Symantec Data Insight Administrator's Guide

Microsoft Windows

3.0

February 2012

Symantec Data Insight Administrator's Guide

3.0

Documentation version: 3.0.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Getting started with Symantec Data Insight administration

This chapter includes the following topics:

About Symantec Data Insight administration

You administer the Symantec Data Insight system through the Management Console. The console has components for system administration, viewing data access information, configuring policies and alerts, and generating reports, which are accessible from the tabs located on the header panel. Navigate to the **Settings** tab on the console to carry out the various Data Insight administration tasks.

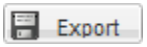
The Console is automatically installed with the Management Server. You access the Console through a Web browser that has a network connection to the Management Server. By default, the Management Server runs on HTTPS port 443. To access it, in the Web browser's address field, type `https://ms-host/`.

The Server Administrator user can see and access all parts of the administration console. Other users can see only the parts to which their roles grant them access. The user account under which you are currently logged on appears at the footer of the Management Console screen.

Operation icons on the Management Console

Table 1-1 shows the operation icons that are located on the console screen:

Table 1-1 Operation icons on the Management Console

Icon	Description
	Go up one level in the navigation control.
	Filter filers, Web applications, shares, site collections, users, and groups. The filter options depend on the current level of hierarchy.
	Clears the filter.
	The settings icon is also used in assigning custodians.
	Screen refresh. Symantec recommends using this refresh button instead of your browser's **Refresh** or **Reload** button.
	Email the data on the current screen to one or more recipients. If the current screens data cannot be sent as an email, the icon is unavailable.
	Exports all data on a panel on the current screen to a `.csv` file.
	Exports all data on the current screen to a `.csv` file.

Data Insight administration tasks

Table 1-2 summarizes the tasks to be performed to set up a new Data Insight installation:

Table 1-2 Data Insight administration tasks

Action	Description
Configure SMTP server settings.	See "Configuring SMTP server settings " on page 29.

Table 1-2 Data Insight administration tasks *(continued)*

Action	Description
Setup notification policies.	See "Configuring email notifications " on page 153.
Configure directory service domain.	See "Adding a directory service domain to Data Insight" on page 46.
Configure data retention settings.	See "Configuring data retention settings" on page 39.
Configure Exclude Rules.	See "Adding exclude rules to Symantec Data Insight " on page 34.
Install license.	See "Managing Data Insight licenses " on page 43.
If monitoring events for NetApp file servers, configure Fpolicy service on collectors.	See "Preparing Symantec Data Insight for Fpolicy " on page 61.
If monitoring events for EMC Celerra file servers, configure Celerra service on collectors.	See "Configuring EMC Celerra filers" on page 67.
If monitoring events for Windows file servers , upload agent packages to collectors.	See "Configuring Windows File Servers " on page 70.
If monitoring events for SharePoint servers, install the Data Insight Web service on the SharePoint server.	See "Installing the Data Insight Web service for SharePoint" on page 104.
Configure file servers. Configure the SharePoint Web applications.	See "Adding filers" on page 76. See "Adding Web applications" on page 105.

Credentials required for configuring NetApp filers

Table 1-3 lists the set of credentials that are required by Symantec Data Insight during system configuration.

Table 1-3 Credentials for configuring NetApp filers

Credential	Details
Credentials required to configure DataInsightFpolicy service. The DataInsightFpolicy service runs on the Collector and processes the events that are sent by the NetApp filer using the Fpolicy RPC interface. This service must be configured on each Collector that is used to connect to NetApp filers. DataInsightFpolicy service also performs miscellaneous tasks, such as gathering storage information from the filer.	The credential should belong to a user in the domain of which the Data Insight Collector node and the NetApp filers are a part. This user should be a part of the Backup Operators group on the filer. If the filers belong to different untrusted domains than the Collector, you can use the Local System account to run the DataInsightFpolicy service. However, when you add filers, the account you specify to configure the DataInsightFpolicy service for the filers must have Backup Operator privileges on the filer.
Credentials required during filer configuration through the Symantec Data Insight Management Console.	Required to discover shares and enabling Fpolicy on the NetApp filer. This credential belongs to the NetApp ONTAP user who has administrative rights on the NetApp filer (for example, root) or a domain user who is part of the Administrators group on the filer. Or, this credential belongs to the NetApp ONTAP user or a domain user who is a non-administrator user on the filer, but has specific privileges. See "Preparing a non-administrator domain user on the NetApp filer for Data Insight" on page 24. **Note:** The domain user can be the same user account that was specified when configuring the DataInsightFpolicy service. If you use the Local System account to configure the DataInsightFpolicy service on the Collector, the user you specify here must also belong to the Backup Operators group on the filer. See "Preparing Symantec Data Insight for Fpolicy " on page 61.

Table 1-3 Credentials for configuring NetApp filers *(continued)*

Credential	Details
Credentials required for scanning of shares.	

Table 1-3 Credentials for configuring NetApp filers *(continued)*

Credential	Details
	Required for scanning of shares from the NetApp filer. When scanning CIFS shares, this credential belongs to the user in the domain of which the NetApp filer and the Symantec Data Insight Collector node are a part. This user must belong to either the Power Users or Administrator's group on the NetApp filer. If the credential is not part of one of these groups, the scanner will not be able to get share-level ACLs for shares of this filer. You do not need this privilege if you do not want to get the share-level ACLs. In this case you will only need privileges to mount the share and scan the file system heirarchy. You must have the share-level READ permission. Additionally, the folder within the share must have the following file system ACLs: ■ Traverse Folder/Execute File ■ List Folder/Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions For scanning NFS shares, Data Insight needs a Unix account with at least read and execute permissions on all folders, alongwith at least read permission on all files. By default, Data Insight uses User ID or Group ID 0 to scan NFS shares. You can configure an alternate User ID or Group ID from the **Settings** > **Advanced Settings** section of the Collector node. See "Configuring advanced settings" on page 128. When monitoring only NFS shares, you can specify **Use Local System account** from the scanning credentials drop-down, else you can specify credentials required to scan CIFS

Table 1-3 Credentials for configuring NetApp filers *(continued)*

Credential	Details
	shares.

Credentials required for configuring EMC Celerra filers

Table 1-4 lists the set of credentials that are required by Symantec Data Insight during system configuration.

Table 1-4 Credentials for configuring EMC Celerra filers

Credential	Details
Credentials required to configure DataInsightCelerra service. The DataInsightCelerra service runs on the Collector and processes events sent by the CAVA services using the Windows RPC interface. This service must be configured on each Collector node that is used to connect to the EMC Celerra filers.	Required by the DataInsightCelerra service to run and authenticate itself with the EMC CAVA service provided by EMC, which runs on the Data Insight Collector node or in a server farm. The credential should belong to the user in the domain of which the Data Insight Collector node and the EMC filer are part.
Credentials required during filer configuration through the Symantec Data Insight Management Console.	Required to discover shares for EMC filer. This credential belongs to the EMC filer Control Station user who has administrative rights including XMLAPI v2 privilege (for example, nasadmin). See "Preparing Symantec Data Insight to receive event notification" on page 68.

Table 1-4 Credentials for configuring EMC Celerra filers *(continued)*

Credential	Details
Credentials required for scanning of shares.	Required for scanning of shares from the EMC filer. This credential belongs to the user in the domain of which the EMC filer and the Data Insight Collector node are a part. Additionally, to be able to obtain share-level ACLs, the credentials must belong to the Domain Administrators group on the file server. You do not need this privilege if you do not want to get the share-level ACLs. In this case you will only need privileges to mount the share and scan the file system heirarchy. You must have the share-level READ permission. Additionally, the folder within the share must have the following file system ACLs: ■ Traverse Folder/Execute File ■ List Folder/Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions See "Configuring EMC Celerra filers" on page 67.

Credentials required for configuring Windows File Servers

Table 1-5 lists the set of credentials that are required by Symantec Data Insight during system configuration.

Table 1-5 Credentials for configuring Windows File Servers

Credential	Details
Credentials required to install agent on the Windows File Server.	This credential belongs to a user in the Administrators group on the Windows File Server. The credential is also used to discover shares and obtain storage utilization information from the filer.

Table 1-5 Credentials for configuring Windows File Servers *(continued)*

Credential	Details
Credentials required to discover shares and obtain storage utilization information on the filer.	Required for monitoring shares or when configuring a Windows File Server cluster. This credential belongs to a user in the Administrators group on the file server. If your configuration is not a Windows cluster or you do not want to collect storage utilization information for the filer, a credential with the privilege to list shares on the filer is sufficient.
Credentials required for scanning shares on the Windows File Server.	Required to scan a share. This credential belongs to a user with necessary share-level permissions and file system ACLs on a Windows File Server share. To be able to obtain share-level ACLs, the credentials must belong to the Power Users or Administrators group on the Windows File Server. You do not need this privilege if you do not want to get the share-level ACLs. To be able to scan a Windows File Server share successfully, you must have the share-level READ permission. Additionally, the folder within the share must have the following file system ACLs: ■ Traverse Folder/Execute File ■ List Folder/Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions

Note: If you neither want Data Insight to install an agent automatically, nor do you want Data Insight to discover shares on the cluster or get storage utilization information, specifying the filer credentials is optional.

Credentials required for configuring Veritas File System (VxFS) servers

Table 1-6 lists the set of credentials that are required by Symantec Data Insight during system configuration.

Table 1-6 Credentials required for configuring VxFS filers

Credentials	Details
Credentials required during filer configuration through the Symantec Data Insight Management Console.	Required to discover shares on the VxFs filer. This credentials belongs to a user on the UNIX server who has administrative rights on the VxFS filer (for example, root). The credential should belong to a root user on the VxFS filer. Optionally, this credential can also belong to a local user who has access to the Data Insight namespace in the Veritas Operations Manager (VOM) agent installed on the VxFS filer. To configure a user other than the root user, you must create or use an existing user account, which you can use to add the filer into the Data Insight namespace. To add a local user account under VOM: **1** Log in as root on the VxFs filer. **2** Change directory to `/opt/VRTSsfmh/di/web/admin`. **3** Create a `.xprtlaccess` file, and add the user to that file. For example, add *vomuser@unixpwd:user*, where vomuser is the name of the local user account.

Table 1-6 Credentials required for configuring VxFS filers *(continued)*

Credentials	Details
Credentials required for scanning on VxFS filer server	Required for scanning of shares from the VxFS filer. For scanning NFS shares, Data Insight needs a Unix account with at least read and execute permissions on all folders, alongwith at least read permission on all files. By default, Data Insight uses the User ID or Group ID 0 to scan NFS shares. You can configure an alternate User ID or Group ID from the **Data Insight Servers** > **Advanced Settings** section of the Collector node. See "Configuring advanced settings" on page 128. Additionally, you must also have share-level READ permissions on the NFS export.

Credentials required for configuring SharePoint servers

Table 1-7 Credentials required for configuring SharePoint servers

Credential	Details
Credentials required to install the Data Insight Web service on the SharePoint Server.	This credential belongs to a user in the Administrators group on the SharePoint server.
Credentials required to discover Web applications or site collections, and to collect scan information and audit data	This credential belongs to a site collection administrator for the configured sites and it must be in the same domain as the SharePoint server. It must have full control permissions not only on the configured Web applications, but also on the Web applications that are added to SharePoint subsequently.

Preparing a non-administrator domain user on the NetApp filer for Data Insight

To configure a NetApp filer from the Management Console, you can use an account which is not in the administrators group on the NetApp filer, but has some specific privileges.

Perform the following steps on the NetApp filer console to add a non-administrator user, for example, *testuser*.

To create a non-administrator user

1. Create a new role, for example *testrole*, using the `useradmin` utility on the filer.
2. Add the login-* and api-* capabilities to the role.

   For example, `useradmin role add testrole -a login-*,api-*`.

   You can also choose to assign specific capabilities to the role.

   Table 1-8 provides a detailed description of each capability.
3. Create a new group, for example, *testgroup* and apply the role *testrole* to it.

   For example, `useradmin group add testgroup -r testrole`.
4. Add the user *testdomain\testuser* to *testgroup*

   For example, `useradmin domainuser add testdomain\testuser -g testgroup`.
5. Add the user *testdomain\testuser* to *Backup Operators* group.

   For example, `useradmin domainuser add testdomain\testuser -g Backup Operators`.

Note: For vfilers, append the above command-line examples with `vfiler run <vfilername>`.

Table 1-8 Additional capabilities for adding a non-administrator user account

Capability	Description
login-http-admin	Enables you to log into the NetApp filer and run commands. With this capability, you can get latency statistics (for scan throttling), volume size information, or discover shares.

Table 1-8 Additional capabilities for adding a non-administrator user account *(continued)*

Capability	Description
api-system-get-ontapi-version api-system-get-version	Enables you to get the ONTAPI version number and the system version number respectively. These are required to set the login handle context properly. Data Insight reports a failure when you test the connection to the filer, if these capabilities are absent Also, if these capabilities are absent, you will not be able to execute any APIs including those required to discover shares, and get latency statistics.
api-fpolicy-set-policy-options	Enables you to set a flag on the NetApp filer to enable ACL change notifications. If you choose not to supply this capability to Symantec, the filer administrator must set this property manually using the root telnet console (`fpolicy options <policyname> cifs_setattr on`).
api-fpolicy-list-info api-fpolicy-create-policy api-fpolicy-enable-policy api-fpolicy-disable-policy api-fpolicy-destroy-policy	Required to enable Data Insight to automatically create and enable Fpolicy on the Netapp filer. Optionally, the filer administrator can set up the policy using the root telnet console.
api-fpolicy-server-list-info	Used to retrieve useful statistics from the NetApp filer, such as, total event count and event failures These APIs are used every 2 hours so they do not load the system. However, absence of these capabilities does not cause any problems.
api-options-set	Used to enable the global Fpolicy flag on the NetApp filer.
api-cifs-share-list-iter-start api-cifs-share-list-iter-next api-cifs-share-list-iter-end	Used to discover shares on the NetApp filer. Absence of these capabilities can result in a failure to discover the shares. Optionally, you can add shares manually from the Data Insight console.

Table 1-8 Additional capabilities for adding a non-administrator user account *(continued)*

Capability	Description
api-perf-object-get-instances-iter-start api-perf-object-get-instances-iter-next api-perf-object-get-instances-iter-end	Used to get CIFS latency information from the NetApp filer, which enables the self-throttling scan feature of Data Insight. Absence of these APIs can cause scanner to fail if you enable the throttled scanning feature.
api-volume-list-info	Used to periodically fetch size information for NetApp volumes.

About the Data Insight dashboard

The Data Insight dashboard displays the status of the following:

- A summary of the incremental and full scans of the configured filers and SharePoint Web applications for the selected time period.
  The graph displays the number of successful, failed, or partial scans on configured shares and SharePoint site collections. On the Scan Summary bar graph, the Y-axis represents the total number of scans and the X-axis represents the time duration. The status of the success of the scan is rendered in different colors.

Viewing summary reports

You can view the summary reports on the Data Insight dashboard.

To view summary reports

1 In the Management Console, click the **Settings** > **Dashboard**.

The dashboard showing the summary of full and incremental scans appears.

For each performance graph, you can do the following:

- Specify the duration for which you want to view the summary. You can view data for the last seven days, last four weeks, last one month, or last three years.

- Move the mouse pointer over the line chart. A tool tip is displays information corresponding to the position of the mouse pointer on the graph.

2 Click an area on the bar to view detailed events for the selected time period.

The **Events** page appears, where you can view the events filtered by the time period represented by the bar that you click.

On the **Events** page you may see little more or little less number of events than indicated on the dashboard. This can happen due to timezone issues.

See "Viewing events " on page 154.

Handling changes in account password

You use various account credentials at the time of configuring the Data Insight system. Accounts are used when configuring the following:

- Fpolicy Service
- Celerra Service
- Filers
- Scanner
- Active Directory

Perform the following steps to ensure that updates to account passwords are synchronized with the passwords used in Data Insight:

To handle changes in account password

1 Determine the places where the account is being used.

2 Log in to the Data Insight console and edit the saved credential password.

For example, navigate to **Settings** > **Saved Credentials**, and edit the credential to update the password.

3 If the password of an account, which is used for Fpolicy service or Celerra service configuration, has changed, you must reconfigure the services as well.

Navigate to Server details page for the corresponding nodes acting as Collectors, click the **Reconfigure Fpolicy** or **Reconfigure Celerra** sections on the page.

See "Managing saved credentials " on page 36.

Chapter 2

Configuring Data Insight global settings

This chapter includes the following topics:

Configuring SMTP server settings

Before Data Insight can send email notifications for events, reports, and alerts you must configure SMTP details for the Management Server.

To edit the SMTP settings

1. In the Management Console, click **Settings** > **Global Settings** > **SMTP Settings**.
2. On the SMTP settings page, click **Edit SMTP Settings**.
3. Enter the following details:
   - A valid SMTP server hostname or IP address.

- The port number for the SMTP mail server used to send email notifications. The default is 25.
- The username for the email server (optional).
- The password for the email server (optional).
- The address from which emails are sent (optional).
- Maximum attachment size. This information is used when Data Insight sends report notifications. Data Insight will not send reports as attachments, if the size of the report is over the specified limit.

4 Click **Save**.

Configuring scanning and event monitoring

Data Insight collects access events using asynchronous APIs, namely, Fpolicy for NetApp filers, the CEE framework for EMC Celerra filers, and filter driver for Windows File Servers. You can configure Data Insight to globally turn on or off receipt of event notifications.

If you want to stop Data Insight from scanning all file systems, you can disable scanning completely. Then, when you want Data Insight to resume scanning at the regularly defined schedule, you can enable scanning.

You can also configure whether you want the Scanner to fetch the Access Control Lists (ACLs) defined on folders and ownership information for files and folders.

To configure scanning and event monitoring

1 In the Management Console, click **Settings** > **Scanning and Event Monitoring**.

In the Management Console, click **Settings** > **Global Settings** > **Scanning and Event Monitoring**.

You can view the state of scanning and event monitoring.

2 To change the state of a process to Enabled or Disabled, click **Edit**.

3 Do one of the following:

- Select the check box for the process that you want to enable.
- Clear the check box for the process that you want to disable.

4 Click **Save** to save the changes.

Table 2-1 Scanning and Event Monitoring options

Option	Description
Scan File System meta-data	Clear the check-box to turn off all future file system scanning on all filers. Once you save the setting, it will also stop all currently running scans.
Get Folder ACLs	Clear the check box if you do not want Scanner to fetch Access Control List (ACLs) for folders during scanning. If you disable this option, the **Workspace** > **Permissions** tab in the Console is disabled and permission related reports will not produce any data. If you do not need permissions data, you can disable this option to make the scans run faster.
Get Ownership information for files and folders	Clear the check box if you do not want Scanner to fetch the Owner attribute for files and folders. Ownership information is used to determine ownership for data when access events are not available. If you do not need this information, you can disable this option to make scans run faster.

Table 2-1 Scanning and Event Monitoring options *(continued)*

Option	Description
Throttling for Netapp filers	Select **Throttle scanning based on cifs latency of the filer** to enable throttling for NetApp file servers. This option is not selected by default. Data Insight collects latency information from NetApp file servers. It can use this information to throttle scanning, if latency of the file server increases above a certain level. This ensures scanner does not put additional load on the file server in peak load conditions. You can configure the following parameters to enable throttling for NetApp file servers: ■ Latency threshold - specify latency in milliseconds, which when crossed, should throttle scanning for the file server. ■ Minimum pause - Specify the minimum duration (in milliseconds) for which the scanner should pause between paths when in throttling mode. ■ Back off value - If increased latency is sustained, pause interval will be increased by the Back off value specified (in milliseconds). ■ Maximum pause - Specify the maximum pause interval for the scanner (in milliseconds). If exceeded, pause interval is no longer incremented by Back off value.
Monitor File System access events	Clear the check box to stop Data Insight from collecting access events from all file servers. In case of NetApp, it means all collector nodes will disconnect their Fpolicy connections to file servers.

About filtering certain accounts, IP addresses, and paths

You can configure Symantec Data Insight to filter data accesses by specific users, IP addresses, file system paths, and URLs. You can combine these criteria together or use them individually to create a filter.

You can create separate exclude rules for file servers and SharePoint servers. For each of these, Data Insight supports two types of filters:

- Exclude rules for access events
- Exclude rules for Scanner

About Exclude rules for access events

You can configure the following types of exclude rules for access events:

Filters for account names or SIDs	Typically used to mask service accounts from registering data accesses into Symantec Data Insight. For example, if an antivirus software performs scans on a mounted share using a specific user account, you can add that user account to a filter. Data Insight omits all accesses made by that service user account.
Filters for IP addresses	Used to filter data accesses from specific IP addresses. Such filters are useful if you have file system scanners configured on certain machines in your environment, whose accesses you want to ignore.
Filters for path names	Filters for path names are of two types, file extension based and path based. The file extension based filter specifies the file extensions to be filtered. The path based filter specifies the path of a folder and filters out all events which have that path prefix. For path-based filtering, you must specify a fully qualified path prefix or a path relative to the root of each share.
Filter for URLs	Used to filter data accesses from specified Web applications or from SharePoint sites.

About Exclude rules for Scanner

Scanner supports filtering out a top-level folder for all shares. You can define rules to exclude the scanning of the specified share, or SharePoint URL by the Scanner process.

Scanner does not support excluding folders under a top-level folder.

Adding exclude rules to Symantec Data Insight

You must create a rule for every filter you want to add to Symantec Data Insight. The rule must contain a value for at least one criterion that you want to exclude.

To add a exclude rule:

1. In the Console, click **Settings** > **Global Settings** > **Exclude Rules**.
2. Click **Add Exclude Rule for File System** or **Add Exclude Rule for SharePoint**, as the case may be.

   From the drop-down, select **Exclude access** or **Exclude scanning**.
3. On the Add Exclude Rule screen, enter the Exclude rule properties.
4. Click **Save**.
5. Click the Export icon at the bottom of the Exclude Rules page to save the data to a `.csv` file.

Add/Edit Exclude rule for access events options

Use this dialog box to add a new exclude rule for access events to Symantec Data Insight or to edit the an existing exclude rule.

Table 2-2 Add/Edit file system Exclude rule for access events options

Field	Description
Rule name	Enter a logical name for the Exclude rule.
Usernames/SIDs	Enter the username or SIDs that you want to exclude. **Note:** The usernames must be present in the Data Insight users database, before they can be added to a exclude rule.

Table 2-2 Add/Edit file system Exclude rule for access events options *(continued)*

Field	Description
IP Addresses	Enter the IP addresses that you want to exclude. This filter only applies to NetApp and EMC Celerra file servers.
Exclude patterns	When defining a file system rule, enter the file extensions or paths that you want to exclude. A CIFS file system path must be fully qualified path in the format, `\\filer\share\folder` or relative to each share, for example, `<name of folder>`. A NFS path must be a fully qualified physical path on the actual file system in the format, `/path/in/the/physical/filesystem`. The logical operator OR is used create a rule with multiple values of the same dimension and the logical operator AND is used to combine values across dimensions in a rule. For example, if you create a rule to ignore user_foo1, user_foo2, and IP_10.209.10.20, it means that all accesses from IP_10.209.10.20 AND (user_foo1 OR user_foo2) will be ignored. When defining a SharePoint rule, enter the URL of the SharePoint Web application or the site.
Pattern Type	Select PREFIX or EXTENSION from the **Pattern Type** drop-down. This field is only available for a file system rule.
Rule is enabled	Select the **Yes** radio button to enable the rule and the **No** radio button to disable it.

