   Class        Group(TID)
-----------------          ----      ---  ----   ---------    ----------
01.08.2008 14:44:37       166.00B     A    T     DEFAULT      GRP2(8)

                           Size      Database Title   Database File
                           ----      --------------   -------------
                          166.00B    db2 nsf 1        ab2nsf1.nsf
                          166.00B    db2 nsf 2        db2b.nsf
                          166.00B    db2 nsf 1        db2g.nsf
                          166.00B    db2 nsf 1        xb2nsf1.nsf
```

Domdsmc Query DB2pendingdbs

This section describes how to use the **domdsmc query db2pendingdbs** command.

Purpose

Domdsmc query db2pendingdbs lists the DB2 enabled Notes databases that are pending activation. These databases reside in an alternate database and the activate process (**"Domdsmc DB2activatedbs" on page 130**) copies them to the Domino DB2 database. The alternate DB2 database is considered available when it is not manually deleted through DB2 server interface, overwritten by another restore operation, or removed from the list of DB2 databases (that contain DB2 enabled Notes databases) available for activation.

```
►►──DOMDSMC──Query──DB2Pendingdbs──┬─────────────────────────────────────┬──────────────►
                                   │                 ┌─domdsm.cfg───┐    │
                                   └─/CONFIGfile=────┴─cfgfilename──┴────┘

►──┬──────────────────────────────────┬──┬──────────────────────────┬───────────────────►◄
   │            ┌─domdsm.log───┐      │  │              ┌─60─┐      │
   └─/LOGFile=──┴─logfilename──┴──────┘  └─/LOGPRUne=───┼─n──┼──────┘
                                                        └─No─┘
```

Parameters

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

***/LOGPRUne**=60|n|No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.
No	Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

Examples

Example 1: The following example queries (and displays) a list of DB2 enabled Notes databases that are pending activation:

```
domdsmc query db2pendingdbs
```

Output example:

```
    Domino Server: Server01
    -------------

    Backup Date           Size      Group    DB2 Database  Database
---------------------  -----------  -----    ------------  --------
01/21/2008 11:53:30        64.00B   GRP1     DOMALT1       db2nsf1.nsf
01/21/2008 11:53:30        64.00B   GRP1     DOMALT1       db2nsf2.nsf
01/21/2008 11:53:30        64.00B   GRP1     DOMALT1       db2nsf3.nsf
01/21/2008 11:53:30        64.00B   GRP1     DOMFULL1      db2nsf1.nsf
01/21/2008 11:53:30        64.00B   GRP1     DOMFULL1      db2nsf2.nsf
01/21/2008 11:53:30        64.00B   GRP1     DOMFULL1      db2nsf3.nsf
01/21/2008 11:53:30        64.00B   GRP2     DOMFULL1      db2nsf4.nsf
01/21/2008 11:53:30        64.00B   GRP2     DOMFULL1      db2nsf5.nsf
01/21/2008 11:53:30        64.00B   GRP2     DOMFULL1      db2nsf6.nsf
```

Example 2: The following example queries a list of DB2 enabled Notes databases that are pending activation. However, there are no databases pending activation:

```
domdsmc query db2pendingdbs
```

Output example:

```
ACD5418I There are no databases pending activation.
```

Domdsmc Query DB2rollforward

This section describes how to use the **domdsmc query db2rollforward** command.

Purpose

Domdsmc query db2rollforward lists the DB2 database rollforward status.

```
►►──DOMDSMC──Query──DB2ROLLforward──┬──────────────────────────────────┬──────►
                                    │               ┌─domdsm.cfg───┐   │
                                    └─/CONFIGfile=──┴─cfgfilename──┴───┘

►──┬───────────────────────────────┬──┬──────────────────────┬────────────────►◄
   │            ┌─domdsm.log───┐   │  │              ┌─60─┐   │
   └─/LOGFile=──┴─logfilename──┴───┘  └─/LOGPRUne=───┼─n──┼───┘
                                                     └─No─┘
```

Parameters

/CONFIGfile=*cfgfilename*

Specifies the name of the Data Protection for Domino preferences file. The file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the ***/logfile*** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60|n|No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.
No	Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the Data Protection for Domino log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

Examples

Example 1: The following example queries (and displays) a list of DB2 databases that are available for rollforward processing after an inplace restore:

```
domdsmc query db2rollforward
```

Output example:

```
Backup Date  Size      Group     DB2 Database State
-----------    --------- ---------- -------
01/26/08   05:34:22   57.00MB   DOMINO     Pending
```

Example 2: The following example queries (and displays) a list of DB2 databases that are available for rollforward processing after an alternate DB2 database restore:

```
domdsmc query db2rollforward
```

Output example:

```
                 DB2 Database Rollforward Status
                 -------------------------------

    Domino Server: polar1
    --------------

  Backup Date                Size        Group     DB2 Database    State
  -----------                 ----        -----     ------------    -----
  01/19/08   13:11:44      1,078.00MB    GRP8     DOM_ALT         Pending
  01/19/08   14:12:01        659.00MB    GRP5     DOM_ALT1        Pending
  01/18/08   13:36:46      1,031.00MB   -          DOM_FULL        Pending
```

Domdsmc Updatedb2pwd

This section describes how to use the **domdsmc updatedb2pwd** command.

Purpose

Domdsmc updatedb2pwd updates the DB2 user password. The password is required to access the DB2 instance where the Domino DB2 database resides. Data Protection for Domino prompts the user for the password the first time and saves the password encrypted in a file. The password is read from this file when access to DB2 is required. The command allows the user to change the password in the file in case the DB2 user password is changed. If you do not enter the old and new passwords on the command, you are prompted for them. When Data Protection for Domino prompts you for the passwords, the password is not displayed on the screen.

```
►►──DOMDSMC──UPDATEDB2Pwd──┬──────────────────────────────────┬─────────────►
                           └─oldpw──┬───────────────────────┬─┘
                                    └─newpw──┬────────────┬─┘
                                             └─verifypw───┘

►──┬─────────────────────────────────┬──┬───────────────────────────────┬──►
   │              ┌─domdsm.cfg───┐   │  │          ┌─domdsm.log───┐     │
   └─/CONFIGfile=─┴─cfgfilename──┴───┘  └─/LOGFile=─┴─logfilename──┴─────┘

►──┬──────────────────────┬─────────────────────────────────────────────►◄
   │              ┌─60─┐  │
   └─/LOGPRUne=───┼─n──┼──┘
                  └─No─┘
```

Parameters

oldpw The current password to change. You are prompted for this value if omitted.

newpw The new password. You are prompted for this value if omitted. When choosing a new password, you can use from 1 to 64 characters.

Valid password characters are as follows:

A-Z	Any letter, A through Z, uppercase or lowercase
0–9	Any number, 0 through 9
+	Plus
.	Period
_	Underscore
-	Hyphen
&	Ampersand

A password is not case-sensitive.

verifypw
The verify password is used to validate the password entered for newpw. You are prompted for this value if omitted.

/CONFIGfile=*cfgfilename*
Specifies the name of the Data Protection for Domino preferences file. The

file name can include a fully-qualified path. If you do not specify a path, it is assumed the preferences file resides in the directory where Data Protection for Domino is installed.

You can also specify the preferences file using the DOMI_CONFIG environment variable.

The default preferences file is domdsm.cfg.

/LOGFile=*logfilename*

Specifies the name of the activity log that is generated by Data Protection for Domino. The log file name is used for the current command and does not update the default log file that is stored in the preferences file. You can use the **set** command to change the default log file name that is stored in the preferences file. The command-line parameter can be used to override the default for one command run. If the specified file does not exist, it is created. If it does exist, new log entries are appended to the file. The file name can include a fully-qualified path. If you do not specify a path, the file is written to the directory where Data Protection for Domino is installed.

You can specify the log file using the DOMI_LOG environment variable.

The default log file is domdsm.log.

When using multiple simultaneous instances of Data Protection for Domino to perform operations, use the **/logfile** parameter to specify a different log file for each instance used. This directs logging for each instance to a different log file and prevents interspersed log file records. Failure to specify a different log file for each instance can result in unreadable log files.

/LOGPRUne=*60|n|No*

Specifies whether to prune log entries. By default, log pruning is enabled and performed once per day. You can use the **set** command to:

- Change the defaults so that log pruning is disabled
- Change the number of days log entries are saved

You can use the ***/logprune*** option to override these defaults for one command run. Note that when the value of ***/logprune*** is a number, the prune is performed even if one has already been performed for the day.

You can specify:

60	Specifies that log entries are saved for 60 days before pruning. This is the default.
n	Specifies the number of days to save log entries. The range of values is 0 to 9999. A value of 0 deletes all entries in the log except for the current command run entries.
No	Do not prune the log.

Changes to the value of the **timeformat** or **dateformat** parameter can result in an undesired pruning of the log file. If you are running a command that may prune the log file and the value of the **timeformat** or **dateformat** parameter has changed, perform one of the following to prevent undesired pruning of the log file:

- Make a copy of the existing log file.
- Specify a new log file with the **/logfile** parameter or **logfile** setting.

Example

The following example changes the DB2 user password to **secret**:

```
domdsmc updatedb2pwd oldpassword secret secret
```

Output example:

```
ACD0260I Password successfully changed.
```

Chapter 4. Protecting Lotus Domino Server data

Details of how to use Data Protection for Domino to protect Lotus Domino servers.

Automating backups

This section describes how to use the Tivoli Storage Manager scheduler with Data Protection for Domino to automate online backups of Domino server databases.

To ensure that this example works, you should install the latest Tivoli Storage Manager backup-archive client. The backup-archive client must reside on the same machine as Data Protection for Domino to use the scheduler service.

After Data Protection for Domino is registered to a Tivoli Storage Manager server and installed and configured on the Domino server, perform the following steps:

1. **On the Tivoli Storage Manager server:**
   a. Define a schedule in the policy domain to which Data Protection for Domino is registered.
   b. Associate the Data Protection for Domino node to the defined schedule.
2. **On the Domino server where Data Protection for Domino is installed:**
   a. Install the Tivoli Storage Manager scheduler client as an AIX, Linux, or UNIX service. If a scheduler already exists for the regular Tivoli Storage Manager backup-archive client, configure another scheduler for Data Protection for Domino. The Tivoli Storage Manager scheduler should have a different node name from the regular Tivoli Storage Manager Backup-Archive client.
   b. Define a command file that contains the Data Protection for Domino commands to perform the desired backup.
   c. Start the scheduler installed for Data Protection for Domino.

Scenario

This example assumes the following environment:

- Data Protection for Domino is registered to a Tivoli Storage Manager server:
  - The node name is *mynode*.
  - The password is *mypassword*.
  - The policy domain is *mydomain*.
  - The user ID of the Domino server is *notesid*.
- For Domino NSF databases, there are several events that can be scheduled. For this example we are going to assume the Domino server is running archival logging and we are using the backup strategy of full backups plus transaction log archives. For this backup strategy, it is suggested you do periodic archival of the transaction logs, incremental backups, selective backups of the logged databases and inactivation of transaction logs. Each of these tasks should have its own schedule as they need to be done at various times.
- For DB2 enabled Notes databases, a scheduled backup strategy can consist of a weekly full DB2 database backup and a daily DB2 backup for the most critical DB2 Group.

- This example shows how to schedule hourly archiving of the transaction logs. From this example and the sample files that are installed, you should be able to schedule the remaining tasks that need to be done.

This method is flexible because you can define a command file with any set of commands you choose. This allows you to use the same method to schedule other back ups on AIX, Linux, or UNIX.

Tivoli Storage Manager server tasks

1. Enter the following command to define the schedule to do an hourly archival of the transaction logs. You can enter this command on the server console or from an administrative client. The administrative client does not have to be running on the same system as the Tivoli Storage Manager server.

   ```
   def sched domagents dom_hourly_archive desc="Domino Hourly Archive"
   action=command objects="/bin/domarc" priority=2 starttime=21:00
   duration=15 duru=minutes period=1 perunits=hours dayofweek=any
   opt=schedcmduser=notesid
   ```

   Tivoli Storage Manager displays this message:

   ```
   ANR2500I Schedule DOM_HOURLY_ARCHIVE
   defined in policy domain DOMAGENTS.
   ```

2. To associate Data Protection for Domino to this schedule, issue the following command:

   ```
   define association domagents dom_hourly_archive mars
   ```

   Tivoli Storage Manager displays this message:

   ```
   ANR2510I Node MARS associated with schedule
   DOM_HOURLY_ARCHIVE in policy domain DOMAGENTS.
   ```

   At this point, a schedule is defined on the Tivoli Storage Manager server that runs a command file called `/bin/domarc`. The schedule starts around 11:00 pm. The schedule is re-executed every hour and can start on any day of the week.

   Note: If you want to confirm that the schedule and association is set correctly, you can use the Tivoli Storage Manager administrative commands **query schedule** and **query association**. See the appropriate Tivoli Storage Manager Administrator's Guide for your server platform for more information.

Tivoli Storage Manager client tasks

This example assumes that you have installed the Tivoli Storage Manager backup-archive client on the Domino server in the in the default installation directory (AIX: `/usr/tivoli/tsm/client/ba/bin64`, and Linux: `/opt/tivoli/tsm/client/ba/bin`) directory and Data Protection for Domino for the Domino server in the default installation directory (AIX: `/usr/tivoli/tsm/client/domino/bin64`. Linux: `/opt/tivoli/tsm/client/domino/bin`) directory. It is also assumed that the system options files in each of these directories has been updated so that the communication parameters point to the Tivoli Storage Manager server.

1. Log in to an account that has root privileges.
2. For AIX: Add the following entry to the `/etc/inittab` file :

   ```
   tdpdom::once:/usr/bin/dsmc sched -optfile=/usr/tivoli/tsm/client
   /domino/bin/dsm.opt /dev/null 2>&1
   #Data Protection for Domino scheduler
   ```

3. The system options file that is defined by Data Protection for Domino is used by the scheduler when validating the node and password. The system options file is also used when contacting the Tivoli Storage Manager server for schedule information. This example assumes that the dsm.sys or dsm.opt file is updated so that the communication parameters point to the Tivoli Storage Manager server to which the Domino databases are to be backed up.

If you see the following message:

```
A communications error occurred connecting to the
Tivoli Storage Manager server
```

You should ensure that the system options file contains entries that point to the correct Tivoli Storage Manager server. You should also ensure that the Tivoli Storage Manager server is running.

4. Now you need to create a script file (or symbolic link to a script file) that is called `/bin/domarc`. You can begin with the domarc.smp file that was placed into the Data Protection for Domino install directory. Notice in this example script:
   a. The default options file (dsm.opt) is overridden on the command line. You may want to change this.
   b. The script ensures the command is run as the Domino server ID. Use the ID you setup.
   c. The **domdsmc** command is run in the background so control is returned to `/usr/bin/dsmc` without needing to wait for the command to complete.

   See *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide* for additional information on the Tivoli Storage Manager backup-archive client environment variables, DSM_DIR, DSM_CONFIG, and DSM_LOG.

   When using the Tivoli Storage Manager scheduler to execute the commands in a command file, you must use the *complete path names* for all file names and non-system commands. This is because the scheduler runs from the AIX, Linux, or UNIX, or system directory. This system directory is where the scheduler looks for input and produces its output by default.

5. At this point the scheduler is installed and configured, but has not started.

   To start the service, issue the following command in the AIX, Linux, or UNIX console window:

   AIX

   ```
   nohup /usr/bin/dsmc sched 2> /dev/null &
   ```

   Linux and UNIX

   ```
   nohup /opt/bin/dsmc sched 2> /dev/null &
   ```

   The following output is displayed:

   ```
   The Tivoli Storage Manager Data Protection for Domino Archive
   Schedule service is starting.

