
# Managing Servers

### Terms you'll need to understand:

- ✓ Transaction logging
- ✓ Activity logging
- ✓ Policy documents
- ✓ Administrator access
- ✓ Network names
- ✓ Directory deployment configurations

### Techniques you'll need to master:

- ✓ Analyzing activity data
- ✓ Applying policy documents to existing users
- ✓ Automating server tasks
- ✓ Changing administrator access
- ✓ Changing server access
- ✓ Configuring Domino network names
- ✓ Creating security policies
- ✓ Decommissioning a server
- ✓ Defining a backup process
- ✓ Defining Domino domains
- ✓ Enabling transaction logging
- ✓ Identifying a registration server
- ✓ Identifying supported protocols
- ✓ Implementing distributed and centralized directories
- ✓ Recertifying a server ID
- ✓ Searching for server references in a domain
- ✓ Setting up authentication with other Domino organizations

# Analyzing Activity Data

The key to analyzing data on a Domino server is the ability to log the information. This process is known as *activity logging*. To set up activity logging on the Domino server, follow these steps:

1. Select the Configuration tab on the Domino Administrator.
2. Select the Server tab and select Configurations in the task pane. Select Edit Configuration in the results pane to open the document.
3. Open the Activity Logging tab and select the Activity Logging Is Enabled check box to open the selection criteria available for the Activity Logging tab.
4. Select the enable logging type to be logged. Valid selections include
   - ➤ Domino.AGENT
   - ➤ Domino.HTTP
   - ➤ Domino.IMAP
   - ➤ Domino.LDAP
   - ➤ Domino.POP3
   - ➤ Domino.SMTP.Session
   - ➤ Domino.SMTP.Message
   - ➤ Domino.Notes.Database
   - ➤ Domino.Notes.Passthru
   - ➤ Domino.Notes.Session
   - ➤ Domino.REPLICA
   - ➤ Domino.MAIL
5. Select a time for the checkpoint interval (choose either Log Checkpoint at Midnight or Log Checkpoint for Prime Shift).


If Log Checkpoint at Midnight is selected in step 5 of the procedure for setting up activity logging on the Domino server, the session activity for the selected options will be added to the log at midnight. If Log Checkpoint for Prime Shift is selected, the session activity for the selected options will be logged at the start and the end of the work shift.

6. Select the Activity Trends tab, and then select the Basics tab (see Figure 14.1).
7. In the Activity Trends Basic Configuration section, select the Enable Activity Trends Collector check box.
8. In the Activity Trends Collector Database path, enter the name of the database to be used. The default name is ACTIVITY.NSF.
9. Enter the time to run the task in the Time of Day to Run Activity Trends Collector field.
10. Select the days of the week to run the task.
11. In the Activity Trends Data Profile Option section, "Use Defaults" is selected by default. Deselecting the Use Defaults check box provides the following options:
    - ➤ Trends Cardinal Interval
    - ➤ Observation Time Bucket Seconds
    - ➤ Maximum Observation List Size
    - ➤ Trends History Interval

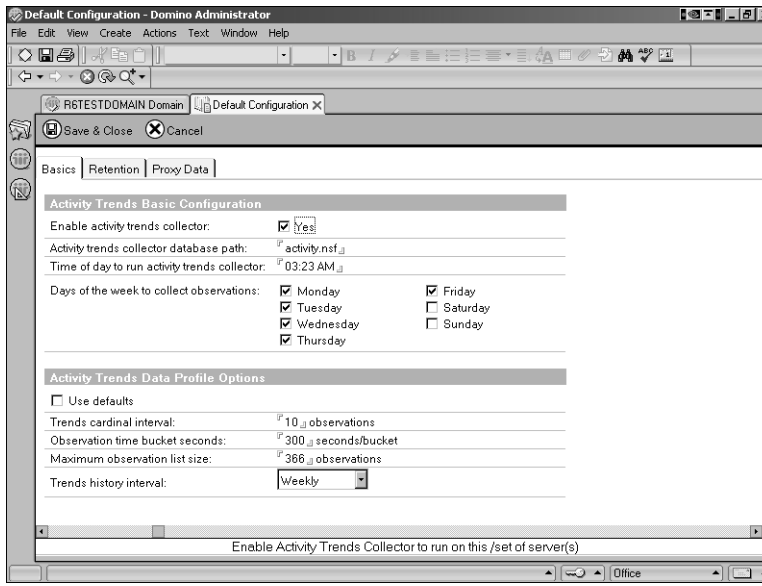


**Figure 14.1** The Activity Trends tab is used to determine when the collector will gather information.

12. Select the Retention tab. To change the default retention period, deselect the Use Defaults check box and change the retention time.
13. Select the Proxy Data tab. A free form box is available to enter a list of databases that can be searched for activity data when requested by Administrator clients.
14. Click Save & Close when all selections have been made.