Add/Edit Exclude rule for Scanner options

Use this dialog box to add a new exclude rule for access events to Symantec Data Insight or to edit the an existing exclude rule.

Table 2-3 Add/Edit file system Exclude rule for Scanner options

Field	Description
Rule name	Enter a logical name for the Exclude rule.
Exclude Patterns	When defining a CIFS file system rule, specify the name of the folder to exclude as `/<name of first level folder>`. For NFS file system rule, specify the name of the folder to exclude as `/<name of first level folder>` When defining a SharePoint rule, enter the URL of the SharePoint Web application or the site.
Rule is enabled	Select the **Yes** radio button to enable the rule and the **No** radio button to disable it.

About saved credentials

An authentication credential can be stored as a saved credential in a central credential store. It can be defined once, and then referenced by any number of filers, shares, and Active Directory servers. Passwords are encrypted before they are stored.

The saved credential store simplifies management of user name and password changes.

You can add, delete, or edit stored credentials.

See "Managing saved credentials " on page 36.

Managing saved credentials

You can add saved credentials to Data Insight, view details of the configured credentials and delete one or more saved credentials on the Saved Credentials details page.

You can add new credentials to the credential store. These credentials can later be referenced with the credential name.

To add a saved credential

1. In the Management Console, click **Settings** > **Saved Credentials**, and click **Create Saved Credentials**.
2. Enter the following information:

Saved Credential Name	Enter your name for this stored credential. The credential name must be unique within the credential store. The name is used only to identify the credential.
Access Username	Enter the user name for authentication.
Access Password	Enter the password for authentication.
Confirm Password	Re-enter the password.
Domain	Enter the name of the domain to which the user belongs.

3. Click **Save**.
4. You can later edit or delete credentials from the credential store.

You can delete or edit a saved credential.

To delete a saved credential

1. In the Management Console, click **Settings** > **Saved Credentials**.
2. Locate the name of the stored credential that you want to remove.
3. Click the **Delete** to the right of the name.

   A credential can be deleted only if it is not currently used for filers, shares, Active Directory, Fpolicy service, or the EMC Celerra service.

To edit a saved credential

1. Locate the name of the saved credential that you want to edit.
2. Click the **Edit** to the right of the name.
3. Update the user name or password.
4. If you change the password for a given credential, the new password is used for all subsequent scans that use that credential.
5. Click **Save**.

For the purpose of access control, only a user assigned the role of Server Administrator can add, edit, and view all saved credentials. A user assigned the

Product Administrator role can add new saved credentials, but can only view and edit those credentials which the user has created.

About archiving data

Data Insight stores system events, alerts, and access events on the Indexer worker node in a pre-determined folder. You can configure Data Insight to automatically archive access events older that the specified interval to another folder to save space. Once the data is archived, it is no longer available for querying. You can, however, restore the data back to the original location on the Indexer node, if needed.

By default, archived data is automatically moved to `$data/indexer/archive` folder on each Indexer worker node. You can also configure a different archive folder on the Indexer nodes. The archive folder is organized by YEAR/MONTH to make restoring easy. Once data is moved to this folder based on the configured archive policy, you can do one of the following:

- Backup the archive folder and delete the archived files from the Indexer node.
- Or, configure a file system archiving solution like Symantec Enterprise Vault File System Archiving to archive all files in the archive folder.

If you want to restore archived data at a later time, you must bring back the appropriate segments from the backup folder to their original location in the archive folder and use the indexcli utility to restore these segments. Once restored, segments are not archived or purged by the data retention policy till they are marked for re-archiving.

See "About purging data" on page 38.

See "Configuring data retention settings" on page 39.

About purging data

If you want Data Insight to automatically delete data, such as access events, system events, and alerts older than specified interval, you can configure a purging policy. Use the `indexcli` utility if you want to purge data at a more granular level than what you can configure on the Data Retention page on the Management Console. Purged data cannot be restored back at a later time.

See "About archiving data" on page 38.

See "Configuring data retention settings" on page 39.

Configuring data retention settings

Data Insight enforces the data retention policy twice a month. Archived index segments can be restored using a command line utility called `indexcli.exe`. The utility is also useful to enforce a more granular archiving or purging policy, if the global option is not sufficient for your needs.

You can configure the duration for which you want Data Insight to retain various types of data and the duration after which you want to purge data. Automatic archiving and purging of data is not enabled by default.

To configure the data retention period

1. Click **Settings** > **Data Retention**.
2. On the Data Retention details page, click **Edit**.
3. Enter the following information:

Archive access data automatically	Do the following: 1 Select the check box to enable archiving of file system or SharePoint events. 2 Enter the age of the data (in months) after which the data must be archived. 3 Enter the path of the archive folder.
Purge access data automatically	Select the check box to enable purging of file system or SharePoint access events, and enter the age of the data (in months) after which the data must be deleted.
Purge Data Insight system events automatically	Select the check box to enable purging of Data Insight system events, and enter the age of the data (in months) after which the data must be deleted. Data Insight system events are displayed on the **Settings** > **Events** page.
Purge alerts automatically	Select the check box to enable purging of alerts, and enter the age of the alerts (in months) after which they must be deleted.
Automatically purge data for deleted shares or site collections	Select the check box to enable purging of data pertaining to deleted shares. This option is enabled by default.

4 Click **Save**.

See "About archiving data" on page 38.

See "About purging data" on page 38.

Configuring Symantec Data Loss Prevention settings

Data Insight pulls information about sensitive files in a storage environment from Symantec Data Loss Prevention (DLP). Data Insight uses this information when raising alerts in response to configured policies. You can retrieve a incident list that flags sensitive files in your storage environment and create a saved report using the Enforce Server Administration Console. Data Insight uses the DLP Reporting API Web Service to request a list of incident IDs by specifying a saved report ID.

Data Insight runs a job at 12:00 a.m. every night to retrieve a list of sensitive files from DLP.

You must configure the settings that allow Data Insight to communicate with Symantec Data Loss Prevention.

To configure Data Loss Prevention settings

1 In the Management Console, click **Settings** > **Data Loss Prevention**.

2 Click **Edit**, and enter the following details:

- The hostname or IP address of the DLP server
- The port through which Data Insight connects to the DLP server.
- The username and password of the account used to access the DLP server.

  Note: Ensure that the credentials belong to an existing DLP user assigned the Reporting API Client role.

- The ID of the Saved Report.

The DLP Enforce Server administration console requires SSL transport for all communication. Data Insight must be able to negotiate the SSL connection with the Enforce server. For this purpose, you must import the certificate to the keystore used by Data Insight.

To import the SSL certificate from the DLP Enforce Server to Data Insight using Firefox

1. Type the URL to connect to a DLP Enforce Server Administration console.
2. On the security certificate warning page, click **I understand the risks**.
3. Click **Add Exception**.
4. On the Add Security Exception page, click **View** to view the certificate details.
5. Click the **Details** tab and click **Export**.
6. From the Save as type drop down, select X.509 Certificate (DER).
7. Click **Save**.

To import the SSL certificate from the DLP Enforce Server to Data Insight using Internet Explorer

1. Type the URL to connect to a DLP Enforce Server Administration console.
2. On the security certificate warning page, click **Certificate Error** next to address bar.
3. Select **View certificates**.
4. Click the **Details** tab, and select the appropriate certificate.
5. Click **Copy to File**
6. In the Certificate Export Wizard, select DER encoded binary.
7. Click **Next**.
8. Enter the name of the file and browse to the location where you want to save the file.
9. Click **Next**
10. Click **Finish** to save the file.

After the SSL certificate is imported, complete the following steps to import the SSL certificate on the Data Insight server.

To import the SSL certificate on the Data Insight server

1. From the Windows Start menu, select **Run** and type `cmd` in the dialog box to open a command prompt window.
2. Run the following command:

   ```
   cd C:\Program Files\Symantec\DataInsight\jre\bin
   ```

   ```
   .\keytool -importcert -alias dlp -keystore c:\
   DataInsight\data\keys\commd.keystore -trustcacerts -file <file
   path of SSL certificate>
   ```

   Specify `changeit` as the password for the keystore.

   You can now pull a list of sensitive files from Symantec Data Loss Prevention (DLP).

Configuring data owner policy

By default, Data Insight infers owners of files or folders based on the access history. The most active user of a file is considered to be the data owner for the purpose of efficient remediation and data management.

However, you can define a global policy to infer the owners of files or folders based on one of the following criteria:

- The number of read events on the file or folder.
- The number of write events on the file or folder.
- The cumulative count of read and write events on the file or folder.
- The creator of the file or folder.
- The user account which last accessed the file or folder.
- The user account which last modified the file or folder.

For example, you can define a policy to consider the count of read and write events on a file to determine the data owner. In this case, the user with the most read and write accesses is considered to be the data owner.

To configure the data owner policy

1. In the Management Console, click **Settings** > **Data Owner Policy**.

   The Data Owner Policy details page displays the current policy.
2. Click **Edit** to select the parameter for inferring the data owner.
3. Click **Save**.

Managing Data Insight licenses

When you purchase Symantec Data Insight, you must install the Data Insight license file. License files have names in the format *name*.slf.

If you do not have a valid license, Data Insight displays a warning in red in the footer of the Management Console screen.

To install a license

1. Obtain the new license file.
2. In the Management Console, click **Settings** > **Licensing**.
3. On the Licensing page, click **Add/Update License**.
4. On the Add new license page, browse to the new Data Insight license file that you have downloaded, and click **Upload**.

Configuring Management Console settings

In the Console Settings view, you can configure global settings that apply to various tasks that you carry out on the Management Console.

To configure the Console settings

1. Click **Settings** > **Console Settings**.
2. Click **Edit**.

   You can edit any of the following settings:

Session Timeout	Your login session on the Management Console times out after certain period of inactivity. The default timeout period is one hour. To configure the session timeout period, enter the time in minutes.
Report Footer Text	You can choose to add a footer to all the reports that you run in the Console. Enter the sentence string that you want to appear in the footer of the report. For example, Proprietary and Confidential.

3. Click **Save**.

For more information about creating reports, see the *Symantec Data Insight User's Guide*.

Chapter 3

Configuring directory service domains

This chapter includes the following topics:

About directory domain scans

Symantec Data Insight periodically scans the configured directory service domains in your organization to fetch information about users and user groups. Data Insight correlates this information with file and folder access logs to provide access and usage reports. This information is stored on the Management Server in the user database. Symantec recommends that you add each such domain to Data Insight whose users access filesystem resources of your organization. The time it takes to scan a directory service domain depends on the number of users and groups in the domain.

For user authentication, Data Insight supports the following implementations of a directory service:

- Microsoft Active Directory

- Network Information Service
- LDAP

By default, Data Insight also automatically scans local users of all Windows File Server agents, all NetApp and Celerra filers, and SharePoint site collections.

See "Adding a directory service domain to Data Insight" on page 46.

Adding a directory service domain to Data Insight

You can configure Data Insight to scan one or more directory service domains.

To add a directory service domain to Data Insight

1. In the console, click **Settings** > **Directory Services** to display the Directory Services listing page.
2. From the **Add New Directory Service** drop-down, select the type of directory service domain you want to add - Active Directory, LDAP, or NIS/NIS+.
3. On the Add New Directory Service screen, enter the server properties.
4. Click **Save**.
5. On the Directory Services listing page, click **Scan Now**.

   Once the initial scan is complete, the users and groups will appear under the **Workspace** tab.

Add/Edit Active Directory options

Use this dialog box to add an Active Directory server to Data Insight, or edit the properties of an existing Active Directory server.

Table 3-1 Add/Edit Active Directory options

Field	Description
Domain Name	Enter the name of the domain which you want to scan. The domain name is used for display purpose only.
Domain Controller IP	Enter the hostname or IP address of the Active Directory domain controller.

Table 3-1 Add/Edit Active Directory options *(continued)*

Field	Description
Scanning Details	Do the following: 1 Select the saved credentials from the drop-down or specify new credentials. 2 Click **Test Credentials** to test the availability of network connection between the Management Server and the Active Directory Server, and also to verify that the credentials given are correct. Symantec recommends that you test the connection before proceeding to ensure that the Management Server is able to scan the Active Directory domain controller.
Bind Anonymously	Select the check box if you want to allow Data Insightto connect to the Active Directory server without a credential.
Disable scanning	Select the check box to disable the scanning of the directory server.

Table 3-1 Add/Edit Active Directory options *(continued)*

Field	Description
Custom Attributes	Add the additional attributes for users that you want Data Insight to extract from LDAP. These custom attributes are included in reports and are also displayed on the Console. To add additional attributes, do the following: 1 Click **Add Attribute** . 2 On the dialog, enter the LDAP display name of the attribute. Optionally, you can also specify a friendly name for the attribute. 3 Click **Add**. **Note:** Data Insight already extracts following attributes from Active Directory: ■ displayName ■ distinguishedName ■ givenName ■ objectSid ■ sAMAccountName ■ memberOf ■ primaryGroupID ■ userAccountControl ■ sn

Add/Edit LDAP domain options

Use this dialog box to add a LDAP directory service server to Data Insight.

Table 3-2 Add/Edit LDAP properties options

Field	Description
Fully Qualified Domain Name	Enter the fully qualified name of the domain that you want to scan. Entering the FQDN will automatically populate the User and Group search Base DN fields.

Table 3-2 Add/Edit LDAP properties options *(continued)*

Field	Description
LDAP server address	Enter the hostname and the port of the LDAP server. By default, the LDAP server runs on HTTPS port 389. If TLS is enabled, the LDAP server runs on port 636, by default.
Type	The type of LDAP schema used by the directory service. Data Insight extracts the attributes from the schema attribute file when scanning the domain. Select one of the following: ■ OPENLDAP ■ Sun ONE You can also create a schema attribute file with customized attributes for each LDAP implementation that does not match the defaults. Ensure that you name the file as `ldap_<ldap_type>.conf` and save it at `C:\DataInsight\data\conf\ldap`.
Search base DN	The Organization Unit (OU) in which all users and groups have been defined.
This directory uses secure connection (TLS)	Select this check box if the LDAP server uses the TLS protocol.

Table 3-2 Add/Edit LDAP properties options *(continued)*

Field	Description
Scanning details	Select the saved credentials from the drop-down or specify new credentials. If you are specifying scanning credential other than the directory administrator, then make sure that you have specified the correct DN for that user. For example, uid=ldapuser,ou=People,dc=openldap,dc=com. You can connect to the LDAP database to verify the DN for an LDAP user. The example below shows the DN of a sample user, ldapuser, created on a Linux openLDAP server: uid=ldapuser,ou=People,dc=openldap,dc=com. The DN string may change depending upon the LDAP schema used. Refer to the LDAP schema to get correct DN for the user. The credentials should belong to an LDAP user who has appropriate privileges to scan the LDAP domain.
Test Credentials	Click to verify that the given credentials are correct and to test the availability of network connection between the Management Server and the LDAP server. Symantec recommends that you test the connection before proceeding to ensure that the Management Server is able to scan the LDAP server.
Bind anonymously	Select the checkbox if you want to allow Data Insightto connect to the LDAP server without a credential.
Disable scanning	Select the check box to disable the scanning of the directory server.

Table 3-2 Add/Edit LDAP properties options *(continued)*

Field	Description
Custom attributes	Add the additional attributes for users that you want Data Insight to extract from LDAP. These custom attributes are included in reports and are also displayed on the Console. To add additional attributes, do the following: 1 Click **Add Attribute** . 2 On the dialog, select whether the attribute applies to an user or group. 3 Enter the LDAP display name of the attribute. Optionally, you can also specify a friendly name for the attribute. 4 Click **Add**.

Add/Edit NIS domain options

Use this dialog box to add a NIS directory service server to Data Insight.

Table 3-3 Add/Edit NIS properties

Field	Description
Fully Qualified Domain Name	Enter the name of the domain that you want to scan.
Hostname/IP address	Enter the hostname or IP address of the NIS server.
Scanning Details	Click **Test Credentials** to verify that the given credentials are correct and to test the availability of network connection between the Management Server and the NIS server. Symantec recommends that you test the connection before proceeding to ensure that the Management Server is able to scan the NIS server.
Disable scanning	Select the check box to disable the scanning of the directory server.

Add/Edit NIS+ domain options

Use this dialog box to add a NIS+ directory service server to Data Insight.

Table 3-4 Add/Edit NIS+ properties

Field	Description
Fully Qualified Domain Name	Enter the name of the domain that you want to scan.
Hostname/IP address	Enter the hostname or IP address of the NIS+ server.
Configured in NIS compatibility mode	This check box is only available when adding a NIS+ server. When configuring a NIS+ server, select the **Configured in NIS compatibility mode** check box if the NIS+ server is configured in the NIS compatibility mode. In this mode, Data Insight can fetch the users and groups data from the NIS+ server remotely in most cases. In non NIS-compatible mode or when Data Insight cannot scan users and groups remotely, you must manually fetch the users and groups data from the NIS+ server. See "Fetching users and groups data from NIS+ scanner" on page 54.
Scanning Details	Click **Test Credentials** to verify that the given credentials are correct and to test the availability of network connection between the Management Server and the NIS+ server. Symantec recommends that you test the connection before proceeding to ensure that the Management Server is able to scan the NIS+ server.
Disable scanning	Select the check box to disable the scanning of the directory server.

Managing directory service domains

You can add directory service domains to Data Insight, view details of the configured domains and scan one or more domains on the Directory Services listing page.

To manage the directory service domain servers

1. In the Console, click **Settings** > **Directory Services** to display the directory services details page.
2. The list of configured directory service domains appears.
3. Review the following information about the configured domains:
   - The name of the domain.
   - The address of the domain server hosting the domain.
   - The type of directory service - Microsoft Active Directory, LDAP, or NIS.
   - The number of users and groups in the directory service domain.
   - The additional attributes that Data Insight extracts for the domain.
4. To scan all domains, click **Scan Now**.

   Note: Data Insight scans all domains together because dependencies might exist between the different domains.

5. To edit the scan schedule for the configured domains, click **Edit Schedule**.

   By default, Data Insight scans all domains at 3:00 a.m. everyday.
6. On the Configure Directory Server Scanning Schedule dialog, change the schedule, and click **Update Schedule**.

   The updated schedule is used for all subsequent scans of the configured domains.
7. To edit the properties of a directory service domain, from the **Select Actions** drop-down, select edit **Edit**.
8. On the directory service properties screen make the necessary changes, and click **Save**.
9. To delete a configured directory service domain, from the **Actions** drop-down, select edit **Delete**.
10. Select OK on the confirmation message.

Fetching users and groups data from NIS+ scanner

If the NIS+ server is configured in a non NIS compatible mode, you must manually fetch users and groups data from the NIS+ server. However, you must still add the NIS plus domain with correct information like domain name and IP address to Data Insight.

To get users and groups data

1. Log in as root to the NIS+ server.
2. Open the command prompt, and type the following commands:

To get users data	`niscat passwd.org_dir > users.txt`
To get the groups data	`niscat group.org_dir > groups.txt`

3. Save the `users.txt` and `groups.txt` files at `C:\DataInsight\data\users\nisplus\`*`example.com`* on the Management Server, where example.com is your domain name.
4. On the Directory Services listing page, click **Scan Now** to import the NIS+ domain data. You can also run the scan job from the command line by executing the following command on the Management Server:

   ```
   configcli execute_job ADScanJob
   ```

Deleting directory service domains

You can delete a configured directory service domain.

To delete an directory service domain

1. In the Console, click **Settings** > **Directory Services** to display the configured directory service domains.
2. Click **Delete** for the domain that you want to delete.
3. Click **OK** on the confirmation message.

Note: Users from a deleted directory domain are removed from Data Insight only after the next directory scan runs.

Scheduling scans

Symantec Data Insight scans configured domains everyday at 3 a.m, by default. You can, however, configure the scanning schedule, as needed.

Data Insight also scans local users of all file servers and site collections that are managed Data Insight. Information from these scans becomes visible in Data Insight after the directory scan runs.

See "About directory domain scans" on page 45.

See "Managing directory service domains " on page 53.

Configuring business unit mappings

Symantec Data Insight allows you to associate a business unit name and business unit owner with each user imported from directory services. This information is later included in the report outputs and also sent to Symantec Data Loss Prevention as a part of ownership information.

To import business unit mappings

1. Create a .csv file, `bucsv.csv`, in the `users` folder in the Data Insight data directory on the Management Server. By default, the `users` directory on the Management Server is located at `C:\DataInsight\data\users`.

   The CSV file must contain the following information:

   - The name of the user in the format, user@domain name.
   - The name of the business unit.
   - The name of the business unit owner.

   For example, *John_Doe@mycompany.com,Sales,Greg Smith*

2. This information is imported into the users database when the next Active Directory scan runs. To so immediately, run the following command:

   ```
   adcli.exe -mode importbu
   ```

Note: The domain name given in the .csv file must be among the domains scanned by Data Insight.

Chapter 4

Configuring file servers

This chapter includes the following topics:

About configuring filers

Symantec Data Insight collects and stores access events from NAS devices to service queries on user activity and data accesses. Before Data Insight can start collecting events, you must ensure that auditing is configured properly on the storage device. Data Insight collects access events using asynchronous APIs, namely, Fpolicy for NetApp filers, the CEE framework for EMC Celerra filers, and file system filter drivers for Windows File Server.

Supported file servers

This section lists the Network Attached Storage devices that Data Insight supports.

Table 4-1 Supported file servers

File server	Version
NetApp ONTAP	7.3 or higher ONTAP 8.x must be configured in ONTAP 8 7 mode.
EMC Celerra	5.6.45 or higher
Windows File Server	Windows Server 2003, 32 bit and 64 bit Windows Server 2008, 64 bit
Veritas File System (VxFS) server	6.0 or higher

Note: Symantec recommends that you upgrade your NetApp filer to the latest available firmware. Symantec recommends ONTAP 7.3.3 or higher.

For all supported versions of NetApp filers, Data Insight supports CIFS protocol over NTFS, NFS protocol, and mixed volume, or qtree.

Configuring NetApp file servers

Before you start configuring NetApp filers, verify the following in case of NetApp filers:

- The filer is accessible from the collector node using the short name or IP address you plan to use when adding the filer.
- There is connectivity to the collector node from the filer using the short name and the Fully Qualified Host Name (FQHN) of the Collector node.
- The DNS lookup and reverse-lookup for hostname of the Collector node from the filer is working fine.
- The standard RPC ports are open in the firewall.
- On Windows 2008 machines which are used as collector nodes, click **Administrative tools** > **Local Security Policy** > **Local Policies** > **Security options** and change following settings:
  - Network access: Named Pipes that can be accessed anonymously - Add NTAPFPRQ to the list.
  - Network access: Let Everyone permissions apply to anonymous users - Enabled
  - Network access: Do not allow anonymous enumeration of SAM accounts - Disabled
  - Network access: Restrict anonymous access to Named Pipes and Shares set to Disabled

  You must restart the machine after making these changes.