   The Tivoli Storage Manager Data Protection for Domino Archive
   Schedule service was started successfully.
   ```

   Note that because the `/etc/inittab` entry (AIX) and the `/etc/rc` entry (UNIX) is used, the Tivoli Storage Manager scheduler service is automatically started each time the system is rebooted.

   Your system is now ready to run automatic hourly archival of the transactions logs.

Scheduler considerations

This section describes important information to be considered when automating backups.

Consider these characteristics when defining a Tivoli Storage Manager schedule.

To use the Tivoli Storage Manager server prompted scheduling mode, ensure the dsm.opt dsm.syssystem options file has the ***tcpclientaddress*** and ***tcpclientport*** options specified. If you want to run more than one scheduler service, use the same ***tcpclientaddress***. However, you must use different values for ***tcpclientport*** (in addition to the different node names). An example of running more than one scheduler service is when you are scheduling Data Protection for Domino as well as the regular backup-archive client. Server-prompted scheduling is supported only when TCP/IP communication is being used. By default, Tivoli Storage Manager uses the client polling schedule mode.

If any changes that affect the scheduler are made to the Data Protection for Dominosystem options file, the scheduler has to be restarted in order to pick up the changes. An example of this is the Tivoli Storage Manager server address, the schedule mode, or the client TCP address or port. This can be done by issuing the following commands:

```
ps -ef | grep sched
```

Then stop the scheduler using the **kill -s** command. However, do not issue the **kill -9** command to terminate the client. The **kill -9** command bypasses client recovery processes. In this example the program ID number is 34738: Issue the `kill -s SIGINT 34738` command then restart the scheduler using the following command:`nohup /usr/bin/dsmc sched 2> /dev/null &`

The dsmsched.log file contains status information for the Tivoli Storage Manager scheduler. This file is written to the current directory where the (**nohup**) **dsmc sched** command was run.

```
/usr/tivoli/tsm/client/ba/bin64/domsched.log
```

You can override this file name by specifying the ***schedlogname*** option in the Tivoli Storage Managersystem options file.

Output from scheduled commands is sent to the log file. After scheduled work is performed, check the log to ensure the work completed successfully. When a scheduled command is processed the schedule log may contain the following entry:

```
Scheduled event eventname completed successfully
```

This indicates that Tivoli Storage Manager successfully issued the scheduled command associated with the *eventname*. No attempt is made to determine the success or failure of the command. If you look in the dsmsched.log file, you will see a log entry with the following text:

```
Finished command. Return code is: 0
```

This indicates that the command file started successfully. The return code is no indication as to the outcome of the scheduled command. You need to view the Data Protection for Domino log file to determine the success or failure of the scheduled command.

If any scheduled backups fail, the scheduler script will exit with the same error code as the failed backup command. A non-zero error code means that backup failed. When this occurs you should follow the instructions in the Troubleshooting section.

Data Protection for Domino creates its own log file with statistics about the backed up database objects when the ***/logfile*** parameter is specified during the **domdsmc** command. In the sample, the log file is domarc.log. This file is different from the Tivoli Storage Manager scheduler log file and must also be different from the file to which the **domdsmc** command output is redirected. In the domarc.smp example script, domsched.log.arc holds the redirected output.

If Data Protection for Domino is not configured to automatically generate the Tivoli Storage Manager password when it expires, then the Tivoli Storage Manager password needs to be specified on the **domdsmc** command. To specify the password, use the ***/adsmpwd*** option in the command file being run by the scheduler (domarc) or specify it in the Data Protection for Domino preferences file.

The Tivoli Storage Manager client scheduler allows only one scheduler process at a time. Other schedules must wait for the first scheduled backup to complete before they can begin. This can be an issue when a scheduled backup is processing at the same time an archivelog backup is scheduled to begin. For example, assume there are two scheduled Data Protection for Domino backups that run under the same node and scheduler service. The database backup runs at 6:00 and the archivelog backup runs every hour. If the database backup takes longer than one hour, the archivelog backup will fail. You can avoid this issue by creating a new node and a new scheduler service for the archivelog backup. This new node and service only launches the batch (.cmd) file for the archivelog backup. However, make sure the Data Protection for Domino dsm.opt file contains the name of the regular Data Protection for Domino node. For example:

- Data Protection for Domino backups use nodename *DOMClient* as specified in the Data Protection for Domino dsm.opt file.
- The new nodename for the archivelog backup is *DOMSched*.
- The scheduler is associated with the *DOMSchedt* node but the batch (.cmd) file that actiually runs the **domdsmc archivelog** command points to the Data Protection for Domino dsm.opt file that contains the nodename *DOMClient*.

As a result, backup objects will be associated correctly to the Data Protection for Domino node, not the node for the scheduler.

Setting up other schedules

Important information to consider when setting up other schedules.

You should run several other schedules for Data Protection for Domino as part of a complete backup strategy for Lotus Domino databases and transaction logs. In order to setup these other schedules, you just need to follow the above procedures with a few modifications. The modifications are centered around when the events should take place.

Use the `SESSIONS` command to improve performance when scheduling tasks in Data Protection for Domino. More information is available in the Performance section of this guide.

Incremental Backup of all databases

- Frequency - once a day

- Sample command file, dominc.smp, exists in the directory where Data Protection for Domino is installed.
- Domdsmc log file created - dominc.log
- Output redirected - domsched.log.inc

Selective Backup of All Logged Databases

- Frequency - once a week, maybe Saturday
- Sample command file, domsel.smp, exists in the directory where Data Protection for Domino is installed.
- Domdsmc log file created - domsel.log
- Output redirected - domsched.log.sel

Inactive Logs

- Frequency - once a week, maybe Sunday, this is to ensure that the selective backup has completed
- Sample command file, domina.smp, exists in the directory where Data Protection for Domino is installed.
- Domdsmc log file created - domina.log
- Output redirected - domsched.log.ina

Back up all DB2 Groups (DB2 enabled Notes databases)

- Frequency - once a day
- Sample command file, domdb2grp.smp, exists in the directory where Data Protection for Domino is installed.
- Domdsmc log file created - domdb2grp.log
- Output redirected - domdb2grp.out

Full DB2 database backup (DB2 enabled Notes databases)

- Frequency - once a week
- Sample command file, domdb2db.smp, exists in the directory where Data Protection for Domino is installed.
- Domdsmc log file created - domdb2db.log
- Output redirected - domdb2db.out

Sample command files

This section provides sample command files.

AIX

This is an example of the **AIX** domarc.smp file.

```
#!/bin/ksh
#
#  ==================================================================
#   domarc.smp command file
#
#   Command file containing commands to do a scheduled archivelog
#   command to IBM Tivoli Storage Manager.
#
#   This file is meant to be executed by the IBM Tivoli Storage Manager
#   central scheduler in response to a defined schedule on the
#   IBM Tivoli Storage Manager server.
#
#   Complete paths must be given for all file names and non-system
#   commands.
#  ===================================================================
#   Update DOM_ID with your Domino Server UNIX_ID
#  ===================================================================

DOM_ID=notes

export DOM_ID_DIR=/usr/tivoli/tsm/client/domino/bin64/domdsmc_${DOM_ID}

#  ===================================================================
#   Put a date and time stamp in a log file for yourself.
#
#   Note: You can change "domsched.log.arc" to whatever you prefer
#  ===================================================================
date >> ${DOM_ID_DIR}/domsched.log.arc

#  ===================================================================
#   Now call the commandline to do the backups.
#
#   Notes:
#   1) You can change "domarc.log" to whatever you prefer.
#   2) domdsmc must be run by the Domino Server ID. If the scheduler
#      is started from /etc/initab, root is the id that will be running
#      this script. For this situation, we need to "su" to the Server
#      ID before running domdsmc.
#
#  ===================================================================

iam=`whoami`

if [ ${iam} = "root" ]
then
     su - ${DOM_ID} "-c /opt/lotus/bin/domdsmc_${DOM_ID} archivelog
     -adsmoptfile=${DOM_ID_DIR}/dsm.schd.opt
     -logfile=${DOM_ID_DIR}/domarc.log"
     >> ${DOM_ID_DIR}/domsched.log.arc &
else
     /opt/lotus/bin/domdsmc_${DOM_ID} archivelog
    -adsmoptfile=${DOM_ID_DIR}/dsm.schd.opt
    -logfile=${DOM_ID_DIR}/domarc.log
    >>${DOM_ID_DIR}/domsched.log.arc &
fi
```

Linux

This is an example of the **Linux** domarc.smp file.

```
#!/bin/bash
#
#  ===================================================================
#   domarc.smp command file
#
#   Command file containing commands to do a scheduled archivelog
#   command to IBM Tivoli Storage Manager.
#
#   This file is meant to be executed by the IBM Tivoli Storage Manager
#   central scheduler in response to a defined schedule on the IBM Tivoli
#   Storage Manager server.
#
#   Complete paths must be given for all file names and non-system
#   commands.
#  ===================================================================
#   Update DOM_ID with your Domino Server ID
#  ===================================================================

DOM_ID=notes
```

```
export DOM_ID_DIR=/opt/tivoli/tsm/client/domino/bin/domdsmc_${DOM_ID}

#  ==================================================================
#    Put a date and time stamp in a log file for yourself.
#
#    Note: You can change "domsched.log.arc" to whatever you prefer
#  ==================================================================
date >> ${DOM_ID_DIR}/domsched.log.arc

#  ==================================================================
#    Now call the commandline to do the backups.
#
#    Notes:
#      1) You can change "domarc.log" to whatever you prefer.
#      2) domdsmc must be run by the Domino Server ID. If the scheduler
#         is started from /etc/initab, root is the id that will be running
#         this script. For this situation, we need to "su" to the Server
#         ID before running domdsmc.
#
#  ==================================================================