After the document has been saved, navigate to the Server tab in the Administrator client, navigate to the Analysis tab, and select Analyze from the Tools pane on the right. After the Analyze tab has been opened, select Activity to open the Server Activity Analysis dialog box (see Figure 14.2). Select the activity types to log (all are selected by default) and the start and end dates. The final step is to select the log database (if you plan to use anything except for the Activity Analysis database). Click OK to save your changes. The Activity Analysis database opens automatically so that collected data can be viewed.

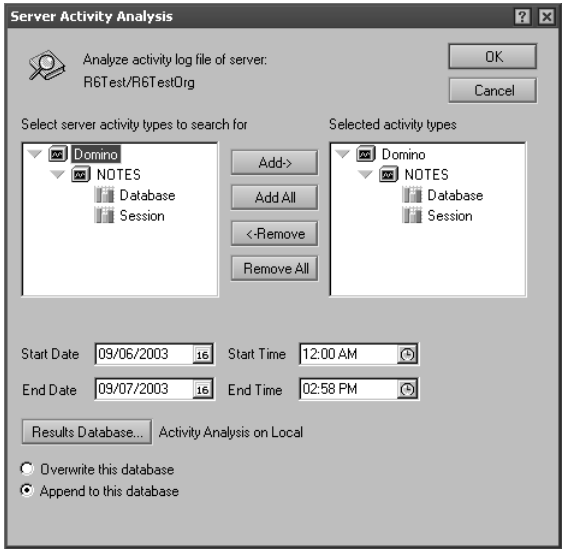


**Figure 14.2** The Server Activity Analysis dialog box is used to select the activity types to log.


Policy documents make management of the Domino domain easier and provide consistency when multiple administrators are involved. Be sure that you understand how policy documents are created and the types available when studying for the exam.

# Applying Policy Documents to Existing Users

*Policy documents* are used to regulate how users can access the system and perform specific functions. Policy documents can be changed after they are assigned and the modified documents will then be applied to all policy users.


All clients and servers participating in policy document deployment must be running a minimum of version 4.67a or greater or directory replication errors will occur.

Policy documents that can be applied to users include

- *Archiving*—Defines policy settings related to a user's ability to archive mail.
- *Desktop*—Enforces consistent client settings. If a client setting is changed and then the workstation logs out of the server, the settings are reset the next time the user logs into the server.
- *Registration*—Implements these policies when a new user is created during registration.
- *Setup*—Enforces settings in the client's location document.
- *Security*—Defines password management and ECL setup.

Types of Domino policies to consider include

- *Explicit policies*—Use this type of policy when specific groups or users in the organization need specific access; explicit policies define their access. Use this policy when making changes to users already defined in the domain, such as when making changes to groups.
- *Organizational policies*—Use this type of policy when specific settings are required for users in a specific Organizational Unit (OU), such as when making changes to a department.

Policies can be assigned to existing users by editing the Person document. To change policies, a user's ACL level needs to be set to at least Editor, or Author level with the UserModifier role assigned. Navigate to the Administration tab and complete the Policy Management section to assign policies to the user. Click Save & Close to update the Person document.

Policies can also be added to users and groups by using the Administrator client. Select the People & Groups tab and under the Tools pane, select either People or Groups and click Assign Policy. Make the desired changes and then click OK to make the change.