Configuring SMB signing

Ensure that Server Message Block (SMB) signing is either turned on or turned off on both the Collector node and the NetApp filer. If SMB signing is turned on, all packets of data sent over a network to a remote host are signed. A mismatch in the setting on the Collector node and the NetApp filer can cause the filer to drop the Fpolicy connection to the Collector node.

To configure SMB signing

1. Check whether the SMB signing option on the NetApp filer, `options.cifs.signing.enable` is set to off or on.
2. On the Collector node assigned to the NetApp filer, open the Windows' Registry Editor (**Start** > **Run** > **regedit**).

3 In Registry Editor, navigate to **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** >**SERVICES** > **lanmanserver** > **Parameters**.

4 Modify the following registry entries:

- `enablesecuritysignature` - Enter the value 0 to turn signing off and enter the value 1 to turn signing on.
- `requiredsecuritysignature` - Enter the value 0 to turn signing off and enter the value 1 to turn signing on.

About Fpolicy

Symantec Data Insight uses the Fpolicy framework provided by Netapp to collect access events from the NetApp filers.

NetApp provides an interface called Fpolicy which allows external applications to receive file access notifications from the NetApp Storage subsystem. Fpolicy allows partner applications to perform tasks like file access screening and auditing. The Fpolicy interface uses Remote Procedure Calls (RPC) and external applications can use these tools to register with the NetApp Filer as Fpolicy servers. Fpolicy supports both CIFS and NFS.

The unit of Fpolicy configuration on the NetApp filer is called a policy, which is identified by a user specified name. You can configure a policy to monitor all or a list of volumes on the NetApp filer along with a specified set of operations. The monitored operations are open, close, read, write, create, delete, rename, and set attribute. As soon as a file operation is performed on a file or folder on the filer which is being monitored, a notification is sent to the registered Fpolicy server asynchronously.

Note: The policy created by Symantec Data Insight should not be shared by any other applications or clients.

By default, Data Insight does not register for read and close events from NetApp filers. Data Insight treats an open event as a read event. This behavior reduces the load on the filer in case of peak traffic loads from third party applications like backups over CIFS. It also does not have an adverse effect for most consumer applications because consumer applications seldom write to a file before first reading it. Data Insight assumes that an open event is almost always be followed by a read event and then optionally by a write event. However, you can customize the default behavior as per your requirements.

See "Enabling export of NFS shares on NetApp" on page 66.

See "Preparing the NetApp filer for Fpolicy" on page 61.

Preparing Symantec Data Insight for Fpolicy

The Symantec Data Insight Fpolicy server can reside on the Management Server and/or on each Collector worker node. The Management Server and/or the Collector worker node must register with the NetApp filer to receive audit information. Before you assign a Data Insight server as a collector for a NetApp filer, you must configure the Fpolicy service on that server.

To set up the environment for Symantec Data Insight Fpolicy service

1. Provision a Windows 2003 or 2008 server in the same directory domain as the filers you wish to monitor using Fpolicy. This machine hosts the Fpolicy server. If your filers belong to different untrusted domains, you can add the server to any one domain.
2. Install the Data Insight Collector worker node or the Data Insight Management Server on this server.
3. Login to the Data Insight Management Console.
4. In the Console, click **Settings** > **Data Insight Servers** to open the listing page for the server.
5. Select the server from the server list to open the details page for the server.
6. Navigate to the Fpolicy Service configuration section, and click **Enable**.
7. Under Credentials, select the saved credentials that the service needs to run as.

   See "Credentials required for configuring NetApp filers" on page 15.
8. Select **Use saved credentials**, to use saved credentials or create new saved credentials.
9. In the **Policy Name** field, enter the policy name that will be enabled on each filer, of this node Collector. The default name is *matpol*.
10. Click **Configure** to apply these settings to the server and start the Fpolicy service.

See "Configuring SMB signing" on page 59.

See "About Fpolicy" on page 60.

Preparing the NetApp filer for Fpolicy

The Symantec Data Insight Fpolicy server registers with the NetApp filer and receives file access events from it. Fpolicy has to be enabled and configured on that NetApp filer. Symantec recommends that you automatically enable auditing when adding filers.

See "Adding filers" on page 76.

However if you want more control on the shares you want to monitor use the manual steps. The manual steps are valid for Netapp ONTAP version 7.0 and higher.

Note: The steps below assume that the name of the policy is *matpol*.

To configure the Fpolicy on the NetApp filer using manual steps

1 Launch a Telnet session with the filer and run the following commands, as appropriate:

- To create a policy:

```
fpolicy create matpol screen
```

- To enable a policy:

```
fpolicy enable matpol -f
```

2 Use the following optional commands for monitoring:

- To set the Fpolicy for CIFS to monitor specific events:

```
fpolicy mon add matpol -p cifs -f read,write,
open,close,delete,rename,create
```

- To set the Fpolicy for NFS to monitor specific events:

```
fpolicy mon add matpol -p nfs -f create,delete,rename,write,
open,link,symlink,setattr
```

- To monitor specific events on NetApp filer versions 7.3 or higher:
  - Enable set attributes operation:

```
fpolicy options cifs_setattr on

fpolicy options nfs_setattr on
```

  - Add events to be monitored:

```
fpolicy mon add matpol -p cifs -f read,write,
open,close,delete,rename,create,setattr
```

```
fpolicy mon add matpol -p nfs -f create,delete,rename,write,
open,link,symlink,setattr
```

- To see details of a configured policy:

  ```
  fpolicy show matpol
  ```

- To disable monitoring of specific events:

  ```
  fpolicy mon remove matpol -p cifs -f read,write,
  open,close,delete,rename,create
  ```

  ```
  fpolicy mon remove matpol -p nfs -f create,delete,rename,write,
  open,link,symlink,setattr
  ```

- To disable use of a policy:

  ```
  fpolicy disable matpol
  ```

- To delete a policy:

  ```
  fpolicy destroy matpol
  ```

3 To add a domain user to the administrator's group:

```
useradmin domainuser add domain-username
-g Administrators
```

Note: The domain user is the user who is configured to run the Fpolicy service on the collector.

To configure a non-administrator user:

See "Preparing a non-administrator domain user on the NetApp filer for Data Insight" on page 24.

4 To display a list of users who are already configured:

```
useradmin domainuser list -g Administrators
```

A list with the SIDs of the configured domain users appears. To resolve the SIDs, run the following command:

```
cifs lookup SID
```

See "Configuring SMB signing" on page 59.

Preparing the NetApp vfiler for Fpolicy

The Symantec Data Insight Fpolicy server can register with the NetApp vfiler and receive file access events from it. Fpolicy has to be enabled and configured on that NetApp vfiler manually.

To configure the Fpolicy on the NetApp vfiler using manual steps

1. Launch a Telnet session with the filer and run the following commands, as appropriate:

   - To get the vfiler name:

     ```
     vfiler status
     ```

     Choose the name of the vfiler that you want to configure and then perform the following operations for that vfiler. Ignore the name, *vfiler0*, which is the default name given to the physical filer by NetApp.

     Note: Consult your system administrator to get the IP address of the vfiler. You will need this IP address while adding the vfiler from the Management Console.

     See "Adding filers" on page 76.

   - To create a policy:

     ```
     vfiler run vfilername fpolicy create matpol screen
     ```

   - To enable a policy:

     ```
     vfiler run vfilername fpolicy enable matpol -f
     ```

2. Use the following optional commands for monitoring:

   - To set the Fpolicy for CIFS to monitor specific events:

     ```
     vfiler run vfilername fpolicy mon add matpol -p cifs
      -f read,write,open,close,delete,rename,create
     ```

     To set Fpolicy for NFS to monitor specific events:

     ```
     vfiler run vfilername fpolicy mon add matpol -p nfs -f create,
     delete,rename,write,open,link,symlink,setattr
     ```

   - To set the Fpolicy for CIFS to monitor specific events on NetApp filer versions 7.3 or higher:

- Enable set attributes operation:

  ```
  vfiler run vfilername fpolicy options cifs_setattr on
  ```

  ```
  vfiler run vfilername fpolicy options nfs_setattr on
  ```

- Add events to be monitored:

  ```
  vfiler run vfilername fpolicy mon add matpol -p cifs
  -f read,write,open,close,delete,rename,create,setattr
  ```

  ```
  vfiler run vfilername fpolicy mon add matpol -p nfs -f create,
  delete,rename,write,open,link,symlink,setattr
  ```

- To see details of a configured policy:

  ```
  vfiler run vfilername fpolicy show matpol
  ```

- To disable monitoring of specific events:

  ```
  vfiler run vfilername fpolicy mon remove matpol -p cifs
  -f read, write,open,close,delete,rename,create
  ```

  ```
  vfiler run vfilername fpolicy mon remove matpol -p nfs -f create,
  delete,rename,write,open,link,symlink,setattr
  ```

- To disable use of a policy:

  ```
  vfiler run vfilername fpolicy disable matpol
  ```

- To delete a policy:

  ```
  vfiler run vfilername fpolicy destroy matpol
  ```

  where, *vfilername* is the name of the vfiler you want to configure.

3 To add a domain user to the administrator's group:

```
vfiler run vfilername useradmin domainuser
add domain-username -g Administrators
```

Note: The domain user is the user who is configured to run the Fpolicy service on the collector. See "Preparing the NetApp filer for Fpolicy" on page 61.

To configure a non-administrator user:

See "Preparing the NetApp filer for Fpolicy" on page 61.

4 To display a list of users who are already configured:

```
vfiler run vfilername useradmin domainuser list
-g Administrators
```

A list with the SIDs of the configured domain users appears. To resolve the SIDs, run the following command:

```
cifs lookup SID
```

Enabling export of NFS shares on NetApp

Before you add a NetApp filer to Data Insight, you must enable the export of NFS shares on the NetApp filer to allow Data Insight to discover the NFS shares on the filer.

To enable export of NFS shares on the NetApp filer

1 On the NetApp FilerView Web console, select **NFS** > **Manage exports**.

2 On the Export wizard, click **Add Export** or you can edit the existing exports to modify them.

3 On the first page of the wizard ensure that you have at least selected read only and root access, Other options can also be specified, as required, and click **Next.**

4 Define the export path and give read only access to the Data Insight Collector node, and click **Next**.

5 On the Read-Write Access page, enable read-write access for all clients or for specific hosts, as per your need.

6 Click **Next**.

7 On the Root Access page, define root access to the the Data Insight Collector node, and click **Next**.

8 On the Security page, accept the default options, and click **Next**.

9 On the Summary page, review the configuration and click **Commit** to save the changes.

See "Adding filers" on page 76.

Configuring EMC Celerra filers

Symantec Data Insight uses the EMC Celerra Event Enabler (CEE) framework to collect access events from the EMC Celerra filers.

As a prerequisite, you must download and install the CEE framework from the EMC Website.

See "Add/Edit EMC Celerra filer options" on page 81.

About EMC Celerra Event Enabler (CEE)

The EMC Celerra Event Enabler (CEE) framework is used to provide a working environment for the following mechanisms:

- EMC Celerra AntiVirus Agent (CAVA)
- EMC Celerra Event Publishing Agent (CEPA)

Symantec Data Insight uses the CEPA functionality of the CEE framework to receive event notifications. The EMC Celerra® Event Publishing Agent (CEPA) is a mechanism that enables Data Insight to register with the EMC Celerra filer to receive event notifications from the filer. You can specify filters for the event type, the CIFS server, and the shares that you want to monitor during registration with the CEPA facility in the CEE framework. CEPA then sends notifications regarding the registered events to Data Insight.

Preparing the EMC Celerra filer for CEPA

The Symantec Data Insight server registers with the EMC Celerra filer through the CEE framework to receive notifications of file access events from it.

See "About EMC Celerra Event Enabler (CEE)" on page 67.

To configure the EMC Celerra filer to send event information to Symantec Data Insight

1 Create a cepp.conf file on the EMC Celerra filer. The following is a sample of the code that the cepp.conf file must contain:

```
surveytime=90

pool name=matrixpool \

servers=<IP Address/Hostname of Windows server running the EMC CAVA service> \

postevents=* \

option=ignore \

reqtimeout=500 \

retrytimeout=50
```

Note: If the server pool contains more than one server, each of the `server` entry should be separated by a "|".

2 Copy the cepp.conf file to the root directory of the Data Mover. Run the following command: `server_file <datamover_name> -put cepp.conf cepp.conf`

For example, `server_file server_2 -put /tmp/CEPA/cepp.conf cepp.conf`

3 Start the CEPP service on the filer. Run the following command:

```
server_cepp <datamover_name> -service -start
```

Ensure that the service has started by running the following command:

```
server_cepp name of data mover -service -status
```

Note: For detailed information about configuring CEPA, refer to the EMC documentation.

Preparing Symantec Data Insight to receive event notification

The EMC Celerra Event Enabler (CEE) can be installed on the same Windows server as the Data Insight Collector node or on a remote server in the same Active Directory domain.

You must perform the following steps to route events from the Windows server on which the EMC CEE is installed to the Collector node.

To prepare Data Insight to receive event notification

1. Provision a Windows 2003 or 2008 server to run the EMC CEE framework in the same Active Directory domain as the filers you wish to monitor.
2. Open Windows' Registry Editor (**Start** > **Run** > **regedit**).
3. In Registry Editor, navigate to `HKEY_LOCAL_MACHINE > SOFTWARE > EMC > Celerra Event Enabler >CEPP > Audit >Configuration`.
4. Double-click **Endpoint**.
5. Modify the registry entry for the EMC CAVA service to allow access to the Data Insight Collector node. Depending on the type of your Data Insight deployment, there can be the following different scenarios:
   - The EMC CAVA service and the Collector node are running on the same machine, and the EMC CAVA service is only being used by Data Insight. In this case, add the Data Insight key, `SymantecDataConnector`, to the **Endpoint** option.
   - The EMC CAVA service and the Collector node are running on the same machine, and the EMC CAVA service is also being used by applications other than Data Insight. In this case, append the Data Insight key, `SymantecDataConnector`, to the **Endpoint** option. Each entry must be separated by a semi-colon.

     Note: The above-mentioned scenarios are automatically configured at the time adding filers.

   - The EMC CAVA service and the Collector node are running on separate machines, and the EMC CAVA service is being used only by Data Insight. In this case, add the Data Insight key in the format, `SymantecDataConnector@<IP address of the Collector>`, to the **Endpoint** option.
   - The EMC CAVA service and the Collector node are running on separate machines, and the EMC CAVA service is also being used by applications other than Data Insight. In this case, append the Data Insight key in the format,`SymantecDataConnector@<IP address of the Collector>`, to the **Endpoint** option.

   If the EMC CAVA service is installed on multiple machines, modify the registry entries on each of these machines.

6 To start the EMC CAVA service, run the following command on the EMC Celerra filer to check the service status. For example,

```
Server_cepp  server_2 -pool -info
```

7 Install Data Insight Collector node.

8 Login to the Data Insight Management Console.

9 Navigate to **Settings** > **Data Insight Servers** to open the Data Insight Servers details page for the Collector.

10 Navigate to the EMC Celerra Service configuration section, and click **Enable** to start the DataInsightCelerra service on the Collector node.

11 Under Credentials, enter the credentials that the service needs to run as. The specified credentials must be that of a domain user.

12 Click **Configure** to apply these settings to the server and start the EMC CAVA service.

Configuring Windows File Servers

Data Insight uses an agent to collect access events from the Windows File Server. The agent resides on the file server. Before you can configure a Windows File Server, you must install the Data Insight agent on the filer. The Data Insight agent consists of a filter driver that monitors the file system and records events that are relevant for Data Insight. It also consists of the Data InsightWinNAS service, which receives the event information from the filter driver and transfers it to the collector node configured for that filer.

If you do not want Data Insight to access events for a Windows File Server, it is possible to configure Windows File Server without an agent. In this case Data Insight scans shares of the filer from the Collector.

You can choose to install the agent on the Windows File Server automatically when adding the filer, or manually. Before you can install the agent automatically, ensure that the commd port 8383 on the Collector node is accessible from the Windows File Server.

For detailed information about installing the agent manually, see the *Symantec Data Insight Installation Guide*.

You can either add a Windows File Server to through the Management Console or if you want to add multiple filers together, you can use the `installcli.exe` utility. The `installcli.exe` utility uses a `.csv` file with the following details as input:

- The hostname or IP address of the Windows File Servers that you want Data Insight to monitor.
- The hostname, IP address, or ID of the Collector node configured to scan the filer.
- The hostname, IP address, or ID of the Indexer node configured for the filer.
- The credentials that Data Insight should use to install the agent on the Windows File Server. The credential should be in the format user@domain. The same credentials should be added to Data Insight as a saved credential previously.
- The IP addresses of the agents. Separate multiple IP addresses with a semi-colon. If you do not want to use an agent to monitor the filer, indicate this with a hyphen (-).
- The credentials required to scan the filer. The credential should be in the format user@domain. The same credentials should be added to Data Insight as a saved credential previously.
- True or false value indicating whether the scan should be enabled according to the specified schedule.
- True or false value indicating whether event monitoring should be enabled.

See "Credentials required for configuring Windows File Servers" on page 20.

To add multiple Windows File Servers

1. Log in to the Data Insight Management Server.
2. Open a Windows command prompt and change to the `installdir\bin` directory, where `installdir\bin` is the installation path for Symantec Data Insight.
3. Type the following command:

   ```
   installcli <name of input file>.csv
   ```

You can also add a clustered Windows File Server to Data Insight. Data Insight supports only a Microsoft Cluster Server (MSCS) configuration.

See "Using the Agent Uploader utility" on page 71.

See "Adding filers" on page 76.

See "Add/Edit Windows File Server options " on page 83.

Using the Agent Uploader utility

Before you can install the agent, ensure that the Windows File Server agent packages are uploaded on the relevant Collector nodes. You can use the Agent

Uploader utility to upload the agent packages to the Collector nodes in your Data Insight configuration.

To upload the agent packages

1. In the Console, click **Settings** > **Agent Uploader**.
2. Browse to the location where the agent packages are saved.
3. Select the Collector nodes on which you want to upload the packages.
4. Click **Upload Bundle**.

The agent installation bundle is a zip file that contains the agent installer and various installation template files. There is one bundle for each processor architecture. You must upload the appropriate bundles to the Collector worker nodes based on the architecture of your file servers. The bundles are available along with the main install media and have the name, Symantec_DataInsight_windows_winnas_3.0_XXX_arch.zip. You can customize the agent installation by extracting the bundle in a temporary location, editing the installation templates as required, recreating the zip bundle, and then uploading the updated bundle to the appropriate Collector nodes using the Agent Uploader utility.

Upgrading the Windows File Server agent

You can upgrade the Windows File Server agent automatically from the Data Insight Management Console.

Note: The option to upgrade the agent automatically appears only if you have configured the Windows File Server to allow Data Insight to automatically install the agent.

To upgrade Windows File Server agent automatically

1. Log on to the Management Console as Administrator.
2. Use the Agent Uploader utility to upload the agent packages on Collector worker nodes corresponding to the Windows File Server agent.

   See "Using the Agent Uploader utility" on page 71..
3. Select **Settings** > **Filers** to view the list of configured Windows File Servers.
4. Click the server on which you want the upgrade the agent.
5. On the configuration details page, click **Upgrade Agent**

6 Windows File Server agent upgrade window appears and displays a progress bar while upgrading.

7 Click **Finish** to exit setup.

Note: To upgrade the Windows File Server agent manually, see the *Symantec Data Insight Installation Guide*. You can upgrade multiple Windows File Server agents using the installcli utility. See "Configuring Windows File Servers " on page 70.

About configuring Veritas File System (VxFS) file servers

A Data Insight agent plugin, `vxdiplugind`, is used to monitor access events on the VxFs file servers. The plugin is part of the VxFS package and is automatically installed on the file server when Veritas Storage Foundation is installed. The plug-in captures events from the VxFS filer that Data Insight is monitoring, and saves it to a temporary database.The event data is then pulled by Data Insight, which fetches the access event information through Veritas Operations Manager (VOM) to gain vital insight into the user activity on the filer.

Data Insight uses NFS to scan all or a portion of VxFS shares remotely from the Collector node. Data Insight only monitors the access events on the VxFS devices exported by NFS.

Before you start configuring VxFS filers, verify the following:

- The file server must be installed with Storage Foundation 6.0 with Rolling Patch 1.

  Note: Data Insight 3.0 supports only a Storage Foundation 6.0 standalone system. Storage Foundation High Availability systems are not suppported at this time.

- The file server must be installed with Veritas Operations Manager (VOM) 4.1.
- NFS version 3.0 is configured on the VxFS filer.
- The LDAP or NIS domains that your users are part of must be configured in Data Insight.
- The Collector node for the VxFs filer must be a Windows 2008 Enterprise server. Ensure that the Collector node monitoring the VxFS filer has services for NFS enabled as file server roles. You can install a role on Windows 2008 Enterprise server through the **Server Manager** > **Add roles** option.

- The filer is accessible from the Collector node using the host name or IP address you plan to use when adding the filer.

See "Adding filers" on page 76.

See "Enabling export of UNIX/Linux NFS shares on VxFS filers" on page 74.

See "Add/Edit Veritas File System server options" on page 87.

Enabling export of UNIX/Linux NFS shares on VxFS filers

These instructions are for Red Hat Enterprise Linux operation system which has standalone Storage Foundation 6.0 installed and a file system created using VxFS. The steps will change depending upon other operating system flavors.

To enable export of NFS shares on VxFS filers

1. Login as root on the VxFS filer and open the `/etc/exports` file.
2. Specify the name of the share that you would like to monitor. For example, `/demoshare`, where the VxFS file system is mounted.

   Ensure that the device entries are added in `/etc/fstab` to automatically mount NFS file systems after reboot.

   Data Insight uses /etc/exports and /etc/fstab for NFS share discovery. Sample entries are shown below:

```
root@RHEL5-VxFS ~]# cat /etc/fstab | grep vxfs

/dev/vx/dsk/openldapdg/vol01 /openldaphome vxfs defaults,_netdev 0 0

/dev/vx/dsk/openldapdg/vol02 /data vxfs defaults,_netdev 0 0

/dev/vx/dsk/openldapdg/vol03 /didata vxfs defaults,_netdev 0 0

[root@RHEL5-VxFS ~]# cat /etc/exports

/openldaphome 10.209.111.167(ro,sync,no_root_squash) 10.217.75.136
(rw,syc) /data/exportshare *(rw,sync,no_root_squash)

/didata *(rw,sync,no_root_squash)
```

3 Specify the root access and read only access to Data Insight Collector node. For example,

```
/demoshare <Collector node IP> (ro,sync,no_root_squash)

ro:read only

no_root_squash: root access.
```

You can specify read `+write`, `root_squash`, `anonuid`, `anongid` or other settings, as required.

4 Run the following command to start the NFS daemon

```
#service nfs start
```

See "Adding filers" on page 76.

Viewing configured filers

In the Management Console, you can view all the filers that Data Insight is configured to monitor.

Use the provided dynamic search filter to search for configured filers based on the IP address or the name of the filer.