iam=`whoami`

if [ ${iam} = "root" ]
then
     su - ${DOM_ID} -c "/opt/lotus/bin/domdsmc_${DOM_ID} archivelog
-adsmoptfile=${DOM_ID_DIR}/dsm.schd.opt
-logfile=${DOM_ID_DIR}/domarc.log"
>> ${DOM_ID_DIR}/domsched.log.arc &
else
     /opt/lotus/bin/domdsmc_${DOM_ID} archivelog
-adsmoptfile=${DOM_ID_DIR}/dsm.schd.opt
-logfile=${DOM_ID_DIR}/domarc.log
>>${DOM_ID_DIR}/domsched.log.arc &
fi
```

Recovery from loss of Domino transaction logs for NSF databases

This section describes how to recover from a loss of the Domino server (including the transaction log) for NSF databases so that archived transaction log files can still be used for database recovery.

When using archival transaction logging, archived transaction log files contain updates to logged databases that may not yet be captured in a full database backup. Recovery of a database to the most current available backup requires restoring the last full backup plus applying updates to that backup from the archived transaction log files. However, in order for archived transaction log files to be used for database recovery, the current transaction log ID must match that of the archived log files. If the current transaction log is lost, creating a new one will result in a new log ID and thus the archived log files would not be usable for database recovery.

1. Recover the non database Domino server files. If necessary, reinstall (but do not configure) the server and restore the non database Domino files (including notes.ini, cert.id, and server.id) using your file backup solution (such as the Backup-Archive Client). Make sure the new installation is configured in the same manner as the damaged one (for example, the same directory structure, directory location, and `logdir` path). Do not launch the new server.
2. Using a text editor, modify the notes.ini file for the Domino server with this setting: `TRANSLOG_Status=0`

3. Using Data Protection for Domino, restore the transaction log file to be used in the log recovery procedure. This should be the last transaction log file archived prior to the loss of the active transaction log.

   Note: Use the `-replace=no` option as an added safety measure.
4. Delete the contents of the Domino transaction log directory except for the log file restored in Step 3.
5. Modify the `notes.ini` file for the Domino server with these settings: `TRANSLOG_Recreate_Logctrl=1TRANSLOG_Status=1`
6. Restore (but do not activate) the databases you want to recover to the latest state within the archived log extents using Data Protection for Domino.
7. Use Data Protection for Domino to activate the databases you are recovering and apply transaction logs. (The TRANSLOG_Recreate_Logctrl parameter in the notes.ini file will be automatically reset to 0).
8. Launch the Domino server. With the disaster recovery complete, it is now safe to start the Domino server and execute server tasks and functions.
9. Use the Selective backup function in Data Protection for Domino to perform full backups of all databases. (This will ensure proper recoverability using subsequent transaction log files).
10. Use Data Protection for Domino to archive the transaction log. The transaction log file used in the recovery procedure will be modified and available for archiving. This transaction log will also have the ID of the current logger.

Alternate server and alternate partition restores for NSF databases

This section provides an overview of alternate server and alternate partition restores.

You must perform alternate server restores when possible to reduce demands on the production Domino server.

A restore operation involves two steps. First, the backup copies of the databases are retrieved for the Tivoli Storage Manager server. Second, the recorded transactions in the log files are applied to the databases. If the transaction log files required to recover the databases have been archived, they will be retrieved from the Tivoli Storage Manager server. These steps can impact performance in the CPU (application of transactions) and in disk input and output (retrieval of the database backup copies and the archived transaction logs).

The transaction log directory must reside on a dedicated physical disk drive for optimal performance. When a dedicated physical disk drive is used, the Domino server can write transactions sequentially to the log, which is faster than writing transactions to random nonsequential parts of a disk. If the restore operation is performed on a production Domino Server, the restore of the transaction log and application of the transactions will interfere with the normal Domino server sequential writing of transactions to the log. This will affect the performance of the Domino server and increase the time required to perform the restore operation. The application of the transaction logs will also compete for CPU cycles with the Domino server.

Restore operations must be performed on an alternate server or on an alternate partition for these reasons.

An alternate server restore is the preferred method since the restore operation has no impact on the performance of the production Domino server. However, the production Domino server and the server on the alternate partition can use separate disk drives for their transaction log directory. If the separate disk drives are used, the production Domino server access to the transaction log will not be affected by the restore operation on the alternate partition.

Note: Domino 6 allows the user to specify an alternate path where to restore the archived transaction logs. If a separate disk drive is used by the alternate path, the alternate path feature can be used to minimize the cost of a restore operation on the production Domino server.

How to perform an alternate server restore for NSF databases

This section describes how to perform an alternate server restore for NSF databases.

This procedure describes how to use an alternate server to restore logged databases.

Production Server Domino Environment

- Installation directory: `/opt/lotus`
- Data Directory: `/production/notesdata`
- Notes User: `notesp`
- Database to be restored: `restoredb.nsf`

Alternate Server Domino Environment

- Installation directory: `/opt/lotus`
- Data Directory: `/alternate/notesdata`
- Notes User: `notesa`

1. Install Domino server on a separate machine.
   a. This must be the same level of Domino server as used on the production server. Do not configure this Domino server.
   b. If using an existing Domino server, make sure the server is stopped.
2. Install Data Protection for Domino on this same machine and perform the following:
   a. Run the **dominstall** program. See “Performing a manual dominstall configuration” on page 23 for more information.
   b. Update the Notes user environment as created by the **dominstall** program.
   c. Update the dsm.opt and dsm.sys files so they contain the same settings as the dsm.opt and dsm.sys files on the production server.
   d. If the ***nodename*** option is not set in the Tivoli Storage Manager server stanza, add the ***nodename*** option and specify the host name of the production server.
   e. Verify that you can successfully run the **domdsmc q adsm** command.
3. Create the following directories (as the Notes user) on the alternate server:
   a. A directory to contain the restored databases. (If using an existing directory, make sure the directory is empty). For example:`/alternate/notesdata/restoredb`
   b. A directory to contain the restored log files. (If using an existing directory, make sure the directory is empty). For example: `/alternatelog`

4. Create (as the Notes user) a notes.ini file on the alternate server with the following values: `[Notes] Directory=<directory for restored databases> KeyFilename=<directory for restored databases>/server.id TRANSLOG_Status=0 TRANSLOG_Style=1 TRANSLOG_Path=<directory for restored transaction logs> TRANSLOG_MEDIAONLY=1`. This notes.ini file can be located in any directory of your choice.
   a. If you place the notes.ini file in the alternate server data directory, save a copy of the existing notes.ini file. For example:`mv notes.ini notes.save`
   b. If you place the notes.ini file in a directory other than the alternate server data directory, update the Data Protection for Domino preferences file (domdsm.cfg by default) to point to the location of this notes.ini file: `DOMDSMC SET Notesinipath=<directory for notes.ini>`
   c. This notes.ini file is used only during this alternate server restore process. Note that transaction logging is disabled at this point. For example, `/alternate/notesdata/notes.ini[Notes] Directory=/alternate/notesdata/restoredb KeyFilename=/alternate/notesdata/restoredb/server.id TRANSLOG_Status=0 TRANSLOG_Style=1 TRANSLOG_Path=/alternatelog TRANSLOG_MEDIAONLY=1`
5. Place a copy of the server.id file (from the production Domino server) on the alternate server in the directory created for restored databases. Change the permissions of the server.id file to be accessible to the alternate server Notes user.
6. Perform an archive of the transaction log (as the Notes user) on the production server. For example: `domdsmc archivelog`
7. Restore (as the Notes user) one of the following on the alternate server:
   a. The last archived transaction log file. This is the transaction log file to be used in the log recovery procedure. For example: `domdsmc restorelogarchive`
   b. A transaction log file to be restored from an old Logger ID. This may be necessary if you are trying to restore and apply transactions for a logged database that used an old Logger ID. See "Domdsmc Activatedbs" on page 53 for a description of when this type of restore may be necessary. Run the **restorelogarchive** command with the ***pick*** option and choose the desired log extent. For example: `domdsmc restorelogarchive` *`logname`* `/pick=showall`
8. On the alternate server, modify (as the Notes user) the `notes.ini` file to enable transaction logging: `TRANSLOG_Status=1` This is the `notes.ini` file created in Step 3 for the alternate server restore process only.

   Note: The Lotus Domino server must be restarted and then stopped so that it can recognize the changes made to the `notes.ini` file.
9. On the alternate server, restore (as the Notes user) but do not activate the databases you want to recover to their latest state. Activation at this step triggers the Domino transaction log recovery process which requires considerable processing time. For example: `domdsmc restore restoredb.nsf`.
10. On the alternate server, activate (as the Notes user) the databases you are recovering and apply transaction logs. For example: `domdsmc activate /applylogs`
11. At this point you can perform the following:
    - copy the recovered databases to the production Domino server, or
    - access the recovered databases through a remote Notes client to copy individual documents.

Do not attempt to open or access the restored databases with the alternate Domino server if the databases are to be copied to the production Domino server. If you access them with the alternate Domino server, they will require corrections to resolve inconsistencies on the production Domino server.

12. If the Domino server used for the recovery is a configured server and you saved the notes.ini file in Step 3, copy that notes.save file back to notes.ini to be able to launch the server.

How to perform an alternate partition restore for NSF databases

This section provides step by step instructions on how to restore an alternate partition for NSF databases.

This procedure describes how to use an alternate partition to restore logged NSF databases.

This procedure assumes the following environment:

Domino Environment

- Installation directory: `/opt/lotus`
- Production Partition Data Directory: `/production/notesdata`
- Production Partition Notes User: `notesp`
- Production Partition Notes Group: `notes`
- Alternate Partition Data Directory: `/alternate/notesdata`
- Alternate Partition Notes User: `notesa`
- Alternate Partition Notes Group: `notes`
- Database to be restored: `restoredb.nsf`

1. Install an alternate partition if one is not available. See your Domino Server documentation for information on how to install an alternate partition.
   a. You do not need to configure this alternate partition.
   b. If using an existing alternate partition, make sure the server on that partition is stopped.
2. Configure Data Protection for Domino for multiple partitions (if you have not already done so):
   a. Run the **dominstall** program. See "Performing a manual dominstall configuration" on page 23 for more information.
   b. Update the alternate partition Notes user environment as created by the **dominstall** program.
   c. Update the dsm.opt file so it contains the same settings as the dsm.opt file on the production server.
   d. Verify that you can successfully run the **domdsmc q adsm** command as the alternate partition Notes user.
3. Create the following directories (as the alternate partition Notes user):
   a. A directory to contain the restored databases. (If using an existing directory, make sure the directory is empty). For example:`/alternate/notesdata/restoredb`
   b. A directory to contain the restored log files. (If using an existing directory, make sure the directory is empty). For example: `/alternatelog`
4. Create (as the alternate partition notes user) a notes.ini file with the following values: `[Notes] Directory=<directory for restored databases>`

`KeyFilename=<directory for restored databases>/server.id TRANSLOG_Status=0 TRANSLOG_Style=1 TRANSLOG_Path=<directory for restored transaction logs> TRANSLOG_MEDIAONLY=1` This notes.ini file can be located in any directory of your choice.

   a. If you place the notes.ini file in the alternate partition data directory, save (as the alternate partition Notes user) a copy of the existing notes.ini file. For example: `mv notes.ini notes.save`
   b. If you place the notes.ini file in a directory other than the alternate partition data directory, update (as the alternate partition Notes user) the Data Protection for Domino preferences file (domdsm.cfg by default) to point to the location of this notes.ini file: `domdsmc set notesinipath=<directory for notes.ini>`
   c. This notes.ini file is used only during this alternate partition restore process. Note that transaction logging is disabled at this point. For example, in the file `/alternate/notesdata/notes.ini[Notes] Directory=/alternate/notesdata/restoredb KeyFilename=/alternate/notesdata/restoredb/server.id TRANSLOG_Status=0 TRANSLOG_Style=1 TRANSLOG_Path=/alternatelog TRANSLOG_MEDIAONLY=1`

5. Place a copy of the server.id file (from the production Domino server) on the alternate server in the directory created for restored databases. Change the permissions of the server.id file to be accessible to the alternate partition Notes user.
6. Perform an archive of the transaction log (as the production server Notes user) on the production server. This allows you to apply the latest updates from the transaction log to the restored database. As the production server Notes user, run the following command: `domdsmc archivelog`
7. Restore (as the alternate partition notes user) one of the following to the transaction log directory:
   a. The last archived transaction log file. This is the transaction log file to be used in the log recovery procedure. Run the following command as the alternate partition Notes user: `domdsmc restorelogarchive`
   b. A transaction log file to be restored from an old Logger ID. This may be necessary if you are trying to restore and apply transactions for a logged database that used an old Logger ID. See “Domdsmc Activatedbs” on page 53 for a description of when this type of restore may be necessary. Run the **restorelogarchive** command (as the alternate partition Notes user) with the ***pick*** option and choose the desired log extent. For example:`domdsmc restorelogarchive` *`logname`* `/pick=showall`
8. As the alternate partition Notes user, modify the notes.ini file to enable transaction logging: `TRANSLOG_Status=1` This is the notes.ini file created in Step 4 for the alternate partition restore process only.
9. As the alternate partition Notes user, restore (but do not activate) the databases you want to recover to their latest state.

   Attention: Warning! Activation at this step triggers the Domino transaction log recovery process which requires considerable processing time. Run the following command as the alternate partition Notes user: `domdsmc restore restoredb.nsf`
10. As the alternate partition Notes user, activate the databases you are recovering and apply transaction logs. Run the following command as the alternate partition Notes user: `domdsmc activate /applylogs`
11. At this point you can perform the following:
    -

   a. copy the recovered databases to the production Domino server, or
   b. access the recovered databases through a remote Notes client to copy individual documents.

   Do not attempt to open or access the restored databases with the alternate Domino server if the databases are to be copied to the production Domino server. If you access them with the alternate Domino server, they will require corrections to resolve inconsistencies on the production Domino server.

12. If the alternate partition has been configured and you saved the notes.ini file in Step 4, copy that notes.save file back to notes.ini to be able to launch the server.

Include and exclude processing

This section provides information related to include and exclude processing.

Considerations

Data Protection for Domino deals only with Domino databases and transaction log files (if archival logging is in effect on the Domino server). Other files that may exist on the server are not backed up by Data Protection for Domino so they need not be excluded. However, if you want to limit the backups to a subset of the databases on your Domino server, the standard include/exclude syntax can be used.

Read the documentation about include/exclude processing included in the base Tivoli Storage Manager backup-archive client as a thorough introduction to processing concepts. Then, review the Examples section below regarding Data Protection for Domino.

Examples

Domino databases are stored by their relative names on the Tivoli Storage Manager server. As result, relative names must be used in include/exclude statements. That means the notes data directory should not be specified, and databases linked to the notes data directory by database or directory links must be referenced by the symbolic name. Do not use fully qualified physical file names.

A single database backup is stored as two objects on the Tivoli Storage Manager server. The objects created are the relative database name and the relative database name plus a *.DATA* extension. For example, a backup of database `mail6\user1.nsf` would result in the following two objects:

1. The relative name of the database:
   ```
   mail6/user1.nsf
   ```
2. The relative name of the database plus *.DATA*:
   ```
   mail6/user1.nsf.DATA
   ```

As a result, when excluding a group of databases (for example, all databases in a directory) and then including a specific subset of that group, you must be sure to include both objects. For example, to exclude all databases in directory `mail6` except for database *user1.nsf*, code the following statements:

```
EXCLUDE mail6/*
INCLUDE mail6/user1.nsf
INCLUDE mail6/user1.nsf.DATA
```

Note: When excluding a specific database, the *.DATA* object need not be excluded explicitly because the *.DATA* object will not be created unless the database is included.
When assigning a group of databases to a management class, you must assign both objects. For example, to assign all databases that match `*.nsf` in the `mail6` subdirectory to the `DOMINO` management class, code the following statement:

```
INCLUDE mail6/*.nsf* DOMINO
```

If archival logging is in effect on the domino server, you must be sure not to exclude the transaction log files from backup. The transaction logs have a base object name of *S######.TXN* (the "#" character represents a number). If you code a broad exclude statement, make sure you include the transaction log files by coding a statement as follows:

```
INCLUDE S*.TXN
```

Exclude databases that increase in size during compression (***compression****yes*) by using the client option, ***exclude.compression***. You must specify the *.DATA* object to exclude a database from compression. For example, to exclude the database `mail6/user1.nsf` from compression, enter:

```
EXCLUDE.COMPRESSION mail6/user1.nsf.*
```

See *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide* for more information about the ***exclude.compression*** option.

You can encrypt Domino databases during backup and restore processing by specifying `enableclientencryptkey=yes` in the dsm.sys file.. In the same file, specify the databases you want encrypted by adding an include statement with the ***include.encrypt*** option. For example, to encrypt all data, specify the following:

```
include.encrypt /.../*
```

To encrypt only the Mydb.nsf database in the default directory, specify the following:

```
include.encrypt Mydb.nsf
include.encrypt Mydb.nsf.DATA
```

or

```
include.encrypt Mydb.nsf*
```

To encrypt all databases in the `mail65` directory, specify the following:

```
include.encrypt mail65/.../*
```

Note that transparent encryption is only available on Tivoli Storage Manager server Version 5.3 (or later).

You can choose to include backup or archive files for data deduplication. To refine the list of files to be included, the `include.dedup` option can be used in combination with the `exclude.dedup` option. By default, all eligible objects are included for data deduplication. The following examples show how to use the include and exclude options:

```
exclude.dedup /FS1/.../*
```

```
include.dedup /FS1/archive/*
```

Exclude all databases named *db1.nsf* regardless of where they appear:

```
EXCLUDE db1.nsf
```

Exclude all databases that match *help5_** in the `help` subdirectory:

```
EXCLUDE help/help5_*
```

Include all databases in the `mail6` directory:

```
INCLUDE mail6/.../*
```

Assign all databases that match `*.nsf` in the `mail` subdirectory to the `MAILDB` management class:

```
INCLUDE mail/*.nsf* MAILDB
```

Exclude all databases in the `mail6` subdirectory from compression:

```
EXCLUDE.COMPRESSION mail6/.../*
```

The default INCLUDE/EXCLUDE lists.

```
EXCLUDE mail.box
EXCLUDE log.nsf
```

Note: You can back up the *log.nsf* database but you can only restore it to an alternate name.

Include all transaction logs:

```
INCLUDE S*.TXN
```

Domino DB2

Include and exclude statements can be specified for table space backups and for full DB2 database backups. The administrator can use include/exclude statements to manage the meta objects (created by Data Protection for Domino) and the data objects (created by DB2 API). The management class assigned to meta objects is forced on the data objects created by the DB2 API. The include/exclude statements specification for meta objects is based on the naming convention for the meta object group leaders. To assign management classes to DB2NSF databases, the user must use the Tivoli Storage Manager object name of the full DB2 group leader object, or the Tivoli Storage Manager object name of the table space group leader object.

Domino DB2 example (full DB2 backup)

The following statement includes all DB2 databases assigned to management class `MGMTC1`, located on partition `NODE000`, that reside on the Domino 7 Server during a full DB2 backup:

```
INCLUDE /domino7.DOMDBS/NODE0000/FULL/DOMINO  MGMTC1
```

The following statement includes all DB2 databases assigned to management class `MGMTC1`, located on all partitions that reside on all available Domino servers during a full DB2 backup:

```
INCLUDE /.../FULL/*    MGMTC1
```

Domino DB2 example (table space backup)

This statement includes DB2 Group `GRP1`:

```
INCLUDE GRP1
```

This statement assigns DB2 Group `GRP2` to management class `DB2GROUPS`:

```
INCLUDE GRP2 DB2GROUPS
```

This statement excludes all DB2 Groups in `CLASS1`:

```
EXCLUDE CLASS1/*
```

This statement includes all DB2 Groups in `CLASS2`:

```
INCLUDE CLASS2/*
```

This statement excludes DB2 Group `GRP1` in `CLASS3`:

```
EXCLUDE CLASS3/GRP1
```

Multiple Domino server partitions

This section provides information about how to set up Data Protection for Domino in multiple Domino server partitions.

This section is valid only if you installed multiple Domino server partitions with the *same*UNIX or Linux user ID. If the Domino server partitions have *unique*UNIX or Linux user IDs, the **dominstall** program sets the environment for you in the .profile file. If you installed multiple Domino server partitions with the *same*UNIX or Linux user ID, it is required that you add the data directory for the partition you want to access to the PATH environment variable before running **domdsmc**. For example, copy the `domdsmc_<notes_user>/<notes_user>.profile` file and then update the PATH variable. To access Partition A, update a copy of the `<notes_user>.profile` file and export the following:

```
PATH=/opt/lotus/bin:/partitionA/notesdata:$PATH
```

To access Partition B, update the other copy of the .profile file and export the following:

```
PATH=/opt/lotus/bin:/partitionB/notesdata:$PATH
```

Otherwise, create multiple Data Protection for Domino preferences files as described below.

To use Data Protection for Domino with multiple Domino server partitions on a single machine, you must specify which partition you want to work with by identifying the location of the notes.ini file for that partition. In addition, when working with multiple Domino partitions, you should have separate Data Protection for Domino log files for each server instance. Since the log file to be used is also specified in the Data Protection for Domino preferences (by the ***logfile*** option), the method to support multiple Domino partitions is to create multiple preference files as follows:

1. Use the **set** command with the ***configfile*** option to define a preferences file for each Domino partition to be supported. Make sure to specify the full path to the preferences file and be sure to set the ***logfile*** value appropriately. For example:

   ```
   domdsmc set notesinipath=/local/notesdata1/   /configfile=domino1.cfg
   domdsmc set logfile=domdsm1.log  /configfile=domino1.cfg
   domdsmc set notesinipath=/local/notesdata2/  /configfile=domino2.cfg
   domdsmc set logfile=domdsm2.log  /configfile=domino2.cfg
   ```

   Other Data Protection for Domino preferences can be set as desired for each partition. However, in order to identify the Domino server, the ***notesinipath*** parameter MUST be specified for each partition.
2. Use the ***configfile*** option when invoking the Data Protection for Domino executable to identify which preferences file is used for the command execution and thus which Domino partition will be accessed. For example:

   ```
   domdsmc selective "*"  /configfile=domino1.cfg
   domdsm  query domino "*"  /configfile=domino2.cfg
   ```

Data Protection for Domino uses the DOMI_CONFIG environment variable to locate the Data Protection for Domino preferences file so it is also possible to adjust that environment variable to point to the desired file before using the **domdsmc** command. If the ***/configfile*** command line parameter is used, it will take precedence over the environment variable value. Make sure to specify the full path to the preferences file.

Multiple Tivoli Storage Manager servers

This section describes how to use Data Protection for Domino with multiple Tivoli Storage Manager servers.

To use Data Protection for Domino with multiple Tivoli Storage Manager servers, create multiple server stanzas in the dsm.sys file, use separate client option files (one for each Tivoli Storage Manager server) specifying the appropriate server name within each and then use the ***/adsmoptfile*** parameter with the Data Protection for Domino executables to identify the desired server.

For example, assuming you have created dsmserv1.opt and dsmserv2.opt to specify different servername values which identify the address and communication parameters necessary to access two Tivoli Storage Manager servers, you can access the two servers as follows:

```
domdsmc selective "*"  /adsmoptfile=dsmserv1.opt
```

```
domdsmc query dbbackup  /adsmoptfile=dsmserv2.opt
```

Data Protection for Domino uses the DSMI_CONFIG environment variable to locate the Tivoli Storage Manager client option file so it is also possible to adjust that environment variable to point to the desired file before using the **domdsmc** command. If the ***/adsmoptfile*** command line option is used, it will override the environment variable value. Make sure to specify the full path to the options file. Please refer to the *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide*, for further information on defining the Tivoli Storage Manager system options file (dsm.sys) with multiple server stanzas.

Problem determination

If an error condition occurs during an Data Protection for Domino event, there are several sources of information you can view to help determine what the problem might be. Information on how to locate information to resolve problems is provided.

The sources of information are listed below.

Data Protection for Domino logs information, by default, to the domdsm.log file in the directory where Data Protection for Domino is installed. This file indicates the date and time of a backup, data backed up, and any error messages or completion codes. This file is very important and should be monitored daily.

The Tivoli Storage Manager API logs API error information, by default, to the dsierror.log file in the directory where Data Protection for Domino is installed. This file does not contain backup statistics.

The Domino server logs information to the AIX, Linux, or UNIX, Domino Event Log. Domino server error information can be obtained by viewing the AIX, Linux, or UNIX, Domino Event Log.

The Tivoli Storage Manager scheduler logs information to both the dsmsched.log and the dsmerror.log files. By default, these files are located in the directory where the Tivoli Storage Manager backup-archive client is installed.

Note: When a scheduled command is processed the schedule log may contain the following entry: `Scheduled event` *`eventname`* `completed successfully` This indicates that Tivoli Storage Manager successfully issued the scheduled command associated with the *eventname*. No attempt is made to determine the success or failure of the command. You should assess the success or failure of the command by evaluating the return code from the scheduled command in the schedule log. The schedule log entry for the command's return code is prefaced with the following text: `Finished command. Return code is:`

The ***statistics*** option provides performance information at the individual database backup or restore level. Statistics are logged to the Data Protection for Domino log file (domdsm.log by default). Make sure this option is specified in the Data Protection for Domino preferences file (domdsm.cfg by default) during backup and restore processing.

If the sources of information listed above do not provide an answer to your problem, contact your IBM service representative. The IBM service representative can provide additional ways to gather diagnostic information.

You may be asked to provide these files as part of the troubleshooting process:

- `dsm.opt`
- `dsmerror.log`
- `dsmsched.log`
- `domdsm.log`
- `dsierror.log`
- `tdpdommustgather.out`

You may be asked to run these commands :

```
echo "------domdsmc query adsm------" >> tdpdommustgather.out
domdsmc query adsm >> tdpdommustgather.out
echo "------domdsmc query domino------" >> tdpdommustgather.out
domdsmc query domino >> tdpdommustgather.out
echo "------domdsmc query preferences------" >> tdpdommustgather.out
domdsmc query preferences >> tdpdommustgather.out
echo "------set------" >> tdpdommustgather.out
set >> tdpdommustgather.out
reg query HKLM\software\ibm\adsm\currentversion /s >> tdpdommustgather.out
```

Information on how to configure Tivoli Storage Manager compression, encryption and deduplication is available in the Using the Application Programming Interface guide in the Tivoli Storage Manager Information Center.

Migration

This section describes migration scenarios.

Backups performed by Data Protection for Domino on a Domino 6.5.x or 7.x Server can be restored using Data Protection for Domino on a Domino 8 Server. However, backups performed by Data Protection for Domino on a Domino 8 Server *can only be restored* by a Domino 8 Server.

The following sections provide two possible migration scenarios. The scenario you choose depends on whether your database environment is using replicated servers. For migration replicated servers should be used. This environment allows for a smooth transition from a Domino 6.5.x or 7.x Server to Domino 8 Server while keeping existing backup data available until you determine that it is no longer required.

Migration in a replicated server environment

The steps required to migrate in a replicated server environment.

Replicated servers means that your environment contains two or more servers with replicated databases.

With replicated servers perform the following:

1. Install the Domino 8 Server on one of the replicated Notes servers.
2. On the same server install Data Protection for Domino 6.3.
3. Stop taking backups on the Domino 6.5.x or 7.x server and begin with full backups using Data Protection for Domino 6.3 (or continue backups in parallel on both servers until full new production environment is in place). Because Domino supports replication between servers, restores of backup data taken with the current Notes Tivoli Storage Manager can be done using the current Notes Tivoli Storage Manager on the Domino 6.5.x or 7.x server and replication will propagate it to the new Domino 8 server. Similarly, if a restore is done to the Domino 8 server using Data Protection for Domino 6.3, that restored database can be replicated to the Domino 6.5.x or 7.x server.
4. Once you are satisfied with the stability of the new Domino 8 server and the new backup scheme, the other replicated server or servers can be upgraded with the new Domino 8 Server and Data Protection for Domino 6.3.

Migration in a nonreplicated server environment

This section describes the tasks required to migrate in a non-replicated server environment.

When a second server is not available for replication, perform the following:

1. Before upgrading the server to Domino 8.5.2 server, take a full offline backup of the databases using the regular Tivoli Storage Manager client.
2. Install Domino 8.5.2 on the server.
3. Install Data Protection for Domino 6.3.
4. Begin with full backups using Data Protection for Domino.

If necessary, the Domino 6.5.x or 7.x version of the databases can be recovered using the regular Tivoli Storage Manager Backup-Archive client.

Using Data Protection for Domino to back up and restore Lotus Domino databases with DAOS

Data Protection for Domino can back up and restore online and offline Domino 8.5 NSF and NTF databases and transaction logs. This document provides an overview of the Data Protection for Domino product, and describes the additional steps necessary to back up and restore Domino 8.5 NLO files.

Overview

IBM Lotus Domino server version 8.5 employs the Domino attachment and object service to save significant space at the file level by sharing data identified as identical between databases (applications) on the same server in NLO files. In databases that use DAOS, the Domino server no longer saves a separate and complete copy of every document attachment. Instead, the server saves a reference to each attached file in an NLO file, and it refers to the same NLO file from multiple documents in one or more databases on the same server.

NLO files can be present on a Domino 8.5 server if DAOS is enabled on the server, and DAOS participation has been elected for some of the NSF databases. NLO files are not supported by Data Protection for Domino. They must be backed up and restored using the Tivoli Storage Manager Backup -Archive Client. If DAOS is not enabled for an individual NSF, or on the server, the current Data Protection for Domino backup and restore procedures is followed.

Note: More information on using Data Protection for Domino to back up and restore Lotus Domino databases can be found in this field guide: https://www.ibm.com/support/docview.wss?uid=swg27015114&aid=1

Domino server backup and restore strategy considerations

You can choose different backup strategies depending on your specific requirements regarding network traffic, backup window, and acceptable restore times. Your choice of strategy includes selecting the type of backup commands to use and the type of transaction logging to be done on the Domino server.

Considerations when using Data Protection for Domino to back up NSF and NTF databases

Data Protection for Domino provides backup and restore functions for the Domino NSF and NTF databases (including template files) and associated transaction logs. However, Data Protection for Domino does not provide a complete disaster recovery solution for a Domino server by itself. You must use the Tivoli Storage Manager backup-archive client with Data Protection for Domino for a complete disaster recovery solution.

Considerations when using the Tivoli Storage Manager backup-archive client to backup NLO files

- Data Protection for Domino does not process NLO files; instead , the Tivoli Storage Manager backup-archive client must be used to back up and restore NLO files.
- NLO files are not modified after they are created, so only new NLO files must be processed when doing an incremental backup. The backup of the NLO files is done after the backup of the NSF and NTF databases. Thus ensuring that the NLO files in the backup are a superset of what is referenced by the NSF databases.
- The DAOS deferred delete interval is set to be longer than the interval between backups. If the backups are done weekly, the shortest DAOS deferred delete interval is eight days. Setting the delete interval longer than the backup interval guarantees that all NLO files are backed up.
- If there is a retention limit for backups, the DAOS delete interval must be set to longer than that retention limit to ensure that all referenced NLO files exist if an NSF database is restored from the oldest backup.

Considerations when using the Tivoli Storage Manager backup-archive client to back up execution and configuration files

There are many files that are part of the Domino server installation, such as execution and configuration files, which include the DAOS configuration file `daos.cfg`. This configuration file is not supported by Data Protection for Domino and must be part of your recovery strategy.

An example is database link files, which have an nsf extension but are not considered databases and are not backed up by Data Protection for Domino. These files must be recovered in a disaster recovery situation. A comprehensive disaster recovery plan can be achieved using the Tivoli Storage Manager backup-archive client with Data Protection for Domino.

Personal copies (replicas) of Domino databases that are stored on Notes clients (not on the Domino server) are not protected by Data Protection for Domino. You can use the Tivoli Storage Manager backup-archive client on the Notes client platform to back up and restore these files or rely on Domino server replication if you must recover them.

Other Considerations

To restore an individual Notes document, you must restore the entire database with another name. Choose a time when the document existed for both the restore /pit and activate /applylogs commands, but before the document was deleted. Then copy the desired document using the Notes client.

Data Protection for Domino can only back up transaction logs from a Domino server that has archival logging in effect. Transaction logs cannot be backed up from a Domino server that has circular or linear logging in effect.

When using archival transaction logging, the frequency of the **`archivelog`** command use depends on the size of your log and the rate of change for logged databases. Perform archival transaction logging several times per day if you generate a large volume of changes at a rapid rate.

When restoring a group of logged databases for which transactions must be applied, activate them together when possible. This avoids restoring the same transaction log files multiple times. Restored transaction log files are deleted during a database recovery by the Domino server. Activating and applying logs to the database separately requires retransmitting log files for each database.

Using Data Protection for Domino to back up a Lotus Domino database with DAOS

Data Protection for Domino can perform full and incremental online backups of individual NSF and NTF databases when archival logging is in effect. If archival logging is not in effect, only full offline backups of NSF databases can be performed. NSF and NTF databases should be backed up using Data Protection for Domino to ensure that an internally consistent image of the NSF is saved, and that the Domino transaction logs are archived as part of the backup process. Attempting to back up an NSF or NTF database without using Data Protection for Domino while the Domino server is running (and possibly in the process of modifying the file), could result in an unusable image being saved. Data Protection for Domino provides two types of database backups, incremental and selective.

Performing an incremental backup

An incremental backup performs a full online backup of Domino databases under the following conditions:

1. The database is within the Domino data path or is symbolically linked to the Domino data path by directory or database links.
2. The database is not excluded from backup by exclude statements within the Tivoli Storage Manager include-exclude options file.
3. If the database is logged, the DBIID has changed.
4. If the database is not logged, it has been modified since the last backup occurred (data and non-data modification dates are checked).
5. The database is new or newly included in the backup.

The **`incremental`** command includes a function that determines if active backup database copies exist on the Tivoli Storage Manager server that were deleted from the Domino server or excluded from backup. If so, they are marked inactive so automatic expiration of these backup copies can occur according to defined management class parameters for backup files.

The **`incremental`** command normally specifies a wildcard qualified name. The databases that match the wildcard qualification and meet the selection criteria for an incremental backup are backed up. Use the Tivoli Storage Manager backup-archive client **`incremental`** command to back up NLO files because when they are written they are never changed.

If selective backups of the NLO files are made, each additional backup of the same file results in an identical additional backup. If incremental backups of the NLO files are made, only a single backup file is created. When backing up NSF and NLO files, first backup the NSF databases and then backup the NLO files.

The Data Protection for Domino command to incrementally back up NSF databases is:

```
domdsmc incr database_selection_criteria
```

The Tivoli Storage Manager backup-archive client command to incrementally back up all NLO files is:

```
 dsmc incr /local.notesdata/daos/* -su=yes
```

The Tivoli Storage Manager backup-archive client incremental backup command of the NLO files must specify the fully qualified path name of the NLO files to be backed up.

Performing a selective backup

A selective backup unconditionally backs up the specified databases, unless they are excluded from backup through exclude statements within the Tivoli Storage Manager include - exclude options file.

You should not use the Tivoli Storage Manager backup-archive client selective command to back up NLO files, because when they are written they are never changed. If selective backups of the NLO files are made, each additional backup of the same file results in an additional identical backup. When backing up NSF, NTF, and NLO files, first backup the NSF and NTF databases, and then incrementally backup the NLO files .

The Data Protection for Domino command to selectively back up NSF databases is:

```
domdsmc sel database_selection_criteria
```

The Tivoli Storage Manager backup-archive client command to incrementally back up all NLO files is:

```
dsmc incr /local.notesdata/daos/* -su=yes
```

Domino Transaction Log Archive

Data Protection for Domino provides the capability to create archives of transaction logs when archival logging is in effect. There are no changes required in archiving Domino transaction logs when DAOS is enabled. A transaction log captures database changes so full database backups are not required as frequently. Updates to a logged database are recorded in the Domino server transaction log. Changes to a database since the last full backup can be applied from the transaction log after the backup is restored from the last full backup. Enabling transaction logging for all databases on a Domino server is not required, so the backup process must handle databases that are logged and not logged.

Domino allows the active transaction log to be backed up as well. The Data Protection for Domino archive log capability stores filled transaction log files on the Tivoli Storage Manager server so that space allocated for these files can be reused by the Domino logger.

The **`archivelog`** command is available when transaction logging on the Domino server is enabled in archival mode. Filled transaction log files must be archived frequently enough to ensure the transaction log never fills completely and stops the Domino server. Transaction log files stored on the Tivoli Storage Manager server are automatically restored as needed for a database recovery. Archived transaction log files are retained on the Tivoli Storage Manager server as long as a database backup exists that needs these log files for a complete recovery.

The Data Protection for Domino command to archive the Domino server transaction log is:

```
domdsmc archivelog
```

When circular or linear loop logging is used on the Domino server (or when logging is disabled on the Domino Server), transaction log files are not archived.

Using Data Protection for Domino to restore a Lotus Domino database with DAOS

The restoration of a Domino NSF or NTF database is a two-step recovery process.

1. Use the Data Protection for Domino **`domdsmc restore`** command to restore one or more databases from the Tivoli Storage Manager server backup storage to the Domino server.
2. Use the Data Protection for Domino **`domdsmc activate`** command to bring the restored databases online for use by the Domino server and optionally apply transactions from the transaction log to update the database to the latest level.

Note: These two steps can be combined into one step by specifying the `/activate=yes` option on the restore command.

When the restored NSF database is enabled for DAOS, one or more NLO files might need to be recovered. To do this you must follow these steps:

1. Determine if there are any missing NLO files referenced by the restored NSF databases.
2. If there are missing NLO files, you must use the Tivoli Storage Manager backup-archive client to restore the required NLO files.

Restore process

The restore process retrieves previously backed up copies of the databases to be restored from the Tivoli Storage Manager server and restores them to the Domino server storage. You can restore the database with the original name (replace) or with a different database file name. The database can be restored to the same name in a different Domino server directory, or to a different Domino server.

The Data Protection for Domino command to restore an NSF database is:

```
domdsmc restore database_name –into restored_database_name
```

Activation

After the NSF and NTF databases have been restored, the Data Protection for Domino **`domdsmc activate`** command is used to apply any changes to the restored databases from the recovery logs and to activate the NSF and NTF databases that are being restored. This activation step brings restored databases online for use by the Domino server.

You can optionally apply transactions from the transaction log to update the database. Transactions can be applied up to a specific point in time or up to the most recent changes recorded in the transaction log. If archival logging is in effect, Data Protection for Domino automatically restores archived transaction log files as needed.

The Data Protection for Domino command to activate and apply logs to one or more databases is:

```
domdsmc activate –applylogs
```

Determine if there are missing NLO files

Issue the DAOS manager **`tell daosmgr listnlo`** command from the Domino server console to discover the names of any missing NLO files that are referenced by the restored NSF databases.

Note: If the DAOS deferred delete interval is longer than the age of the restored backup, there will be no missing NLO files. However, if the age of the backup is greater than the DAOS deferred delete interval, you may have to restore the missing NLO files.

The server command to determine the NLO files that must also be restored is:

```
 Tell daosmgr listnlo –o missingnlo.txt missing nsf_database_name
```

The file `missingnlo.txt` contains a list of NLO files that are referenced by the restored NSF database and that are not found on the Domino server.

Restore the missing NLO files

Use the Tivoli Storage Manager backup-archive client **`dsmc restore`** command to restore the missing NLO files. The option `–latest` on the restore command specifies that the latest copy, whether active or inactive, should be used. If this option is not specified and the NLO file has been expired by an incremental backup, the restore operation fails and you get the message:

```
"ANS1302E No object on server match query"
```

The server command to restore the missing NLO files is:

```
 dsmc restore –filelist missingnlo.txt –latest
```

Resynchronize the DAOS catalog

To ensure DAOS has the correct reference counts after the missing NLO files have been restored, you must run the **`tell daosmgr resync`** command from the Domino server console. If the catalog is still synchronized after the restoration, this command will close.

Restore at document level

Data Protection for Domino restores Domino databases at the database level. To restore a document in a database, the entire database and the necessary NLO files must first be restored. Then they must be copied to the “live” NSF database. A database can be restored to the production server under a temporary name , and the desired document can be copied to the appropriate database. If, for performance reasons, the production server cannot be used in the restore process, the database can be restored to an alternate server and copied to the production server.

You must perform alternate server restores when possible to reduce demands on the Domino production server. Alternate server restores can be performed to an alternate partition or to a separate Domino server by using these steps:

1. Inform the user of the location of the restored NSF database.
2. The user can copy the necessary documents from the restored NSF to the live NSF.
3. When the user has finished copying the data from the restored NSF to the live NSF, delete the restored NSF.
4. If the document includes a DAOS attachment, restore any missing NLO files and resynchronize the DAOS catalog with the **`tell daosmgr resync`** command to repair the reference counts.

Restore of Archived Transaction Logs

This Data Protection for Domino function allows a single archived transaction log file to be restored independently of a routine database restore. Restoring a single archived transaction log file assists with disaster recovery operations. By retrieving the most recent archived log file, it is possible to rebuild the Domino transaction log control file. This allows archived transaction log files to be used to recover restored database backups to a more current state, even after a loss of the active transaction log. More than one archived transaction log file can be restored at a time.

The Data Protection for Domino command to restore an archived log is:

```
Domdsmc restorelogarchive log_name
```

Disaster recovery for a Lotus Domino database with DAOS

You must use the Tivoli Storage Manager backup-archive client with Data Protection for Domino for a complete disaster recovery solution.

Disaster recovery of a Domino server requires:

1. Rebuilding the directory structure.
2. Restoring the non-database files with the Tivoli Storage Manager backup-archive client.
3. Recovering the database files to the latest level with Data Protection for Domino.

To recover a Domino server:

1. Make sure that the new installation is configured in the same manner as the damaged installation. For example, both installations must have the same directory structure, directory location, and logdir path.

   Note: The existence of NLO files changes this step only when NLO files are recovered along with other non-database files, such as `notes.ini`.
2. Use the Tivoli Storage Manager backup-archive client to recover the non-database Domino server files, such as `notes.ini`, `cert.id` and `server.id`. If a Domino attachment and object service is present, the NLO files must also be recovered at this time.

3. Use a text editor to modify the `notes.ini` file for the Domino server with this setting: `TRANSLOG_Status=0`
4. Use Data Protection for Domino to restore the transaction log file to be used in the log recovery procedure. This is the last transaction log file archived before the loss of the active transaction log.
5. Delete the contents of the Domino transaction log directory, except for the log file restored in Step 4.
6. Use a text editor to modify the `notes.ini` file for the Domino server with these settings: `TRANSLOG_Recreate_Logctrl=1TRANSLOG_Status=1`
7. Use Data Protection for Domino to restore (but not to activate) the databases you want to recover to the latest level within the archived log extents.
8. Use the Tivoli Storage Manager backup-archive client to recover the latest NLO files.
9. Use Data Protection for Domino to activate the databases you are recovering and apply transaction logs. The **`TRANSLOG_Recreate_Logctrl`** parameter in the `notes.ini` file is automatically reset to 0.
10. Launch the Domino server. With the disaster recovery complete, it is now safe to start the Domino server and run the server tasks and functions.
11. Use the selective backup function in Data Protection for Domino to perform full backups of all databases. This ensures correct recoverability using subsequent transaction log files.
12. Use Data Protection for Domino to archive the transaction log. The transaction log file used in the recovery procedure is modified and available for archiving. This transaction log has the ID of the current logger.

Chapter 5. Reference information

Frequently asked questions and best practices containing troubleshooting information for Data Protection for Lotus Domino.

Frequently asked questions

Here are some frequently asked questions regarding Data Protection for Domino.

Why do I receive a "DB2 CONNECTION ERROR" message when performing an inplace restore for a DB2 database that is enabled for roll-forward recovery?

When a DB2 database is enabled for roll-forward recovery, and the database is used for an inplace restore, the Domino server cannot connect to the DB2 database until after the roll-forward operation completes. As a result, the command output displays this message text:

```
Starting Domino DB2 database rollforward...
Initializing Domino connection...
Restart Analysis (0 MB): 100%
04/21/2007 12:02:57 AM  A RM error occurred.: An error occurred accessing the db
2 datasource.

DB2 CONNECTION ERROR:  Domino unable to connect to DB2 database 'DOMDB2' as user
 'db2admin'...
[IBM][CLI Driver] SQL1117N  A connection to or activation of database "DOMDB2" c
annot be made because of ROLL-FORWARD PENDING.  SQLSTATE=57019

DB2 CONNECTION ERROR:  set DEBUG_DB2CONNECT=0 to suppress this message.
04/21/2007 12:02:57 AM  Unable to initialize DB2 services.  DB2-based nsfs will
be unusable.: An error occurred accessing the db2 datasource.
```

There is no DB2 connection error and therefore, this message text can be ignored.

Why does my backup session timeout even though I used the `sessions` option?

This situation can occur when the number of specified backup sessions exceeds the number of available mount points. Each session requests a mount point from the Tivoli Storage Manager server when backup processing begins. If a mount point is in use (unavailable), then the mount point is not released for use by a new session until the backup (on that mount point) is complete. Because of this behavior, it is possible that a session (waiting for an available mount point) may timeout, causing the backup attempt to fail. To avoid this situation, make sure that the number of available mount points (from the Tivoli Storage Manager server) is equal to the number of sessions specified with the `sessions` option. It is the responsibility of the user to determine the number of available mount points as Data Protection for Domino does not determine this information.

How can I avoid being prompted for a Domino server password when backing up encrypted databases?

Use the Domino server Administrator to select the "Don't prompt for a password from other Notes-based programs" option in the Domino Server ID file.

Can I run multiple domdsmc instances?

You can run multiple instances of **domdsmc** for backup processing. This can improve performance when backing up many databases. It can also improve resource utilization if your data is located in sequential access storage pools on multiple drives. Running multiple instances of **domdsmc** is controlled using the `SESSION` option. This is described in the DOMDSMC SET SESSION section of this guide.

The `SESSION` option specifies the number of sessions to open to the Tivoli Storage Manager server. This option applies to NSF database backups only.

Can I restore an individual document?

To restore an individual document, the entire database must first be restored and then the document copied. A database can be restored to the production server under a temporary name and the desired document can be copied to the appropriate database. If for performance reasons, the production server cannot be used in the restore process, the database can be restored to an alternate server and copied to the production server. You should preform alternate server restores when possible to reduce the demands on the Domino Production server. Alternate server restores can be performed to an alternate partition or to a separate Domino server. See "Alternate server and alternate partition restores for NSF databases" on page 177 for details on performing this procedure.

Can I back up and restore private folders with Data Protection for Domino?

Data Protection for Domino performs backup and restore processing at the database level. The contents of the entire database is processed. As a result, a private folder is processed if it is stored in the database. Data Protection for Domino does not back up or restore private folders located in a desktop file.

What are the .nsf and .nsf.DATA Tivoli Storage Manager server objects?

The nsf.DATA object contains the actual file data from the Domino server database. The .nsf object contains information about the .nsf file but no actual file data. Both files are created on the Tivoli Storage Manager server during Data Protection for Domino backup processing.

When issuing an include statement, make sure to include both files. For example:

```
include dbname.nsf
include dbname.nsf.data
```

or

```
include dbname.nsf*
```

What is a `.pdb` file and where is it located?

The `.pdb` file tracks the Domino databases that are in a state of pending activation. It is used during **query pendingdbs** processing. Do not attempt to edit this file.

The location of the`.pdb` file depends on the following rules:

1. If the DOMI_CONFIG environment variable is set, the `.pdb` file is created in the directory specified by this environment variable.
2. If the DOMI_DIR environment variable is set, the `.pdb` file is created in the directory specified by this environment variable.
3. If the DOMI_CONFIG and DOMI_DIR environment variables are not set, the `.pdb` file is created in the default installation directory.
4. If the DOMI_CONFIG and DOMI_DIR environment variables are not set and Data Protection for Domino is not installed in the default installation directory, the `.pdb` file is created in the current working directory.

Can I manually edit the Data Protection for Domino preferences file (domdsm.cfg)?

You must use the **`set`** command to edit the preferences file. If edited manually, hidden characters can be introduced that negatively affect parsing.

How do I encrypt my backups?

You can encrypt your Domino databases during Data Protection for Domino backup and restore processing by specifying *enableclientencryptkey=yes* in the `dsm.sys` file and adding an include statement with the `include.encrypt` option.

- See "Additional options" on page 38 for more information about the `enableclientencryptkey` option.
- See "Include and exclude processing" on page 182 for examples of `include.encrypt` statements.

Can I restore a database to a platform that is different from the platform from which it was backed up?

Data Protection for Domino does not support restore processing across platforms. For example, you cannot restore a backup performed on an AIX system to a Windows machine. You must restore Data Protection for Domino backups to the same platform from which it was backed up.

Can I run multiple scheduled backups simultaneously?

The Tivoli Storage Manager client scheduler allows only one scheduler process at a time. Other schedules must wait for the first scheduled backup to complete before they can begin. This can be an issue when a scheduled backup is processing at the same time an archivelog backup is scheduled to begin. See "Scheduler considerations" on page 172 for an example of how to maintain a scheduled database backup and scheduled archivelog backup.

How do I automate (schedule) a backup?

See "Automating backups" on page 169.

How do I recover from the loss of a Domino transaction log?

See "Recovery from loss of Domino transaction logs for NSF databases" on page 176

How do I perform an alternate Domino server restore?

See "How to perform an alternate server restore for NSF databases" on page 178.

How do I perform an alternate Domino partition restore?

See "How to perform an alternate partition restore for NSF databases" on page 180.

Where do I find error information?

See "Problem determination" on page 187.

How do I include and exclude files?

See "Include and exclude processing" on page 182.

How do I migrate backups from earlier versions?

See "Migration" on page 188.

How do I use Data Protection for Domino with multiple Domino server partitions?

See "Multiple Domino server partitions" on page 185.

How do I use Data Protection for Domino with multiple Tivoli Storage Manager servers?

See "Multiple Tivoli Storage Manager servers" on page 186.

How do I compress backups?

Add the line `COMPRESS YES` to the `dsm.opt` file.

How do I enable data deduplication for Data Protection for Domino?

The Tivoli Storage Manager server must be enabled for data deduplication and the node must be enabled. In the `dsm.sys` file add the line `DEDUPLICATION YES`

See this document for more information: Data deduplication in Tivoli Storage Manager V6.2 and V6.1

Where can I find out more about data deduplication with Tivoli Storage Manager?

More information is available in these documents:

- Data deduplication in Tivoli Storage Manager V6.2 and V6.1
- Data deduplication best practices for Tivoli Storage Manager V6.2

What happens when the connection is broken between the Data Protection for Domino client and the Tivoli Storage Manager server?

When the connection is broken between the Data Protection for Domino client and the Tivoli Storage Manager server, the client attempts to reconnect to the server. The Domino client attempts to reconnect during the **`COMRESTARTDURATION`** timeframe.

Note: In certain circumstances some connection errors may not be recoverable. For example, when the network adapter is disabled and re-enabled on an AIX server the session may not reconnect successfully.

How do I cancel a session between a Data Protection for Domino client and a Tivoli Storage Manager server?

This task must be carried out by a Tivoli Storage Manager administrator with access to the Tivoli Storage Manager administrator password.

1. Log on to the server console using the Tivoli Storage Manager administrator command-line interface.
2. Enter the **`query session`** command to list all the active sessions.
3. Locate the Domino client session you want to cancel by looking for the node name under the client name column. Take note of the session number.

   Note: There may be more than one session listed for the Domino client. In TCPIP communication, cancelling any one of these sessions cancels all of the sessions. In LAN-free communication, you must cancel the session that has the session stage RecW.
4. Cancel the session by entering the **`cancel session <session number>`** command.

Best practices

This section describes best practices when using Data Protection for Domino.

These practices assist in achieving the best use of Data Protection for Domino.

Restoring to an alternate Domino Server

Restoring databases to an alternate Domino server eliminates the demands placed on the production Domino server because restore processing and applying transaction logs are both performed on the alternate server. You can also specify a fully qualified alternate restore path with the TRANSLOG_RECOVER_PATH variable in the NOTES.INI file (available with Domino 6 or later) in order for Data Protection for Domino to restore transaction logs to an alternate path. See "Alternate server and alternate partition restores for NSF databases" on page 177 for detailed instructions about this procedure.

Maintaining a scheduled database backup and scheduled archivelog backup

The Tivoli Storage Manager client scheduler allows only one scheduler process at a time. Other schedules must wait for the first scheduled backup to complete before they can begin. This can be an issue when a scheduled backup is processing at the same time an archivelog backup is scheduled to begin. See "Scheduler considerations" on page 172 for an example of how to maintain a scheduled database backup and scheduled archivelog backup.

Using multiple instances to increase performance

Use the `SESSIONS` option to run multiple instances and improve performance. More information is available in the Performance section of this guide.

Naming conventions

Using names for your Data Protection for Domino nodes, management classes, and policy domains that are different from names used for your client nodes, management classes, policy domains or Domino partitions greatly reduces the possibility of confusion and error throughout your Data Protection for Domino environment.

Reducing query processing time

To reduce query processing time when querying the Tivoli Storage Manager server for databases to restore via the Data Protection for Domino GUI, specify a database name using letters and a wildcard character (*) in the By Database Name field. For example, specifying `a*` displays all databases in the selected folder that begin with the letter *a*. Make sure to click the Update button after entering your database query.

Appendix. Accessibility features for the Tivoli Storage Manager product family

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in the Tivoli Storage Manager family of products:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The Tivoli Storage Manager Information Center, and its related publications, are accessibility-enabled. The accessibility features of the information center are described at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3/topic/com.ibm.help.ic.doc/iehs36_accessibility.html.

Keyboard navigation

On Windows, the Tivoli Storage Manager product family follows Microsoft conventions for all keyboard navigation and access. Drag and Drop support is managed using the Microsoft Windows Accessibility option known as MouseKeys. For more information about MouseKeys and other Windows accessibility options, please refer to the Windows online help (keyword: MouseKeys).

On other operating systems, these products follow the operating-system conventions for keyboard navigation and access.

Vendor software

The Tivoli Storage Manager product family includes certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for the accessibility information about its products.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

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 grant 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.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

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.

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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 is for planning purposes only. The information herein is subject to change before the products described become available.

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 illustrate 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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Intel, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

Glossary

This glossary includes terms and definitions for IBM Tivoli Storage Manager and IBM Tivoli Storage FlashCopy Manager products.

To view glossaries for other IBM products, go to http://www.ibm.com/software/globalization/terminology/.

The following cross-references are used in this glossary:

- *See* refers the reader from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- *See also* refers the reader to a related or contrasting term.

A

absolute mode
In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup even if the file has not changed since the last backup. See also *modified mode*.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights. For example, an access control list is associated with a file that identifies the users who can access that file and their access rights.

access mode
An attribute of a storage pool or a storage volume that specifies whether the server can write to or read from the storage pool or storage volume. The access mode can be read/write, read-only, or unavailable. Volumes in primary storage pools can also have an access mode of destroyed. Volumes in copy storage pools can also have an access mode of offsite.

acknowledgment
The transmission of acknowledgment characters as a positive response to a data transmission.

ACL See *access control list*.

activate
To validate the contents of a policy set and then make it the active policy set.

active-data pool
A named set of storage pool volumes that contain only active versions of client backup data.

active file system
A file system to which space management has been added. With space management, tasks for an active file system include automatic migration, reconciliation, selective migration, and recall. Contrast with *inactive file system*.

active policy set
The activated policy set that contains the policy rules in use by all client nodes that are assigned to the policy domain. See also *policy domain* and *policy set*.

active version
The most recent backup copy of a file stored. The active version of a file cannot be deleted until a backup process detects that the user has either replaced the file with a newer version or has deleted the file from the file server or workstation. Contrast with *inactive version*.

activity log
A log that records normal activity messages that are generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors.

adaptive subfile backup
A type of backup that sends only changed portions of a file to the server, instead of sending the entire file. Adaptive subfile backup reduces network traffic and increases the speed of the backup.

administrative client
A program that runs on a file server, workstation, or mainframe that administrators use to control and monitor the Tivoli Storage Manager server. Contrast with *backup-archive client*.

administrative command schedule
A database record that describes the planned processing of an administrative command during a specific time period. See also *client schedule*.

administrative privilege class
See *privilege class*.

administrative session
A period of time during which an administrator user ID communicates with a server to perform administrative tasks. Contrast with *client node session*.

administrator
A user who is registered to the server as an administrator, and who is authorized to perform tasks and issue commands through the assignment of an administrative privilege class.

Advanced Program-to-Program Communication (APPC)
An implementation of the SNA LU 6.2 protocol that allows interconnected systems to communicate and share the processing of programs.

agent node
A client node that has been granted proxy authority to perform operations on behalf of another client node, which is the target node.

aggregate
An object, stored in one or more storage pools, consisting of a group of logical files that are packaged together. See also *logical file* and *physical file*.

aggregate data transfer rate
A performance statistic that indicates the average number of bytes that were transferred per second while processing a given operation.

APPC See *Advanced Program-to-Program Communication*.

application client
A program that is installed on a system to protect an application. The Tivoli Storage Manager server provides backup services to an application client.

archive

To copy programs, data, or files to other storage media, usually for long-term storage or security. Contrast with *retrieve*.

archive copy

A file or group of files that was archived to server storage.

archive copy group

A policy object containing attributes that control the generation, destination, and expiration of archived files.

archive-retention grace period

The number of days that the storage manager retains an archived file when the server is unable to rebind the file to an appropriate management class. See also *bind*.

association

(1) The defined relationship between a client node and a client schedule. An association identifies the name of a schedule, the name of the policy domain to which the schedule belongs, and the name of a client node that performs scheduled operations.

(2) On a configuration manager, the defined relationship between a profile and an object such as a policy domain. Profile associations define the configuration information that is distributed to a managed server when it subscribes to the profile.

audit To check for logical inconsistencies between information that the server has and the actual condition of the system. The storage manager can audit information about items such as volumes, libraries, and licenses. For example, when a storage manager audits a volume, the server checks for inconsistencies between information about backed-up or archived files that are stored in the database and the actual data that are associated with each backup version or archive copy in server storage.

authentication

The process of checking a user's password before permitting user access to the Tivoli Storage Manager server. Authentication can be turned on or off by an administrator with system privilege.

authentication rule

A specification that another user can use to either restore or retrieve files from storage.

authority

The right to access objects, resources, or functions. See also *privilege class*.

authorization rule

A specification that permits another user to either restore or retrieve a user's files from storage.

authorized user

A user who has administrative authority for the Tivoli Storage Manager client on a workstation. This user changes passwords, performs open registrations, and deletes file spaces.

AutoFS

See *automounted file system*.

automatic detection

A feature that detects, reports, and updates the serial number of a drive or library in the database when the path from the local server is defined.

automatic migration
The process that is used to automatically move files from a local file system to storage, based on options and settings that are chosen by a root user on a workstation. See also *threshold migration* and *demand migration*.

automatic reconciliation
The process that is used to reconcile file systems at regular intervals. The intervals are set by a user with root user authority. See also *reconciliation*.

automounted file system (AutoFS)
A file system that is managed by an automounter daemon. The automounter daemon monitors a specified directory path, and automatically mounts the file system to access data.

B

backup-archive client
A program that runs on a workstation or file server and provides a means for users to back up, archive, restore, and retrieve files. Contrast with *administrative client*.

backup copy group
A policy object containing attributes that control the generation, destination, and expiration of backup versions of files. A backup copy group belongs to a management class.

backup-retention grace period
The number of days the storage manager retains a backup version after the server is unable to rebind the file to an appropriate management class.

backup set
A portable, consolidated group of active versions of backup files that are generated for a backup-archive client.

backup set collection
A group of backup sets that are created at the same time and which have the same backup set name, volume names, description, and device classes. The server identifies each backup set in the collection by its node name, backup set name, and file type.

backup version
A file or directory that a client node backed up to server storage. More than one backup version can exist in server storage, but only one backup version is the active version. See also *active version* and *inactive version*.

bind To associate all versions of a file with a management class name. See *rebind*.

bindery
A database that consists of three system files for a NetWare server. The files contain user IDs and user restrictions.

C

cache To place a duplicate copy of a file on random access media when the server migrates a file to another storage pool in the hierarchy.

cache file
A snapshot of a logical volume created by Logical Volume Snapshot Agent. Blocks are saved immediately before they are modified during the image backup and their logical extents are saved in the cache files.

CAD See *client acceptor*.

central scheduler
A function that permits an administrator to schedule client operations and administrative commands. The operations can be scheduled to occur periodically or on a specific date. See *client schedule* and *administrative command schedule*.

client A software program or computer that requests services from a server.

client acceptor
An HTTP service that serves the applet for the web client to web browsers. On Windows systems, the client acceptor is installed and run as a service. On AIX, UNIX, and Linux systems, the client acceptor is run as a daemon, and is also called the *client acceptor daemon* (CAD).

client acceptor daemon (CAD)
See *client acceptor*.

client domain
The set of drives, file systems, or volumes that the user selects to back up or archive data, using the backup-archive client.

client node
A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

client node session
A session in which a client node communicates with a server to perform backup, restore, archive, retrieve, migrate, or recall requests. Contrast with *administrative session*.

client options file
An editable file that identifies the server and communication method, and provides the configuration for backup, archive, hierarchical storage management, and scheduling.

client option set
A group of options that are defined on the server and used on client nodes in conjunction with client options files.

client-polling scheduling mode
A method of operation in which the client queries the server for work. Contrast with *server-prompted scheduling mode*.

client schedule
A database record that describes the planned processing of a client operation during a specific time period. The client operation can be a backup, archive, restore, or retrieve operation, a client operating system command, or a macro. See also *administrative command schedule*.

client/server
Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

client system-options file
A file, used on AIX, UNIX, or Linux system clients, containing a set of processing options that identify the servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. This file is also called the dsm.sys file. See also *client user-options file*.

client user-options file
A file that contains the set of processing options that the clients on the system use. The set can include options that determine the server that the client contacts, and options that affect backup operations, archive operations, hierarchical storage management operations, and scheduled operations. This file is also called the dsm.opt file. For AIX, UNIX, or Linux systems, see also *client system-options file*.

closed registration
A registration process in which only an administrator can register workstations as client nodes with the server. Contrast with *open registration*.

collocation
The process of keeping all data belonging to a single-client file space, a single client node, or a group of client nodes on a minimal number of sequential-access volumes within a storage pool. Collocation can reduce the number of volumes that must be accessed when a large amount of data must be restored.

collocation group
A user-defined group of client nodes whose data is stored on a minimal number of volumes through the process of collocation.

commit point
A point in time when data is considered consistent.

Common Programming Interface for Communications (CPI-C)
A call-level interface that provides a consistent application programming interface (API) for applications that use program-to-program communications. CPI-C uses LU 6.2 architecture to create a set of interprogram services that can establish and end a conversation, send and receive data, exchange control information, and notify a partner program of errors.

communication method
The method by which a client and server exchange information. See also *Transmission Control Protocol/Internet Protocol*.

communication protocol
A set of defined interfaces that permit computers to communicate with each other.

compression
A function that removes repetitive characters, spaces, or strings of characters from the data being processed and replaces the repetitive characters with control characters. Compression reduces the amount of storage space that is required for the data.

configuration manager
A server that distributes configuration information, such as policies and schedules, to managed servers according to their profiles. Configuration information can include policy and schedules. See also *managed server* and *profile*.

conversation
A connection between two programs over a session that allows them to communicate with each other while processing a transaction.

copy backup
A full backup in which the transaction log files are not deleted so that backup procedures that use incremental or differential backups are not disrupted

copy group
A policy object containing attributes that control how backup versions or archive copies are generated, where backup versions or archive copies are initially located, and when backup versions or archive copies expire. A copy group belongs to a management class. See also *archive copy group*, *backup copy group*, *backup version*, and *management class*.

copy storage pool
A named set of volumes that contain copies of files that reside in primary storage pools. Copy storage pools are used only to back up the data that is stored in primary storage pools. A copy storage pool cannot be a destination for a backup copy group, an archive copy group, or a management class (for space-managed files). See also *primary storage pool* and *destination*.

CPI-C See *Common Programming Interface for Communications*.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

damaged file
A physical file in which Tivoli Storage Manager has detected read errors.

data access control mode
A mode that controls whether a command can access a migrated file, see a migrated file as zero-length, or receive an input/output error if it attempts to access a migrated file. See also *execution mode*.

database backup series
One full backup of the database, plus up to 32 incremental backups made since that full backup. Each full backup that is run starts a new database backup series. A number identifies each backup series.

database snapshot
A complete backup of the entire database to media that can be taken off-site. When a database snapshot is created, the current database backup series is not interrupted. A database snapshot cannot have incremental database backups associated with it. See also *database backup series*. Contrast with *full backup*.

data deduplication
A method of reducing storage needs by eliminating redundant data. Only one instance of the data is retained on storage media. Other instances of the same data are replaced with a pointer to the retained instance.

data manager server
A server that collects metadata information for client inventory and manages transactions for the storage agent over the local area network. The data manager server informs the storage agent with applicable library attributes and the target volume identifier.

data mover
A device that moves data on behalf of the server. A network-attached storage (NAS) file server is a data mover.

data storage-management application-programming interface (DSMAPI)