# Automating Server Tasks

Server tasks can be automated in one of two ways, either by assigning them in the Notes.ini file to run when the server starts or by creating a program document. Compacting databases or running system utilities are examples of programs used in Program documents. To create a Program document, open the Domino Administrator and navigate to the Configuration tab. Select Servers, Programs, and select Add Program. Complete these fields on the Basics section of the Basics tab:

- Program Name
- Command Line
- Server to Run On
- Comments (used to assist the administrator to define the purpose of the Program document)

The Basics tab also has a section where the Schedule is defined. The valid fields in this section are

- Enabled/Disabled
- Run at Times
- Repeat Interval of
- Days of Week

Select the criteria needed for this document and click Save & Close. Entering Show Schedule at the server prompt shows all tasks, including programs that are enabled on the server.


Lotus has broken the Domino Administrator out from a single user to multiple users that have varying access to perform different tasks. To prepare for the exam, study the different types of administrators and test them in your development environment.

# Changing Administrator Access

Domino allows for multiple levels of administrators. They include

- *Full access administrator*—All levels of access to the system, including operating system and Domino system configuration access. This is the highest level of access available on the Domino system.
- *Administrator*—Access at this level is the same as a database administrator and full-console administrator access.
- *Full console administrator*—View-only access to the Domino Console. This level of administrator is not able to make changes to the system configuration.
- *System administrator*—Limited to the restrictions of operating system administrator only

*Administrator access*, or defining how an administrator can change server configurations, is set using the Domino Administrator client. Select the Configuration tab, and then open the Server document. Navigate to the security page and add or change users to groups as needed.


Full access administrators, administrators, and database administrators have full access to delete databases even if they are not explicitly listed as managers in the ACL of the database. Take care when defining these users to ensure that only properly authorized users are able to delete databases.

Full access administrators can be prevented from accessing the server by adding the line SECURE_DISABLE_FULLADMIN=1 in the Notes.ini file. This does not act the same as a deny user list, however, and if a user is explicitly defined in the Domino Directory or a database with specific access, that setting will override the setting in the .ini file.

Options for setting up full access administrators include

- Generate a full admin ID file that can only be used by full access administrators.
- Generate a certifier ID with OU-level full administrator access and certify users.
- Don't assign anyone and only add users to the Full Access Administrator field as needed.


Understanding how users and servers access the Domino domain is key for anyone studying to be a certified administrator. As you prepare for the exam, be sure that you understand how to change server access and the access control types that are available.

# Changing Server Access

Server access is enabled by completing the information in the Server Access section on the Security tab of the Server document. Modification of the fields on the Security tab allow an administrator to change access to the server.

Available server access control types include

- *Access Server*—This field is used to define users and groups who can access the server.
- *Not Access Server*—This field defines users and groups who are prohibited from accessing the server. This field is typically used for users who have left the company or may have been moved to a different Domino domain.
- *Create Database & Templates*—This field defines users who can create new database and template files and can also execute copy commands.
- *Create New Replicas*—This field defines users who can create new replicas of databases or template files.
- *Create Master Templates*—This field defines users who can create master templates. Master templates have a template name defined in the database properties. If this field is left undefined, no users will have the ability to create master templates.
- *Allowed to Use Monitors*—This field defines users and groups who are permitted to use monitors on the server.
- *Not Allowed to Use Monitors*—This field defines users who cannot use monitors on the server.
- *Trusted Servers*—This field defines which servers can access the server.

# Configuring Domino Network Names

A Notes named network is a group of servers that have the same network name and use the same port type to communicate. The *network name* is used

to identify these servers as a group. Domino network names are defined on the Ports tab of the Server document. To create a Notes named network, complete the information on the Notes Network Ports tab under the Notes Network section. The default name for networks is Network1, but this can be changed during registration or by editing this field. The maximum allowable networks are 31. Servers in the same Notes network can route mail without requiring Connection documents.

# Creating Security Policies

*Policy documents* are used to maintain consistent standards in the domain. Security policy documents are used to maintain execution control lists and password data on Notes and Internet passwords. Editor access to the Domino directory and PolicyCreator and PolicyModifier roles are required to create security policies. To create a security policy, follow these steps:

1. Using the Administrator client, navigate to the People & Groups tab and select the Settings view.
2. Select the Add Settings button in the main view and choose the Security option from the drop-down list. The Basics tab will now be displayed.
3. Complete the Name and Description fields on the Basics tab.
4. Navigate to the Password Management tab. Change these settings as needed based on the configuration for the server:
   - ➤ Allow users to change Internet password over HTTP
   - ➤ Update Internet password when Notes client password changes
   - ➤ Check Notes password
   - ➤ Enforce password expiration
   - ➤ Required change interval
   - ➤ Allowed grace period
   - ➤ Password history
   - ➤ Required password quality
5. Navigate to the Execution Control List tab and complete these steps as required for the specific server configuration:
   - ➤ *Admin ECL*—Select Edit to used a predefined Admin ECL setting or select New to create a new set of criteria to be used.