To view configured filers

1 In the Console, click **Settings** > **Filers** .

The screen displays the list of configured filers

2 Review the following information about the filers:

- The object ID of the filer. This numerical value is used to identify the filer when troubleshooting issues with the filer. This column is hidden by default. To view this column, click on the column header and select **Columns** > **ID**.
- The name of the filer.
- The type of filer -NetApp, EMC Celerra, Windows File Server, or Veritas File System (VxFS) server.
- Whether file system event monitoring is Enabled or Disabled.
- The Collector node for the filer.
- The indexer node for the filer.

3 Click the Export icon at the bottom of the page to save the data on the screen to a `.csv` file.

Managing filers

On the filer details page, you can view detailed information about a configured filer, edit the filer's configuration, delete the filer, disable the filer, and manage the monitored shares on the filer.

To review filer details

1. In the Console, click **Settings** > **Filers** .
2. Click the filer that you want to review, or click the **Select Action** drop-down and select **View**.

   The filer details screen appears.

To view filer events

1. In the Management Console, click **Settings** > **Filers**.
2. Click the **Select Action** drop-down for the corresponding server in the filers listing table, and select **Event Log**.

   The event log for that filer appears.
3. To download Data Insight logs for the filer for troubleshooting purposes, click the **Select Action** drop-down for the corresponding filer, and select **Download Logs**.

   Data Insight downloads a compressed folder containing the logs related to this filer from all relevant Data Insight servers.

   See "Downloading Data Insight logs" on page 158.

Adding filers

You must add filers that you want Symantec Data Insight to monitor.

To add filers

1 In the Console, click **Settings** > **Filers**.

The Filers page displays the list of available filers.

2 On the Filers page, click the **Add New Filer** drop-down, and select the type of filer you want to add.

3 On the New Filer screen, enter the filer properties, and click **Add New Filer**.

If you are adding a Windows File Server, Data Insight can automatically install an agent on the filer. This agent enables Data Insight to receive event notifications from the filer.

For detailed information about installing the agent manually, see the *Symantec Data Insight Installation Guide*.

See "About configuring filers" on page 58.

Add/Edit NetApp filer options

Use this dialog box to add a new NetApp filer to Symantec Data Insight or to edit the configuration of an existing filer.

Table 4-2 Add/Edit NetApp filer options

Field	Description
Filer hostname or IP address	Enter the hostname or IP address of the filer that you want Data Insight to monitor. **Note:** The hostname or IP address should be the same as the filer name is entered in Symantec Data Loss Prevention targets.
Collector	From the drop-down, select the Collector worker node configured to scan the filer. Data Insight connects to the filer from this server. It is recommended that the Collector worker node share a fast network with the filer. **Note:** When monitoring NFS shares, ensure that the Collector node monitoring the filer must have services for NFS enabled as file server roles. You can install the role on Windows 2008 through the **Server Manager** > **Add roles** option.

Table 4-2 Add/Edit NetApp filer options *(continued)*

Field	Description
Indexer	From the drop-down, select the Indexer worker node configured for the filer. Events and meta-data collected from the filer is processed and stored on the Indexer node.
Filer administrator credentials	See "Credentials required for configuring NetApp filers" on page 15. Specifying the filer administrator credentials is optional, if you choose to not monitor events on the filer, nor enable share discovery.
Test credentials	Click to test the availability of network connection between the Collector worker node and the filer, and to test the validity of specified credentials. Symantec recommends that you test the connection before proceeding to ensure that Data Insight is able to connect to the filer.
Filer is vfiler	Select the check box to indicate that this filer is a NetApp vfiler.
Enable CIFS monitoring	Select this check box to enable monitoring of CIFS shares.
Enable NFS monitoring	Select this check box to enable monitoring of NFS shares.
Select domain	From the drop-down, select the domain to which the NetApp filer belongs. This option is enabled when monitoring NFS shares.

Table 4-2 Add/Edit NetApp filer options *(continued)*

Field	Description
Monitoring details	Select **Automatically discover and monitor shares on this filer** to have Data Insight automatically discover shares of the filer and add them configuration. Discovery of shares takes place as soon as you add a new filer and then twice each day at 2:00 a.m. and 2:00 p.m. You can also choose to add shares manually. See "Adding shares" on page 95.
Exclude shares from discovery	Enter the details of shares which should not be included during discovery. This option is available if you select **Automatically discover all shares on this filer.** Specify comma separated patterns that you want to ignore. Patterns can have 0 or more wildcard * characters. For example, tmp* ignores `tmp_A`, `tmp_abc`, *$ ignores shares `C$`, `EXT$` and others.
Enable storage utilization analytics	Select the check box to allow Data Insight to gather storage utilization information from the filer. This information is used when generating Filer Utilization and Filer Growth Trend reports. The DataInsightFpolicy service running on the Collector node gathers information about storage utilization on the filer.
Enable file system event monitoring	Select to enable event monitoring on the filer.
Enable Fpolicy automatically	Select to automatically enable Fpolicy on the filer. If you clear this check box, you must manually enable Fpolicy on the filer. See "Preparing the NetApp filer for Fpolicy" on page 61.

Table 4-2 Add/Edit NetApp filer options *(continued)*

Field	Description
Register for explicit Read events	Select the option to register for explicit Read events. When this option is not selected, OPEN events are treated as READ events. **Note:** NFSv3 does not support OPEN events. This means that you will not see READ events for NFS shares when this check box is cleared. Symantec recommends that you do not register for explicit Read events. This can increase the load on the filer during peak traffic from third party applications such as backups over CIFS.
Enable filer scanning	Select the check box to enable filer scanning according to the specified schedule.
Scanning schedule for full scans	Select one of the following to define a scanning schedule for shares of this filer: ■ Use Collector's default scanning schedule. ■ Use custom schedule. See "Custom schedule options" on page 90. Symantec Data Insight periodically scans shares of the filer to obtain file metadata and security descriptors. Each Collector worker node by default initiates a full scan of shares at 7:00 p.m. on the last Friday of each month.
Scanner credentials	See "Credentials required for configuring NetApp filers" on page 15.
Scan new shares immediately	Select this option to scan newly added shares immediately, instead of waiting for the normal scan schedule. Scanning proceeds only when scanning is permitted on the Collector node.

See "Enabling export of NFS shares on NetApp" on page 66.

Add/Edit EMC Celerra filer options

Use this dialog box to add a new EMC Celerra filer to Symantec Data Insight or to edit the configuration of an existing filer.

Table 4-3 Add/Edit EMC Celerra filer options

Field	Description
CIFS Server Name	Enter the hostname of the CIFS server exported by the filer. Entering the IP address of the CIFS server is not permitted
Control Station Hostname/IP address	Enter the IP address of the filer's Control Station.
Collector	From the drop-down, select the collector worker node configured to scan the filer. Data Insight connects to the filer from this server. It is recommended that the Collector worker node share a fast network with the filer
Indexer	From the drop-down, select the Indexer worker node configured for the filer.
Control Station Credentials	Enter the credentials for the filer's Control Station.
Virtual Data Mover	Select the check box if the filer is running a virtual data mover. This field is used to handle physical paths returned for virtual data movers.
Test credentials	Click to test the availability of network connection between the Collector worker node and the filer and the validity of the specified credentials. Symantec recommends that you test the connection before proceeding to ensure that Data Insight is able to connect to the filer

Table 4-3 Add/Edit EMC Celerra filer options *(continued)*

Field	Description
Monitoring details	Select **Automatically discover and monitor shares on this filer** to have Data Insight automatically discover shares of the filer and add them configuration. Discovery of shares takes place as soon as you add a new filer and then twice each day at 2:00 a.m. and 2:00 p.m. You can also choose to add shares manually. See "Adding shares" on page 95.
Enable file system event monitoring	Select to enable event monitoring on the filer.
Enable filer scanning	Select the check box to enable filer scanning according to the specified schedule.
Scanning schedule for full scans	Select one of the following to define a scanning schedule for shares of this filer: ■ **Use the Collector's scanning schedule** ■ **Use custom schedule** See "Custom schedule options" on page 90. From the drop-down, select the appropriate frequency option. Symantec Data Insight periodically scans shares of the filer to obtain file metadata and security descriptors. Each Collector worker node by default initiates a full scan of shares on the last Friday of each month. **Note:** You can also customize the schedule per share using the Add/Edit Share dialog box.
Scanner credentials	See "Credentials required for configuring EMC Celerra filers" on page 19.
Scan new share immediately	Select this option to scan newly added shares immediately, instead of waiting for the normal scan schedule. Scanning will still run only when scanning is permitted on the Collector node.

Add/Edit Windows File Server options

Use this dialog box to add a new Windows File Server to Symantec Data Insight or to edit the configuration of an existing filer.

Table 4-4 Add/Edit Windows File Server options

Field	Description
Is a MSCS clustered file server	Select the check box if the Windows File Server is part of a Microsoft Cluster Server configuration.
Windows server name/Cluster name	Enter the host name or IP address of the filer that you want Data Insight to monitor. In case of a clustered Windows File Server, enter the host name or IP address of the cluster. **Note:** The hostname or IP address should be same as the filer name entered in Symantec Data Loss Prevention Discover targets.
Select Collector node for this filer	From the drop-down, select the collector worker node configured to scan the filer. Data Insight connects to the filer from this server. It is recommended that the Collector worker node share a fast network with the filer.
Select Indexer node for this filer	From the drop-down, select the Indexer worker node configured for the filer.
Monitor mode	Select one of the following monitoring options: ■ **Monitor this filer using an agent** If you select this option, Data Insight is able to monitor all file system events on the filer and scan file system metadata. ■ **Monitor this filer without an agent** If you select this option, Data Insight scans the filer using CIFS to discover shares and obtain file metadata. However, in this case, Data Insight will not be able to monitor file system events.

Table 4-4 Add/Edit Windows File Server options *(continued)*

Field	Description
Agent names for this filer	This option is visible when adding a clustered file server that is monitored using an agent, but where the agent is installed manually. Select one or more agent nodes from the list that belong to this cluster. This option is also visible when editing a clustered file server.
Let Data Insight install the agent automatically	Select to allow Data Insight to install or upgrade the agent on the Windows File Server. Data Insight automatically installs the Windows File Server agent on the filer using the WMI interface and also registers the filer with the Management Server.
Node names to install agent	This option is only visible if you have selected **Is a MSCS clustered file server**. In the text box, enter comma-separated IP addresses or hostnames of the Windows File Server nodes, on which you want to install the agent.
Filer Administrator Credentials	Enter the credentials that Data Insightshould use to install the agent on the Windows File Server. See "Credentials required for configuring Windows File Servers" on page 20.
Test Connection	Click to test the availability of network connection between the Collector worker node and the filer, and the validity of the specified credentials. Symantec recommends that you test the connection before proceeding to ensure that Data Insight is able to connect to the filer.

Table 4-4 Add/Edit Windows File Server options *(continued)*

Field	Description
Automatically discover and monitor all shares on this filer	Use this option to have Data Insight automatically discover shares of the filer and add them configuration. You can choose to exclude certain shares using the **Exclude shares** field. Discovery of shares takes place as soon as you add a new filer and then twice each day at 2:00 a.m. and 2:00 p.m.
Exclude following shares from discovery	Enter the details of shares which should not be included in share discovery. This option is available if you select **Automatically discover all shares on this filer**. Specify comma separated patterns that you want to ignore. Patterns can have 0 or more wildcard * characters. For example, `tmp*` ignores shares `tmp_A`, `tmp_abc`, `*$` ignores shares `C$`, `EXT$` and others.
Collect storage utilization information for the filer	Select to enable Data Insight to collect storage utilization information from the filer. This information is used to create Filer utilization and Filer Growth Trend reports.
Enable file system event monitoring	Select to enable event monitoring on the filer.
Enable filer scanning	Select the check box to enable filer scanning according to the specified schedule.

Table 4-4 Add/Edit Windows File Server options *(continued)*

Field	Description
Scanning schedule for full scans	Select one of the following to define a scanning schedule for shares of this filer: ■ **Use the Collector's scanning schedule** ■ **Define custom schedule** From the drop-down, select the appropriate frequency option. See "Custom schedule options" on page 90. Symantec Data Insight periodically scans shares of the filer to obtain file metadata and security descriptors. Each Collector worker node by default initiates a full scan of shares on the last Friday of each month. **Note:** You can also customize the schedule per share using the **Add/Edit Share** dialog box.
Scanner credentials	Select one of the following: ■ **Use LOCAL SERVICE credentials** Select to use the LOCAL SERVICE account to scan shares of the filer. This option is available only for the filers monitored using an agent. If you select this option, ensure that the LOCAL SYSTEM account to has appropriate privileges to scan the shares. If the account does not have adequate privileges, the scans for such shares will fail if performed using this account. ■ **Use saved credentials** Select the saved credentials from the drop-down or specify new credentials. See "Credentials required for configuring Windows File Servers" on page 20.

Table 4-4 Add/Edit Windows File Server options *(continued)*

Field	Description
Scan new shares immediately	Select this option to scan newly added shares immediately, instead of waiting for the normal scan schedule. Scanning will still take place during the hours when scanning is permitted on the Collector node.

Add/Edit Veritas File System server options

Use this dialog box to add a new Veritas File System (VxFS) filer to Symantec Data Insight or to edit the configuration of an existing filer.

Table 4-5 Add/Edit Veritas File System (VxFS) filer options

Field	Description
Filer hostname or IP address	Enter the hostname or IP address of the filer that you want Data Insight to monitor. **Note:** The hostname or IP address should be the same as the filer name entered in Symantec Data Loss Prevention Discover targerts.
Collector	From the drop down, select the Collector worker node configured to scan the filer. Data Insight connects to the filer from this server. It is recommended that the Collector worker node share a fast network with the filer. **Note:** Ensure that the Collector node monitoring the NFS must have services for NFS enabled as file server roles. You can install the role on Windows 2008 through **Server Manager** > **Add roles** option.
Indexer	From the drop down, select the Indexer worker node configured for the filer. Events and meta-data collected from the filer is processed and stored on the Indexer node.

Table 4-5 Add/Edit Veritas File System (VxFS) filer options *(continued)*

Field	Description
Login credentials	See "Credentials required for configuring Veritas File System (VxFS) servers" on page 21. Specifying filer administrator credentials is optional, if you choose not to monitor events on the filer, nor enable share discovery.
Test credentials	Click to test the availability of network connection between the Collector worker node and the filer, and to test the validity of the specified credentials. Symantec recommends that you test the connection before proceeding to ensure that Data Insight is able to connect to the filer.
Monitoring details	Select **Automatically discover and monitor shares on this filer** to have Data Insight automatically discover shares of the filer and add them configuration. Discovery of shares takes place as soon as you add a new filer and then twice each day at 2:00 a.m. and 2:00 p.m. You can also choose to add shares manually. See "Adding shares" on page 95.
Exclude shares from discovery	Enter the details of shares which should not be included during discovery. This option is available if you select **Automatically discover all shares on this filer.** Specify comma separated patterns that you want to ignore. Patterns can have 0 or more wildcard * characters. For example, tmp* ignores `tmp_A`, `tmp_abc`, *$ ignores shares `C$`, `EXT$` and others.

Table 4-5 Add/Edit Veritas File System (VxFS) filer options *(continued)*

Field	Description
Enable file system event monitoring	Select to enable file system monitoring on the filer. Enter the following details: ■ Time to live - The value indicates the time for which the VxFS plugin will try to communicate with Data Insight. If communication fails after the specified time, the plugin will terminate and stop capturing events from the VxFS filer. The default TTL value is 24 hours. ■ Records per file - The number of records after which the events are flushed to the Collector node. You can also enable an advanced setting to flush the records to the Collector node every 10 minutes, irrespective of the number of records specified. By default, the limit is set to 100000 records per file. See "Configuring advanced settings" on page 128. ■ Domain: The name of the LDAP or NIS domain that the filer is a part of. The VxFS filer that you want to add should not be part of two domains at the same time.
Enable filer scanning	Select the checkbox to enable filer scanning according to the specified schedule.
Scanning schedule for full scans	Select one of the following to define a scanning schedule for shares of this filer: ■ **Use the Collector's scanning schedule** ■ **Define custom schedule** Symantec Data Insight periodically scans shares of the filer to obtain file metadata and security descriptors. Each Collector worker node by default initiates a full scan of shares at 7:00 p.m. on the last Friday of each month. **Note:** You can customize the schedule per share using the Add/Edit Share dialog box.

Table 4-5 Add/Edit Veritas File System (VxFS) filer options *(continued)*

Field	Description
Scanner credentials	See "Credentials required for configuring Veritas File System (VxFS) servers" on page 21.
Scan newly added shares immediately	Select this option to scan newly added shares immediately, instead of waiting for the normal scan schedule.

See "Enabling export of UNIX/Linux NFS shares on VxFS filers" on page 74.

Custom schedule options

Table 4-6 describes the options that you can use to define the frequency of the scans.

Table 4-6 Custom schedule options

Option	Description
Never	Runs the scan as and when required.
Once	Runs the scan once at the specified time and date.
Daily	Runs the scan once every day. You must specify the time when the scan should be run.
Weekly	Runs the scan once every week. You can choose to run it on every weekday, or on specific weekdays. Also, you must specify the time when the scan should be run.
Monthly	Runs the scan once every month. You must specify the day of the month and the time when the scan should be run.
Custom Cron	Runs the scan according to a defined cron schedule. You can build strings in the cron format to specify custom schedules such as every Friday at noon, or weekdays at 10:30 a.m., or every 5 minutes between 9:00 a.m and 10 a.m. on Wednesdays and Fridays.

Editing filer configuration

After you add a filer to Data Insight, you can edit the filer's configuration. For example, you might need to edit any of the following:

- The IP address or hostname of the filer.
- The username and password of the user authorized to log in to the filer.
- The IP address or hostname of the Collector worker node configured to scan the filer.
- The scanning schedule.
- The scanner credentials.
- Whether all shares are to be monitored.
- Whether new shares are to be scanned immediately.

To edit filer configuration

1. In the Console, click **Settings** > **Filers**.

   This displays the list of available filers.
2. Do one of the following:
   - In the filer summary table. click the **Select Action** drop-down and select **Edit**.
   - Click the filer whose configuration you want to edit. On the Filer detail screen, click **Edit**.
3. On the Edit Filer screen, make the necessary configuration changes.
4. Click **Save**.

Deleting filers

You can delete a configured filer.

To delete a filer

1. In the Console, click **Settings** > **Filers** to display the configured filers.
2. Do one of the following:
   - In the filer summary table, click the **Select Action** drop-down, and select **Delete**.
   - Click the filer you want to delete, and on the filer details page, click **Delete filer**.
3. If the filer you want to delete is a Windows File Server, the system asks you whether you want to uninstall the agent for the filer.

   Click **OK** to uninstall the agent.
4. Click **OK** on the confirmation message.

Managing shares

On the Monitored Shares details page you can view the detailed information about configured shares and run a customized scan on the configured shares.

Use the provided dynamic search filter to search for configured shares based on the name of the share.

To view configured shares

1. In the Console, click **Settings** > **Filers**.
2. Click the filer on which the share resides.
3. On the Filer Detail screen, click **Monitored Shares**.

   Review the following information about the shares:

   - The name of the share.
     If this share belongs to a clustered filer, then the name should appear as *fileserver@share*, where, *fileserver* is the name of the file server within the cluster that hosts the share.
   - The scanning schedule for the share.
   - The date and time of the last full scan of the share.
   - The date and time of the last incremental scan.
     Incremental scans are scans of the file system that includes only those paths that have changed since the last full scan. Incremental scans are much faster than full scans and they take place once every night at 7:00 p.m. You can configure incremental scans on the **Settings** > **Data Insight Servers** > **Advanced Settings** page.
   - The time this share's index was last updated with scan information.
     After every scan, the index is updated with information about the changes to the folder hierarchy on a share. This indicates whether the last update was successful or failed. It also indicates the number of scan files pending for this share on the Indexer and the number of files that failed to be indexed. Such files are present in the `$data/indexer/err` folder on the Indexer. If there are failed files on the Indexer, you can move them from the `err` folder to `$data/inbox` folder and attempt a full scan of the share. If the information fails to be indexed again, contact Symantec Support.
   - The time this share's index was last updated with access event information.
     As new access events come in, the index for the share is periodically updated with information about the new access events. This indicates whether the last update was successful or had failed. It also indicates the number of audit files pending for this share on the Indexer and the number

of files that failed to be indexed. Such files are present in the `$data/indexer/err` folder on the Indexer. If there are failed files on the Indexer, you can move them to the `$data/inbox` folder on the Indexer. If they fail to be indexed again, contact Symantec Support.

4 Click the Export icon at the bottom of the page to save the data on the Monitored Shares panel to a `.csv` file.

You can also add a new share, edit the share's configuration, delete the share, start an unscheduled scan for a share, view the scan history of a share, and download Data Insight logs from this page.

To view the scan history of a share

1 In the Console, click **Settings** > **Filers**.

2 Click the filer on which the share resides.

3 On the Filer Detail screen, click **Monitored Shares**.

4 Click the **Action** drop-down for the corresponding share, and select **Scan History**.

The scan history for the share appears. You can view the details in a tabular format or in a Timeline view. The tabular view displays the following details of a scan:

- The start and end time of the scan.
- The time taken for the scan.
- The type of scan, whether full or incremental.
- The Collector node associated with the share.
- The details of the scan. For example, if a scan has failed, the **Details** column indicates the exit code for the error message.
- The user account that initiated the scan.

The Timeline view displays an hourly and daily overview of the scans run on the share, including information about the status of the scan, whether failed, successful, partially successful, or aborted.

To view events pertaining to a share

1 In the Console, click **Settings** > **Filers**.

2 Click the filer on which the share resides.

3 On the filer details screen, click **Monitored Shares**.

4 Click the **Action** drop-down for the corresponding share, and select **Event Log**.

The event log for that share appears.

5 To download the Data Insight logs for the share, click the **Select Action** drop-down for the corresponding share, and select **Download Log**.

Data Insight downloads a compressed folder containing logs for this share from all relevant Data Insight servers.

See "Downloading Data Insight logs" on page 158.

To scan one or more shares in a batch

1 On the Monitored shares tab, click the Scan button.

2 On the Scan Shares pop-up, select one of the following:

- **Scan all** - To scan all the configured shares immediately.
- **Scan with last scan status** - To scan shares based on the following criteria:
  - Shares on which the last scan has failed completely.
  - Shares that have never been scanned before.
  - Shares on which the last scan has failed on certain paths.

3 Select one or more of the following conditions:

- Scan shares that have not been scanned for *n* number of day Enter the interval in the field.
- Include shares matching specified patterns. You can enter multiple patterns separated by a comma. You can also specify one or more wildcards in the pattern. For example vol*, *$.
- Exclude shares matching specified patterns. You can enter multiple patterns separated by a comma. You can also specify one or more wildcards in the pattern. For example vol*, *$.
- Select **Add to the top of the scan queue** to add the scan to the top of the scan queue.

4 Select **Start scanning**.

Note: You can use a command line utility, `scancli.exe`, to further customize the scan, view the scan jobs running on a specified node, or display the scan status for specified shares. For details, See scancli.exe on page 172.

Adding shares

After you add a filer, you can add shares present on the filer that you want Data Insight to monitor. You need to perform this operation if you have selected **Shares will be added manually** option when adding a filer.

