Symantec Data Insight Release Notes

5.0.2

April 2016

Symantec Data Insight Release Notes

Documentation version: 5.0.2.1

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

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 the company to answer your questions in a timely fashion.

Our 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 our support offerings, you can visit our website at the following URL:

www.veritas.com/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.veritas.com/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 Technical Support
  - Recent software configuration changes and network changes

Licensing and registration

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

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/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
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Contents

Chapter 1

Overview of this release

This chapter includes the following topics:

About Symantec Data Insight

Many organizations struggle with identifying data users and owners for their unstructured data. This challenge is compounded with the fact that organizations lack visibility into the types of content and data that is spread across their computing environment.

With Symantec Data Insight, users can monitor file access to automatically identify the data user of a file based on the access history. This method enables more efficient remediation and data management.

Data Insight scans the unstructured data systems and collects full access history of users across the data. It helps organizations monitor and report on access to sensitive information.

Data Insight helps the organizations solve the problem of identifying data owners and responsible parties for information in spite of incomplete or inaccurate metadata or tracking information. This helps support large-scale business owner-driven remediation processes and workflows.

Data Insight provides the following information:

- Who owns the data
- Who is responsible for remediation
- Who has seen the data
- Who has access to the data

- What data is most at-risk
- Frequency of usage of data

The ownership and the usage information from Data Insight can be used for the following purposes:

- Data owner identification
  Data Insight enables rule-based inference of data owners based on actual usage. Data owner information may not reflect the responsible party. The responsible party or data owner can be a line manager in the business unit, the head of a department, or an information security officer. Symantec Data Insight provides the information to tie the most active user of a file to a manager or responsible party for remediation steps.
- Data custodian identification
  Data Insight enables the assignment of one or more users as custodians of a data repository. Custodian tagging is typically used to determine the person responsible for remediation. The assigned custodian need not have made any accesses on the files and folders. In addition to the physical paths, you can also assign custodians on DFS paths.
- Data leak investigation
  In the event of a data leak, you may want to know who saw a particular file. On the Symantec Data Insight Management Server, you can view detailed information and an audit history of who accessed the data.
- Locate at-risk data
  Data Insight enables organizations to find which shares or folders have overly permissive access rights. Organizations can use this data to prioritize risk-reduction efforts such as the discovery of sensitive data or a review of permissions (or access control rights) to limit access to only those individuals who have a business need.
- Manage inactive data
  Data Insight enables better data governance by letting you archive inactive and orphan data using Enterprise Vault. Additionally, you can decide to manage the archived data by applying retention rules, deleting the archived data, or by putting legal hold on the archived data.
- Provide advanced analytics about activity patterns
  Data Insight enables you to analyze the activity on high-risk folders by providing in-depth analysis of usage and collaborative activity. The analysis helps you classify users based on configured attributes to better understand the activity pattern of users in your environment.
- Permission remediation

Data Insight leverages the usage analytics provided by audit logs to provide recommendations for revoking permissions of inactive or disabled users on a path. You can then analyze the business impact of applying the recommendations and configure settings to handle the permission changes.

It also enables you to search for specific permissions and revoke them where necessary as also modifying group membership directly from the **Workspace**.

- Remediation using the Self-Service Portal

  Data owners and custodians can take remediation actions using the Self-Service portal. Custodians can log in to the Self-Service Portal to do the following:

  - View Data Loss Prevention (DLP) policy violations and remediate DLP incidents using Smart Response rules.
  - Review permission on resources and make recommendations to allow or revoke user access on resources.
  - Provide confirmation about whether the custodians indeed own the data resources that are assigned to them.

- Raise alerts

  You can configure policies to raise alerts when there is anomalous activity on sensitive data.

What's new in Symantec Data Insight

This section describes the new features included in Symantec Data Insight.

Since 5.0.2

Symantec Data Insight 5.0.2 includes the following new features and enhancements.

Support for smart connect mapping to access zone

EMC Isilon publishes shares through access zone. In some configurations, access zone names are not DNS resolvable or may not be used for protocol access. SmartConnect hostname is typically used to access a share instead of access zone name.. Data Insight discovers access zone names and uses these names for scanning the shares. This enhancement allows you to configure alternate names against access zone using a CSV file as input.

The CSV file must be in the following format:

filer name, access zone name, SmartConnect name.

The CSV file must be placed in the directory `DATADIR/conf` on the Management server. The name of the CSV is isilon.csv. When DiscoverySharesJob_mrg runs

the next time, it discovers and scans shares using alternate name provided in the CSV file.

Configuring Box cloud resources through proxy server

To connect to box cloud resource over the Internet through proxy server, use the following steps:

To configure the proxy settings:

- Create a `proxy.properties` file and place it under `C:\DataInsight\data\console\cloud` on the Management server and Collector node of the configured Box account.

Note: If the folder `cloud` is not present, create it manually.

The fields in proxy properties file are:

- proxy.ip = <IP address of the proxy server>
- proxy.port = 8080
- proxy.scheme = http
- proxy.user = username
- proxy.password = password

  Note: You can provide a plain text password or an encrypted one.

- proxy.authType = NTLM

Note: In case port or authType are not applicable, leave them blank.

Support for internet shortcuts for Hitachi and Isilon NAS devices

Data Insight lets you configure a post-processing action for files archived using Enterprise Vault, such as deleting the original file and replacing it with a shortcut. The shortcut can either be a placeholder that points to the new file location inside the archive, or an internet link to the archived item.

Data Insight creates an internet shortcut to the archive location for files located on Hitachi and Isilon NAS devices. For archived paths on other supported NAS devices supported by Enterprise Vault for creation of placeholder shortcuts, Data Insight allows only placeholder shortcuts.

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

Since 5.0.1

Symantec Data Insight 5.0.1 includes the following new features and enhancements.

Support for archiving data from EMC Isilon and Hitachi NAS filer servers

Data Insight now lets you archive data stored on EMC Isilon and Hitachi NAS filer servers. You can easily archive inactive or orphan data from these file servers using Enterprise Vault. If you do not have Enterprise Vault configured for your system, you can define a custom action to archive data using any third party archiving facility. This support is also extended to Records Classification workflow. Records Classification workflow helps you classify the sensitive files that must be retained for a legally mandated period.

To know more about managing your inactive data, refer to *Symantec Data Insight User's Guide*.

Support for NetApp ONTAP 8.3 in Cluster-Mode

Symantec Data Insight now supports monitoring storage devices running NetApp ONTAP 8.3 in Cluster-Mode. To know more about managing your NetApp file servers, refer to *Symantec Data Insight Administrator's Guide*.

Since 5.0

Symantec Data Insight 5.0 includes the following new features and enhancements.

Support for Box for Enterprise

Cloud storage services, such as Box allow vast amounts of data to be stored outside the enterprise's control and audit trail. Data Insight now enables you to monitor the Box accounts to fetch metadata on the files and folders stored in these accounts. For information about configuring Data Insight to monitor your Box accounts, see the *Symantec Data Insight Administrators Guide*.

Note that every Box account corresponds to a share in the Data Insight configuration. It fetches activity and ownership information for each Box account.

Currently you can configure only a single Box account in Data Insight.

Enhanced monitoring with the Data Insight Workspace

The new Data Insight **Workspace** changes the navigation paradigm for viewing the analytics data for configured storage repositories and users.

By default, the **Workspace** tab displays a dashboard that enables interactive navigation. It lets you drill down to the deepest level of the file system hierarchy to view analytics for configured data sources and users. The information on the dashboard is summarized in tile-like panels. You can view details of the displayed data by navigating to the **List View** of the tile.

The **Workspace** lets you change the perspective of the data for a more meaningful analysis. For example, the **Security** view displays information about the number of sensitive files, open shares, and a list of Data Loss Prevention (DLP) policies that are violated on a path. Whereas, the **Activity** context provides information such as the number of access events, number of active files, and the number of users who have accesses on the path. When you change a view, Data Insight automatically re-organizes the columns that are displayed inside a tile or a list view.

Additionally, the **Workspace** tab also provides a number of filters that help you limit and modify the data that is included in a view.