- *Update Mode*—Choose Refresh or Replace.
- *Update Frequency*—Choose When Admin ECL changes, Once Daily, or Never.

6. Complete the desired changes, and then click Save & Close to save the document.

# Decommissioning a Server

A server is decommissioned when it is no longer needed in the domain or when the users and databases are being consolidated to another server and the server is being permanently retired. Domino uses a tool called the Decommission Server Analysis tool to assist administrators in determining the impact on removing a server from the domain. When the tool is run, a database is generated that compares the existing server with the new server, so that the administrator has an idea what needs to be changed on the new server to guarantee a smooth transition. However, the database is meant to be a starting point and should not be considered an all-inclusive guide for all points that should be considered when using the tool.

For the Decommission Server Analysis tool to operate, both servers must be in the same domain and their hierarchical names must be consistent.

You must properly prepare for the server decommissioning process. Before decommissioning a server, be certain you have taken care of the following items:

- Make sure that system backups are complete and verified.
- Verify that database formulas do not have explicit server reference information.
- Update configuration information in the directory that may have the existing server name defined in it, such as Connection and Program documents.
- Document all cross certificates and make sure that all certifier IDs are available to cross certify the new server.
- If the existing domain has Connection documents to external domains, be certain to notify the other domain administrators of the planned change.
- Notify users of the change.
- Verify that all protocols and named networks are set up correctly.

- Be certain that both servers contain matching databases with the same replica ID.
- Verify that all mail routing configuration information is correct and in place.

When you have verified that all of the preceding tasks have been performed, you can run the Decommission Server Analysis tool.


Be sure that administrator access is properly defined on both the source and target servers. If the access is not defined properly, the decommission process may fail or the report may not contain the correct information.

Complete the following steps to run the Decommission Server Analysis tool:

1. Using the Administrator, select the Server tab and then choose the Analysis tab.
2. Navigate to the Tools pane and Analyze tab. Select Decommission Server.
3. A dialog box appears. Verify that the source server to be commissioned is correct.
4. Select the target server that will replace the existing server.
5. The default name for the Results database is DECOMSRV.NSF. If the name of the database needs to be changed, select the Results Database button and select a new database.
6. The default setting for writing to the database is Append. Using this setting, if an existing database is in place, the tool will write the information to the end of the database. If Overwrite is selected, new results will be created and the previous information will be deleted.
7. Select OK to use these settings and continue with the analysis.

When the tool has completed the analysis, the database should open to the Reports view. Examine the reports and correct any discrepancies before completing the decommissioning of the server.

# Defining a Backup Process

Domino is versatile in that it provides two ways to back up your data. The typical method of backups can be used, such as tape or digital media, or

transaction logging can be used. When using a traditional version of backing up the server, you should consider the following:

- Verify that the backup utility can back up open files. Domino keeps the LOG.NSF,NAMES.NSF,MAIL.BOX, and the server ID file open at all times. If the backup software being used will not backup open files, create a Program document that will stop the server, run the backup routine, and then restart the server to make sure these files are archived.
- Keep an archived version of the server ID file, administrator ID files, and all certifier IDs stored in a secure location.
- Maintain an up-to-date copy of the Domino Directory on a local workstation.

# Defining Domino Domains

Domains are defined by creating Domain documents. Multiple document types are available based on the requirements needed to route mail. The following types of documents are available:

- *Adjacent domain document*—This document is used to route mail between servers that are not in the same Notes named network.
- *Nonadjacent domain document*—This document serves three functions:
  - Supplies next-hop routing information to route mail
  - Prohibits mail from routing to the domain
  - Provides Calendar server synchronization between two domains
- *Foreign domain document*—This document is used for connections between external applications. A typical application used is a fax or pager gateway.
- *Foreign SMTP domain document*—This document is used to route Internet mail when the server does not have explicit DNS access.
- *Global domain document*—This document is used to route mail to Internet domains. Configuration information regarding message conversion rules are defined in the document.