To add a share

1. In the Console, click **Settings** > **Filers** to expand the Filer node.
2. Click the filer for which you want to add a share.
3. On the Filer Detail screen, click **Monitored Shares**.
4. On the Monitored Shares screen, click **Add New Share**.
5. On the **New Share** screen, enter the share properties, and click **Add New Share**.

See "Add New Share/Edit Share options " on page 95.

Add New Share/Edit Share options

Use this dialog box to add a new share to Symantec Data Insightor to edit the configuration of an existing share.

Table 4-7 Field Descriptions

Field	Descriptions
Share name	Enter the name of the share you want to add. For example, *share1*. If this share belongs to a clustered filer, enter share name FileServer@ShareName.
Physical path on filer	Enter the physical path of the share on the filer. For example, `F:\<Share name>`.
Scanning schedule	Select one of the following to define a scanning schedule: ■ **Use filer's scanning schedule** ■ **Define custom schedule** From the drop-down, select the appropriate frequency option. See "Custom schedule options" on page 90.

Editing share configuration

After you add a share to Data Insight, you can edit the share's configuration. For example, you might need to edit the scanning schedule.

To edit share configuration

1. In the Console, click **Settings** > **Filers** to expand the Filer node.

   This displays the list of available filers. Click the appropriate filer to open the Filer details page.
2. Select the share whose configuration you want to edit, click the **Select Action** drop-down and select **Edit**.
3. On the Edit Share screen, make the necessary configuration changes.
4. Click **Save**.

Deleting shares

You can delete a configured share.

To delete a share

1. In the Console, click **Settings** > **Filers** to display the configured filers.
2. Click the filer, on which the share that you want to delete exists.
3. On the filer details page, under **Monitored Shares**, select the share that you want to delete.
4. Click the **Select Action** drop-down and select **Delete**.
5. Click **OK** on the confirmation message.

About configuring a DFS target

Symantec Data Insight supports Microsoft Distributed File System (DFS) targets.

DFS simplifies access to and management of shares by mapping a single logical namespace to shared folders on multiple filers. You can create folders within a DFS to create an additional level of hierarchy. For example, if you have a NetApp filer, NETAPP01, which has a shared folder called `NetAppShare1`. You can link a target, `HQ\Sales\Test`, present on a DFS server, DFSSvr01, to the subfolder named `Finance` within `NetAppShare1`.

You must first import the DFS mappings to physical shares in to Data Insight before you can view data using DFS hierarchy.

Configuring a DFS target

Before you can configure a DFS target you must configure all file servers which map to your DFS targets.

To set up a DFS target

1. Log in to the Management Console.
2. Create a .csv file containing the following information:
   - The name of the DFS server.
   - The DFS target.
   - The name of the filer that contains the share that you want to map to the DFS target.
   - The share on the filer.
   - Path under the physical share, if the DFS folder is mapped to a folder under physical share, else this value can be blank.

   For example, *DFSSvr01,HQ\Sales\Test,NETAPP01,NetAppShare1,\Finance.*
3. Click the **Settings** tab.
4. Click **Filers**, and select **Import DFS Mappings**.
5. In the Add new DFS mappings dialog, browse to the location of the .csv file, and click **Upload**.
6. Alternatively, open a Windows command prompt, and change to the `installdir\bin` directory, where `installdir\bin` is the installation path for Symantec Data Insight.
7. Type the following command:

   ```
   configdb -H  <name of the .csv file>
   ```

About the DFS utility

The DFS utility, `MXDFSSCAN.EXE`, maps root level DFS paths to actual storage server or share paths. It is used to export the DFS components (roots, root targets, links, and link targets) for all Windows DFS namespaces. The utility finds out physical level storage/filer link for all Domain DFS paths. It takes DFS root UNC path as input, for example, `\\<DFS domain>\root`. This utility only enumerates online links and skips all offline links. It generates the output in .csv format.

The `MXDFSSCAN.EXE` is a command line utility.

Running the DFS utility

Ensure that the DFS servers are accessible from the machine you use to run the DFS utility.

To run the DFS utility

1. From the Windows Start menu, select **Run** and type `cmd` in the dialog box to open a command prompt window.
2. Change to the `installdir\bin` directory, where `installdir\bin` is the installation path for Symantec Data Insight.
3. Type the following command:

   ```
   mxdfsscan -n \\<DFS domain>\root -f dfsmap.csv
   ```

   where,

   `-n` is the name of the DFS root

   `-f` is the file name to which the DFS mappings have to be exported.

   `-e` is the option to exclude domain DFS paths. For example,

   ```
   mxdfsscan.exe -n \\MSAD\newroot -f dfsmap.csv -e exclude.txt
   ```

   An exclude list can have max 128 exclude entries. For example,

   ```
   \\DFS\root\AP\NUY

   \\DFS\root\users
   ```

   `-c` is the option to traverse a specified number of intermediate DFS servers to find a physical storage path. If the -c option is not specified then the utility takes the default value 5. This option helps avoid circular links in a DFS environment. If there are more hops then it logs all such links into `dfs_log_links.txt`.

Importing DFS mapping

You can import DFS mappings to Data Insight from the Management Console. To import DFS mappings, complete the following steps.

To import DFS mappings

1. Create a .csv file that contains information about the DFS mappings.

   See "Running the DFS utility" on page 98.
2. In the Console, click **Settings** > **Filers** to display the list of available filers.
3. Click **Import DFS mappings**.

4 On the Import DFS mappings window, browse to the location of the `.csv` file that contains information about the mapped DFS namespaces.

5 Click **OK**.

Chapter 5

Configuring SharePoint monitoring

This chapter includes the following topics:

About SharePoint server monitoring

You can use Symantec Data Insight to monitor unstructured data residing on servers running any of the following:

- Microsoft SharePoint™ 2010
- Microsoft Office SharePoint™ Server 2007 (MOSS 2007)

Data Insight monitors accesses to the data in the following SharePoint library types:

- Document library - Stores documents in the .pdf, .doc, .xls, .txt and other such file extensions.
- Picture library - Stores images.

Data Insight monitors access events on the SharePoint servers and maps all SharePoint access types such as checkout, view, check in, write, update, delete, and move to Data Insight meta access types - Read, Write, Delete, and Rename.

Before you use Data Insight to scan a SharePoint server, you must have completed the following tasks:

- Set up your SharePoint servers and created the SharePoint site collections and sites that you want Data Insight to monitor. To be able to configure Data Insight, you must also know the URLs of the target SharePoint Web applications.
- Ensure that .NET Framework 3.0 or 3.5 is installed on the Collector node that is responsible for the discovering site collections and collecting audit logs.
- Configured a policy for each Web application.
  See "Configuring a Web application policy" on page 102.
- Installed and configured the Data Insight Web service on the SharePoint server.
- Enabled auditing on the SharePoint server. You can enable auditing from the Management Console when you add Web applications, or directly from the SharePoint server.

Configuring a Web application policy

When configuring SharePoint from the Data Insight console, you must specify an account for monitoring the configured site collections. This account must be a site collection administrator for the configured sites and it must be in the same domain as the SharePoint server. It must have full control permissions not only on the configured Web applications, but also on the Web applications that are added to SharePoint subsequently. The account should have the necessary privileges to set the appropriate audit flags, gather metadata about site collection content, and gather audit data from SQL Server databases for SharePoint.

To enable Data Insight to gather audit and metadata from multiple site collections using a single user account, you must configure a policy for each Web Application from the SharePoint Central Administration Console.

To configure a policy for Web Application in SharePoint 2007

1. In the Central Administration Web site, click **Application Management**.
2. Under the Application Security section, click **Policy for Web application**.

3 Click **Add Users**.

4 In the Web Application drop-down list, select the Web application that contains the site collections that you want Data Insight to monitor.

5 Select the appropriate zone. You can select **(All Zones)** if you want the user to be given permissions on all zones for the Web application.

6 Click **Next**.

7 Choose the user account that will have Full Control.

8 In the Choose Permissions section, select **Full Control - Has full control**

9 Specify whether this account operates as SharePoint System account. If you select the **Account operates as System** check box, all accesses made by this user account are recorded with the user name, *SharePoint System*.

10 Click **Finish**.

To configure a policy for Web Application in SharePoint 2010

1 In the Central Administration Console, click **Application Management**.

2 Under the Web Applications section, click **Manage Web Applications**.

3 In the table displaying Web application details, select the appropriate Web application.

4 Click **User Policy**.

5 In the Policy for Web Application popup, click **Add Users**.

6 Select the appropriate zone. You can select **(All Zones)** if you want the user to be given permissions on all zones for the Web application.

7 Click **Next**.

8 Choose the user account that will have Full Control.

9 In the Choose Permissions section, select **Full Control - Has full control**

10 Specify whether this account operates as SharePoint System account. If you select the **Account operates as System** check box, all accesses made by this user account are recorded with the user name, *SharePoint System*.

11 Click **Finish**.

About the Data Insight Web service for SharePoint

Before you can configure SharePoint monitoring in Data Insight, you must install the Data Insight Web service on the SharePoint server. The Data Insight Web service performs the following functions:

- Enables or disables auditing on the SharePoint server.
  You can enable or disable auditing of access events at the site collection level, either manually or from the Data Insight Management Console when adding Web applications.
- Discovers site collections within a Web application.
- Discovers all Web sites and lists or libraries within a site collection
- Retrieves access event data from the SharePoint server. Data Insight uses this data to service queries on user activity and data access.
- Deletes audit logs from a site collection.

Installing the Data Insight Web service for SharePoint

To enable Data Insight to collect access events, you must install the Data Insight Web service, on a SharePoint server. When installing in a SharePoint farm, you must ensure that the Web service is configured on on all front-end Web servers in the farm. Perform the following steps on any one front-end Web server in your SharePoint farm. The Web server installer automatically deploys the Web service to all front-end Web servers in the farm.

To install the Data Insight Web service

1. Log on to the SharePoint server as an account that has SharePoint administrator privileges.
2. Load the Data Insight media on your SharePoint server.
3. Navigate to the folder where you have extracted or copied the installers.
4. To start the installation, double-click `Symantec_DataInsight_sharepoint_3.0_N.exe`, where, N is the build number.
5. Work through the installation wizard.
6. Click **Finish** to complete the installation process.
7. Verify whether the Web service is deployed as expected.

After installing the Data Insight Web service, you must verify whether it is successfully deployed on all front-end Web servers in the SharePoint farm.

To verify the deployment of the Web service in SharePoint 2007

1. In the Central Administration console, click the **Operations** tab.
2. Under Global Configurations section, click **Solution Management**.

3 Verify that the status for Data Insight solution for SharePoint is set to **Deployed**.

4 Click the link for the solution. Verify that the solution is deployed to all the front-end Web servers in the farm by checking the value of **Deployed To** field.

To verify the deployment of the Web service in SharePoint 2010

1 In the Central Administration console, click the **Operations**.

2 Under the Farm Management section, click **Manage Farm Solutions**.

3 Verify that the status for Data Insight solution for SharePoint is set to **Deployed**.

4 Click the link for the solution. Verify that the solution is deployed to all the front-end Web servers in the farm by checking the value of **Deployed To** field.

Viewing configured SharePoint Web applications

In the Management Console, you can view all the SharePoint Web applications that Data Insight is configured to monitor.

To view configured Web applications

1 In the Console, click **Settings** > **SharePoint Web Applications**.

The screen displays the list of configured Web applications.

2 Review the following information about the Web applications:

- The URL of the Web application.
- The status of the Web application — whether scanning and event monitoring are enabled for this Web application.
- The Collector node for the Web application.
- The Indexer node for the Web application.
- Click on a configured Web application to view its detailed information, or click the **Select Actions** drop-down and select **View**.
  The Web application details page appears.

Adding Web applications

You must install the Data Insight Web service on the SharePoint server, before you can add the Web applications that you want Data Insight to monitor. In case the Web service is not installed, Data Insight prompts you to install it before you can proceed with adding Web applications.

To add web applications

1. In the Console, click **Settings** > **SharePoint Web Applications**.

   The SharePoint page displays the list of configured Web applications.

2. Click **Add SharePoint Web Application**.

3. On the Add Web Application screen, enter the URL of the Web application you want to add and enter the properties.

4. Click **Save**.

Add/Edit Web application options

Use this dialog box to add a new Web application to Symantec Data Insight or to edit the configuration of an existing web application.

Table 5-1 Add/Edit Web application options

Field	Description
Web application URL	Enter the URL of the web application that you want Data Insight to monitor.
Collector for this Web application	From the drop-down, select the Collector worker node configured to scan the SharePoint server. Data Insight connects to the SharePoint server from Collector node. It is recommended that the Collector worker node share a fast network with the SharePoint server.
Indexer for this Web application	From the drop-down, select the Indexer worker node configured to scan the SharePoint server.
Default Site Collection Administrator	Enter the credentials that Data Insight should use to provide authenticated access to the Data Insight Web service on the SharePoint server. See "Configuring a Web application policy" on page 102.

Table 5-1 Add/Edit Web application options *(continued)*

Field	Description
Verify credential	Click to test the availability of network connection between the Collector worker node and the SharePoint server, and to test the validity of specified credentials. You must first ensure that the Data Insight Web service is already installed on the SharePoint server. Symantec recommends that you verify the credentials before proceeding to ensure that Data Insight is able to connect to the SharePoint server.
Automatically discover and add all site collections in the selected Web applications to Data Insight	This checkbox is selected by default. This option allows you to automatically include all site collections in the selected Web application for the purpose of monitoring. Clear the check box to add site collections manually. You can do this from the Web Application details page.
Exclude following site collections from discovery	Enter the details of the site collections which should not be included during discovery. This option is available if you select **Automatically discover and add site collections in the added SharePoint Web Applications**. Specify comma separated patterns that you want to ignore. Patterns can have 0 or more wildcard * characters. For example, https://webapp1/sites/test* ignores site collections https://webapp1/sites/testsite1 and https://webapp1/sites/testsite2.
Monitor access for this Web application	Select to enable monitoring of access events for the Web application.

Table 5-1 Add/Edit Web application options *(continued)*

Field	Description
Automatically enable auditing for site collections of this Web application	Select to automatically enable event monitoring for all site collections of this Web application . You can also choose to manually enable auditing by logging in to the SharePoint server. For this purpose, you must have site collection administrator privileges on the SharePoint server.
Delete audit logs from SharePoint database after importing in Data Insight.	Select to delete audit logs from SharePoint to prevent the Web application database from growing too large. By default, Data Insight deletes audit logs that are older than two days. You can choose to customize how often Data Insight should delete old audit logs from the Data Insight Servers node on the Management Console. See "Configuring advanced settings" on page 128.
Enable scanning for this Web application	Select the checkbox to enable SharePoint scanning according to the specified schedule.
Scanning schedule for full scans	Select one of the following to define a scanning schedule for the SharePoint servers in this farm: ■ **Use the Collector's scanning schedule.** ■ **Define custom schedule for farm.** From the drop-down, select the appropriate frequency. See "Custom schedule options" on page 90. Symantec Data Insight periodically scans site collections to obtain file metadata. Each Collector worker node by default initiates a full scan the SharePoint servers at 11:00 p.m. each night. **Note:** You can also customize the schedule for each site collection using the Add/Edit Site Collection dialog box.

Table 5-1 Add/Edit Web application options *(continued)*

Field	Description
Scan newly added site collections immediately	Select this option to scan newly added site collections immediately, instead of waiting for the normal scan schedule. Scanning will still proceed only when scanning is permitted on the Collector node.

Editing Web applications

After you add a Web application to Data Insight, you can edit its configuration. For example, you might need to edit any of the following:

- The user authorized to log in to the SharePoint server.
- The Collector worker node configured to scan the SharePoint server.
- Enable or disable Web application scanning or audit.
- The scanning schedule.

To edit Web applications

1. In the Console, click **Settings** > **SharePoint Web Applications**.
2. Do one of the following:
   - In the Web application summary table, click the **Select Actions** drop-down and select **Edit**.
   - Click the Web application whose configuration you want to edit. On the Web application detail screen, click **Edit**.
3. Make the changes on the Edit Web Application screen and click **Save**.

Deleting Web applications

You can delete a configured Web application.

To delete a Web application

1. In the Console, click **Settings** > **SharePoint Web Applications**.
2. Do one of the following:
   - In the Web application summary table, click the **Select Actions** drop-down and select **Delete**.

- Click the Web application that you want to delete. On the Web application detail screen, click **Delete**.

3 Select the check box to disable auditing on the Web application.

4 Click **Yes** on the confirmation dialog box.

Adding site collections

You can configure Data Insight to scan one or more site collections within a Web application.

To add site collections

1 In the Console, click **Settings** > **SharePoint Web Applications**.

2 In the Web application summary table, click the Web application that the site collections are a part of.

3 Click the **Monitored Site Collections** tab.

The screen displays a list of all configured site collections.

4 Click **Add Site Collection**.

5 On the Add New Site Collection dialog, enter the site collection properties, and click **Add New Site Collection**.

See "Add/Edit site collection options" on page 110.

Add/Edit site collection options

Use this dialog box to add a new site collection to a configured Web application or to edit the configuration of an existing site collection.

Table 5-2 Add/Edit site collection options

Field	Description
Site Collection URL	Enter the URL of the site collection that you want to add.
Site Collection Title	Enter a logical name for the site collection.

Table 5-2 Add/Edit site collection options *(continued)*

Field	Description
Scanning schedule	Select one of the following to define a scanning schedule for the site collection: ■ **Use Collector's scanning schedule** ■ **Define custom scanning schedule** From the drop-down, select the appropriate frequency. ■ See "Custom schedule options" on page 90. Symantec Data Insight periodically scans site collections to obtain metadata. Each Collector worker node by default initiates a full scan of the SharePoint servers at 11:00 p.m. each night.

sManaging site collections

On the site collections details page, you can view detailed information about a site collection, and edit or delete the site collection. You can also run a scan on the site collection from this page.

Use the provided dynamic search filter to search for configured sites based on the name of the site.

To view configured site collections

1. In the Console, click **Settings** > **SharePoint Web Application**.
2. In the Web application summary table, click the Web application that the site collections are a part of.

   The screen displays a list of all configured site collections.
3. On the Web application details page, click **Monitored Site Collections**.
4. On the Site Collections listing page, review the following information about the configured site collections.
   - The name of the site collection.
   - The scanning schedule for the site collection.
   - The date and time of the last full scan of the site collection.
   - The time this site collection's index was last updated with scan information.

After every scan, the index is updated with information about the changes to the folder hierarchy on a site collection. This column indicates whether the last update was successful or has failed. It also indicates number of scan files pending for this site collection on the Indexer and the number of files that failed to be indexed. The scan failed files are present in the `$data/indexer/err` folder on the Indexer. If you do have failed files on the indexer, you can move them from the `err` folder to the `$data/inbox` folder and attempt a full scan of the site collection.
If the scan information again fails to be indexed, contact Symantec support.

- The time this site collection's index was last updated with access event information.
  As new access events come in, the index for the site collection is periodically updated with information about the new access events. This indicates whether the last update was successful or has failed. It also indicates number of audit files pending for this site collection at the Indexer and the number of files that failed to be indexed. Audit files are present in the `$data/indexer/err` folder on the Indexer. If you do have failed files on the indexer, you can try moving them back to `$data/inbox` folder on the Indexer.
  If the new audit information again fails to be indexed, contact Symantec support.
- Click the Export icon at the bottom of the page to save the data on the **Monitored Site Collections** panel to a .csv file.

You can also edit the properties of the site collection, start an unscheduled scan of the site collection, delete the site collection, view the event log or scan history of the site collection, or download logs for troubleshooting purposes.

To edit a site collection

1. On the Web application details page, click **Monitored Site Collections**.
2. Select the site collection that you want to edit, and from the **Select Action** drop-down, select **Edit**.
3. On the Edit site collection screen, make the necessary configuration changes.
4. Click **Save**.

To delete a site collection

1. On the Web application details page, click **Monitored Site Collections**.
2. Select the site collection that you want to delete, and from the **Select Action** drop-down, select **Delete**.
3. Click **OK** on the confirmation message.

To view the scan history of a site collection

1 On the Web application details page, click **Monitored Site Collections**.

2 Select the site collection for which you want to view the scan history, and from the **Select Action** drop-down, select **Scan History**.

The scan history for the site collection appears. You can view the details in a tabular format or in a Timeline view. The tabular view displays the following details of a scan:

- The start and end time of the scan.
- The time taken for the scan.
- The type of scan, whether full or incremental.
- The Collector node associated with the site collection.
- The details of the scan. For example, if a scan has failed, the **Details** column indicates the exit code for the error message.
- The user account that initiated the scan.

The Timeline view displays an hourly and daily overview of the scans run on the site collection, including information about the status of the scan, whether failed, successful, partially successful or aborted.

To view events pertaining to a site collection

1 In the Console, click **Settings** > **SharePoint Web Applications**.

2 On the Web application details screen, click **Monitored Site Collections**.

3 Click the **Select Action** drop-down for the corresponding site collection, and select **Event Log**.

The event log for that site collection appears.

4 To download the logs for the site collection, click the **Select Action** drop-down for the corresponding site collection, and select **Download Logs**.

Data Insight downloads a compressed folder containing the logs for this site collection from all relevant Data Insight servers.

See "Downloading Data Insight logs" on page 158.

To scan site collections in a batch

1 On the Monitored site collections tab, click the **Scan** button.

2 On the Scan Site Collections pop-up, select one of the following:

- **Scan all** - To scan all the configured site collections immediately.

- **Scan with last scan status** - To scan site collections based on the following criteria:
  - Site collections on which the last scan has failed completely.
  - Site collections that have never been scanned before.
  - Site collections on which the last scan has failed on certain paths.

3 Select one or more of the following conditions:

- Scan site collections that have not been scanned for *n* number of days. Enter the interval in the field.
- Include site collections matching specified patterns. You can enter multiple patterns separated by a comma. You can also specify one or more wildcards in the pattern. For example vol*, *$.
- Exclude site collections matching specified patterns. You can enter multiple patterns separated by a comma. You can also specify one or more wildcards in the pattern. For example vol*, *$.
- Select **Add to the top of scan queue** to add the scans to the top of the scan queue.

4 Select **Start scanning**.

Note: You can use a command line utility, `scancli.exe`, to further customize the scan, view the scan jobs running on a specified node, or display the scan status for specified site collections. For details, See scancli.exe on page 172.

See "Adding site collections" on page 110.

See "Add/Edit site collection options" on page 110.

Removing a configured Web application

If you want to remove an existing SharePoint Web application from Data Insight you must complete the steps in the correct order.

To remove a Web application from Data Insight

1. Delete the configured Web applications from the Data Insight console.

   Deleting the Web application enables you to disable auditing for the monitored SharePoint Web applications

   See "Deleting Web applications" on page 109.

2. On the SharePoint server, disable auditing of the Web applications that are deleted from Data Insight.
3. Uninstall the Data InsightWeb service from the SharePoint server.

Chapter 6

Configuring containers

This chapter includes the following topics:

About containers

A container can consist of similar entities such as filers, shares, Web applications, site collections, or DFS paths. Grouping the entities under a single container allows you to easily define the scope of a role assigned to a user.

For example, User1 is assigned the Product Administrator role. You can further define the scope of the role by selecting a container that contains only the filers that you want User1 to access.