With this release, the new dashboard and list views on the **Workspace** tab display the risk score for users and data sources. The risk score takes into account multiple parameters to provide a risk profile for users and data sources. It helps you monitor users with a high risk score and effectively protect your data sources by identifying the risk to critical data sources.

For more information about the new Data Insight dashboard and list view on the **Workspace** tab, see the *Symantec Data Insight User's Guide*.

New Permissions Search report

The Permissions Search report uses the permission query template as input to search for permissions to specific trustees (users, groups, or unresolved SIDs) that match or violate the rules defined in the template. The Permissions Search report lets you search for individual Access Control Entries (ACEs) or Access Control Lists (ACLs). You can use the output of a Permissions Search report to remediate permissions in your organization.

The Permissions Query Template is a container for multiple frequently-used rules that you can use as input to create a permission search report. You can apply the template to your data set to do the following:

- Review access to trustees on shares and folders.
- Ensure that your organization adheres to security policies and permission best practices.

- Identify all the compliance violations for permission hygiene.
- Remediate access to global groups such as Everyone

You can create different templates to classify the rules in different categories such as one template for all compliance rules, or one template for rules to evaluate violations of best practices.

Data Insight provides some predefined rules.

Following are examples of predefined rules:

- Trustee is Everyone – Searches for all the paths, under the data sources selected in report input, that have permissions assigned to Everyone.
- Trustee is Disabled – Looks for all paths where a disabled user account has been granted permissions.

In addition to the predefined rules, you can create custom rules containing complex conditions using the permission query template creation popup. One or more rules can be used in a single template.

If there are multiple rules, Data Insight uses the match-type criteria that you select to evaluate the rules.

For more information about creating a permission query template and about the Permission Search report, see the *Symantec Data Insight User's Guide*.

Ability to make permission changes from the Workspace tab

Data Insight enables you to orchestrate the following permission changes directly from the user-centric views of the **Workspace** tab. You can do the following:

- Remove a user from a group of which the user is a direct member.
- Remove a direct member group from a group.
- Revoke the permissions of a trustee who has explicit permissions on a path. If the trustee inherits permissions on a path, then the option to revoke the trustee's permission is not available.

Note that only the user with the Server Administrator role can take permission remediation action from the **Workspace** tab.

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

Permission change events reporting in Audit Logs

With this release, Data Insight captures the Permission Change events on paths. You can view the details of permission changes to a folder on the **Audit Logs** tab. The details of the Permission Change event provide information about the following:

- If a trustee (user or group) is allowed or denied permission on a path.
- If a trustee's permissions are removed on a path.
- If a trustee is given additional permission or denied certain permission on a path. For example, if a user 'X' has *Read* and *Write* permissions on a folder. If the user is also subsequently allowed *Modify* permission on the folder, Data Insight records an *Permission Change* event.

Currently, Data Insight fetches only the file system permission changes for CIFS paths only. It does not fetch Permission Change events for NFS or SharePoint paths. Permission changes at the share level are not reported.

Availability of real-time alerts

With this release, Data Insight enables you to create policies that trigger real-time alerts when a selected set of users perform any access events on the paths that violate configured DLP policies.

Data Insight sends the alert notifications to a configured set of recipients. The policy violations are also published in the Windows Applications and Services logs as DataInsightAlerts events.

For more information, see the *Symantec Data Insight Administrator's Guide*.

Support for non-administrator domain user for NetApp Cluster-Mode devices

With this release, you can use credentials of a domain user account which is not part of the Administrators group on the NetApp filer to discover shares and to enable FPolicy on the NetApp cluster.

SSL support for configuring Cluster-Mode devices in Data Insight

You can now enable secure communication between Data Insight and Cluster-Mode NetApp devices through an SSL connection by using self-signed or CA-signed digital SSL certificate.

For more information on generating the SSL certificate and preparing the NetApp cluster for SSL authentication, see the *Symantec Data Insight Administrator's Guide*.

Usability and supportability enhancements

The following usability and supportability enhancements have been implemented:

Enhancements to the System Overview dashboard

In this release, the following enhancements have been added to the **System Overview** dashboard:

- The dashboard displays alert notifications about any global settings that have not been configured.
- It provides an option to directly navigate to a specific device or directory service, or product server configuration page.
- It lets you navigate directly to the **Scanning and Event Monitoring** page to configure or edit the global scan settings.

For more information, see the *Symantec Data Insight Administrator's Guide*.

Scan Status and scan progress enhancements

The following enhancements have been made in the scanning dashboard: and to the scan status and scan progress reporting.

- Option to navigate to the global scan settings page directly from the **System Overview** and **Scan Status** dashboards.
- Alert notification on the **System Overview** dashboard if scanning is disabled for a device.
- **Scan Status(Consolidated)** column on the **Scan Status** page of the Scanning dashboard and on the **Monitored shares** or **Monitored Site Collections** list pages:
  - **Scan Status (Consolidated)** column tooltip: Clicking on the status icon launches the **Scan Status** popup
  - A new state “ATTENTION” for stale data introduced. The state is displayed as ATTENTION when the age of last successful scan is greater than 90 days.
  - New **Scan Status** option under **Select Action** that launches the Scan Status popup.
  - Status description for Scan Status (Consolidated).
  - Status description for Full and Incremental scan (Based on the exit codes of scans)
  - Recommendation about corrective action to be taken by the user in case of an unsuccessful Full and Incremental scan.
  - Information about the possible impact in case of unsuccessful scans.

- Scan History and Scan Errors tabs are moved under the new **Scan Status** popup which were earlier available under **Select Action** drop-down on **Settings** > **Scanning** > **Scan Status** page

For more information, see the *Symantec Data Insight Administrator's Guide*.

Data Loss Prevention configuration enhancements

The DLP configuration screen has been enhanced in to display the scan summary panel at the top. The panel displays the following information:

- Last scan status
- Next scan schedule
- Number of paths fetched
- Number of paths discarded
- Ability to view list of discarded paths in last scan
- Ability to run DLP sensitive files scan on demand
- Ability to override default DLP scan schedule

Bulk operations for storage devices

With this release, you can carry out the following bulk operations in Data Insight:

- Add multiple filers, shares, web Applications, or site collections by uploading a CSV file containing the list of resources to be added to the Data Insight configuration.
- Enable or disable the monitoring of shares or site collections or delete them from the Data Insight configuration in bulk from the **Settings**> **Filer** > **Monitored Shares** or **Monitored Site Collections** page.
- Start the paused scans for multiple shares or site collections at once from the **Settings**> **Scanning** > **In Progress Scans** page.

For more information, see the *Symantec Data Insight Administrator's Guide*.

Collector and Indexer Node selection based on performance statistics

You can now make an informed decision the Data Insight nodes that you can assign as the Collector and Indexer for a storage device, depending on the performance statistics for the node.

When you configure a storage device in Data Insight, you can choose the Collector or Indexer node that you want to assign to a device based on useful statistics, such as free disk space, backlog size, average CPU, and memory consumption.

Similarly, when you want to migrate the device to another Indexer node, Data Insight displays the configured Indexer nodes in the deployment and their performance statistics. The information enables you to make a more informed decision.

For more information, see the *Symantec Data Insight Administrator's Guide*.

DQL report enhancements

DQL reports now include support for the following:

- Multiple DQL queries
  You can type multiple DQL queries under the **Query** tab of the Report Configuration wizard. The resulting output database contains sets of tables that have results from the two queries. The names of the tables in the report output database are in the form table_<n>, where <n> indicates the query number for which the table is generated. For instance, membership_2 indicates that the membership table in the output database contains results from the second query in the report input.
- You can now insert single-line comments using -- or multi-line comments using /* and */ in DQL queries. To verify this, create a DQL report and under the **Query** tab, type a query. Also insert a few comments using -- or /* and */. For example, in the following query, the text after -- and the text between /* and */ will not be executed. Therefore, the output database will contain details from only the membership table.
- Link to View Empty DQL Output Database Schema
  The Query tab of the DQL report creation/editing wizard now provides a link to view the output database schema. This is useful in case you want to know the schema to be able to execute a SQL statement against the output database.
- DQL doesn't provide all functions that SQL provides. If you want to extract information from the output database, the only way possible to do so until Data Insight 4.5 was to write complex scripts. With this release, Data Insight provides a text area in DQL reports to enter SQL queries for post-processing of DQL output, as shown below.
- The following new DQL query templates have been added:
  - A query to fetch devices that are part of any container configured in Data Insight.
  - A query to fetch msu (shares) that are part of any container configured in Data Insight.