# Enabling Protocols

Domino supports various protocols that are enabled on the Ports tab of the server document. The following protocols can be enabled:

- *HTTP*—Used for Web access
- *IIOP*—Used to allow Java code to run on the server
- *LDAP*—Used for addressing services
- *POP3*—Used to access Internet mail, typically used by clients such as Netscape Navigator
- *IMAP*—Used to access Internet mail, typically used by clients such as Microsoft Outlook
- *SSL*—Used to provide data encryption and security

Select a protocol based on the intended use when changing the Server document settings.

# Enabling Transaction Logging

*Transaction logging* is available for Domino servers running release 5 or later and databases using release version 5 or later On Disk Structure (ODS). Database changes are sent to a transaction log database and then written later to the target database. Transaction logging offers benefits for the following system activities:

- Backup throughput is increased because transaction logs back up quicker than normal databases.
- Disaster recovery is more complete in that data that was stored in the transaction log can be supplemented to the full system recovery so data is not lost. Data that is stored in the transaction log file is written to the database when the log file is recovered from tape.
- Database views are stored in the log file so database views may not need to be rebuilt.


Although transactional logging is a form of backup, it does not replace a true archiving system, such as tape or optical media. In the event of a server crash, full system backups will be needed to recover. In addition, special backup software is required that specifically backs up the transactional log, so make sure that it is supported by the software vendor.

Transactional logging also creates a unique database instance ID (DBIID) for each database. When transactions are added to the log, the DBIID is assigned so that the source database can be recorded. DBIID tags are assigned at the following times:

- The first time transaction logging occurs
- In some instances when the Compact task is executed, such as reducing file size
- When fixup is used to correct a corrupted database
- When a database is moved to a server using transaction logging

## Transaction Logging Versions

You can choose from three different versions of transaction logging, including Circular, Linear, and Archived. Here are descriptions of each of these transaction logging versions:

- *Circular*—This version of logging uses up to 4GB of disk space and then begins writing over the oldest log information in the database. The transaction log database should be backed up daily using this deployment version.
- *Linear*—This version of logging is similar to circular logging, but can use more than 4GB of disk space.
- *Archived*—This version of logging creates transaction logs as needed. Log files are not overwritten; they are archived. Ensure that the logs are being backed up regularly or the server might run out of disk space

## Implementing Transaction Logging

Transaction logging needs to be properly planned before it can be implemented. Steps to complete before implementing transaction logging include

- Make sure the server hardware is properly configured. Use a disk array with at least RAID 1 support and a dedicated disk controller.
- Define a backup plan and use software that supports Domino servers running transaction logging.
- Plan to use logging on all available databases, but remember that only databases using the R5 ODS or later will be able to use transaction logging.
- Decide which version of logging to use (Circular, Linear, or Archived).

To set up transaction logging on the server, follow these steps:

1. Using the Domino Administrator, select the Configuration tab, select the Server document, and then click Edit Server Document.
2. Select the Transactional Logging tab.
3. In the Transactional Logging field, select either Enabled or Disabled.
4. In the Log Path field, enter the explicit path to the transaction log database.
5. In the Logging Style field, select either Circular, Linear, or Archived.
6. The default selection for the Use All Available Space On Log Device is No. If you use the default selection, in the Maximum Log Space field, enter the amount of space in megabytes to be used for the transaction log database.

   If you select Yes in the Use All Available Space On Log Device field, the next option, Maximum Log Space, is removed as a valid selection.
7. Choose Enabled or Disabled in the Automatic Fixup Of Corrupt Databases field. If Automatic Fixup is not enabled, administrators will need to manually perform database maintenance when errors occur.
8. In the Runtime/Restart Performance field, choose from the valid options in the drop down menu: Favor Runtime, Standard, and Favor Restart Recovery Time.
9. In the Quota Enforcement field, choose from these valid options:
   - ➤ Check Space Used in File when Adding a Note
   - ➤ Check Filesize when Extending the File
   - ➤ Check Filesize when Adding a Note
10. Select Save & Close to start transaction logging.