Managing containers

You can add containers to Data Insight, view details of the configured containers and delete one or more containers on the Containers listing page.

To manage containers

1. In the Console, click **Settings** > **Containers** to display the Containers details page.
2. The list of configured containers appears.

Adding containers

You must add containers to Data Insight that group the filers, Web applications, shares, site collections or DFS paths, as required.

To add a new container

1 In the Console, click **Settings** > **Container**.

2 On the Containers page, click **Add new container**.

3 On the Add new container screen, enter the container properties, and click **Add new container**.

4 Enter

Add new container/Edit container options

Use this dialog box to add a container to Symantec Data Insight or to edit the configuration of an existing container.

Table 6-1 Add new container/ Edit container options

Field	Description
Container Name	Enter a logical name for the container.
Container Type	From the drop-down, select **Filer/Web Application**, **Shares/Site Collection**, or **DFS paths**. Based on the selection, Data Insight filters the list of entities. Do the following to select the resources: 1 Select the **Physical Hierarchy** radio button to view the configured file servers or SharePoint Web applications. Or select the **DFS Hierarchy** radio button to view the configured DFS paths in a domain. 2 The selected data set is listed in the **Selected resources** pane.

Chapter 7

Configuring Data Insight product users

This chapter includes the following topics:

About Data Insight users and roles

Before a user can log in to Symantec Data Insight, you must add an account for that user. The user can then use that account to log in to the Console. The user account can be any account that is valid on the Management Server system. This includes local system accounts as well as users belonging to the domain which the Management Server is a part of.

When you create an user account, a role (set of access privileges) is associated with the account. Roles specify access privileges to the Symantec Data Insight system. For example, a role might let users view access and permissions data, but prevent them from adding or deleting filers. Data Insight role-based access control governs access to product features and functionality. Roles consist of the user privileges that determine what a user can see and do in the Management Console.

The Data Insight administrator (a user mapped to the predefined Server Administrator role) assigns roles to users. Users can be mapped to one role only. Data Insight ships with predefined roles that you can assign to user accounts.

Table 7-1 summarizes the various Data Insight roles.

Table 7-1 Symantec Data Insight roles

Role name	Description
Server Administrator	Allows the user to perform all actions in the product GUI that includes setting up all infrastructure (including filers, users, and others) and view all the access and permissions data.
Product Administrator	Allows the users to manage filer settings and optionally to view all the access and permissions data for the given filers. Product administrator role, configured for a select set of filers/Web applications, is not allowed to add new filers or delete configured filers.
User	Allows the users to view all the product access and permissions data. Users in this role do not have access to any settings tasks.
Storage User	Allows the users to view storage-related data in the **Workspace** tab, but does not allow them to view permissions data or audit logs. Users in this role do not have access to the **Settings** tab.

Reviewing current users and privileges

You can review the current Data Insight users and the roles assigned to them on the Product Users listing page. On this page you can also review the filers and Web applications that these users are allowed to monitor.

To review current users and privileges

1. In the Console, double-click **Settings** > **Product Users** to display the Product Users listing page.
2. Click the Export icon at the bottom of the page to save the data to a `.csv` file.

Adding user

This section describes how to add users to Symantec Data Insight.

To add new a Data Insight user

1. In the Console, click **Settings** > **Data Insight Users** to display the Product Users listing page.
2. Click **Add New Data Insight User**.
3. On the Configure new product user page, enter the user properties, click **Add New Data Insight User**.

   See "Configure new Data Insight user /Edit Data Insight user options " on page 121.

Configure new Data Insight user /Edit Data Insight user options

Use this dialog box to add a new user to Data Insight, or edit the properties of an existing user.

Table 7-2 Add/Edit Data Insight user options

Field	Description
Username	Enter the username for the user.
Domain name	Enter the name of the domain to which the user belongs.
Role	From the drop-down, select the role you want to assign the user. See Table 7-1 on page 120.
Select view options	From the drop-down, select **Allowed** or **Denied**. Setting this option to **Allowed** enables the user to view the screens on the **Workspace** and **Reports** tabs. This option is only available if the user is assigned the Product Administrator role.
Allow access to Workspace data	Select the check box to enable the user to view the screens on the **Workspace** and the **Reports** tabs This option is only available if the user is assigned the Product Administrator role.

Table 7-2 Add/Edit Data Insight user options *(continued)*

Field	Description
Resources/Containers to grant access to	Select one of the following: ■ **All filers/Web applications (Includes the ones added in the future)** ■ **Selected Filers/Web applications** ■ **Selected Shares/Site Collections** ■ **Selected DFS paths** ■ **Containers** If you select **Selected filers/Web Applications** , **Selected Shares/Site Collections**, **Selected DFS paths**, or **Containers** , the system displays a list of the appropriate configured entity. Use the arrows to select the entities you want the user to monitor. **Note:** A user, assigned the Server Administrator role, has the scope set to **All Filers/Web Applications**, by default. The scope by DFS paths is applicable only for User and Storage User roles.

Editing users

After you add a user to Data Insight, you can edit the user properties. For example, you might need to edit any of the following:

- The role assigned to the user
- The view option for the user
- The filers and/or Web applications that the user is allowed to monitor

To edit the properties of a user

1. In the Console, double-click **Settings** > **Data Insight Users** to display the Product Users listing page.
2. Click the **Edit** button for the corresponding user.
3. On the Edit Data Insight user page, make changes. as necessary, and click **Save**.

   See "Configure new Data Insight user /Edit Data Insight user options " on page 121.

Deleting users

You can delete Data Insight users.

To delete an user

1. In the Console, double-click **Settings** > **Data Insight Users** to display the Product Users listing page.
2. Select the user, and click **Delete**.
3. Click **OK** on the confirmation message.

Configuring authorization for Symantec Data Loss Prevention users

Symantec Data Loss Preventions makes Web Services calls into Data Insight to obtain ownership information for sensitive files and folders. However, you must first provision a Data Insight account for Symantec Data Loss Prevention in Data Insight.

You can provision a Active Directory service account OR a local system account and assign it the Server Administrator privilege. Symantec Data Loss Prevention can use this account to access Data Insight data.

Chapter 8

Configuring Data Insight product servers

This chapter includes the following topics:

About Data Insight product servers

A Data Insight product server is any server which has Symantec Data Insight software installed. This includes the Management Server, zero or more Collectors, zero or more Indexers, and zero or more Windows File Server agents. You can view information about configured product servers, check the status of running scans, and change advanced settings from the **Settings** tab of the Management Console.

Managing Data Insight product servers

On the servers listing page you can view detailed information about all configured servers, get a list of currently running scans, edit the server's configuration, and delete the server.

To view configured product servers

1. In the Console, click **Settings** > **Data Insight Servers** to display list of configured product servers.
2. Use the provided dynamic search filter to search for configured servers based on the name of the server.
3. Review the following information about the servers:
   - The name of the server.
   - The role of the server.
   - The status of the server — whether the server is online or offline.
   - The version of the Data Insight software installed on the server.
4. Click the Export icon at the bottom of the page to save the data on the screen to a `.csv` file.

To view server events

1. In the Console, click **Settings** > **Data Insight Servers**.
2. Click the **Select Action** drop-down for the corresponding server in the servers listing table, and select **Event Log**.

   The event log for that server appears.

To delete a server

1. In the Console, click **Settings** > **Data Insight Servers**.
2. Click the **Select Action** drop-down for the corresponding server in the servers listing table, and select **Delete**.

See "Configuring advanced settings" on page 128.

Viewing Data Insight server details

You can view the server details on the **Overview** tab and enable services to register the Data Insight server with the NetApp or EMC Celerra filer.

To review server details

- Click the server that you want to review, or click the **Select Action** drop-down and select **View**.

  The **Overview** tab of the server details screen appears. It displays the following information:

  - Server Address

This is the address of the server configured when the server was added. Remote product servers use this address when communicating with this server. At this time, Data Insight does not support changing the address of the server.

- Server Status
  Indicates whether the server is online or offline. Each worker node periodically heartbeats with the Management Server. A server is marked OFFLINE, when it fails to send a heartbeat for two minutes.
- Server Roles
  This indicates the roles that the server plays. Possible server role values are Management Server, Indexer, Collector, and Windows File Server Agent.
- Filer Name
  If the server is a Windows File Server Agent, the name of the associated file server is displayed here.
- Data Insight version
  Indicates the version of Data Insight installed on this server.
- Operating System
  Indicates the operating system installed on this server.
- CPUs
  Indicates the number of CPUs available on this server.
- Memory
  Indicates the RAM installed on this server in MBs.

Depending on the type of the filers managed by this Collector, you can enable the Fpolicy or EMC Celerra service on the server from this page.

To enable or reconfigure the Fpolicy or EMC Celerra service

1. On the Overview tab, click **Enable** to enable the Fpolicy or EMC Celerra service on the server.
2. From the Select saved credential drop-down, select the credential that the service uses to run.

   Note: In case of a NetApp file server, if the file server belongs to a different untrusted domain, select the Local System account to run the DataInsightFpolicy service.

3. If configuring the Fpolicy service, enter the name of the policy.

4 If configuring the EMC Celerra service, select the location of the server on which the EMC CAVA service is installed.

5 Click **Configure**.

See "Credentials required for configuring EMC Celerra filers" on page 19.

See "Configuring advanced settings" on page 128.

Viewing in-progress scans

You can view a list of currently running scans on the **In-progress scans** tab.

To review the in-progress scans

1 On the product server details page, click **In progress** scans..

2 Review the following information from the in-progress scans table:

- **Object Name** - Name of the object being scanned.
- **Object Type** - The type of object being scanned. This can be a share, site collection or Active Directory.
- **Task Name** - Indicates the type of the scan.
- **Task State** -Whether the task is RUNNING or IN QUEUE.
  If none of the tasks are in RUNNING state, it usually means a scan pause window is in effect. You can configure the pause interval for the server from Advanced setting page for the server. To override the pause schedule for a share or site collection and start the scan immediately, from the Action drop-down, select **Override pause schedule**.
  See "Configuring advanced settings" on page 128.
- **Start Time** - Time the scan started if it's in RUNNING state.
- **Time elapsed** - Indicates how long the scan has been running.
- **Task Statistics**- Indicates the statistics of the in-progress scans. It shows the number of folders scanned and the files or folders scanned per minute.

3 Click **Cancel** to cancel a particular scan or click **Cancel All** to cancel all scans.

Configuring advanced settings

You can edit various settings of the server from **Settings** > **Data Insight Settings** > **Advanced Settings** page.

The advanced settings are divided into the following categories:

- Filesystem settings - Configures how the server scans file systems. Data Insight performs two types of scans on the configured shares:
  - Full scans
    During a full scan, Data Insight scans the complete share. These scans can run for several hours, if the share is very big. Typically, a full scan should be run once for a newly added share. After that, you can perform full scans less frequently based on your preference. Ordinarily, you need to run a full scan only to scan those paths which might have been modified while event monitoring was not running for any reason. In all other cases, the incremental scan is sufficient to keep information about the file system meta data up-to-date.
  - Incremental scans
    During an incremental scan, Data Insight re-scans only those paths of a share that have been modified since the last full scan. It does so by monitoring incoming access events to see which paths had a CREATE or WRITE event on it since the last scan.
- Indexer settings - Configures how the indexes are updated with new information. This setting is applicable only for Indexers.
- Audit events preprocessor settings - Configures how often raw access events coming from file servers must be processed before they are sent to the Indexer.
- High Availability settings - Configures how this server is monitored.
  Each server periodically monitors its CPU, memory, state of essential services, number of files in its inbox, outbox, and err folders. Events are published if these numbers cross the configured thresholds. Also, each worker node periodically heartbeats with the Management Server. The Management Server publishes events if it does not receive an heartbeat from a node in the configured interval.
- Report settings - Configures memory settings for reports. This setting is applicable only for the Management Server.
- Windows File Server Agent settings - Configures the behavior of the Windows File Server filter driver. This setting is applicable only for the Windows File Server Agent server.
- SharePoint settings - Configures the duration for which old audit logs are kept on the SharePoint server. Audit logs that are fetched from the SharePoint server are automatically deleted from the Data Insight database. You can disable this feature at the Web application level.
- Veritas File System Server (VxFS) settings - Configures how Data Insight scans the VxFS filer.

- NFS settings - Configures how Data Insight scans NFS shares.
- Troubleshooting settings - Configures settings that aid troubleshooting.

To configure advanced settings

1. In the Console, click **Settings** > **Data Insight Servers**.
2. Click the server, for which you want to configure the advanced settings.
3. Click **Advanced settings**.
4. Click **Edit**.

Note: Some settings require you to restart the DataInsightComm service on the server before the changes take effect. These settings are indicated by an asterix against their name. If you want to reset the setting back to the default value, you can leave the value blank.

Each of the categories for the advanced settings are described in detail below.

Table 8-1 Filesystem settings - Full scan settings

Setting	Description
Total scanner threads	The Collector can perform multiple full scans in parallel. This setting configures how many full scans can run in parallel. The default value is 2 threads. Configure more threads if you want scans to finish faster.
Scan multiple shares of a filer in parallel	This setting indicates if the scanner can perform a full scan on multiple shares of the same filer in parallel. The setting disabled by default.
Maximum shares per filer to scan in parallel	If multiple shares of a filer can be scanned in parallel, this setting puts a limit on the total number of shares of a filer that you can scan in parallel.
Default scan schedule	Specifies how often full scans need to be performed. You can override this setting at a filer or share level. By default, full scans are scheduled to repeat last Friday of each month.

Table 8-1 Filesystem settings - Full scan settings *(continued)*

Setting	Description
Pause scanner for specific times	You can configure the hours of the day when scanning should not be allowed. This ensures that Data Insight does not scan during peak loads on the filer. The setting is enabled by default. Scans resume from the point they were at before they were paused.
Pause scanner schedule	Configures when scanning should not be allowed to run. By default, scanning is paused from 7a.m to 7p.m, Monday to Friday. You can specify multiple scanner pause schedules for different days of the week. For example, you can choose to pause scanning from 7:00 a.m to 7:00 p.m. on weekdays and from 7:00 a.m. to 9:00 a.m. on Saturdays and Sundays. To add a scanning schedule: 1 Click **Add**. 2 On the Pausing schedule pop-up, select the time period and the days on which you want to pause scanning. 3 Click **Save**. You can also edit or delete existing scanning schedules.

Table 8-2 Filesystem settings - Incremental scan settings

Setting	Description
Total scanner threads	The Collector can perform multiple incremental scans in parallel. This setting configures how many incremental scans can run in parallel. The default value is 2 threads. Configure more threads if you want scans to finish faster.

Table 8-2 Filesystem settings - Incremental scan settings *(continued)*

Setting	Description
Scan multiple shares of a filer in parallel	The setting indicates whether the scanner can perform an incremental scan on multiple shares of the same filer in parallel. The setting is enabled by default.
Maximum shares per filer to scan in parallel	If multiple shares of a filer can be scanned in parallel, this setting puts a limit on total number of shares of a filer that can be scanned in parallel. The default value is 2.
Default scan schedule	Specifies how often incremental scans must be performed. By default, incremental scans are scheduled to run at 7 p.m each night. Schedule incremental scans more or less frequently based on how up-to-date you need information in Data Insight to be.
Pause scanner for specific times	You can configure hours of the day when scanning should not be allowed. This ensures that Data Insight does not scan during peak loads on the filer. This setting is enabled by default. Scans resume from the point they were at before they were paused.
Pause scanner schedule	Configures when scanning should not be allowed to run. By default, scanning is paused from 7 a.m to 7 p.m, Monday to Friday.

Table 8-3 Filesystem settings - Common settings

Setting	Description
Scanner snapshot interval	Scanning a big share can take several hours. The scanner periodically saves information to a disk so that information is visible sooner without waiting for the entire scan to finish. You can configure how often information is saved to the disk by the scanner. By default, the scanner creates a snapshot of new information every 600 seconds (10 minutes). The minimum value you can set for this parameter is 600.

Table 8-4 Indexer settings

Setting	Description
Total indexer threads	The indexer processes incoming scan and access event information for various shares and updates the per-share database. This setting configures how many databases can be updated in parallel. By default 2 threads are configured. Specify a larger value for bigger setups where indexer is not able to keep up with incoming rate of information, which is indicated by observing too many files in the inbox of the Indexer worker node. However, you must ensure that the Indexer has adequate CPU and memory when configuring a higher number of indexer threads. You need approximately 1 GB of RAM per indexer thread.
Limit maximum events processed in memory	By default, the indexer processes all new incoming events in memory before saving to the disk. If your are falling short of RAM on your Indexer, you can limit the maximum number of events that the indexer will process in memory before it saves them to the disk. Note that specifying a small number will make the indexing very slow.

Table 8-4 Indexer settings *(continued)*

Setting	Description
Reconfirm deleted paths when reconciling full scan information	After indexing full scan data, Data Insight computes paths that no longer seem to be present on the file system. Set this option to true to have Data Insight re-confirm if those paths are indeed deleted using an incremental scan before removing them from the index.
Indexer schedule	Specify how often an index should be updated with new information. By default, all new data is consumed once every 4 hours. Indexer gets better throughput if more information is given to it when indexing. However, if you configure a very high value, new information will not be visible in the Console for a much longer period.
Indexer integrity checking schedule	Data Insight checks the integrity of its databases once a week. If any errors are found in the database, an event is published. You can configure a different schedule if required.

Table 8-5 Audit events preprocessor settings

Setting	Description
Audit events preprocessor schedule	Incoming raw audit events from file servers must be pre-processed before sending them to the Indexer. At this stage, collector.exe applies various heuristics to the raw events and also removes transient events. By default, raw events are processed every 2 hours.
Batch size (MB)	The maximum size of the raw audit event files that a single Collector thread can process. The default batch size is 2 GB.

Table 8-5 Audit events preprocessor settings *(continued)*

Setting	Description
Total Collector threads	The Collector can run multiple pre-processors in parallel. This setting configures how many instances can run in parallel.

Table 8-6 High availability settings

Setting	Description
Ping timeout (in minutes)	If a worker node does not heartbeat in the specified interval, Management server will publish an event to that effect. This setting is only applicable for the Management Server.
CPU threshold	If CPU used on this server is consistently over the specified percentage, an event is published. (Default value: 90%)
Memory threshold	If Memory used on this server is consistently over the specified percentage, an event is published. (Default value: 80%)
Disk usage threshold	If disk usage, either for the system drive or data drive, is over the specified threshold, an event is published. (Default value: 80%)
Error files threshold	If Data Insight is not able to process an incoming file for some reason, that file is moved to an `err` folder. Data Insight publishes an event if number of files in the `err` folder crosses the specified threshold. (Default value: 50)
Data files threshold	If Data Insight is not able to process incoming data fast enough, the number of files in the transient folders, `inbox` and `outbox`, goes on building up. Data Insight publishes an event if number of files crosses the configured threshold. (Default value: 5000)

Table 8-7 Reports settings

Setting	Description
Maximum memory when generating report output	Specifies the maximum memory that can be used for generating a report output. By default, it is 1024 MB on a 32bit machine and 2048 MB on a 64 bit machine.

Table 8-8 Windows File Server agent settings

Setting	Description
Maximum kernel ring buffer size	The Windows File Server filter driver puts events in an in-memory buffer before the DataInsightWinnas service, consumes them. By default, it uses a 10MB buffer. You can use a bigger buffer. Data Insight publishes an event that indicates events are being dropped due to a high incoming rate. Note that this buffer is in kernel and is limited on a 32 bit OS.
Ignore accesses made by Local System account	The Windows File Server filter driver ignores accesses made by processes running with Local System account. This ensures that Data Insight can ignore most events originating from the operating system processes or other services like anti-virus and backup. Clear this check box to enable monitoring accesses made by LOCAL SYSTEM account. This is not recommended on a production file server.

Table 8-9 Veritas File System server settings

Setting	Description
Flush events on VxFS filer before audit	Set this option to true, if you want to force VxFS to flush its events to disk each time Data Insight requests for information. This option is useful in Proof-of-Concept (POC) setups and enables you to see events faster.
Maximum number of audit threads	This option determines how many filers to fetch audit information from in parallel.

Table 8-10 NFS settings

Setting	Description
Set default credentials for NFS scanner	Set this option to true if you want to allow Data Insight to use the specified User and Group ID to log in to scan NFS shares.
User ID	The ID of the NFS user that the Data Insight uses to scan the filer. You can set the value to 0 to allow root access from the Data Insight scan hosts.
Group ID	The ID of the group that the Data Insight uses to scan the filer. You can set the value to 0 to allow root access from the Data Insight scan hosts.

Table 8-11 SharePoint settings

Setting	Description
Automatically delete audit events from SharePoint server that are older than (days)	When configuring a SharePoint Web application, you can choose to let Data Insight delete audit logs that have already been fetched from SharePoint. By default, Data Insight deletes audit logs older than two days. You can change the interval using this setting.
Schedule to fetch audit events from SharePoint server	Data Insight fetches new audit events from SharePoint periodically. By default, it does so every 2 hours. You can configure a different schedule.
Total scanner threads	The Collector can perform multiple full scans in parallel. This setting configures how many full scans can run in parallel. The default value is 2 parallel threads. Configure more threads if you want scans to finish faster.
Scan multiple site collections of a web application in parallel	This setting indicates if the scanner can perform a scan on multiple site collections of the same web application in parallel. The setting disabled by default.

Table 8-11 SharePoint settings *(continued)*

Setting	Description
Maximum site collections per web application to scan in parallel	If multiple site collections of a web application can be scanned in parallel, this setting puts a limit on the total number of site collections of a web application that you can scan in parallel
Default scan schedule	Specifies how often scans need to be performed. You can override this setting at a web application or site collection level. By default, scans are scheduled to repeat 11:00 p.m. each night.
Pause scanner for specific times	You can configure the hours of the day when scanning should not be allowed. This ensures that Data Insight does not scan during peak loads on the SharePoint servers. The setting is enabled by default. Scans resume from the point they were at before they were paused.
Pause scanner schedule	Configures when scanning should not be allowed to run. By default, scanning is paused from 7:00 a.m to 7:00 p.m, Monday to Friday.

Table 8-12 Troubleshooting settings

Setting	Setting
Preserve intermediate files	As new data comes into a Data Insight system, it moves between various modules. In this process the original files are deleted and a new processed file is generated for the next stage of processing. To aid troubleshooting, select this check box to retain the intermediate data files. These files get stored in `attic` folder in the data directory.
Preserve raw audit event files	Events processed by the Audit Pre-processor stage are deleted once consumed. If this setting is enabled, raw audit event files will be preserved in the `attic` folder in the data directory.

See "Managing Data Insight product servers" on page 125.

Chapter 9

Configuring policies

This chapter includes the following topics:

About Data Insight policies

A policy is a set of conditions that you configure to monitor access events on files and folders stored on various repositories. Symantec Data Insight policies help you detect the sources of threat, access patterns on sensitive data, and anomalous user behavior. Data Insight receives information about sensitive files from Symantec Data Loss Protection (DLP).

Policies must include at least one condition that is configured to detect abnormal access patterns or user behavior. Data Insight generates an alert whenever it detects any violation of a condition in a configured policy.