New Report Administrator role

With this release, a Report Administrator role is added to facilitate sharing of reports among report administrators and also to enable them to view and modify reports

created by other users. By default, a user with the Report Administrator role can view reports, run reports, edit reports, and if the role is so configured, take remediation actions.

A user added to Data Insight with the Report Administrator role can only view the **Workspace** and **Reports** tabs. The user has access to all filers, SharePoint web Applications, and containers.

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

Enhancements to Duplicate Files report

Files are considered as duplicates of each other if they have the same extension and logical size.

With this release, the Duplicate Files report is enhanced to show the following:

- The duplicate set - the group of all duplicate files with the same extension and size with in a share are considered to one set. For example, all duplicate files with the extension .docx and the logical size of 40.00 KB are part of one set. Note that this report lists duplicate files within a share and not across all shares on the data resource.
- The number of reclaimable files.
- The potential reclamation size for the duplicate sets.

For more information about how Data Insight calculates the number of reclaimable files and the potential size of these files, see the *Symantec Data Insight User's Guide*.

Support for SharePoint paths in Entitlement Review workflows

With this release, Data Insight supports the creation of Entitlement Review workflow for SharePoint paths.

For more information about remediation workflows, see the *Symantec Data Insight Administrator's Guide*.

Support for Linux version 7.0

With this release, Data Insight provides support for Linux version 7.0.

You can now install the Data Insight Indexer on systems running Linux version 7.0.

Chapter 2

System requirements

This chapter includes the following topics:

System requirements for Symantec Data Insight components

Table 2-1 lists the minimum system requirements for Symantec Data Insight components.

Table 2-1 Minimum system requirements for Symantec Data Insight components

Component	System requirements
Management Server	■ Windows Server 2008 or 2008 R2, 2012 or 2012 R2. The operating system must be 64 bit. ■ 8 GB RAM ■ 4 CPUs

Table 2-1 Minimum system requirements for Symantec Data Insight components *(continued)*

Component	System requirements
Indexer worker node	■ Windows Server 2008, or 2008 R2, 2012 or 2012 R2. The operating system must be 64 bit. Red Hat Enterprise Linux version 5.0 update 5 or higher, version 6.0 update 3 or higher, or version 7.0; 64 bit only. ■ 8 GB RAM ■ 4 CPUs RHEL version 5.0 update 5 or higher is only supported if you are upgrading from an earlier version of Data Insight.
Collector worker node	■ Windows Server 2008, or 2008 R2; 64 bit Windows Server 2012 or Windows Server 2012 R2. The operating system must be 64 bit. ■ 4 GB RAM ■ 2 CPUs
Self-Service Portal node	■ Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2. The operating system must be 64 bit. ■ 8 GB RAM ■ 4 CPUs
Windows File Server agent node	■ Windows Server 2008. The operating system; 64 bit Windows Server 2012 or Windows Server 2012R2. The operating system must be 64 bit. ■ 4 GB RAM ■ 2 CPUs **Note:** Windows 2003 and 32-bit on Windows 2008 is supported only for backward compatibility with Windows File Server nodes installed with Data Insight versions 4.0, 4.5. and 5.0.
SharePoint Web Service	Microsoft SharePoint 2007, SharePoint 2010, or SharePoint 2013

Note: The type and scope of deployment should be determined with the help of Symantec.

List of ports

This section lists the default ports used by various Data Insight services, and devices that Data Insight communicates with.

Table 2-2 List of default ports

Component	Default Port
Management Server	Management Console, HTTPS port 443 Communication service, HTTPS port 8383 DataInsightConfig service, port 8282 Workflow Service HTTPS, port 8686 Standard RPC ports 139 and 445
Collector worker node\ Indexer plus Collector worker node	Communication service, HTTPS port 8383 Standard RPC ports 139 and 445 DataInsightConfig service, port 8282 NetApp Cluster-Mode service, TCP port 8787 (configurable) Generic Collector service, HTTPS port 8585 (configurable)
Indexer worker node	Communication service, HTTPS port 8383 DataInsightConfig service, port 8282
File Server	For Net App filers - HTTP port 80 (optional), standard RPC ports 139 and 445, and 2049 (TCP,UDP) and 111 (TCP,UDP) for NFS For NetApp Cluster-Mode, HTTP port 80 On EMC Control Station - HTTP port 80 and HTTPS port 443 On Windows File Servers managed without an agent - Standard RPC ports 139 and 445 For Veritas File System servers - HTTPS port 5634, and 2049 (TCP,UDP) and 111 (TCP,UDP) for NFS
Windows File Server agent node	Communication Service, HTTPS port 8383 DataInsightConfig service, port 8282 Standard RPC ports 139 and 445

Table 2-2 List of default ports *(continued)*

Component	Default Port
SharePoint Web Service	SharePoint Web Service is accessed over the same port as the configured Web Applications. This port on the SharePoint Web Servers should be accessible from the Collector node.
LDAP Directory Server	Port 389 or 636 (for TLS)
NIS Server	Ports 111 (TCP,UDP), 714 (TCP), 711 (UDP)
NIS+ Server in NIS compatibility mode	Ports 111 (TCP,UDP), 714 (TCP), 711 (UDP)
Symantec Data Loss Prevention (DLP)	HTTPS port 443
Symantec Enterprise Vault Server	HTTP port 80 or as configured by Enterprise Vault Server web service.
Self-Service Portal server	Portal Service, HTTPS port 443 Workflow Service, HTTPS port 8686 DataInsightConfig, service port 8282 Communication service, HTTPS port 8383

Note: The default ports for Data Insight components are configurable at the time of installation.

Operating system requirements

Table 2-3 provides an overview of Symantec Data Insight operating system requirements:

Table 2-3 Symantec Data Insight operating system requirements

Operating system supported	Notes
Windows Server 2008	Windows Server 2008 (64-bit) Standard Edition and Enterprise Edition Windows Server 2008 R2 (64-bit) Standard Edition and Enterprise Edition

Table 2-3 Symantec Data Insight operating system requirements *(continued)*

Operating system supported	Notes
Windows Server 2012	Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit)
Red Hat Enterprise Linux	Version 5.0 update 5 or higher Version 6.0 update 3 or later Version 7 Only 64 bit packages are supported. **Note:** RHEL version 5.0 update 5 or higher is only supported if you are upgrading from an earlier version of Data Insight.
VMware	64 bit on Windows 2008 64 bit on Windows 2012 Red Hat Enterprise Linux version 6 update 3 or later Red Hat Enterprise Linux version 7 **Note:** You must ensure that VMware Tools is installed on VMware virtual machines.

Note: Windows 2003 or 32-bit on Windows 2008 is supported only for backward compatibility with Windows File Server nodes installed with Data Insight versions 4.0 and 4.5.

Web server version

Symantec Data Insight uses Apache Tomcat 7.0.53.

Supported browsers

Table 2-4 provides an overview of the browser support for Symantec Data Insight

Table 2-4 Symantec Data Insight Supported browsers

Browser	Versions
Internet Explorer	■ Version 10 and version 11.

Table 2-4 Symantec Data Insight Supported browsers *(continued)*

Browser	Versions
Mozilla Firefox	■ Version 38.0 or higher
Google Chrome	■ Version 43.0.2357.124 or higher

Note: Symantec recommends that you install the latest available version of a browser.

Supported file servers and platforms

Table 2-5 lists the Network Attached Storage (NAS) devices and SharePoint platforms that Data Insight supports.

Table 2-5 Supported file servers and platforms

Device	Version
Hitachi NAS	Hitachi NAS 12.x.
NetApp ONTAP	From version 7.3.5 to version 8.1.x ONTAP 8.0.x and ONTAP 8.1.x are supported in 7-mode only. ONTAP 8.2.x is supported in 7-mode and Cluster-Mode. ONTAP 8.3 is supported in Cluster-Mode.
EMC Celerra	Version 5.6.45 or higher, VNX
EMC Isilon	OneFS version 7.1 or higher
Windows File Server	Windows Server 2008, or 2008 R2, 32 bit and 64 bit Windows Server 2012, or 2012 R2 64 bit **Note:** 32-bit on Windows 2008 is supported only for backward compatibility with Windows File Server nodes installed with Data Insight versions 4.0 and 4.5.
Veritas File System (VxFS) server	6.0.1 or higher, configured in standalone or clustered mode using Symantec Cluster Server (VCS) **Note:** For VCS support, Clustered File System (CFS) is not supported.