# Identifying a Registration Server

Domino uses a Registration server to define changes made to the Directory and then replicates the changes to all servers in the domain. By using a single instance of the Directory for all changes, consistency is maintained throughout the domain.

A registration server is defined using the Administrator client. To do so, follow these steps:

1. Click the File menu and select Preferences.
2. Select Administration Preferences from the submenu.
3. From the available selections, click Registration. This tab allows an administrator to select a registration server.
4. Select the Registration Server button.
5. Select the server to be used as the registration server and click OK. Click OK again to close the Administration Preferences dialog box. The registration server is now set.

# Implementing Distributed and Centralized Directories

Domino provides multiple options when presenting directories in the domain. The key point to remember is that the Domino Directory is accessed by all users as well as servers, so care should be taken to ensure that user and server access is optimized for the best throughput. Three ways to provide directory access are

- *Distributed*—This method assumes that each server has a replica copy of the directory on each server in the domain. This method is optimal when many users are on the network or the communications infrastructure may have many points of congestion.
- *Centralized*—This method uses the administration server as the central point for the directory and configuration directories. Configuration directories host Server, Connection, and Configuration Setting documents. Typically, a second server also has these directories for disaster recovery purposes in the event that the registration server fails.
- *Hybrid*—This method uses a combination of distributed and centralized. Local users may use the centralized directory, whereas remote users would have a local copy of the directory on their server so that bandwidth would not be an issue.

# Recertifying a Server ID

Periodically, certificates associated with a server ID expire. When this occurs, the ID needs to be recertified. To recertify a server ID, the administrator must have either Author access to the Domino directory and the ServerModifier role assigned or Editor access to the directory. In addition, the administrator must have Author access or greater to the certification log. The following steps allow a server ID to be recertified:

1. Using the Administrator client, select the Configuration tab and select the Server document for the server to be recertified.
2. Open the Certification tab under the Tools pane and select Certify; the Choose a Certifier dialog box appears.
3. Click the Server button to select the Registration server and click OK.
4. In the Registration Server dialog box, choose an option to determine how you will register the server. The options include
   - ➤ *Supply Certifier ID and Password*—If you choose this option, a file navigation box appears. This option is used if a certifier ID is used to authorize access to the domain. Navigate to the required certifier id and select OK.
   - ➤ *Use the CA Process*—This option allows the administrator to recertify the ID without having access to the certifier ID or the certifier password, by using a Certificate Authority (CA), instead. If you choose this option, use the drop-down box it provides to select a CA-configured certifier from the ones available on the server.
5. After you've selected one of the two options, click OK. If Supply Certifier ID and Password is chosen, a dialog box appears requiring the certifier password. Enter the password and click OK to continue.
6. A file navigation box appears prompting for the ID to be certified. Select the server's ID file and click OK; the Certify ID dialog box appears.
7. In the Expiration Date field, choose a setting to determine when the server will need to be recertified. The default time is two years, but can be changed as needed.
8. In the Subject Name List field, type a common name for the ID if desired (this field is optional). This is used to identify the user in the Directory.

9. In the Password Quality field, use the slide bar to determine the quality of password security to assign to the ID file. The default location of the slider is to the extreme left, which is No Password and a value of 0. Sliding the bar to the extreme right forces a very strong password and a value of 16. Although it is true that this is optimal for servers, each time the server is loaded, a password will be required at the console before the server will start.
10. Select Certify to continue and recertify the ID; a dialog box appears asking if the administrator wants to certify another ID.
11. Select Yes to certify more IDs or No to exit the certification process.

# Searching for Server References in a Domain

Domino provides the ability to search for files across multiple servers using a tool called Domain Search. Database information that is searchable includes documents, files, and file attachments.

Setting up Domain Search requires a server to be designated as the indexing server. This server creates a master index that contains all of the results from search queries run in the domain. The database that is used by Domain Search is Domain Catalog. The databases in the domain are then searched by the indexing server using a search spider. Based on the size of the domain, this task could take a few hours, a few days, or a few weeks.

Indexing is an intensive task and proper consideration should be taken to make sure that the indexing server is adequately configured to handle the work. Multiple processors, disk arrays with high-speed access, and large amounts of RAM are recommended for the indexing server. Lotus recommends a dedicated indexing server if more than six servers in the domain will be participating in the Domain Search, but use this as a "rule of thumb" only based on the configuration of the domain. When a user's search is performed, the indexing server accesses the Domain Catalog and returns search results that are valid based on the user's access restrictions.