Policies can be configured with three severities, namely, high, medium, and low. You can assign the severity level to a policy based on your organizational needs. For example, the Information Security team can define policies to monitor accesses on the share `\Finance`. For this purpose, they can configure a policy with a medium severity to monitor accesses on folders containing Finance policies and guidelines files. Whereas, they can configure a policy with a high severity to monitor accesses on files containing payroll information. When an alert is generated for a policy violation, the severity of the policy is associated with the alert.

Data Insight comes packaged with the following out-of-the-box policies that you can configure according to your needs:

- Data Activity Trigger policy

Use this policy to define the maximum cumulative count of the meta operations on the selected paths. For example, if you have defined the maximum accesses per day as 500 on the share `\\netapp1\finshare`, and the total access count by the active set of users exceeds 500, then Data Insight generates an alert.

- User Activity Deviation policy
  Use this policy to define the threshold of deviation from the baseline activity. The baseline activity on a file or folder is the average number of accesses that are considered normal based on past access counts. If the activity, by the selected users, on the selected data exceeds the specified threshold of the baseline (for example, three standard deviations above the baseline activity), or the maximum accesses allowed per day, Data Insight generates an alert. You can configure how many standard deviations a user is allowed to deviate from the defined baseline.
- Data Activity User Whitelist-based policy
  Use this policy to define a whitelist of users based on the Active Directory custom attributes, who can access selected shares or paths. Also, you can create such a policy with multiple conditions with multiple values for the same custom attributes .
  If users, other than those defined in the whitelist, access selected data, Data Insight generates an alert.

Managing policies

You can view, edit and delete configured policies, and add new policies to Data Insight from the **Policies** tab.

To manage policies

1. In the Console, click the **Policies** tab.

   The left pane displays the default policy groups.
2. Click a policy group.

   The policy listing page displays the configured policies for that policy group.
3. To edit an existing policy, from the Actions drop-down, click **Edit**.
4. To delete a policy, select the corresponding checkbox and click **Delete**.

To add a new policy

1. In the Console, click the **Policies** tab.

   The left pane displays the default policy groups.
2. Click the policy group that you want to base your policy on.

3 On the policy listing page, click **Add new policy**. Or in the tree-view panel, right-click the policy type, and select **Add**.

4 On the Add new policy page, select the options to create the policy.

Click the collapsed panels on the page to expand them.

5 Click **Save**.

By default, policies are evaluated at 12:00 a.m. every night. You can schedule policies to be evaluated more frequently for proof-of-concept (POC) setups. Note that a schedule that is too aggressive can put excessive load on the Indexer.

You can set a custom schedule to evaluate policies from the **Settings** tab. The schedule must be specified in the cron format.

To set a custom schedule for policies

1 Click **Settings** > **Data Insight Servers**.

2 Click the entry for the Management Server.

3 On the page for the Management Server node, click **Advanced Settings**.

4 Click **Edit**.

5 Scroll to bottom of the page and expand the **Set custom properties** section. Specify property name to be job.PolicyJob.cron and property value to be the new schedule. Schedule needs to be specified in cron format

6 In the Property name field, enter job.PolicyJob.cron.

7 In the Property value fields, enter the values as follows:

To evaluate values every N minutes, specify value as 0 0/N * * * ? *.	For example, to evaluate policies every 10 minutes, specify value as 0 0/10 * * * ? *.
To evaluate policies every N hours, specify value as 0 0 0/N * * ? *.	For example, to evaluate policies every 2 hours, specify value as 0 0 0/2 * * ? *.

See "Create Data Activity Trigger policy options" on page 143.

See "Create User Activity Deviation policy options" on page 145.

See "Create Data Activity User Whitelist-based policy options" on page 147.

Create Data Activity Trigger policy options

Use this dialog to create a new Data Activity Trigger policy. Click the collapsed panels on the page to expand them and enter the relevant information in each panel of the dialog. Options selected in the respective panels are displayed in the Summary panel on the right of the page.

Table 9-1 Create Data Activity Trigger policy options

Option	Description
Policy Information	Enter information in the following fields: ■ **Name** - The name of the policy. ■ **Description** - A short description of the policy. ■ **Policy Type** - Data Activity Trigger is selected by default. ■ **Severity** - The severity of the policy. From the drop-down, select High, Medium, or Low. The severity level associated with the policy helps you decide the possible course of action when an event that matches the policy occurs. Select the **Enable Policy** check box to enforce the policy. The policy is not evaluated if the check box is not selected.
Configure Policy	Select the following conditions to configure the policy: ■ **Select Activity** - Select the type of accesses to be monitored on the selected data set. Select the **Meta Access** radio button to monitor only the high-level access events that Data Insight maps from the detailed file system and SharePoint access events. Select the **Detailed Access** radio button to monitor specific file system and SharePoint access events. ■ **Additional Condition** - From the **Minimum accesses per day for alerts** drop down select the minimum number of accesses on the selected data set on that day that are required before an alert is triggered.

Table 9-1 Create Data Activity Trigger policy options *(continued)*

Option	Description
Data Selection	Do the following to select the resources: 1 Select the **Physical Hierarchy** radio button to view the configured file servers or SharePoint Web applications. Or select the **DFS Hierarchy** radio button to view the configured DFS paths in a domain. 2 Click a path to select it. 3 To limit the scope of the files to be monitored, select **Select all files in folder** or **Select only sensitive files**. If you select the **Select all files in folder** option, accesses on all files in the folder are evaluated for determining any violation of the policy. If you select the **Select only sensitive files** option, accesses on only the sensitive files in the folder are evaluated for determining any violation of the policy. **Note:** The list of sensitive files is obtained from Symantec Data Loss Prevention (if configured). 4 The selected data set is listed in the **Selected resources** pane.
Notification	Enter one or more specific email addresses for people to whom you want to send alerts.

Create User Activity Deviation policy options

Use this dialog to create a new User Activity Deviation policy. Click the collapsed panels on the page to expand them and enter the relevant information in each panel of the dialog. Options selected in the respective panels are displayed in the Summary panel on the right of the page.

Table 9-2 Create User Activity Deviation policy options

Option	Description
Policy Information	Enter the following information: ■ **Name** - The name of the policy. ■ **Description** - A short description of the policy. ■ **Type** - User Activity Deviation is selected by default. ■ **Severity** - The severity of the policy. The severity level associated with the policy helps you decide the possible course of action when an event that matches the policy occurs. Select the **Enable Policy** check box to enforce the policy. The policy is not evaluated if the check box is not selected.
Configure Policy	Do the following: 1 From the drop-down, select the time range for the baseline activity. Baseline activity is then computed as the average access in that time range. From the **Threshold Configuration** drop-down, select the threshold of normal activity. The threshold is the acceptable number of standard deviations that a user is allowed to deviate. Accesses above the defined threshold trigger an alert. 2 **Additional Condition** - From the drop-down, select the minimum accesses per day per user. Alerts are raised only if the total accesses exceed the minimum value specified. This prevents Data Insight from raising too many alerts when baselines are very low.

Table 9-2 Create User Activity Deviation policy options *(continued)*

Option	Description
Data Selection	Do the following to select the resources: 1 Select the **Physical Hierarchy** radio button to view the configured file servers or SharePoint Web applications. Or select the **DFS Hierarchy** radio button to view the configured DFS paths in a domain. 2 Click a path to select it. The selected data set is listed in the Selected resources pane.
User Selection	Do the following: 1 Select the **Users** or **Group** radio button to view configured users or groups respectively. The list of users and groups is sorted alphabetically. Click the star icon to display all the configured users or groups. You can use the Domain filter search bar to filter users or groups according to domains. You can also filter the users according to their Active Directory custom attributes. 2 Click a user or group to select it.
Notification	Enter one or more specific email addresses for people to whom you want to send alerts.

Create Data Activity User Whitelist-based policy options

Use this dialog to create a new Data Activity User Whitelist-based policy. Click the collapsed panels on the page to expand them and enter the relevant information in each panel of the dialog. Options selected in the respective panels are displayed in the Summary panel on the right of the page.

Table 9-3 Create Data Activity User Whitelist-based policy options

Option	Description
Policy Information	Enter the following information: ■ **Name** - The name of the policy. ■ **Description** - A short description of the policy. ■ **Type** - Data Activity User Whitelist-based is selected by default. ■ **Severity** - The severity of the policy. The severity level associated with the policy helps you decide the possible course of action when an event that matches the policy occurs. Select the **Enable Policy** check box to enforce the policy. The policy is not evaluated if the check box is not selected.
Configure Policy	**Select Activity** - Select the type of accesses to be monitored on the selected data set. Select the **Meta Access** radio button to monitor only the high-level access events that Data Insight maps from the detailed file system and SharePoint access events. Select the **Detailed Access** radio button to monitor specific file system and SharePoint access events.

Table 9-3 Create Data Activity User Whitelist-based policy options *(continued)*

Option	Description
Data Selection	Do the following to select the resources: 1 Select the **Physical Hierarchy** radio button to view the configured file servers or SharePoint Web applications. Or select the **DFS Hierarchy** radio button to view the configured DFS paths in a domain. 2 2 Click a path to select it. 3 To limit the scope of the files to be monitored, select **Select all files in folder** or **Select only sensitive files** If you select the **Select all files in folder** option, accesses on all files in the folder are evaluated for determining any violation of the policy. If you select the **Select only sensitive files** option, accesses on only the sensitive files in the folder are evaluated for determining any violation of the policy. The selected data set is listed in the Selected resources pane. **Note:** Data Insight obtains information about sensitive files from Symantec Data Loss Prevention (DLP). See "Configuring Symantec Data Loss Prevention settings" on page 40.
Whitelist Conditions	Do the following: 1 Click **Add Condition**. 2 Select the criteria to build the condition. Use the expression builder to select users based on their Active Directory custom attributes. You can add multiple conditions to a Data Activity User Whitelist-based policy.

Table 9-3 Create Data Activity User Whitelist-based policy options *(continued)*

Option	Description
Notifications	Enter one or more specific email addresses for people to whom you want to send alerts.

See "Configuring Symantec Data Loss Prevention settings" on page 40.

Managing alerts

An alert is a signal generated by a policy when the condition specified in the policy is violated.

You can view alerts on the **Alerts** tab on the Management Console.

To manage alerts

1. In the Console, click the **Alerts** tab.

   You can view all the alerts that were generated by Data Insight on the listing page.

2. In the Alerts Summary, click the drop-down arrow on any column header and select Columns. Then, select the parameters you want to show or hide. You can sort by:

   - The name of the policy.
   - The severity of the alert.
   - The type of policy associated with the alert - Data Activity Trigger, User Activity Deviation, or Data Activity User Whitelist-based.
   - The name of the user account that violated the policy.
   - The date on which the alert was generated.
   - The resolution, if any, taken in response to the alert.

3. To send alerts in email, select the alerts and click **Send Email**.
4. Enter the email addresses and click **Send**.
5. To enter the resolution for an alert, select the alert, click in the Resolution column for the alert and type in the resolution.

   To update the resolution for multiple alerts, select the alerts and click **Update Resolution** at the top of the summary table.

To delete alerts

- To delete an alert, select an alert and click **Delete**.

  To delete alerts by severity, click Delete and select the severity. This deletes all alerts that match the selected severity.

  To delete alerts older than a certain date, click Delete and select the date at the top of the table.

  Note: You can configure automatic deletion of alerts older than the specified interval on the Data Retention screen. However, you cannot restore the alerts once they are deleted.

  See "Configuring data retention settings" on page 39.

Chapter 10

Events and Notifications

This chapter includes the following topics:

Configuring email notifications

Data Insight provides email notifications for important events happening in the product. For example, CIFS scan failure or an Active Directory scan failure. Notifications are sent out every 15 minutes, if new events are available. Email notifications are not enabled by default.

Note: Before you enable email notifications, you must enable configure the SMTP settings.

See "Configuring SMTP server settings " on page 29.

To configure email notifications

1. In the Management Console, click **Settings** > **Global Settings** > **Event Notifications**
2. On the Event Notifications page, select **Enable event notifications** checkbox.
3. In the Email recipients field, enter a comma separated list of email addresses to be notified.

4 Select the severity of events for which the email notifications must be sent.

5 Click **Save**.

Enabling Windows event logging

Symantec Data Insight can publish events to the Windows Event log. Events are published on the same machine where they originate. Event logging is enabled by default.

To configure Windows event logging

1 In the Management Console, click **Settings** > **Global Settings** > **Event Notifications**.

2 Select the **Enable Windows logging** checkbox.

3 Select the severity of events for which you want to enable Windows logging.

4 Click **Save**.

About high availability notifications

Data Insight raises events for various conditions that might result in a loss of availability of a Data Insight system or component. Events are raised for the following conditions:

- Changes in the state of various essential services
- Saturation of the data volume
- Worker node misses heartbeat with the Management Server
- Accumulation of excessive files on the worker node
- Loss of connection between the filers and the Collector
- Excessive usage of CPU, memory, or disk space for extended period

Viewing events

You can monitor Symantec Data Insight recent system events on the **Events** page. The report displays entries for all system events. These events include the following information about an event:

- Time
- Severity
- Event summary

- Symantec Data Insight server where the event originated
- The user if any performing the action
- The object for which the event originated

To view system events

1 Do one of the following:

- To view all system events, in the Management Console, click **Settings** > **Diagnostics** > **Events**.
- To view events pertaining to a configured filer, in the Management Console, click **Settings** > **Filers** > **Select Action** > **Event Log**.
- To view events pertaining to a configured Web Application, in the Management Console, click **Settings** > **SharePoint Web Applications** > **Select Action** > **Event Log**.
- To view events pertaining to configured Data Insight servers, in the Management Console, click **Settings** > **Data Insight Servers** > **Select Action** > **Event Log**.
- To view events pertaining to a share, navigate to the filer details page, select the **Monitored Shares** tab, select the share and click **Actions** > **Event Log**.
- To view events pertaining to a site collection, navigate to the Web application details page, select the **Monitored Site Collections** tab, select the site collection and click **Actions** > **Event Log**.
- To view events pertaining to the success or failure of full and incremental scans for a selected time period, use the Dashboard on the **Settings** tab of the console. On the bar-graph, click the bar pertaining to the day, week, month, or year for which you want to view events.
  See "Viewing summary reports" on page 26.

A list of recent system events appears.

2 You can choose to filter the events further using one or all of the following criteria:

- By time
- By any text appearing in the event summary
- By severity
- By the product server on which the event originates

  Enter the filter criteria in the relevant fields and click **Go**.

3 Click the Export icon at the bottom of the page to save the data to a `.csv` file.

Viewing scan errors

You can view a list of all the paths on which a scan has failed. In the tree view panel, the folder icon displays a red cross mark for the paths on which a scan has failed. The scan errors displayed are from the latest scan completed on the share.

You must have View privileges on the share to view the scan errors on that share.

To view scan errors

1. In the Management Console, click **Settings** > **Diagnostics** > **Scan Errors**.
2. To view the list for scan errors on a particular path, click in the **Select Share** field, and from the **Select Resource** pop-up, select the path.

   On the **Select Resource** pop-up, you can also search for specific shares or site collections, and filter the results.
3. Select a share or a URL to view the failed scans on that path.
4. Click the Export icon at the bottom of the page to save the data to a `.csv` file.

The red cross mark icon appears for a path as soon as a scan fails. However, the Scan Errors view displays a list of scan errors only after the index for the share is updated. Thus, sometimes, there can be a lag of up to four hours between the indication appearing on tree-view panel and the corresponding scan errors being displayed on the Scan Errors view.

In some cases, the scan may exit with code 32768, which means that some paths could not be scanned. Thus, some paths are not displayed in the scan errors listing page, if these paths do not exist in the Data Insight index for the share.

Viewing scan history of a share or site collection

You can view the entire scan history of share.

To view the scan history of a share/site collection

1. In the Management Console, click **Settings** > **Filers/SharePoint Web applications**
2. On the filers listing page, click a configured filer/Web application, or click **Select Action** > **View**.
3. Click the **Monitored Shares/Monitored Site Collections** tab.
4. Click **Select Action** > **Scan History** to view the scan history of a configured share.

Appendix A

Troubleshooting

This appendix includes the following topics:

About general troubleshooting procedures

This section provides an overview of the general troubleshooting procedures that you can use to help discover and troubleshoot common problems.

You can use the **Events** page on the Data Insight Management Console to get a quick overview of the node on which the error has occurred.

To troubleshoot a problem, it helps to consider the following:

- Check for prior occurrence.
  Check existing troubleshooting information to see if the problem has occurred before and if there is a workaround available to troubleshoot the same. A good source for this type of information is the *Symantec Data Insight Release Notes*. The Release Notes contain a list of known issues for Data Insight and a list of possible workaround.
- Consider recent alterations.
  If a system is having problems immediately after some kind of maintenance, , software upgrade, or other change, the problem might be linked to those changes.

Location of Data Insight logs

Symantec Data Insight log files are located in the Data Insight installation directory, `<INSTALLDIR>\log`. Typically the installation directory is located at `C:\Program Files\Symantec\Data Insight\log`.

Table A-1 describes the logs that are relevant for troubleshooting.

Table A-1 Data Insight logs

webserver0.0.log	This file contains the log messages from the Web service process.
commd0.0.log	This file contains the log messages from the scheduler service.
adcli.log	This file contains the log messages from the Active Directory scanner process, `adcli.exe`.

Downloading Data Insight logs

To troubleshoot errors, you can download the Data Insight logs relevant to a file server, share, SharePoint Web application, or SharePoint site collection from the **Settings** tab of the Management Console.

To download Data Insight logs

1. On the relevant listing page, click the **Select Action** drop-down, and select **Download Logs** for the data repository you want to troubleshoot.
2. On the **Download Logs** pop-up, select the check box for the information that you want to include in the logs.

   You can select one or all of the following information:

   - **Config database** - Select this option to include the configuration database in the download. Secret information, such as passwords are purged from the copied database.
   - **Indexer database** - Select this option to include the index for the problematic shares or site collections in the download.
   - **Error files** - Select this option to includes scan or audit files that have not been indexed in the download.
   - **User database** - Select this option to include the cached Active Directory information in the download.

Note: Contact Symantec Support to help you determine which of these options you should select when troubleshooting an issue.

Appendix B

Command File Reference

This appendix includes the following topics:

fg.exe

`fg.exe` – A script that modifies the file group configuration for Data Insight.

SYNOPSIS

```
fg -C -N <name of file group>

fg -D -N <name of file group>

fg -L -d

fg -L -N <name of file group> -d

fg -R -N <name of file group> -t <name of extension>
```

DESCRIPTION

fg is a script used to modify the configuration for sorting files into file groups. By default, Data Insight sorts files into 18 file groups based on the file extensions.

OPTIONS

`-i <username>`
(Required) The fully-qualified username of the user running the command, for example, user@domian. This user should have Server Administrator privileges in Data Insight.

`-A` Adds an extension to an existing file group.

`-C` Creates a new file group.

`-D` Deletes an existing file group.

`-L` Lists existing file groups.

`-R` Removes an extension from an existing file group.

`-N` Name of the file group to be created or deleted.

`-d` Shows file group details when listing existing file groups.

`-t <name of extension>`
The file extension to add or delete from the file group (For example, doc).

`-h` Prints the usage message.

EXAMPLES

EXAMPLE 1: The following command creates a new file group.

```
fg -i <username> -C -N <name of file group>
```

EXAMPLE 2: The following example adds a new extension to an existing file group.

```
fg -i <username> -A -N <name of file group>  -t <name of extension>
```

EXAMPLE 3: The following example deletes an extension from an existing file group.

```
fg -i <username> -R -N <name of file group>  -t <name of extension>
```

EXAMPLE 4: The following command deletes a file group.

```
fg -i <username> -D -N <name of file group>
```

EXAMPLE 5: The following command displays a detailed listing of all configured file groups.

```
fg -i <username> -L -d
```

EXAMPLE 6: The following command displays a detailed listing of a particular file group.

```
fg -i <username> -L -N <name of file group> -d
```

NOTES

By default, Data Insight sorts files into 18 file groups. If you add a new file group to Data Insight, you must run the following commands for each share's index to update the mappings for the newly-added file groups:

```
idxwriter.exe –i <path to Index directory> --dirhash
```

```
idxwriter.exe –i <path to Index directory> --filehash
```

indexcli.exe

`indexcli.exe` – a utility that manages the index segments available on an Indexer worker node.

SYNOPSIS

```
indexcli.exe
             --display|--archive|--purge|--restore|--rearchive|--list-jobs
             |--stop-jobs [OPTIONS]

indexcli.exe -A <name of the index segments to be archived>

indexcli.exe -c

indexcli.exe -D <name of the index segments to be purged>

indexcli.exe -d

indexcli.exe -h

indexcli.exe -j

indexcli.exe -r

indexcli.exe -t

indexcli.exe -u
```

ARCHIVE OPTIONS

```
indexcli.exe -A -a ¦ -f <FILERS> ¦ -m
<SHARES> ¦ -S <SITECOLLS> ¦ -w <WEBAPPS> ¦ -I
 <MONTHS>
```

`-a` Archives all index segments older than the specified interval.

`-f <name of filer(s)>`
Archives all index segments for the specified list of filers.

`-I <interval in months>`
Archives segments older than the specified interval. The segments which have been restored earlier, are not archived.

`-m <name of share(s)>`
Archives all index segments for the specified list of shares.

`-S,--sitecoll <SITECOLLS>`

Archives segments for specified list of Microsoft SharePoint site collections.

`-w, --webapp <WEBAPPS><`

Archives segments for specified list of Microsoft SharePoint Web applications.

PURGE OPTIONS

```
indexcli.exe -D -a ¦ -f <FILERS> ¦
-m <SHARES> ¦ -S <SITECOLLS> ¦ -w <WEBAPPS> ¦
-I <MONTHS>
```

`-a` Purges all index segments older than the specified interval.

`-f <name of filer(s).`

Purges all index segments for the specified list of filers.

`-I ,interval in months.`

Purges segments older than the specified interval. The segments which have been explicitly restored earlier, for which the lease is still valid, are not purged.

`-m <name of share(s)>`

Purges all index segments for the specified list of shares.

`-S,--sitecoll <SITECOLLS>`

Purges segments for specified list of Microsoft SharePoint site collections.

`-w, --webapp <WEBAPPS><`

Purges segments for specified list of Microsoft SharePoint Web applications.

DISPLAY OPTIONS

```
indexcli.exe -d -a ¦ -f <FILERS> ¦
-m <SHARES> ¦ -S <SITECOLLS> ¦ -w <WEBAPPS> ¦
-s <STATES>
```

`-a` Displays information for all shares.

`-f <name of filer(s)>`

Displays information for the specified list of filers.

`-m <name of share(s)>`

Displays information for the specified list of shares.

`-s <name of state>`

Displays index segments for the given state only. Multiple stars can be comma separated. Possible states are, ARCHIVING, RE-ARCHIVING, ARCHIVED, RESTORING, RESTORED, RESTORE, FAILED, or DELETED.

`-S,--sitecoll <SITECOLLS>`

Displays information for a specified list of Microsoft SharePoint site collections.

`-w, --webapp <WEBAPPS><`

Displays information for a specified list of Microsoft SharePoint Web applications.