Table 2-5 Supported file servers and platforms *(continued)*

Device	Version
Microsoft SharePoint	Microsoft SharePoint Server 2007 Microsoft SharePoint Server 2010 Microsoft SharePoint Server 2013
Box (Cloud-based content manangement platform)	-
Symantec Data Loss Prevention (DLP)	Versions 12.0.1, 12.5, and 14.0
Symantec Enterprise Vault	Versions 10.0.4, 11.0, and 11.0.1

Note the following:

- Symantec strongly recommends that you upgrade your NetApp filer to the latest available firmware. Symantec recommends ONTAP 7.3.5 or higher.
- For all supported versions of 7-mode NetApp filers, Data Insight supports CIFS protocol over NTFS and NFS protocol v3. NFS v4 is not supported.
  For supported versions of Cluster-Mode NetApp filers, Data Insight supports only CIFS protocol over NTFS. NFS protocol is not supported.
  Data Insight supports the following volume/qtree styles:
  - NTFS and Mixed for CIFS protocol.
  - UNIX and Mixed for NFS protocol on 7-mode Netapp filers only.
- For all supported versions of EMC Celerra/VNX and EMC Isilon, Data Insight supports only CIFS protocol over NTFS. NFS protocol is not supported. Data Insight supports the latest Common Event Enabler (CEE), version 6.3.1. Data Insight still supports the older version of CEE and VEE, but Symantec recommends that you move to the latest EMC Common Event Enabler, which you can download from the EMC website
- To use the Self-Service Portal to remediate DLP incidents, ensure that Symantec Data Loss Prevention (DLP) version 12.5 or higher is installed. Data Insight uses the DLP Smart Response Rules to remediate incidents, which are introduced in DLP version 12.5.

Chapter 3

Software limitations

This chapter includes the following topics:

Scanner limitations

The following notes cover limitations pertaining to the Scanner process of Data Insight:

- In case of Windows 2012 Severs used as Windows File Servers, the Scanner does fetch a group having permission based on a condition. For example, "all users who have *xyz* as manager have full access to the share/folder". However, the indexer discards it currently. The console does not display the group as having Dynamic ACL. The other permissions on the path are shown properly. Resilient File System (ReFS) is supported only for scanning. Auditing is not supported since the drive cannot be attached to the filter driver.
- Scanner does not support share names of more than 200 characters.
- Scanner modifies the access time of directories while traversing the filesystem.

Windows File Server support

Windows filter driver does not capture IP address from which accesses are made.

Console limitations

The following notes cover limitations pertaining to the Data Insight Management Console.

Expression builder limitation

When creating a Data Activity User Whitlist-based policy, Data Insight allows you to add multiple whitelist conditions to a policy. However, all these conditions are used in conjunction with each other to form the policy. The multiple conditions cannot be used separately.

Special characters not supported in NFS paths

The following special characters are not supported in NFS paths:

/ \ : * ? " < > |

Size on disk not displayed

The size on disk for archived folders is not displayed under on the **Workspace** > **Folders** > **Overview** tab.

Filer rename not supported

Data Insight does not allow you to rename a file server entry after it is added to the Data Insight configuration.

Data Insight scans and GUI do not display certain details and options

The following table lists known limitations where the Data Insight scan or Data Insight GUI does not capture a certain detail or configuration option.

Table 3-1 Dashboard items not supported

Context	Limitation
Creator of the folder is the Administrators group	Owner field appears empty if the ownership method is 'Creator'.

Table 3-1 Dashboard items not supported *(continued)*

Context	Limitation
For a Cloud source of type Box	A Data Insight scan does not capture the following information: ■ Created_by ■ Owned_by ■ Modified_by
For a data source where you import the sensitive file information by a CSV file	GUI does not display an option to edit the DLP scan schedule under **Settings** > **Data Loss Prevention**
Summary view of a Share	Does not display individual counts for Read, Write, and Other activities. It only displays the total activity count. For a breakdown of Read, Write, and Other counts, click **Expand Profile** > **Audit Logs** for the Share.
Summary view for a Data Source, Share, Folder, or File	Does not display the number of files that violate a DLP policy
Permissions view of SharePoint paths	Does not display the Remove Permissions option.
Dashboard Custom view	GUI does not support the option to preview and edit the component columns of the Custom view
DFS Names column in the Workspace view	Alphabetical sorting is not supported
Audit Logs tab for a SharePoint or NFS path	Permission Change criteria in the Access dropdown may display incorrect result
Audit Logs tab for a CIFS path	Permission Change criteria under Access dropdown does not display records for permission changes at Share level.
Permission search report for any users or groups	Does not display Trustee scope details
Under **Settings**> **SharePoint web application**>**Monitored site collections**	Add Bulk delete, bulk disable/enable options are not available.

Social Network Map limitation

The Social Network Map does not render in Internet Explorer 9.

Report configuration limitation in Path Permission reports

When configuring Path Permissions reports, Data Insight does not let you exclude groups for SharePoint site collection URLs.

Known limitations for NetApp Cluster-Mode support

Limitations exist in the current support for NetApp Cluster-Mode file server. Data Insight does not support the following:

- Scanning of Home directories on clustered NetApp file servers.
- Monitoring of ACL change (SECURITY) events. However, you can enable Setattr event monitoring manually.
- FPolicy communication using SSL.
- Scanning of local user on the clustered NetApp cluster.

Known limitations for Hitachi NAS support

The following limitations exist for the Data Insight support for monitoring of Hitachi NAS devices:

- Scanning of NFS support is not supported.
- Scans initiated using Local User credentials are not supported.
- Capacity report not supported.
- Throttling for event monitoring is not supported.

Real-time Sensitive Data Activity Policy does not support Box devices

Real-time Sensitive Data Activity Policy skips sensitive files from Box devices when the policy generates alerts.

Chapter 4

Known Issues

This chapter includes the following topics:

Console display issues

The following issues relate to displays in the Console.

Multi-byte characters not supported

Adding a new container or Data Insight user with multi-byte characters is not supported.

Toolbar error

In some instances, the Pagination and refresh toolbars may get disabled after browser refresh.

The workaround is to close the tab and to re-open it.

Emailing contents of a table

Emailing contents of a table might fail in certain cases. Current workaround is to save contents of the table using the Save icon and emailing the `.csv` manually.

Incorrect status of folder displayed

The **Workspace** > **Folder Activity** > **Inactive sub-folders** page may display a folder as inactive for a selected time period, even when file(s) within the directory have been deleted in the specified time range and there are no other events on

files within the directory This is because a delete event on a file is not considered as activity for the purpose of showing the activity status of the folder.

Incorrect information in Inactive Directories report

Inactive Directories report contains deleted directories even though the file or directory was deleted during the selected time period.

Unwanted access events displayed

If you rename a SharePoint site, few unwanted access events pertaining to accesses to `.aspx` and `.asmx` pages are also displayed. This stops occurring after some time.

Data Insight cannot capture the IP addresses for events on certain platforms

For Windows File Servers, VxFS filers, and SharePoint sites Data Insight does not capture the IP addresses for access events.

Report includes only physical paths

If you select the **All Resources** check box, Data Insight generates reports only on the physical paths even if you select DFS radio button.

Progress bar display error

When using the **Settings** > **Upload Manager** option to upload agent packages on selected nodes, the progress bar gets activated for all nodes in the view.

For example, there are three nodes listed, and you select one of the nodes for uploading the agent packages using the Agent Uploader utility. When you click the Upload button, the progress bar gets activated for all three nodes in the view.

Error fetching permissions data

If the **Inherited from** column on the **Folder Permissions** >**File System Access Control List** page shows **Parent Object**, you can cross-launch from the icon, but it will result in a page that shows an Error fetching data dialog.