A set of functions and semantics that can monitor events on files, and manage and maintain the data in a file. In an HSM environment, a DSMAPI uses events to notify data management applications about operations on files, stores arbitrary attribute information with a file, supports managed regions in a file, and uses DSMAPI access rights to control access to a file object.

default management class
A management class that is assigned to a policy set. This class is used to govern backed up or archived files when a file is not explicitly associated with a specific management class through the include-exclude list.

deduplication
See *data deduplication.*

demand migration
The process that is used to respond to an out-of-space condition on a file system for which hierarchical storage management (HSM) is active. Files are migrated to server storage until space usage drops to the low threshold that was set for the file system. If the high threshold and low threshold are the same, one file is migrated.

desktop client
The group of backup-archive clients that includes clients on Microsoft Windows, Apple, and Novell NetWare operating systems.

destination
A copy group or management class attribute that specifies the primary storage pool to which a client file will be backed up, archived, or migrated.

device class
A named set of characteristics that are applied to a group of storage devices. Each device class has a unique name and represents a device type of disk, file, optical disk, or tape.

device configuration file
(1) For a server, a file that contains information about defined device classes, and, on some servers, defined libraries and drives. The information is a copy of the device configuration information in the database.

(2) For a storage agent, a file that contains the name and password of the storage agent, and information about the server that is managing the SAN-attached libraries and drives that the storage agent uses.

device driver
A program that provides an interface between a specific device and the application program that uses the device.

disaster recovery manager (DRM)
A function that assists in preparing and using a disaster recovery plan file for the server.

disaster recovery plan
A file that is created by the disaster recovery manager (DRM) that contains information about how to recover computer systems if a disaster occurs and scripts that can be run to perform some recovery tasks. The file includes information about the software and hardware that is used by the server, and the location of recovery media.

domain
A grouping of client nodes with one or more policy sets, which manage data or storage resources for the client nodes. See *policy domain* or *client domain*.

DRM See *disaster recovery manager*.

DSMAPI
See *data storage-management application-programming interface*.

dynamic serialization
A type of copy serialization in which a file or folder is backed up or archived on the first attempt regardless of whether it changes during a backup or archive.

E

EA See *extended attribute*.

EB See *exabyte*.

EFS See *Encrypted File System*.

Encrypted File System (EFS)
A file system that uses file system-level encryption.

enterprise configuration
A method of setting up servers so that the administrator can distribute the configuration of one of the servers to the other servers, using server-to-server communication. See also *configuration manager*, *managed server*, *profile*, and *subscription*.

enterprise logging
The process of sending events from a Tivoli Storage Manager server to a designated event server. The event server routes the events to designated receivers, such as to a user exit. See also *event*.

error log
A data set or file that is used to record error information about a product or system.

estimated capacity
The available space, in megabytes, of a storage pool.

event (1) An administrative command or a client operation that is scheduled to be run using Tivoli Storage Manager scheduling.

(2) A message that an Tivoli Storage Manager server or client issues. Messages can be logged using Tivoli Storage Manager event logging.

event record
A database record that describes actual status and results for events.

event server
A server to which other servers can send events for logging. The event server routes the events to any receivers that are enabled for the sending server's events.

exabyte (EB)
For processor storage, real and virtual storage, and channel volume, 1 152 921 504 606 846 976 bytes. For disk storage capacity and communications volume, 1 000 000 000 000 000 000 bytes.

exclude
The process of identifying files in an include-exclude list. This process

prevents the files from being backed up or migrated whenever a user or schedule enters an incremental or selective backup operation. A file can be excluded from backup and space management, backup only, or space management only.

exclude-include list
See *include-exclude list*.

execution mode
A mode that controls the space-management related behavior of commands that run under the **`dsmmode`** command.

expiration
The process by which files, data sets, or objects are identified for deletion because their expiration date or retention period has passed.

expiring file
A migrated or premigrated file that has been marked for expiration and removal from storage. If a stub file or an original copy of a premigrated file is deleted from a local file system, or if the original copy of a premigrated file is updated, the corresponding migrated or premigrated file is marked for expiration the next time reconciliation is run.

extend
To increase the portion of available space that can be used to store database or recovery log information.

extended attribute (EA)
Names or value pairs that are associated with files or directories. There are three classes of extended attributes: user attributes, system attributes, and trusted attributes.

extent The part of a file that is created during the data-deduplication process. Extents are compared with other file extents to identify duplicates.

external library
A type of library that is provided by Tivoli Storage Manager that permits LAN-free data movement for StorageTek libraries that are managed by Automated Cartridge System Library Software (ACSLS). To activate this function, the Tivoli Storage Manager library type must be EXTERNAL.

F

file access time
On AIX, UNIX, or Linux systems, the time when the file was last accessed.

file age
For migration prioritization purposes, the number of days since a file was last accessed.

file device type
A device type that specifies the use of sequential access files on disk storage as volumes.

file server
A dedicated computer and its peripheral storage devices that are connected to a local area network that stores programs and files that are shared by users on the network.

file space
A logical space in server storage that contains a group of files that have been backed up or archived by a client node, from a single logical partition, file system, or virtual mount point. Client nodes can restore,

retrieve, or delete their file spaces from server storage. In server storage, files belonging to a single file space are not necessarily stored together.

file space ID (FSID)
A unique numeric identifier that the server assigns to a file space when it is stored in server storage.

file state
The space management mode of a file that resides in a file system to which space management has been added. A file can be in one of three states: resident, premigrated, or migrated. See also *resident file*, *premigrated file*, and *migrated file*.

file system migrator (FSM)
A kernel extension that intercepts all file system operations and provides any space management support that is required. If no space management support is required, the operation is passed to the operating system, which performs its normal functions. The file system migrator is mounted over a file system when space management is added to the file system.

file system state
The storage management mode of a file system that resides on a workstation on which the hierarchical storage management (HSM) client is installed. A file system can be in one of these states: native, active, inactive, or global inactive.

frequency
A copy group attribute that specifies the minimum interval, in days, between incremental backups.

FSID See *file space ID*.

FSM See *file system migrator*.

full backup
The process of backing up the entire server database. A full backup begins a new database backup series. See also *database backup series* and *incremental backup*. Contrast with *database snapshot*.

fuzzy backup
A backup version of a file that might not accurately reflect what is currently in the file because the file was backed up at the same time as it was being modified.

fuzzy copy
A backup version or archive copy of a file that might not accurately reflect the original contents of the file because it was backed up or archived the file while the file was being modified. See also *backup version* and *archive copy*.

G

General Parallel File System
A high-performance shared-disk file system that can provide data access from nodes in a cluster environment.

gigabyte (GB)
In decimal notation, 1 073 741 824 when referring to memory capacity; in all other cases, it is defined as 1 000 000 000.

global inactive state
The state of all file systems to which space management has been added when space management is globally deactivated for a client node. When

space management is globally deactivated, hierarchical storage management (HSM) cannot perform migration, recall, or reconciliation. However, a root user can update space management settings and add space management to additional file systems. Users can access resident and premigrated files.

Globally Unique Identifier (GUID)
An algorithmically determined number that uniquely identifies an entity within a system.

GPFS™
See *General Parallel File System*.

GPFS node set
A mounted, defined group of GPFS file systems.

group backup
The backup of a group containing a list of files from one or more file space origins.

GUID See *Globally Unique Identifier*.

H

hierarchical storage management (HSM)
A function that automatically distributes and manages data on disk, tape, or both by regarding devices of these types and potentially others as levels in a storage hierarchy that range from fast, expensive devices to slower, cheaper, and possibly removable devices. The objectives are to minimize access time to data and maximize available media capacity.

hierarchical storage management (HSM) client
A client program that works with the Tivoli Storage Manager server to provide hierarchical storage management (HSM) for a system. See also *hierarchical storage management* and *space manager client*.

HSM See *hierarchical storage management*.

HSM client
See *hierarchical storage management client*.

I

ILM See *information lifecycle management*.

image A file system or raw logical volume that is backed up as a single object.

image backup
A backup of a full file system or raw logical volume as a single object.

inactive file system
A file system for which space management has been deactivated. Contrast with *active file system*.

inactive version
A backup version of a file that is either not the most recent backup version, or that is a backup version of a file that no longer exists on the client system. Inactive backup versions are eligible for expiration processing according to the management class assigned to the file. Contrast with *active version*.

include-exclude file
A file containing statements to determine the files to back up and the associated management classes to use for backup or archive. See also *include-exclude list*.

include-exclude list
A list of options that include or exclude selected files for backup. An exclude option identifies files that should not be backed up. An include option identifies files that are exempt from the exclusion rules or assigns a management class to a file or a group of files for backup or archive services.

incremental backup
(1) A copy of all database data that has changed since the most recent successful full backup operation. An incremental backup is also known as a *cumulative backup image* because each incremental backup includes the contents of the previous incremental backup.

(2) The process of backing up information in the database that is new or changed since the last full backup. Contrast with *full backup*. See also *database backup series*.

(3) For Data Protection for Microsoft Exchange Server, a backup in which the transaction logs are backed up and then cleared.

individual mailbox restore
See *mailbox restore*.

information lifecycle management (ILM)
GPFS policy-based file management for storage pools and file sets.

inode
The internal structure that describes the individual files on AIX, UNIX, or Linux systems. An inode contains the node, type, owner, and location of a file.

inode number
A number specifying a particular inode file in the file system.

IP address
A unique address for a device or logical unit on a network that uses the IP standard.

J

job file
A generated file that contains configuration information for a migration job. The file is XML format and can be created and edited in the hierarchical storage management (HSM) client for Windows client graphical user interface.

journal-based backup
A method for backing up Windows clients and AIX clients that exploits the change notification mechanism in a file to improve incremental backup performance by reducing the need to fully scan the file system.

journal daemon
On AIX, UNIX, or Linux systems, a program that tracks change activity for files residing in file systems.

journal service
In Microsoft Windows, a program that tracks change activity for files residing in file systems.

K

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 210 or 1 024 bytes. For disk storage capacity and communications volume, 1 000 bytes.

L

LAN See *local area network.*

LAN-free data movement
The movement of client data between a client system and a storage device on a storage area network (SAN), bypassing the local area network. This process is also referred to as *LAN-free data transfer*.

LAN-free data transfer
See *LAN-free data movement*.

leader data
Bytes of data, from the beginning of a migrated file, that are stored in the file's corresponding stub file on the local file system. The amount of leader data that is stored in a stub file depends on the stub size that is specified.

library
(1) A repository for demountable recorded media, such as magnetic disks and magnetic tapes.

(2) A collection of one or more drives, and possibly robotic devices (depending on the library type), which can be used to access storage volumes.

library client
A server that uses server-to-server communication to access a library that is managed by another storage management server. See also *library manager*.

library manager
A server that controls device operations when multiple storage management servers share a storage device. See also *library client*.

local (1) Pertaining to a device, file, or system that is accessed directly from a user system, without the use of a communication line.

(2) For HSM products, pertaining to the destination of migrated files that are being moved.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

local shadow volumes
Data that is stored on shadow volumes localized to a disk storage subsystem.

LOFS See *loopback virtual file system.*

logical file
A file that is stored in one or more server storage pools, either by itself or as part of an aggregate. See also *aggregate* and *physical file*.

logical occupancy
The space that is used by logical files in a storage pool. This space does

not include the unused space created when logical files are deleted from aggregate files, so it might be less than the physical occupancy.

logical unit (LU)
An access point through which a user or application program accesses the Systems Network Architecture (SNA) network to communicate with another user or application program.

logical unit number (LUN)
In the Small Computer System Interface (SCSI) standard, a unique identifier that is used to differentiate devices, each of which is a logical unit (LU).

logical volume
A portion of a physical volume that contains a file system.

logical volume backup
A backup of a file system or logical volume as a single object.

Logical Volume Snapshot Agent (LVSA)
Software that can act as the snapshot provider for creating a snapshot of a logical volume during an online image backup.

loopback virtual file system (LOFS)
A file system that is created by mounting a directory over another local directory, also known as mount-over-mount. A LOFS can also be generated using an automounter.

LU See *logical unit*.

LUN See *logical unit number*.

LVSA See *Logical Volume Snapshot Agent*.

M

macro file
A file that contains one or more storage manager administrative commands, which can be run only from an administrative client using the MACRO command. Contrast with *Tivoli Storage Manager command script*.

mailbox restore
A function that restores Microsoft Exchange Server data (from IBM Data Protection for Microsoft Exchange backups) at the mailbox level or mailbox-item level.

managed object
In Tivoli Storage Manager, a definition in the database of a managed server that was distributed to the managed server by a configuration manager. When a managed server subscribes to a profile, all objects that are associated with that profile become managed objects in the database of the managed server. In general, a managed object cannot be modified locally on the managed server. Objects can include policy, schedules, client option sets, server scripts, administrator registrations, server definitions, and server group definitions.

managed server
A Tivoli Storage Manager server that receives configuration information from a configuration manager using a subscription to one or more profiles. Configuration information can include definitions of objects such as policy and schedules. See also *configuration manager*, *subscription*, and *profile*.

management class

A policy object that users can bind to each file to specify how the server manages the file. The management class can contain a backup copy group, an archive copy group, and space management attributes. See also *copy group*, *space manager client*, *bind*, and *rebind*.

maximum transmission unit

The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the maximum transmission unit for Ethernet is 1500 bytes.

MB See *megabyte*.

media server

In a z/OS® environment, a program that provides access to z/OS disk and tape storage for Tivoli Storage Manager servers that run on operating systems other than z/OS.

megabyte (MB)

(1) 1 048 576 bytes (2 to the 20th power) when used in this publication.

(2) For processor storage, real and virtual storage, and channel volume, 2 to the power of 20 or 1 048 576 bits. For disk storage capacity and communications volume, 1 000 000 bits.

metadata

Data that describes the characteristics of data; descriptive data.

migrate

To move data from one storage location to another. In Tivoli Storage Manager products, migrating can mean moving data from a client node to server storage, or moving data from one storage pool to the next storage pool defined in the server storage hierarchy. In both cases the movement is controlled by policy, such as thresholds that are set. See also *migration threshold*.

migrated file

A file that has been copied from a local file system to Tivoli Storage Manager storage. For HSM clients on UNIX or Linux systems, the file is replaced with a stub file on the local file system. On Windows systems, creation of the stub file is optional. See also *stub file* and *resident file*. For HSM clients on UNIX or Linux systems, contrast with *premigrated file*.

migrate-on-close recall mode

A mode that causes a migrated file to be recalled back to its originating file system temporarily. Contrast with *normal recall mode* and *read-without-recall recall mode*.

migration job

A specification of files to migrate, and actions to perform on the original files after migration. See also *job file*.

migration threshold

High and low capacities for storage pools or file systems, expressed as percentages, at which migration is set to start and stop.

mirroring

The process of writing the same data to multiple locations at the same time. Mirroring data protects against data loss within the recovery log.

mode A copy group attribute that specifies whether to back up a file that has not been modified since the last time the file was backed up. See *modified mode* and *absolute mode*.

modified mode
In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup only if it has changed since the last backup. A file is considered a changed file if the date, size, owner, or permissions of the file have changed. See also *absolute mode*.

mount limit
The maximum number of volumes that can be simultaneously accessed from the same device class. The mount limit determines the maximum number of mount points. See also *mount point*.

mount point
On the Tivoli Storage Manager server, a logical drive through which volumes in a sequential access device class are accessed. For removable-media device types, such as tape, a mount point is a logical drive that is associated with a physical drive. For the file device type, a mount point is a logical drive that is associated with an I/O stream. The number of mount points for a device class is defined by the value of the mount limit attribute for that device class. See also *mount limit*.

mount retention period
The maximum number of minutes that the server retains a mounted sequential-access media volume that is not being used before it dismounts the sequential-access media volume.

mount wait period
The maximum number of minutes that the server waits for a sequential-access volume mount request to be satisfied before canceling the request.

MTU See *maximum transmission unit*.

N

Nagle algorithm
An algorithm that reduces congestion of TCP/IP networks by combining smaller packets and sending them together.

named pipe
A type of interprocess communication that permits message data streams to pass between peer processes, such as between a client and a server.

NAS See *network-attached storage*.

NAS node
A client node that is a network-attached storage (NAS) file server. Data for the NAS node is transferred by a NAS file server that is controlled by the network data management protocol (NDMP). A NAS node is also called a NAS file server node.

native file system
A file system that is locally added to the file server and is not added for space management. The hierarchical storage manager (HSM) client does not provide space management services to the file system.

native format
A format of data that is written to a storage pool directly by the Tivoli Storage Manager server. Contrast with *non-native data format*.

NDMP
See *Network Data Management Protocol*.

NetBIOS
See *Network Basic Input/Output System*.

network-attached storage (NAS) file server
A dedicated storage device with an operating system that is optimized for file-serving functions. A NAS file server can have the characteristics of both a node and a data mover.

Network Basic Input/Output System (NetBIOS)
A standard interface to networks and personal computers that is used on local area networks to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not have to handle the details of LAN data link control (DLC) protocols.

Network Data Management Protocol (NDMP)
A protocol that allows a network storage-management application to control the backup and recovery of an NDMP-compliant file server, without installing vendor-acquired software on that file server.

network data-transfer rate
A rate that is calculated by dividing the total number of bytes that are transferred by the data transfer time. For example, this rate can be the time that is spent transferring data over a network.

node A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

node name
A unique name that is used to identify a workstation, file server, or PC to the server.

node privilege class
A privilege class that gives an administrator the authority to remotely access backup-archive clients for a specific client node or for all clients in a policy domain. See also *privilege class*.

non-native data format
A format of data that is written to a storage pool that differs from the format that the server uses for operations.

normal recall mode
A mode that causes a migrated file to be copied back to its originating file system when it is accessed.

O

offline volume backup
A backup in which the volume is locked so that no other system applications can access it during the backup operation.

online volume backup
A backup in which the volume is available to other system applications during the backup operation.

open registration
A registration process in which users can register their workstations as client nodes with the server. Contrast with *closed registration*.

operator privilege class
A privilege class that gives an administrator the authority to disable or halt

the server, enable the server, cancel server processes, and manage removable media. See also *privilege class*.

options file
A file that contains processing options. On Windows and NetWare systems, the file is called dsm.opt. On AIX, UNIX, Linux, and Mac OS X systems, the file is called dsm.sys.

originating file system
The file system from which a file was migrated. When a file is recalled using normal or migrate-on-close recall mode, it is always returned to its originating file system.

orphaned stub file
A file for which no migrated file can be found on the Tivoli Storage Manager server that the client node is contacting for space management services. For example, a stub file can be orphaned when the client system-options file is modified to contact a server that is different than the one to which the file was migrated.

out-of-space protection mode
A mode that controls whether the program intercepts out-of-space conditions. See also *execution mode*.

P

pacing
In SNA, a technique by which the receiving system controls the rate of transmission of the sending system to prevent overrun.

packet In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole.

page A defined unit of space on a storage medium or within a database volume.