RESTORE OPTIONS

```
indexcli.exe -r -a ¦ -f <FILERS> ¦
-m <SHARES> ¦ -S <SITECOLLS> ¦ -w <WEBAPPS> -C -F <FROM> ¦ >
¦ -R <RANGE>
[-L <MONTHS> ¦ -l <MONTHS> ¦ -y]
```

`-a` Restores the index segments for all shares.

`-C` If the continue-on-error option is not specified, the restore command fails if the segment files required to restore data for the specified parameters are not available.

`-f <name of filer(s)>`

Restores all index segments for the specified list of filers.

`-F <month from which the segments need to be restored>`

Specify the month in the format, YYYY/MM. For example, `indexcli.exe -r -F 2010/01` restores segments from January 2010 till date.

`-L <interval in number of months>`

Resets lease on segments restored earlier using `-l` option. Specify the new lease interval in months. This will replace previous lease interval. Setting the value to 0 will make the lease permanent.

`-l <interval in number of months>`

Restores segments for a temporary lease in months. After the lease expires, restored segments will be automatically re-archived. If this option is not specified, segments remain restored till you re-archive them with the `-u`, --rearchive, option.

`-m <name of share(s)>`

Restores all index segments for the specified list of shares.

`-S,--sitecoll <SITECOLLS>`

Restores segments for a a specified list of Microsoft SharePoint site collections.

`-w, --webapp <WEBAPPS><`

Restores segments for a specified list of Microsoft SharePoint Web applications.

`-R <range in months>`

Restore all index segments for the specified month range. Specify the month in the format, YYYY/MM-YYYY/MM. For example, `indexcli.exe -r -R 2010/01-2010-03` restores segments from January 2010 to March 2010.

`-y` Instead of restoring segments, this option displays list of files that must be available before restoring the specified segments.

RE-ARCHIVE OPTIONS

```
indexcli.exe -u -a ¦ -f <FILERS> ¦
-m <SHARES>  ¦ -S <SITECOLLS> ¦ -w <WEBAPPS>
-F <FROM> ¦ -R <RANGE>
```

`-a` Re-archives all previously restored index segments.

`-f <name of filer(s)>`

Re-archives previously restored index segments for the specified list of filers.

`-F <month FROM which the segments need to be restored>`

Specify the month in the format, YYYY/MM. For example, `indexcli.exe -u -F 2010/01` restores segments from January 2010 till date.

`-m <name of share(s)>`

Re-archives previously restored index segments for specified list of shares.

`-S,--sitecoll <SITECOLLS>`

Re-archives previously restored segments for a specified list of Microsoft SharePoint site collections.

`-w, --webapp <WEBAPPS><`

Re-archives previously restored segments for a specified list of Microsoft SharePoint Web applications.

`-R <range in months>`

Restore all index segments for the specified month range. Specify the month in the format, YYYY/MM-YYYY/MM. For example, `indexcli.exe -u -R 2010/01-2010-03` restores segments from January 2010 to March 2010.

EXAMPLES

EXAMPLE 1: The following command archives index segments for specified list of filers.

```
indexcli.exe -A -f \\filer1,\\filer2,ID1,ID2
```

EXAMPLE 2: The following command archives index segments for specified list of shares.

```
indexcli.exe -A -m \\filer1\share1,\\filer2\shares2,ID3,ID4
```

EXAMPLE 3: The following command purges index segments for specified list of filers.

```
indexcli.exe -D -f \\filer1,\\filer2,ID1,ID2
```

EXAMPLE 4: The following command purges segments for specified list of shares.

```
indexcli.exe -D -m \\filer1\share1,\\filer2\shares2,ID3,ID4
```

EXAMPLE 5: The following command restores index segments for specified list of filers.

```
indexcli.exe -r -f <\\filer1,\\filer2,ID1,ID2>
```

EXAMPLE 6: The following command restores index segments for specified list of shares.

```
indexcli.exe -r -m \\filer1\share1,\\filer2\shares2,ID3,ID4
```

EXAMPLE 7: The following command re-archives previously restored index segments for specified list of filers.

```
indexcli.exe -u -f \\filer1,\\filer2,ID1,ID2
```

EXAMPLE 8: The following command re-archives previously restored index segments for specified list of shares.

```
indexcli.exe -u -m \\filer1\share1,\\filer2\shares2,ID3,ID4
```

EXAMPLE 9: The following command archives segments for specified list of Microsoft SharePoint site collections.

```
indexcli.exe -S,--sitecoll<http://sp_webapp:8000/sc1,ID2,ID3...>
```

EXAMPLE 10: The following command archives segments for specified list of Microsoft SharePoint Web applications.

```
indexcli.exe - w,--webapp<http://sp_webapp:8000,ID2,ID3,...>
```

EXAMPLE 11: The following command purges segments for specified list of Microsoft SharePoint site collections.

```
indexcli.exe -S,--sitecoll<http://sp_webapp:8000/sc1,ID2,ID3...>
```

EXAMPLE 12: The following command purges segments for specified list of Microsoft SharePoint Web applications.

```
indexcli.exe - w,--webapp<http://sp_webapp:8000,ID2,ID3,...>
```

EXAMPLE 13: The following command displays information for specified list of Microsoft SharePoint site collections.

```
indexcli.exe -S,--sitecoll<http://sp_webapp:8000/sc1,ID2,ID3...>
```

EXAMPLE 14: The following command displays information for specified list of Microsoft SharePoint Web applications.

```
indexcli.exe - w,--webapp<http://sp_webapp:8000,ID2,ID3,...>
```

EXAMPLE 15: The following command restores segments for specified list of Microsoft SharePoint site collections.

```
indexcli.exe -S,--sitecoll<http://sp_webapp:8000/sc1,ID2,ID3...>
```

EXAMPLE 16: The following command restores segments for specified list of Microsoft SharePoint Web applications.

```
indexcli.exe - w,--webapp<http://sp_webapp:8000,ID2,ID3,...>
```

EXAMPLE 17: The following command re-archives previously RESTORED segments for specified list of Microsoft SharePoint site collections.

```
indexcli.exe -S,--sitecoll<http://sp_webapp:8000/sc1,ID2,ID3...>
```

EXAMPLE 18: The following command re-archives previously RESTORED segments for specified list of Microsoft SharePoint Web applications.

```
indexcli.exe - w,--webapp<http://sp_webapp:8000,ID2,ID3,...>
```

reportcli.exe

`reportcli.exe` – a utility to execute and list configured reports, check the status of the reports, and cancel report runs.

SYNOPSIS

```
reportcli.exe --list-jobs¦——list-reports¦--list-outputs
--execute¦--cancel¦--help [OPTIONS]

reportcli.exe -c

reportcli.exe -e

reportcli.exe -h

reportcli.exe -j

reportcli.exe -l

reportcli.exe -o
```

OPTIONS

`-j` Lists the report jobs that are currently running.

`-l` Lists all configured reports.

`-o -m <TOP_N> -r <Report Name>`

Lists all report outputs. The following attributes apply:

`-m --max <TOP_N>`	Limits output to specified number of records, and lists the latest output first. If the number of records is not specified, prints status for the last run.
`-r - -report <Report Name>`	Prints status of jobs for the specified report. You can either specify the report ID or the report name.

`report.exe -e [-d <OUTPUT_DIR> -r <REPORT NAME> -w <MAX_WAIT>`

Executes report. The following attributes apply:

`-d --output <OUTPUT_DIR>`	The generated report output, including the SQLite database is copied to the specified directory. If you specify this option, you do not have to pass the –-w option.
`-r --report<REPORT NAME>`	Executes the specified report. You can either specify the report ID or the report name.
`--w --wait <MAX_WAIT>`	Returns the report output only after the report execution is complete or the specified wait time in minutes is exceeded. Specify –1 to wait forever.

`report.exe -c -i <JOB_ID>`

Cancels execution of the specified report job.

scancli.exe

`scancli.exe` – scancli.exe - a utility that scans shares and site collections.

SYNOPSIS

```
scancli.exe --start¦ --stop¦ --list-jobs¦ --help [OPTIONS]
```

`-s --start`

Scans specified shares or site collections.

`-c --stop`

Cancels scans for specified shares or site collections.

`-l --list-jobs`

Lists currently running jobs.

`-d --display`

Displays scan status for specified shares or site collections. To view real time scan queue information, use the `-l --list-jobs`option.

`-h --help`

Displays help.

SCAN OPTIONS

```
scancli.exe -s -a ¦ -f <FILERS> ¦ -m <SHARES> ¦ -S <SITECOLLS> ¦w <WEBAPPS>
[-D] [-e <EXCLUDE] [-F ¦ -N ¦ -p] [-I <INCLUDE>] [-i <DAYS>] [-t]
```

`-a - - all`

Scans all shares and site collections.

`-D - -disabled`

By default, disabled devices or those for which scanning has been disabled are not included in the scan. Specify this option to include shares or site collections of disabled devices.

`-e - -exclude <EXCLUDE>`

Exclude shares or site collections matching specified patterns. Separate multiple patterns with a comma. You can specify one or more wildcards in the pattern, for example, vol*,*$.

`-f - -filer <FILERS>`

Scans shares of the specified filers. For example, `-f - -filer >\\filer1, filer2, ID1,..>`.

`-F - -failed`

Select shares or site collections whose last scan failed completely. This does not include those that have never been scanned before or those which succeeded partially (*).

`-I - -Include <INCLUDE>`

Include shares or site collections matching the specified patterns. Separate multiple patterns with a comma. You can specify one or more wildcards in the pattern. For example, `-I - -Include >vol*,*$ >`

`-i - -interval <DAYS>`

Select shares or site collections that have not been scanned for specified number of days. This includes shares which have never been scanned before (*).

`-m - -share <SHARES>`

Scans specified list of shares. For example, `-m - -share >\\filer1\share1, share2, ID3...>`.

`-n - -never`

Select shares or site collections that have never been scanned before (*).

`-p - -partial`

Select shares or site collections whose last scan succeeded partially, that is, those shares or site collections for which the scan completed but with failure to fetch information for some paths (*).

`-S - -sitecoll <SITECOLLS>`

Scans the specified list of Microsoft SharePoint site collections.

`- t - -top`

Adds shares or site collections to top of the scan queue.

`-w - -webapp <WEBAPPS>`

Scans site collections for specified list of Microsoft SharePoint Web applications.

Note: (*) indicates that the option can only be used on the Management Server.

STOP SCAN OPTIONS

```
scancli.exe -l -a ¦ -f <FILERS> ¦ -m <SHARES> ¦ -S <SITECOLLS> ¦w <WEBAPPS>
[-D] [-e <EXCLUDE] [-I <INCLUDE>]
```

`-a - - all`

Stops scans for all shares and site collections.

`-e - -exclude <EXCLUDE>`

Exclude shares or site collections matching specified patterns. Separate multiple patterns with a comma. You can specify one or more wildcards in the pattern, for example, vol*,*$.

`-f - -filer <FILERS>`

Stops scans for shares of the specified filers.

`-I - -Include <INCLUDE>`

Include shares or site collections matching the specified patterns. Separate multiple patterns with a comma. You can specify one or more wildcards in the pattern.

`-m - -share <SHARES>`

Stops scans for the specified list of shares.

`-S - -sitecoll <SITECOLLS>`

Stops scans for the specified list of Microsoft SharePoint site collections.

`-w - -webapp <WEBAPPS>`

Stops scans for site collections for specified list of Microsoft SharePoint Web applications.

LIST JOB OPTIONS

```
scancli.exe -l [-n --node <NODE>]
```

`-n --node <`*`Node ID or Node name`*`>`

Lists scan jobs on the specified node. Specify either node ID or node name. If not specified, localnode is assumed.

DISPLAY OPTIONS

```
scancli.exe -d -a ¦ -f <FILERS> ¦ -m <SHARES> ¦ -S <SITECOLLS> ¦w <WEBAPPS>
[-D] [-e <EXCLUDE] [-F ¦ -N ¦ -p] [-I <INCLUDE>] [-i <DAYS>]
```

`-a - - all`

Displays scan status for all shares and site collections.

`-e - -exclude <EXCLUDE>`

Exclude shares or site collections matching specified patterns. Separate multiple patterns with a comma. You can specify one or more wildcards in the pattern, for example, vol*,*$.

`-f - -filer <FILERS>`

Dispalys scan status for the shares of the specified filers.

`-F - -failed`

Displays scan status for the shares or site collections whose last scan failed completely. This does not include those that have never been scanned before or those which succeeded partially (*).

`-I - -Include <INCLUDE>`

Include shares or site collections matching the specified patterns. Separate multiple patterns with a comma. You can specify one or more wildcards in the pattern.

`-i - -interval <DAYS>`

Displays scan status for shares or site collections that have not been scanned for specified number of days. This includes shares which have never been scanned before (*).

`-m - -share <SHARES>`

Displays scan status for specified list of shares.

`-n - -never`

Displays scan status for shares or site collections that have never been scanned before (*).

`-p - -partial`

Displays scan status for shares or site collections whose last scan succeeded partially, that is, those shares or site collections for which the scan completed but with failure to fetch information for some paths (*).

`-S - -sitecoll <SITECOLLS>`

Displays scan status for the specified list of Microsoft SharePoint site collections.

`-w - -webapp <WEBAPPS>`

Displays scan status for the site collections for specified list of Microsoft SharePoint Web applications.

Note: `-w - -webapp <WEBAPPS>` option can only be used on the Management Server.

EXAMPLES

EXAMPLE 1: The following command scans all shares of a filer, netapp1.

```
scancli – –start – – filer <netapp1>
```

EXAMPLE 2: The following command scans all shares and site collections for which a full scan failed 3 or more days ago.

```
scancli – –start – –all – –failed – –ineterval <3>
```

The following command scans all site collections of a Web application that have not been scanned for the past 30 days or have never been scanned.

```
scancli – –start – –webapp https://sitecoll:8080 – –interval 30
```

Appendix C

Configuring a NetApp filer - an example

This appendix includes the following topics:

Prerequisites

Before you can configure Fpolicy on the NetApp filer, you must ensure that the following setup is available:

- A user account in Active Directory that has either Administrator or Backup Operator privileges on the filer.
- A server machine running Windows 2003 Server operating system. Symantec Data Insight is installed on this machine. For detailed installation procedure see the *Symantec Data Insight Installation Guide*.

  Note: The machine on which Data Insight is installed must be added to a Domain Controller. See "Adding a machine to a Domain Controller" on page 178.

- A NetApp filer running DATA OnTap version 7.3 or higher. CIFS license is installed on this filer.

- One or more client machines to test the product.

Adding a machine to a Domain Controller

Before you install Symantec Data Insight, ensure that the machine is added to a Domain Controller. For the purpose of this procedure, we use the domain name HALDOMAIN.LOCAL. The domain must be the same as that of the filer.

To add a machine to a Domain Controller

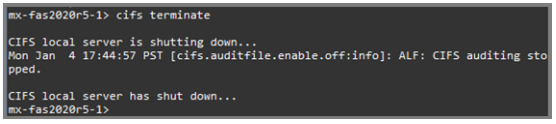
1. Right-click on **My Computer** and select **Properties**.
2. On the System Properties window, select the **Computer Name** tab.
3. Under To rename this computer or join a domain, click **Change**.
4. On the Computer Name Changes window, under Member of, select **Domain** and enter HALDOMAIN.LOCAL.
5. Click **OK**.
6. When prompted to enter the username and password, use an account that is either part of the Administrators group. For example, *ccuser*.
7. Restart the machine for the changes to take effect.

Configuring a NetApp filer

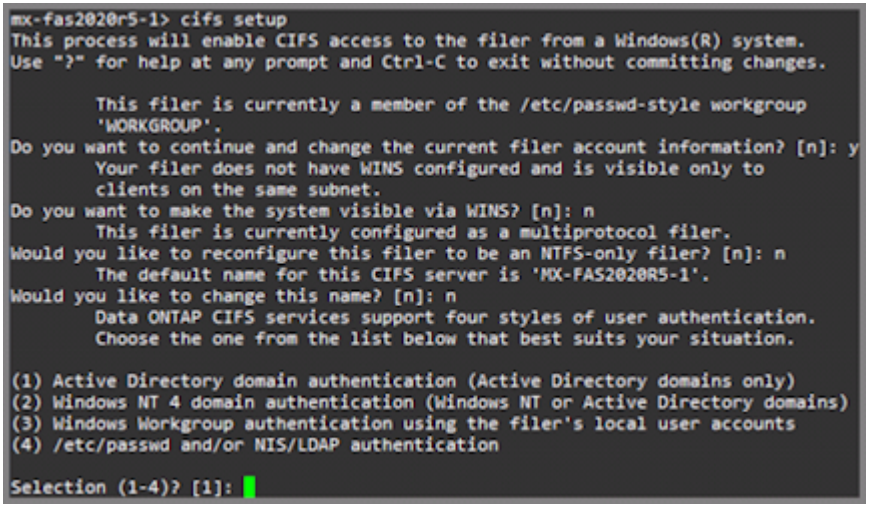
The NetApp Filer that is monitored by Symantec Data Insight must also be part of the same domain as the server machine on which Symantec Data Insight software is installed. The NetApp filer used in the example below is called *Mx-fas2020r5-1*.

To configure a NetApp filer

1. Login to the NetApp filer from a Windows command prompt as an administrator.
2. Terminate CIFS before adding the filer to a domain.



3 Run the `cifs setup` command to set up CIFS to enable Active Directory domain authentication.

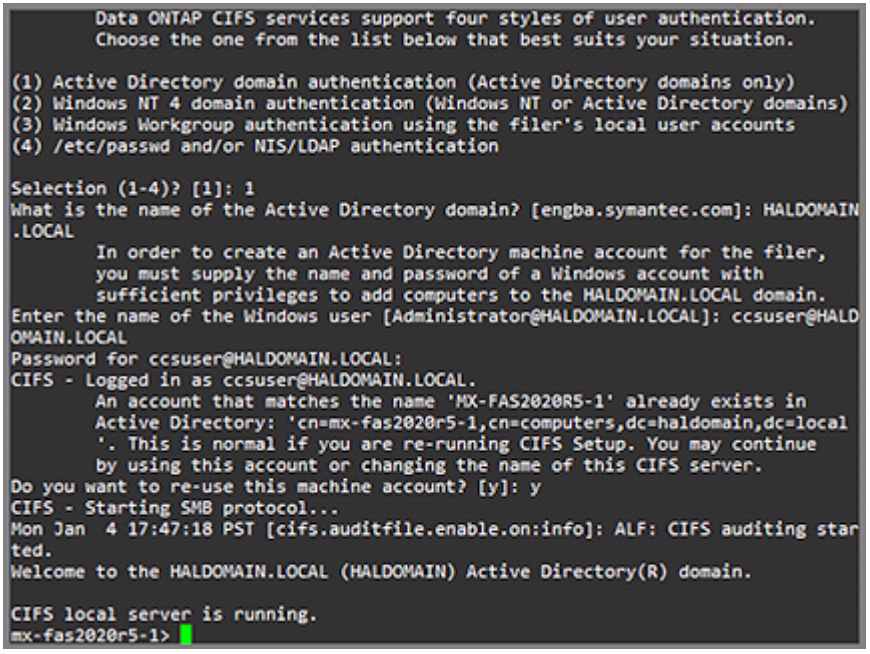


4 When prompted with **Do you want to continue and change the current filer account information? [n]**, type **y**. If the Filer was already setup, then choose the default answers for the questions that follow; else configure the filer as appropriate.

5 When prompted to choose user authentication, choose option **1**.

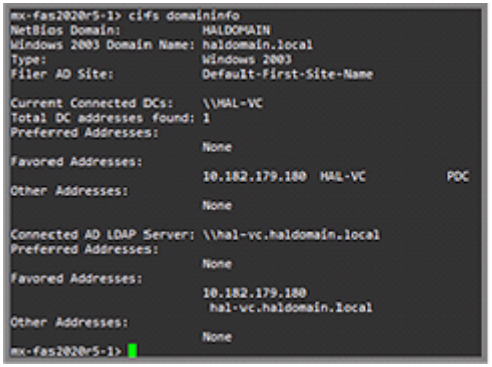
6 Enter the username as *ccuser* and domain name *HALDOMAIN.LOCAL*. This displays the message, CIFS – Starting SMB protocol...; Welcome to the HALDOMAIN.LOCAL (HALDOMAIN) Active Directory ®) domain.

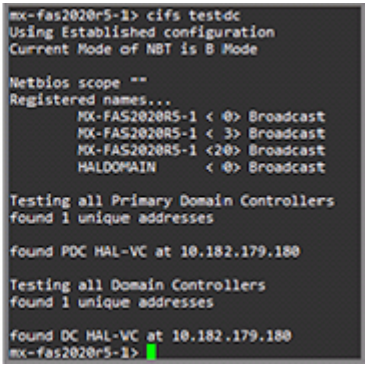
ccuser is an example user. You must choose a user who has administrator rights in the domain.



7 Confirm that CIFS is configured correctly. Run the following commands:

- `cifs domaininfo`
- `cifs testdc`





8 Add *ccuser@HALDOMAIN.LOCAL* to the Administrators group on the filer. Run the following commands:

- `Mx-fas2020r5-1> useradmin domainuser add ccuser -g Administrators`
- `Mx-fas2020r5-1> useradmin domainuser list -g Administrators`

```
mx-fas2020r5-1> useradmin domainuser add ccsuser -g Administrators
SID = S-1-5-21-1545124705-3188965610-3907368782-1329
Domain User <ccsuser> successfully added to Administrators.
mx-fas2020r5-1> useradmin domainuser list -g Administrators
List of SIDS in Administrators
S-1-5-21-1786140056-615959809-1253050676-500
S-1-5-21-1786140056-615959809-1253050676-131073
S-1-5-21-1545124705-3188965610-3907368782-1351
S-1-5-21-1545124705-3188965610-3907368782-512
S-1-5-21-1545124705-3188965610-3907368782-1329
For more information about a user, use the 'cifs lookup' and 'useradmin user lis
t' commands.
mx-fas2020r5-1>
```

9 Run the `fpolicy` command to ensure that FPolicy is enabled on the filer. Typically, if CIFS license is enabled on the filer, then FPolicy is also automatically enabled.

```
mx-fas2020r5-1> fpolicy

CIFS file policy is enabled.


File policy test (file screening) is enabled.

No file policy servers are registered with the filer.

Operations monitored:
File open,File create,File rename,File close,File delete,File read,File write
Directory rename,Directory delete,Directory create
 Above operations are monitored for NFS and CIFS

List of extensions to screen:
 ???

List of extensions not to screen:
 Extensions-not-to-screen list is empty.

Number of requests screened          :  0
Number of screen failures            :  0
Number of requests blocked locally   :  0
```

Configuring Data Insight to receive Fpolicy notifications

Before you assign a Data Insight server as a collector for a NetApp filer, you must configure the Fpolicy service on that server.

Configuring the filer in Data Insight

To add the NetApp filer

1. From the Symantec Data Insight Management Console do the following:
   - Add the NetApp filer *mx-fas2020r5-1*.
   - Add a share on *mx-fas2020r5-1* that you want Data Insight to monitor. See "Adding shares" on page 95.
2. Log into the filer.
3. un the command `fpolicy servers show matpol` to verify that the server machine on which Symantec Data Insight is installed is configured to handle FPolicy events.

Index