Inconsistency between permissions view of Windows and Data Insight

On a given path, for example, /foo, if a group, for example, G1, is allowed full control and Everyone is denied full control, then the effective permissions for G1 on the

given path, shown through the Windows security permissions view, is **Allow full control**. However, the Data Insight view displays **Deny Full Control**.

The actual observed behavior is consistent with the permissions displayed on the Data Insight view . For example, if a user belonging to group G1 tries to access /foo, Windows displays an **Access Denied** error.

Error fetching data displayed

If any screen displays the pop-up, *Error fetching data*, it indicates that first-time data collection is in progress or the Data Insight config service is unavailable.

If first time data collection has already taken place and you have reasons to believe that DataInsightConfig service is unavailable, log on to the Management Server / Indexer worker node and run the command `net start DataInsightConfig` (or on Linux: /opt/DataInsight/bin/DataInsightConfig start) to restart this service. On Windows 2008 or 2012, check the folder `Program Files\DataInsight\dumps` for any crash dumps. On Windows 2003, run the command `drwtsn32.exe` to check for crash dumps. If you find one or more crash dumps, contact Veritas support.

Error in inactive users information

When you navigate to **Workspace** >**Folders** > **User Activity** > **Inactive Users**, the sub-tab displays information about active users in addition to inactive users.

This error occurs only in case of a file. For a share and folders within the share, **Inactive Users** sub-tab displays the correct data.

Change in date range not reflected when you navigate to other tabs

When you navigate to **Workspace** >**Folders Activity** > **By Sub-folders and Files**, right-click on any chart and select **Audit Logs**, the Audit Logs page displays data for the default date range. The date range selected on the **Folder Activity** tab does not get transferred to the **Audit Logs** tab.

You must select the date range again on the **Audit Logs** tab, and click **Go** to view the data.

Scan status incorrectly displayed on scanning dashboard

The scan status is displayed incorrectly when a scan is queued and later canceled or when you pause a scan and subsequently cancel it. For such canceled scans, Data Insight does not reflect the scan status and scan history correctly.

Audit Logs tab shows incorrect path for CREATE events on SharePoint 2007 server

For SharePoint 2007, CREATE event paths are displayed incorrectly in audit logs. As a result exclude rules for access events do not exclude CREATE events. Due to incorrect path a new folder structure is created in the navigation pane.

Workaround

You can disable capturing of CREATE events by disabling the event handler for SharePoint 2007 server. To disable the events:

- Run the following command to determine the site collection ID:
  'configdb –p –T sitecoll'
- Run the following command to disable the event:
  'sharepoint_utilclient.exe –m <sitecollection ID> -e 0

Newly added Enterprise Vault server are not displayed in the Filer Mapping page

When a new Enterprise Vault server is added to Data Insight, the newly added server is not displayed in the drop-down list for selecting the Enterprise Vault server on the **Filer Mapping** page. This issue is seen only if the **Filer Mapping** tab is already open.

Workaround

Close the already opened **Filer Mapping** tab, then reopen it.

Duplicate entry for the Enterprise Vault server is allowed

The same Enterprise Vault (EV) server entry is allowed to be added multiple times, when adding a EV server from the **Settings** > **Data Management** > **Add New EV Server** page.

Ensure that you do not enter a duplicate entry for a EV server.

Dashboard report fails, if filers and domains are not configured in Data Insight

If no filers and/or domains are configured in Data Insight, the execution of Dashboard data computation cycle from **Settings** > **Advanced Analytics** tab fails.

Social Network Map fails to render for the shares that have large number of active users

The Social Network Map takes a long time to render for the shares that have a large number of active users or access events within the time period configured under **Settings** > **Advanced Analytics** > **Configuration** tab. For example, the Social Network Map may take several minutes to render for shares with more than 500 users with a dense collaboration network.

The time it takes to render the map may go past the default session timeout.

Mismatch between permission entries displayed in Windows interface and Data Insight console

The file system ACL displayed for user in the Microsoft Windows interface and on the Data Insight console do not match. In case of a Windows File Server path, a user is displayed as having Special and List permissions on the Windows interface. However, the same user is shown to have only Special permission in the Data Insight console.

Incorrect file size may be displayed for archived files in an EMC Celerra file server

Once a file is archived, the logical size of the file is displayed as the size of the file on the **Workspace** > **Overview** tab . However,when a file stored on a EMC Celerra file server is archived, its size on disk is assumed to be the block size it occupies in the physical disk. Data Insight displays the block size as the logical size of the file, which may be inaccurate.

EVFolderPoint.xml file may be displayed in the Workspace

`EVFolderPoint.xml` is a hidden configuration file. For some archived files, the `EVFolderPoint.xml` file may appear in the navigation pane and other locations.

Incorrect recommendation count displayed

On the **Workspace** tab of the console, if multiple permission recommendations are displayed for a group, and if some recommendations are removed from the list, the change does not reflect in total count of recommendations.

Permission recommendations for renamed folders may not be accurate

Data Insight computes the remediation suggestions for permissions on the basis of the latest version of a folder. Since Data Insight doesn't retrospectively consider the access events for a renamed folder, the recommendation for such folders may be inaccurate.

The Consumption by File Group report fails

When any file group is added without specifying its constituent extensions, the Consumption by File Group report fails to run.

Broken membership in case of local groups leads to misleading permissions

Data Insight cannot distinguish between built-in groups defined on various machines, for example, a Windows File Server. As a result, the Data Insight permissions views and reports may not be completely accurate for these groups.

Built-in groups are not excluded for Path Permissions reports

You cannot exclude built-in groups when configuring Path Permissions reports.

Some filers are not auto-mapped for wrongly configured Enterprise Vault servers

Data Insight does not automatically map a file server to its corresponding filer in Enterprise Vault, if you first add an Enterprise Vault server with a wrong host name and credentials and then edit the details to correct them.

Workaround

Manually map the filer to its corresponding filer in Enterprise Vault server.

Exception is displayed while trying to archive a batch of file using the Enterprise Vault

The following exception is seen when a batch of file is attempted to archive:

```
Archive:System.ServiceModel.FaultException`1[www.symantec.com.EnterpriseVault.API.FileSystemArchiving.Data.TimeoutFault]: The File System Archiving task service failed to start. Check that the File System Archiving task service is enabled in the configuration file,
```

<Enterprise_Vault_installation_folder>\EvFSAArchivingTask.exe.config.
(Fault Detail is equal to
www.symantec.com.EnterpriseVault.API.FileSystemArchiving.Data.TimeoutFault)

Workaround

From the Management Console, navigate to **Settings** > **Action Status**. Select the appropriate record, and in **Select Actions** list, click **Run Again** > **Unsuccessful**.

DFS share mapping and its configuration is not removed when the corresponding physical share is deleted

On deletion of a physical share, its corresponding DFS share mapping and the configuration for the DFS share entry are not deleted.

Hidden columns are displayed in reports in the .csv format

The .csv file for a report displays the columns which are set to be hidden from the output during configuration of the report.

Workaround

Use Microsoft Excel's feature to hide unwanted columns.

In Data Inventory reports, the DLP policy names are not displayed against the files

In Data Inventory reports, there is no column to display the Data Loss Policy (DLP) names associated with sensitive files.

Workaround

In the Management Console, navigate to **Workspace** and view the DLP policies associated with sensitive files.

Delay in rendering of some views

Certain views such as the Social Network Map view can take several minutes to load for shares that have a large number of access events or paths.

Successful partial scan does not change failed consolidated scan status

In the **Scan Status** page of the **Scanning** dashboard, if a consolidated status displays as *Failed*, a subsequent partial scan cannot change it back to *Partial* or

Successful. Also, the **Last Known Good State** does not change following a partial or successful.

Inconsistency in scan status observed from the Workspace and the Scan History view

Sometimes on the **Workspace** tab, a file is indicated to be never scanned, but the scan history for that file may indicate some successful scans. This occurs when there are forward slashes in name of the share.

The inferred owner name in Summary panel of Workspace Data tab and User Activity summary page do not match

The inferred owner name in ContextMap view may be different than that displayed on the **User Activity** summary page. This happens because both the views use different methods to calculate the inferred owner and also consider different activity time periods.