Proper planning is the most important consideration when setting up the Domain Search. Indexing unnecessary files, such as Administration Requests databases, catalogs, and libraries, adds no value to the search and wastes space.

When setting up the Domain Search program, set the search spider to run at a time when server use is low, typically at night.

Follow these steps to set up the Domain Search:

1. Create the Domain Catalog on the indexing server. Create a new database using the CATALOG.NTF as the database template.
2. Using the Domino Administrator, open the Configuration tab and select the server to be used as the indexing server. Click Edit Server to open the Server document.
3. Navigate to the Server Tasks tab, choose the Domain Indexer tab, and select enabled for the Domain Catalog field. In the Limit Domain Wide Indexing to the Following Servers field, select the servers to add to the search.
4. Click Save & Close to save the document.
5. This task requires a server restart before it starts. Restart the server when possible and then verify that the Directory Indexer task has started by issuing a `show tasks` command at the server prompt.

# Setting Up Authentication with Other Domino Organizations

For Domino organizations to be capable of exchanging data, they must share a common certificate. This is accomplished by using an organization certifier ID file. Cross certifying a user or server ID with an organizational certifier guarantees that both IDs have a common certificate. Domino uses two types of certifier IDs related to organizations:

- *Organization certifier ID*—The default name for this ID file is CERT.ID. This ID file is created when the server is deployed. This ID typically includes the company name and is the highest point on the hierarchy tree.
- *Organization unit certifier IDs*—This level of organizational certifier is typically used to delineate the next level on the hierarchy tree, usually identifying county or department names.

# Creating a New Organization Certifier ID

To create a new organization certifier ID, follow these steps:

1. Using the Administrator client, select the Configuration tab and open the Tools pane. Select Registration, and then click Organization from the menu; the Register Organization Certifier dialog box appears.
2. Enter the organization name and choose a country code (the latter is optional).
3. In the Certifier Password field, enter a new password that will be required when certifying IDs for the new organization.
4. Use the Password Quality slider to determine the quality of password security to assign to the ID file. The default location of the slider is to the extreme left, which is no password and a value of 0. Sliding the bar to the extreme right forces a very strong password and a value of 16. Although it is true that this is optimal for servers, each time the server is loaded, a password will be required at the console before the server will start.
5. In the Security Type field, choose North American or International.
6. In the Mail Certification Requests To field, choose Administrator.
7. Optionally, add a location and comments.
8. Click Register to create the new certifier ID.

# Creating a New Organizational Unit ID

To create a new Organizational Unit ID, complete these steps:

1. Using the Administrator client, select the Configuration tab and select the Server document for the server to be recertified.
2. Open the Certification menu selection under the Tools pane and select Organization Unit; the Register Organization Certifier dialog box appears.
3. Click the Server button to select the Registration server and click OK. You are then presented with two options:
   - *Supply Certifier ID and Password*—A file navigation box appears when this option is selected. Navigate to the required certifier ID and select OK. If you choose this option, go to step 4.

- *Use the CA Process*—This option allows the administrator to recertify the ID without having access to the certifier ID or the certifier password. A drop-down box is provided to allow the administrator to select a CA-configured certifier from the ones available on the server.

4. If you chose Supply Certifier ID And Password in step 3, a dialog box appears requiring the certifier password. Enter the password and select OK; the Register Organizational Unit Certifier dialog box appears.
5. Select the registration server, and then select the certifier ID.
6. Select Set ID file to define the location for the new certifier ID being created.
7. Complete the Organizational field by entering a name for the new Organizational Unit.
8. Complete the Certifier password field by entering a new password.
9. Use the Password Quality slider to determine the quality of password security to assign to the ID file. The default location of the slider is to the extreme left, which is No Password and a value of 0. Sliding the bar to the extreme right forces a very strong password and a value of 16. Although it is true that this is optimal for servers, each time the server is loaded a password will be required at the console before the server will start.
10. In the Security Type field, choose North American or International.
11. In the Mail Certification Requests To field, choose Administrator.
12. Optionally, enter a location and/or comments.
13. Click Register to create the new ID file.