partial-file recall mode
A recall mode that causes the hierarchical storage management (HSM) function to read just a portion of a migrated file from storage, as requested by the application accessing the file.

password generation
A process that creates and stores a new password in an encrypted password file when the old password expires. Automatic generation of a password prevents password prompting. Password generation can be set in the options file (`passwordaccess` option). See also *options file*.

path An object that defines a one-to-one relationship between a source and a destination. Using the path, the source accesses the destination. Data can flow from the source to the destination, and back. An example of a source is a data mover (such as a network-attached storage [NAS] file server), and an example of a destination is a tape drive.

pattern-matching character
See *wildcard character*.

physical file
A file that is stored in one or more storage pools, consisting of either a single logical file, or a group of logical files that are packaged together as an aggregate. See also *aggregate* and *logical file*.

physical occupancy
The amount of space that is used by physical files in a storage pool. This

space includes the unused space that is created when logical files are deleted from aggregates. See also *physical file*, *logical file*, and *logical occupancy*.

plug-in
A self-contained software component that modifies (adds, or changes) the function in a particular system. When a plug-in is added to a system, the foundation of the original system remains intact.

policy domain
A grouping of policy users with one or more policy sets, which manage data or storage resources for the users. The users are client nodes that are associated with the policy domain.

policy privilege class
A privilege class that gives an administrator the authority to manage policy objects, register client nodes, and schedule client operations for client nodes. Authority can be restricted to certain policy domains. See also *privilege class*.

policy set
A group of rules in a policy domain. The rules specify how data or storage resources are automatically managed for client nodes in the policy domain. Rules can be contained in management classes. See also *active policy set* and *management class*.

premigrated file
A file that has been copied to Tivoli Storage Manager storage, but has not been replaced with a stub file on the local file system. An identical copy of the file resides both on the local file system and in Tivoli Storage Manager storage. Premigrated files occur on UNIX and Linux file systems to which space management has been added. Contrast with *migrated file* and *resident file*.

premigrated files database
A database that contains information about each file that has been premigrated to Tivoli Storage Manager storage. The database is stored in a hidden directory named `.SpaceMan` in each file system to which space management has been added.

premigration
The process of copying files that are eligible for migration to Tivoli Storage Manager storage, but leaving the original file intact on the local file system.

premigration percentage
A space management setting that controls whether the next eligible candidates in a file system are premigrated following threshold or demand migration.

primary storage pool
A named set of volumes that the server uses to store backup versions of files, archive copies of files, and files migrated from client nodes. See also *destination* and *copy storage pool*.

privilege class
A level of authority that is granted to an administrator. The privilege class determines which administrative tasks the administrator can perform. See also *node privilege class*, *operator privilege class*, *policy privilege class*, *storage privilege class*, and *system privilege class*.

profile
A named group of configuration information that can be distributed from a configuration manager when a managed server subscribes. Configuration information can include registered administrator IDs, policies, client schedules, client option sets, administrative schedules, storage manager command scripts, server definitions, and server group definitions. See also *configuration manager* and *managed server*.

Q

quota
(1) For HSM on AIX, UNIX, or Linux systems, the limit (in megabytes) on the amount of data that can be migrated and premigrated from a file system to server storage.

(2) For HSM on Windows systems, a user-defined limit to the space that is occupied by recalled files.

R

randomization
The process of distributing schedule start times for different clients within a specified percentage of the schedule's startup window.

raw logical volume
A portion of a physical volume that is comprised of unallocated blocks and has no journaled file system (JFS) definition. A logical volume is read/write accessible only through low-level I/O functions.

read-without-recall recall mode
A mode that causes hierarchical storage management (HSM) to read a migrated file from storage without storing it back on the local file system. The last piece of information read from the file is stored in a buffer in memory on the local file system. Contrast with *normal recall mode* and *migrate-on-close recall mode*.

rebind
To associate all backed-up versions of a file with a new management class name. For example, a file that has an active backup version is rebound when a later version of the file is backed up with a different management class association. See also *bind*.

recall
In Tivoli Storage Manager, to copy a migrated file from server storage back to its originating file system using the space management client. See also *transparent recall*, *selective recall*, and *recall mode*.

recall mode
A mode that is assigned to a migrated file with the `dsmattr` command that determines how the file is processed when it is recalled. It determines whether the file is stored on the local file system, is migrated back to Tivoli Storage Manager storage when it is closed, or is read from Tivoli Storage Manager storage without storing it on the local file system.

receiver
A server repository that contains a log of server and client messages as events. For example, a receiver can be a file exit, a user exit, or the Tivoli Storage Manager server console and activity log. See also *event*.

reclamation
The process of consolidating the remaining data from many sequential-access volumes onto fewer, new sequential-access volumes.

reclamation threshold
The percentage of space that a sequential-access media volume must have before the server can reclaim the volume. Space becomes reclaimable when files are expired or are deleted.

reconciliation
The process of synchronizing a file system with the Tivoli Storage Manager server, and then removing old and obsolete objects from the Tivoli Storage Manager server.

recovery log
A log of updates that are about to be written to the database. The log can be used to recover from system and media failures. The recovery log consists of the active log (including the log mirror) and archive logs.

register
To define a client node or administrator ID that can access the server.

registry
A repository that contains access and configuration information for users, systems, and software.

remote
(1) Pertaining to a system, program, or device that is accessed through a communication line.

(2) For HSM products, pertaining to the origin of migrated files that are being moved.

resident file
On a Windows system, a complete file on a local file system that might also be a migrated file because a migrated copy can exist in Tivoli Storage Manager storage. On a UNIX or Linux system, a complete file on a local file system that has not been migrated or premigrated, or that has been recalled from Tivoli Storage Manager storage and modified. Contrast with *stub file* and *premigrated file*. See *migrated file*.

restore
To copy information from its backup location to the active storage location for use. For example, to copy information from server storage to a client workstation.

retention
The amount of time, in days, that inactive backed-up or archived files are kept in the storage pool before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

retrieve
To copy archived information from the storage pool to the workstation for use. The retrieve operation does not affect the archive version in the storage pool.

roll back
To remove changes that were made to database files since the last commit point.

root user
A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

S

SAN See *storage area network*.

schedule
A database record that describes client operations or administrative commands to be processed. See *administrative command schedule* and *client schedule*.

scheduling mode
The type of scheduling operation for the server and client node that supports two scheduling modes: client-polling and server-prompted.

scratch volume
A labeled volume that is either blank or contains no valid data, that is not defined, and that is available for use.

script
A series of commands, combined in a file, that carry out a particular function when the file is run. Scripts are interpreted as they are run. Contrast with *Tivoli Storage Manager command script*.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective backup
The process of backing up certain files or directories from a client domain. The files that are backed up are those that are not excluded in the include-exclude list. The files must meet the requirement for serialization in the backup copy group of the management class that is assigned to each file. Contrast with *incremental backup*.

selective migration
The process of copying user-selected files from a local file system to Tivoli Storage Manager storage and replacing the files with stub files on the local file system. Contrast with *threshold migration* and *demand migration*.

selective recall
The process of copying user-selected files from Tivoli Storage Manager storage to a local file system. Contrast with *transparent recall*.

serialization
The process of handling files that are modified during backup or archive processing. See *dynamic serialization*, *static serialization*, *shared static serialization*, and *shared dynamic serialization*.

server
A software program or a computer that provides services to other software programs or other computers.

server options file
A file that contains settings that control various server operations. These settings affect such things as communications, devices, and performance.

server-prompted scheduling mode
A client/server communication technique where the server contacts the client node when tasks must be done. Contrast with *client-polling scheduling mode*.

server storage
The primary, copy, and active-data storage pools that are used by the server to store user files such as backup versions, archive copies, and files migrated from space manager client nodes (space-managed files). See also *active-data pool*, *primary storage pool*, *copy storage pool*, *storage pool volume*, and *volume*.

session
A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data.

session resource usage
The amount of wait time, processor time, and space that is used or retrieved during a client session.

shared dynamic serialization
A value for serialization that specifies that a file must not be backed up or archived if it is being modified during the operation. Tivoli Storage Manager retries the backup or archive operation a number of times; if the file is being modified during each attempt, Tivoli Storage Manager will back up or archive the file on its last try. See also *serialization*. Contrast with *dynamic serialization*, *shared static serialization*, and *static serialization*.

shared library
A library device that is used by multiple storage manager servers.

shared static serialization
A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. Tivoli Storage Manager attempts to retry the operation a number of times. If the file is in use during each attempt, the file is not backed up or archived. See also *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *static serialization*.

snapshot
An image backup type that consists of a point-in-time view of a volume.

space-managed file
A file that is migrated from a client node by the space manager client. The space manager client recalls the file to the client node on demand.

space management
The process of keeping sufficient free storage space available on a local file system for new data by migrating files to server storage. Synonymous with *hierarchical storage management*.

space manager client
A program that runs on a UNIX or Linux system to manage free space on the local file system by migrating files to server storage. The program can recall the files either automatically or selectively. Also called *hierarchical storage management (HSM) client*.

space monitor daemon
A daemon that checks space usage on all file systems for which space management is active, and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold.

sparse file
A file that is created with a length greater than the data it contains, leaving empty spaces for the future addition of data.

special file
On AIX, UNIX, or Linux systems, a file that defines devices for the system, or temporary files that are created by processes. There are three basic types of special files: first-in, first-out (FIFO); block; and character.

SSL See *Secure Sockets Layer*.

stabilized file space
A file space that exists on the server but not on the client.

stanza A group of lines in a file that together have a common function or define a part of the system. Each stanza is identified by a name that occurs in the first line of the stanza. Depending on the type of file, a stanza is ended by the next occurrence of a stanza name in the file, or by an explicit end-of-stanza marker. A stanza can also be ended by the end of the file.

startup window
A time period during which a schedule must be initiated.

static serialization
A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. If the file is in use during the first attempt, the storage manager cannot back up or archive the file. See also *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *shared static serialization*.

storage agent
A program that enables the backup and restoration of client data directly to and from storage attached to a storage area network (SAN).

storage area network (SAN)
A dedicated storage network that is tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy
(1) A logical order of primary storage pools, as defined by an administrator. The order is typically based on the speed and capacity of the devices that the storage pools use. The storage hierarchy is defined by identifying the next storage pool in a storage pool definition. See also *storage pool*.

(2) An arrangement of storage devices with different speeds and capacities. The levels of the storage hierarchy include: main storage, such as memory and direct-access storage device (DASD) cache; primary storage (DASD containing user-accessible data); migration level 1 (DASD containing data in a space-saving format); and migration level 2 (tape cartridges containing data in a space-saving format).

storage pool
A named set of storage volumes that are the destination that is used to store client data. A storage pool contains backup versions, archive copies, and files that are migrated from space manager client nodes. A primary storage pool is backed up to a copy storage pool. See also *primary storage pool*, *copy storage pool*, and *active-data pool*.

storage pool volume
A volume that has been assigned to a storage pool. See also *volume*, *active-data pool*, *copy storage pool*, and *primary storage pool*.

storage privilege class
A privilege class that gives an administrator the authority to control how storage resources for the server are allocated and used, such as monitoring the database, the recovery log, and server storage. See also *privilege class*.

stub A shortcut on the Windows file system that is generated by the hierarchical storage management (HSM) client for a migrated file that allows transparent user access. A stub is the sparse file representation of a migrated file, with a reparse point attached.

stub file
A file that replaces the original file on a local file system when the file is migrated to storage. A stub file contains the information that is necessary to recall a migrated file from Tivoli Storage Manager storage. It also contains additional information that can be used to eliminate the need to recall a migrated file.

stub file size
The size of a file that replaces the original file on a local file system when the file is migrated to Tivoli Storage Manager storage. The size that is specified for stub files determines how much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

subscription
In a Tivoli environment, the process of identifying the subscribers that the profiles are distributed to. For Tivoli Storage Manager, a subscription is the process by which a managed server receives configuration information associated with a particular profile on a configuration manager. See also *managed server*, *configuration manager*, and *profile*.

system privilege class
A privilege class that gives an administrator the authority to issue all server commands. See also *privilege class*.

Systems Network Architecture (SNA)
The description of the logical structure, formats, protocols, and operational sequences for transmitting information through and controlling the configuration and operation of networks.

T

tape library
A set of equipment and facilities that support an installation's tape environment. The tape library can include tape storage racks, mechanisms for automatic tape mounting, a set of tape drives, and a set of related tape volumes mounted on those drives.

tape volume prefix
The high-level-qualifier of the file name or the data set name in the standard tape label.

target node
A client node for which other client nodes (called agent nodes) have been granted proxy authority. The proxy authority allows the agent nodes to perform operations such as backup and restore on behalf of the target node, which owns the data.

TCA See *trusted communications agent*.

TCP/IP
See *Transmission Control Protocol/Internet Protocol*.

threshold migration
The process of moving files from a local file system to Tivoli Storage Manager storage based on the high and low thresholds that are defined for the file system. Contrast with *demand migration*, *selective migration*, and *migration job*.

throughput
In storage management, the total bytes in the workload, excluding overhead, that are backed up or restored, divided by elapsed time.

timeout
A time interval that is allotted for an event to occur or complete before operation is interrupted.

timestamp control mode
A mode that determines whether commands preserve the access time for a file or set it to the current time.

Tivoli Storage Manager command script
A sequence of Tivoli Storage Manager administrative commands that are stored in the database of the Tivoli Storage Manager server. The script can run from any interface to the server. The script can include substitution for command parameters and conditional logic.

tombstone object
A small subset of attributes of a deleted object. The tombstone object is retained for a specified period, and at the end of the specified period, the tombstone object is permanently deleted.

Transmission Control Protocol/Internet Protocol (TCP/IP)
An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types.

transparent recall
The process that is used to automatically recall a file to a workstation or file server when the file is accessed. See also *recall mode*. Contrast with *selective recall*.

trusted communications agent (TCA)
A program that handles the sign-on password protocol when clients use password generation.

U

UCS-2 A 2-byte (16-bit) encoding scheme based on ISO/IEC specification 10646-1. UCS-2 defines three levels of implementation: Level 1-No combining of encoded elements allowed; Level 2-Combining of encoded elements is allowed only for Thai, Indic, Hebrew, and Arabic; Level 3-Any combination of encoded elements are allowed.

UNC See *Universal Naming Convention name*.

Unicode
A character encoding standard that supports the interchange, processing, and display of text that is written in the common languages around the world, plus some classical and historical texts. The Unicode standard has a 16-bit character set defined by ISO 10646.

Unicode-enabled file space
Unicode file space names provide support for multilingual workstations without regard for the current locale.

Unicode transformation format 8
Unicode Transformation Format (UTF), 8-bit encoding form, which is designed for ease of use with existing ASCII-based systems. The CCSID value for data in UTF-8 format is 1208.

Universal Naming Convention (UNC) name
A name that is used to access a drive or directory containing files shared across a network. The UNC name includes the system name and a SharePoint name that represents the shared drive or directory.

Universally Unique Identifier (UUID)
The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier.

UTF-8 See *Unicode transformation format 8*.

UUID See *Universally Unique Identifier*.

V

validate
To check a policy set for conditions that can cause problems if that policy set becomes the active policy set. For example, the validation process checks whether the policy set contains a default management class.

version
A backup copy of a file stored in server storage. The most recent backup copy of a file is the active version. Earlier copies of the same file are inactive versions. The number of versions retained by the server is determined by the copy group attributes in the management class.

virtual file space
A representation of a directory on a network-attached storage (NAS) file system as a path to that directory.

virtual volume
An archive file on a target server that represents a sequential media volume to a source server.

volume
A discrete unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. See also *scratch volume*, and *storage pool volume*.

volume history file
A file that contains information about volumes that have been used by the server for database backups and for export of administrator, node, policy, or server data. The file also has information about sequential-access storage pool volumes that have been added, reused, or deleted. The information is a copy of volume information that is recorded in the server database.

Volume Shadow Copy Service
A set of Microsoft application-programming interfaces (APIs) that you can use to create shadow copy backups of volumes, exact copies of files, including all open files, and so on.

VSS See *Volume Shadow Copy Service*.

VSS Backup
A backup operation that uses Microsoft Volume Shadow Copy Service (VSS) technology. The backup operation produces an online snapshot (point-in-time consistent copy) of Microsoft Exchange data. This copy can be stored on local shadow volumes or on Tivoli Storage Manager server storage.

VSS Fast Restore
A function that uses a Microsoft Volume Shadow Copy Service (VSS)

software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on local shadow volumes.

VSS Instant Restore
A volume-level hardware-assisted Microsoft Volume Shadow Copy Service (VSS) function where target volumes that contain the snapshot are copied back to the original source volumes.

VSS offloaded backup
A backup operation that uses a Microsoft Volume Shadow Copy Service (VSS) hardware provider (installed on an alternate system) to move IBM Data Protection for Microsoft Exchange data to the Tivoli Storage Manager server. This type of backup operation shifts the backup load from the production system to another system.

VSS Restore
A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on Tivoli Storage Manager server storage to their original location.

W

wildcard character
A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace the wildcard character.

workstation
A terminal or personal computer at which a user can run applications and that is usually connected to a mainframe or a network.

worldwide name
A 64-bit, unsigned name identifier that is unique.

workload partition (WPAR)
A partition within a single operating system instance.

Index

A

accessibility features 203
activation 11
archive logs 2

B

backups
  Tivoli Storage Manager
    scheduler 169
books
  See publications

C

customer support
  contact xiii

D

Data Protection for Domino
  operating environment 1
  security 13
Data Protection for Domino for AIX
  installing 18
database
  restoring Domino server 10, 11
definitions 209
disability 203
disaster recovery
  strategy for 5
documentation
  See publications
domarc file
  example of 171
Domino database
  restoring 10, 11
Domino server
  restoring 10, 11

E

education
  see Tivoli technical training x
example of
  domarc file 171
  Tivoli Storage Manager
    scheduler 169

F

file
  example of domarc 171
fixes, obtaining xii
full backup 5
full DB2 database backup 9
full plus transaction log archives 5

G

glossary 209

I

IBM Publications Center vii, x
IBM Support Assistant xii
installation
  installing Data Protection for Domino for AIX 18
Internet, searching for problem resolution xi, xii

K

keyboard 203
knowledge bases, searching xi

L

log, transaction
  restoring 10, 11
  strategy for 5

M

manuals
  See publications

O

operating environment
  overview 1

P

Passport Advantage xiii
problem determination
  describing problem for IBM Software Support xiv
  determining business impact for IBM Software Support xiii
  submitting a problem to IBM Software xiv
publications
  download vii
  order vii
  search vii
  Tivoli Storage FlashCopy Manager x
  Tivoli Storage Manager viii

R

recovery, disaster
  strategy for 5
restore process 10, 11
restoring
  Domino database 10, 11

S

scheduler
  example of to automate backups 169
security 13
software support
  describing problem for IBM Software Support xiv
  determining business impact for IBM Software Support xiii
  submitting a problem xiv
Software Support
  contact xiii
support contract xiii
support information x
support subscription xiii

T

Tivoli technical training x
training, Tivoli technical x
transaction log
  restoring 10, 11
  strategy for 5

Product Number: 5608-E06

Printed in USA

SC27-4021-00