The Inactive Subfolders tab displays deleted paths

The **Inactive Subfolders** tab under **Workspace** > **Folder Activity** also displays those inactive paths which have been deleted.

Incorrect product update recommendations may be shown for Indexer nodes

The update recommendation applicable to a Linux type Indexer may be shown for an Windows type Indexer. These recommendations are displayed under the **Settings** > **Data Insight Servers** > **Overview** page for the Indexer node.

Scan-resync fails to update the folder size

The scan-rsync feature doesn't update the folder size while deleting a file.

Pipe character in share name not supported

A pipe character in a share name is not supported and can cause the Communication Service to stop functioning completely when Data Insight scans this share.

Workaround

Delete the share containing the pipe symbol from Data Insight and restart the Communication Service on the Management Server.

Enabling or disabling of audits for site collections may take longer time

This delay is observed when you attempt to automatically enable or disable auditing of site collections you may observe a delay if the web application has more than 500 or more site collections The **Edit Web Application** page remains unresponsive till the background operation completes.

Workaround

Close the tab for the **Edit Web Application** page. You can resume other Data Insight operations, while letting the unresponsive operation to run in the background.

Data Inventory Reports may produce incorrect output in certain cases

During the configuration for a Data Inventory Report, if you specify the **Number of Records** and also select the **Summary and Sensitive file details** option, then incorrect output is produced when you run the report.

Workaround

Avoid specifying any value for **Number of Records** if you need to select the **Summary and Sensitive file details** option. This setting would give you a report output displaying all the possible records.

Custom action with Expand Folder option fails to expand non-CIFS paths

If the **Expand Folder** option is set to **Yes** when you configure a custom action, and if the custom action is run on NFS and SharePoint paths, the custom action fails to expand the folders for such paths. Hence, due to absence of paths, the **Action Status** tab continuously displays the in-progress status..

Data Insight SharePoint Agent may encounter an exception while fetching attributes

During a full scan, Data Insight SharePoint Agent sometimes encounters an exception when it fetches the `access by` or `modified by` metadata attributes of files and folders residing in document libraries in SharePoint. Thus these attributes are not registered by Data Insight.

Report log displays warning message for step-progress

For reports that have been run before you install Data Insight 4.5, the report logs display the following warning message:

```
Cannot fetch Report progress, step type execute report
java.sql.SQLException: [SQLITE_ERROR] SQL error or missing database
(no such table: step_progress).
```

Before the 4.5 release, Data Insight did not collect and store information regarding step-level progress details of the reports. Thus when Data Insight attempts to fetch the details to be displayed in the **Report progress view** for such reports, it fails to find the information. As a result, the progress details in the **Report progress view** displayed as blank and the warning message is generated in the report logs.

The value of the custodian name variable name may not be displayed correctly

During the workflow template creation, when you apply formatting to custodian name variable in the **Customize Email Message** page, the value of the variable name is not displayed in the email sent to the custodian.

Sorting by paths or custodians does not work in the Ownership Confirmation workflow creation wizard

Sorting by paths or custodians does not work under the **Resource-Custodian Selection** tab of the Ownership Confirmation workflow creation wizard.

A workflow that is in submitted state cannot be canceled.

When you create a workflow and submit it, it goes to the **Submitted** state. At this state if you attempt to cancel the workflow, an error message will be displayed.

Workaround

You can cancel the workflow when it eventually transitions to the **In-progress** state. Note that the workflows with a large number of paths, may take a long time to transition from the **Submitted** state to the **In-progress** state.

The count of resources to which a custodian is assigned is displayed incorrectly.

Under the **Resource-Custodian Selection** tab of workflow creation wizard, the count of resources to which a custodian is assigned may sometimes display an incorrect value.

For Entitlement Review workflows there is no provision to display the excluded users and groups.

For a submitted Entitlement Review workflow the users and groups that have been excluded during configuration of the workflow are not displayed on the summary pane of the wizard.

Custodian assignment may take a long time to complete.

Attempt to assign custodians to a few hundred sub-folders under a share at a time may take a long time.

Permission remediation emails may display incorrect values for some variables

In the Entitlement Review workflow creation wizard, if you select the **Apply configured permission remediation action automatically** check box, upon submission of the workflow the emails triggered for permission remediation incorrectly display the `Action ID` as unknown and the `Requester_name` as `DI Support`.

The search filter on the workflow creation wizard may not function

In the workflow creation wizard, under **Data Selection** tab if you choose the option **Select paths having custodians** from the **Resource selection** drop-down list the search filter may not function. This anomaly is observed in case of DFS paths.

The sort functionality does not work for NFS paths in the Self-Service portal.

The sort functionality does not work for the NFS paths in Ownership Confirmation workflow in the Self-Service portal.

Multi-byte characters are incorrectly rendered in the HTML or CSV report outputs

In the report output multi-byte characters render incorrectly when the output is viewed in either HTML or CSV format. This can happen if your CSV reader expects a BOM character at the beginning of the UTF-8 file.

Workaround

For CSV output, execute the following command from `<InstallDIR>\bin\` folder on the Management Server to have Data Insight insert the BOM character in CSV files, and re-run the report:

```
configdb.exe -O -J "matrix.reports.csv.bom" -j "true"
```

Currently no workaround is available for the HTML outputs.

Custom actions displayed as disabled

When you attempt to edit a report and click the **Post Processing Action** tab, all the options are shown as disabled.

Workaround

Clear the **Take action on data generated by report** check box and select it again to enable the options.

SID History displayed as parent group

When a user is migrated from one domain to another, on the user-centric Permissions view, the **File System Access Control List** tab incorrectly displays the user's SID history as the parent group from which the user inherits the permissions.

Ownership Confirmation workflow does not work for certain NFS paths

Ownership Confirmation workflow works for NFS path in the form `filer:/a`, but does not work for NFS paths in the form `filer:/a/b`.

When creating an Ownership Confirmation workflow, on the workflow creation wizard, on the `Data Selection` tab, the paths such as `filer:/a/b` do not appear at all. The **Path** column shows up blank and if you click the row, it shows the error message "Unable to add path. No sensitive files present".

On the wizard, you click **Select All Resources**, these paths are added to the selected resources list, but under the Resource-Custodian Selection tab, they appear as deleted resources.

SharePoint create event displayed incorrectly

Data Insight does not capture a create event on folders when you use Windows Explorer to add new folders to a document or picture library in a SharePoint site collection. The create event on the folder is displayed as a create event on a file.

Custom attribute widget issue

When creating a Custodian Summary report, the Custom attributes widget allows you to select group attributes along with the user attributes. Although for the purpose of creating a Custodian Summary report, you should only select the user attributes, as groups cannot be assigned as custodians.

Incorrect disk space computation displayed on Workspace tab for NFS shares

The Data Insight NFS Scanner captures the logical disk space occupied by applications on the file servers. Even though the physical disk space occupied by installed applications, such as VMWare is much less, the Scanner displays the logical number on the **Workspace** tab, which can be misleading.

Error displayed while adding a VxFS filer

When you add Veritas File System (VxFS) file server which is part of a Veritas Cluster Server (VCS) configuration, Data Insight automatically discovers the VxFS shares configured under the VCS configuration. During this process, Data Insight discovers other NFS shares that are present on a native UNIX-based file system.

Although NFS shares are discovered and displayed on the **Monitored Shares** page, the auditing of access events for these shares will not happen. Scanning of these shares may work, but it is not officially supported.

Users not deleted after deleting Active Directory server

When you delete an Active Directory server, the users for that server are deleted only after the next Active Directory scan.

Add/Upgrade license succeeds irrespective of the license file type

If you already have a valid license installed, and when you want to add or upgrade the license, Data Insight displays the message *License installed successfully* even for an invalid file.

Creating non-domain saved credentials

The **Domain** field is mandatory when creating saved credentials. If you want to create non-domain saved credentials, you can do so by using the **Add Filer** or **Edit Filer** pages and selecting **Add new** in the drop-down list provided for filer administrator credentials . You may need to do so when you want to connect to NetApp or EMC Celerra devices by using non-domain credentials.

On Internet Explorer 9, the user edge for Social Network map is not highlighted when the user is clicked

On Internet Explorer 9, when you click a user in the Social Network Map, the user edge is not highlighted.