# Exam Prep Questions

## Question 1

What role is required for an administrator to be able to recertify a server ID?

- ❍ A. ID Modifier
- ❍ B. ServerModifier
- ❍ C. Server ID Moderator
- ❍ D. Mod_Ser_Complete

Answer B is correct. To recertify a server ID, the administrator must have either Author access to the Domino directory and the ServerModifier role assigned or Editor access to the directory.

## Question 2

Which of the following are valid options available when setting up activity logging? Choose all that apply.

- ❑ A. Domino.Agent
- ❑ B. Domino.IMAP
- ❑ C. Domino.POP3
- ❑ D. Domino.SMTP.POP4

Answers A, B, and C are correct. Valid selections available when setting up activity logging include Domino.AGENT, Domino.IMAP, and Domino.POP3.

## Question 3

Which of these configuration types of providing access to the Domino Directory is valid? Choose all that apply.

- ❑ A. Circular
- ❑ B. Distributed
- ❑ C. Decentralized
- ❑ D. Hybrid

Answers B and D are correct. The three valid configuration types to access the Domino Directory are Distributed, Centralized, and Hybrid.

## Question 4

Which of the following statements is true regarding transactional logging?

- ❍ A. While transactional logging is enabled, normal system backups are not required.
- ❍ B. Transactional logging is available for all versions of Domino running version 4.6.3 or later.
- ❍ C. Transaction logging requires database ODS version 5 or later.
- ❍ D. Any user can run transaction logging on their personal mailbox to conserve disk space.

Answer C is correct. Transaction logging is available for Domino servers running release 5 or later and databases using release version 5 or later ODS.

## Question 5

What steps can be taken in the Notes.INI file to prohibit Full access administrators from accessing the server?

- ❍ A. Add the line SECURE_ADMINSTRATOR_LOGIN=1.
- ❍ B. Encrypt the NOTES.INI file with private key encryption.
- ❍ C. Delete the Catalog task from the Server@Run list.
- ❍ D. Add the line SECURE_DISABLE_FULLADMIN=1.

Answer D is correct. Adding the line SECURE_DISABLE_FULLADMIN=1 in the Notes.ini file tells the server to ignore the Full Administrators field in the Domino Directory and explicit access for full administrators will need to be defined in database and applications.

## Question 6

What versions of transaction logging allows for databases greater than 4GB in size?

- ❍ A. Spiral
- ❍ B. Circular
- ❍ C. Linear
- ❍ D. Metrical

Answer C is correct. Linear transaction logging is similar to circular logging, but can use more than 4GB of disk space.

## Question 7

What is the default name of the database used for activity logging?

- ❍ A. ACTIVITY.NSF
- ❍ B. COLLECTION.NSF
- ❍ C. ACTIVITYSTAT.NSF
- ❍ D. ACTIVITY.LOG

Answer A is correct. The default database name used for activity logging is ACTIVITY.NSF.

## Question 8

Regarding password quality, which of the following statements are true? Choose all that apply.

- ❑ A. Password quality is selected by choosing radio buttons with preset levels defined.
- ❑ B. The strongest password selection has a value of 15.
- ❑ C. Values are set using a slide bar.
- ❑ D. A value of 0 signifies no password is defined.

Answers C and D are correct. Password quality is set using a slide bar to determine the quality of password security to assign to the ID file. The default location of the slider is to the extreme left, which is no password and a value of 0. Sliding the bar to the extreme right forces a very strong password and a value of 16.

## Question 9

What is the purpose of a Program document?

- ❍ A. Automation of server tasks
- ❍ B. Mail routing
- ❍ C. Database replication
- ❍ D. File purging

Answer A is correct. Server tasks can be automated in one of two ways, either by assigning them in the Notes.ini file to run when the server starts or by creating a Program document.

## Question 10

What is the purpose of the IIOP protocol?

- ❍ A. Provide communications channels to IIS servers.
- ❍ B. Allow java code to run on the system.
- ❍ C. Generate SMTP mail.
- ❍ D. Regulate Web server authentication.

Answer B is correct. The IIOP protocol allows java code to run on the Domino server.

# Need to Know More?

The Lotus Developers Domain: `www-10.lotus.com/ldd`.

Upgrading to Domino 6: Performance Benefits: `www.ibm.com/redbooks`.