Workaround

Open a new tab on Internet Explorer and come back to the tab displaying the Data Insight Management Console. Click the user again, and the edges are highlighted.

Error message may appear while applying recommendations

If recommendations have unresolved security identifiers (SIDs), clicking **Apply Changes** under the **Workspace** > **Permissions** > **Recommendations** tab displays an error message.

For Box type source, navigation back from a shared folder may fail

The following issue occurs only in Cloud sources of Box type.

If you navigate to a shared folder of a particular user, and then navigate one level up, you cannot directly navigate back to the folder tree of that user. Instead, you reach the folder tree of the owner of the shared folder.

Search for well-known SIDs may yield partial results

Under Workspace, in the Go-to bar, if you enter a well-known SID, partial results are displayed as suggestions.

For example, if you enter the well-known SID S-1-5-32-544 (for Administrators), the Administrators group for only one domain is displayed as a suggestion. In contrast, if you search for the string 'Administrators', the Administrators group for all domains configured in Data Insight are displayed.

DLP policy filter displays some obsolete policies

When you try to filter a user risk profile based on DLP policies, some deleted or non-existent policies appear among the filter options.

Some user attributes may be unavailable as filters in User Risk dashboard

If you do not configure some user attributes as analytics attributes in Data Insight, then you cannot use those attributes to filter users in the User Risk dashboard.

Workaround

Use one of the following workarounds:

- Add the attribute to the analytics attribute list to use it as a filter in the User Risk dashboard results.

OR

- Use a DQL query to filter users on the required attribute.

Users and groups associated with re-added filers or SharePoint web applications are deleted

If you delete a filer or a SharePoint web application from Data Insight, and then re-add them, then the users and groups associated with that filter or application appear to be marked as deleted.

Workaround

After re-adding the filer or the SharePoint web application, run an Active Directory scan to retain the users and groups that were previously associated with the filer or the application.

Exact string may fail to display desired suggestion in go-to bar

In rare cases, even if you provide an exact string for a user or user group in the go-to bar, the exact matching suggestion may not be displayed.

This issue is due to an internal limitation on the number of suggestions that can be displayed at a time.

Low screen resolution clips Pagination bar, columns

If you set the screen to a low resolution then the Pagination bar (which appears at the bottom of the screen) in the Profile view of Workspace gets clipped. GUI-based tasks such as scroll to next page, export, and email are affected.

If you select a large number of columns in a custom view, some columns may also be hidden or clipped. The number of columns affected depends on the custom selection and screen resolution.

Workaround

To avoid columns from being clipped or hidden, create a custom view with fewer columns.

There is no workaround for the Pagination bar issue. You must use the recommended screen resolution of 1600 * 1024.

Exclusion rules for SharePoint paths are case-sensitive

You can configure an exclusion rule for SharePoint paths by navigating to **Settings**>**Exclude Rules**>**Add Rule for Sharepoint**.

If the string that you specify does not exactly match the case of the physical SharePoint path, then the rule is not implemented.

Default landing page for Storage Administrator role is incorrect

Users in the Storage Administrator role by default land in the Security view, instead of the Storage view.

Results of a filter remain persistent in Directory Services view

If you navigate to **Settings**>**System Overview**>**DirectoryServices** and filter the results, then the filtered results persist even if you subsequently apply a different filter.

Workaround

Do one of the following:

- Close the previous results tab and then apply the required new filter

OR

- Navigate to **Settings**>**Directory Service**s>**Domains** and then apply the required new filter.

Workspace may incorrectly indicate Box devices as inactive

Workspace may incorrectly display Box type Cloud sources as inactive. This issue occurs due to a limitation in the way Data Insight determines active and inactive files in Box type devices. Data Insight may therefore also indicate incorrect size for active and inactive data in Box type devices.

The limitation is as follows. Data Insight does not learn the last access time for a file from Box, as it learns from other devices. Data Insight therefore marks a file as active, only when it records any activity for that file. Therefore regardless of whether a file was active a minute, a month, or an year before the device is added to Data Insight, the file gets marked as inactive.

You may not be able to search for activity by users with I18N characters

In the **Audit Logs** view for a path, the search for user names does not work with Chinese characters.

Permissions Search Report fails if attribute filters include I18N characters

If you run a Permissions Search report based on a template that contains I18N parameters under the Attribute filter, then the report may fail to display correct results.

Navigating across tabs resets filters in Workspace

If you set filters for Workspace under any view, then the filters get reset if you navigate to any other tab such as Policies, Reports, Settings, Users, Groups, or Data.

Permission search report does not display nested DFS paths

If you configure nested DFS paths, then the DFS column may appear blank in the Permission Search result.

Devices pie chart does not display Box devices in System Overview page

The **Devices** pie chart on the **System Overview** page does not display devices of Box type. Unlike other devices, you cannot therefore click the pie chart to view the associated data source tab (Cloud Source tab in case of Box devices).

Forward slash appears in Access details paths report for Box devices

For Box type devices, the Access details path report uses forward slash '/' to display some paths. The paths should consistently use the backward slash "\".

Custom columns in Data tab may not remain persistent after navigating hierarchy

In the Data tab, if you configure a custom view for a filer, folder, or file, and then navigate up or down that hierarchy, the view selection gets reset to default.

Data Insight 4.0 customers may need to reconfigure analytics attribute for User's email address

In Data Insight 4.0, if an analytics attribute is configured to serve as an email address for Users, then the attribute disappears from the analytics attributes list after upgrade to Data Insight 5.0.

Workaround

A Data Insight administrator must navigate to **Settings** >**Advanced Analytics** >**Attributes**, and reconfigure the attribute.

Server notifications may reflect incorrect file count

In the Server section of the System overview notification for the number of files under Inbox, Outbox, Indexer err folder, Scanner err folder, and Collector err folder may display an incorrect file count.

Remove Permissions panel in Permissions Search report may not display list of paths and trustees

In case of a large number of records for a Permissions Search report, the Remove Permissions panel may not display the list of paths and trustees to be removed in the Remove Permissions panel.

As a result, you may be unable to complete the Remove Permissions remediation action.

User Risk Dashboard does not display analytics attributes after upgrade

After upgrade, the attribute filter under User Risk Dashboard does not display the Analytics attributes that were configured before the upgrade.

Workaround

Run a fresh Active Directory scan on the Data Insight Management Server.

Inclusion/Exclusion attribute queries do not work for Group custom attributes

Inclusion/Exclusion attribute queries do not work for Group custom attributes Inclusion/Exclusion by attribute queries do not work for Group custom attributes under **Settings**>**Watchlist Settings**.

However, the same queries work well for User custom attributes.

For re-added filer or SharePoint web applications, users and groups may appear to be deleted

If you try to re-add filer or a SharePoint web application after deleting it, then the local users and groups belonging to that device may be marked as deleted

Workaround

After you delete a filer or SharePoint web application, run an directory service scan. You can then re-add the filer or the application.

Unable to search for activity by users with Chinese characters

In the Audit logs view under the Profile tab for a share, if you search for user names with Chinese characters, the search fails.

GUI displays incorrect creator name for NFS share added as CIFS share

For NetApp devices, if you create an NFS share and add it to Data Insight as a CIFS share, then Data Insight fails to discover the creator. The GUI indicates that the creator of the share is ‘SHAREPOINT/System’. The related rollover text maps it to Sid: S-1-0-0, associated with user ‘Nobody’.

In Chrome, dashboard may not highlight selected row

In some versions of Chrome, if you click to select a row in any view of the Data Insight dashboard, then the row is not highlighted as expected. Instead, by default the first row in that view remains highlighted.

The dashboard however displays the required information for the selected row as expected.

Workaround

Use one of the other supported browsers.

Other Issues

This section lists some additional issues.

Capacity Reports are generated for all filers irrespective of RBAC configuration

If a Data Insight user who has privileges only on a subset of filers, creates/runs a Capacity report, the report is generated for all filers.

Events display error

If a scan fails on an Active directory domain, the **Settings** > **Events** page displays that the Active Directory scan was successful. If three domains are added Data Insight, and while scanning, if a scan fails on one or two of the three domains even then the **Events** page displays this event as a Successful (INFO) event, instead of Failed (ERROR) event.

Error in displaying selected result entry

For built-in groups in a multi-domain environment, when you search for a group, clicking any of the result entry opens the tab for the first domain's built-in group.

For example, three domains are added to Data Insight. When you search for the group Administrators on the **Workspace** > **Group** sub-tab, three entries appear in the result in the tree-view pane. Data Insight opens the details for the first entry in the list, even if you select the second or third entry.

Workaround

Select the group from the tree panel. It displays the required information.

Vfilers wrongly capture open events on folder paths as events on file paths

The audit files for shares on vfilers are saved in the `err` folder on Indexer node. Vfilers can sometimes record file open events on directory paths. Data Insight treats these paths as files, and registers these events as file reads. Subsequently, when file open events are received on paths which are files and are children of the directory paths which are wrongly captured as file paths, index writer treats these events as invalid and discards entire audit file.

Upgrade your NetApp filer to the latest available firmware version to avoid this issue.

Deletion of a Collector node fails even after disassociating all filers

Deletion of a Collector node, which has DFS server mappings, is successful only after you delete the DFS server mappings associated with that node.

User with Product Administrator role unable to edit share

A user assigned the role of Product Administrator cannot edit a share.

Workaround

A user with Product Administrator privilege on the filer on which the share exists can edit the share.

Unable to restore tabs

Restoring tabs for DFS and SharePoint paths does not work.

Workaround

Close the in-progress view window, and manually open the required tabs.

Scan resync does not work for certain scenarios

If a file is deleted and a folder with the same name is created, and if Data Insight does not capture this event for any reason, then the file continues to appear in the tree.

Security event not monitored

Security events, such as set attributes are not monitored for NetApp filers using the NFS protocol.

Create event not captured

Create event on zip files is not captured for NFS shares.

Container and directory service name limitation

Container name and directory service names cannot have > and < less than symbols.

Incorrect default schedule displayed

The default schedule for fetching audit events from the SharePoint server appears as a cron string on **Data Insight Servers**> **Advanced settings**. The cron string translates to mean that the scans will run every 45 mins, in place of every hour.

Special characters in NFS paths cause NFS scanner to fail

Special characters in NFS paths which windows does not allow to contain, (?,",<,> etc) cause NFS scanner to fail for paths containing these characters.

Incorrect default schedule displayed

Schedule to fetch audit events from SharePoint server shows invalid default value.

Error in deleting report output

Custodian reports do not delete pdf files in report output folder for two custodians.

Port number for LDAP directory server required

When adding an LDAP directory domain to Data Insight, the test connection for the LDAP directory server fails if the port number is not specified alongwith the LDAP server address.

Workaround

Specify the LDAP server address in the format, `server_address:port`. For example, `ldap.company.com:389`.

Exclamation mark in user name not supported

Installation of the Windows File Server agent for Data Insight fails if using the credentials of a user who has exclamation mark (!) in the user name.

Duplicate policy name issue

On the **Policies** tab, while creating a new policy, duplicate policy names are allowed. Also, Symantec Data Insight does not verify email address field value when a new policy is created.

A security event does not change last modified by value for a destination folder

When **Last accessed on** /**Last modified on** date changes for an event, the corresponding **Last accessed by**/**Last modified by** value must also change. However, a security event does not change the last modified value of a destination folder as it does for a Write event.

The job scheduling settings require modification

The **Advanced Settings** page for Data Insight servers allows you to schedule jobs. For example, it allows you to specify schedule to run scans and collect audit data. The only way to specify such a schedule is to select “Monthly” in the drop-down and then specify the day, for example 31. However, in this case, the scan does not run in months that do not have 31 days. It runs on the 31st day of the months that have 31 days.

The scan history graph does not display the data as expected

The scan history graph does not display the data as expected in all cases. For monthly data only six bars are visible instead of twelve bars. And for weekly data only three bars are visible instead of four bars.

Limited support in the Entitlement Review report

The Entitlement Review report does not have NFS support.

Issue with launching installer from mapped drive

When the Data Insight installer is launched through a mapped drive, it reports that port 443 is in use, even if the port is not being used by any other application.

Workaround

The workaround is to copy the installer locally to C: drive and then launch the installer.

Issue with same NFS export and CIFS share name

Data Insight does not support similar names for shares exported out of NFS file system and CIFS share names. However, same share names for NFS and CIFS are supported across the filers.

The scanned shares and the total scan count does not match

The total scan count data is not the same when computed through scan history chart and scan history page.

When shares are disabled or deleted, the scan history chart and the scan history page must show the updated results. However, currently the scan history chart does not provide the updated scan result.

Access Summary for Paths report displays all active users of a share

If you run the Access Summary for Paths report against a subdirectory within a share, the report shows all active users for that share regardless of whether they have performed any activity on the subfolder within the share or not. The counts for users who have no activity on the subfolder are shown as 0.

Limited support for claims-based authenticated Web applications for SharePoint

Data Insight does not fully support Web applications which have authenticated mode set to claims based. If claims-based authenticated Web applications are configured in Data Insight, ensure that the authentication mode of the claims-based Web applications also have windows authentication enabled. This can be done using the Microsoft SharePoint Central Administration Console which is available on the SharePoint server.

Data Insight is not able to resolve the SAML provider user who performed activity on the site collections within those Web applications. The user names appear with a prefix 'Unknown User ID...' in such scenarios.

Push-installation on Windows 2003, 64-bit Collectors fails

When you try to install Data Insight on a Collector node that is hosted on a Windows 2003, 64-bit computer, from the Management Console by using the Add New Server feature, the installation fails because of memory constraints.

Workaround

Manually install Data Insight on the Collector.

Inactive users view and report does not consider share-level permissions

The Inactive Users view and the Inactive Users report do not take into account share-level permissions.

For example, a group containing 5 members has share-level permissions. All five members of the group have Full Control ACL entry for file system. Out of the 5 members who have permissions on the share, 2 are inactive.

In this case, ideally the Inactive Users view and the Inactive Users report should show only 2 users. However, the Inactive Users view and report does not consider the share level permissions, hence all users in the Active Directory except the 3 active users are displayed.

Attempt to archive a file using the Enterprise Vault fails

When a file path contains the ampersand symbol(&), attempt to archive the file fails, due to an internal Enterprise Vault error.

Group Change Analysis report does not report loss of access if users part of built-in groups

If you select a group for revoking permissions, and run a Group Change Analysis report, the report does not list users who are part of a built in group, such as Administrators.

For example, if Group XYZ is selected for revoking permissions. The group has 11 members, 6 of whom are members of Administrators group. The share has activity by users A, B, and C who are members of Group XYZ. When you run a Group Change Analysis report, the output lists only users A and B as losing access. The report does not list User C because the user is part of the Administrators group.

Filer Mapping page does not reflect the changes in the settings for the Enterprise Vault servers

When you edit the entry for an Enterprise Vault server, the corresponding changes are saved in the Data Insight internal database for Enterprise Vault. But the newly entered values are not reflected in the **Filer Mappings** page on the Management Console.

Generic device issue

Data Insight is not able to scan NFS shares hosted on EMC Isilon file servers.

Connection to the Enterprise Vault server fails if host name is used

When Data Insight attempts to connect to Enterprise Vault server using host name, the connection fails with error *401: Unauthorized*.

Workaround

Attempt to connect using the alias for the Enterprise Vault server. Make sure that in the Management Server, an entry is made for the alias in the hosts file.

Stop DataInsightFPolicy service before shutting down a Collector node

Veritas recommends that you first stop the DataInsightFpolicy service before powering off or shutting down a Collector machine. Gracefully shutting down the DataInsightFpolicy service allows Data Insight to gracefully un-register from all the monitored filers, Thus, the filer does not attempt to send events to the Collector while it is powered off.

Data Insight cannot retrieve retention categories with certain characters

Data Insight periodically fetches configured retention categories from Enterprise Vault (EV). File System Archiving (FSA) cannot find retention categories with Chinese, Japanese, and special characters in the name.

Hence, you will not be able assign retention categories with Chinese, Japanese, and special characters when archiving data from the Data Insight Management Console.

Issue with assigning NIS and LDAP users as custodians

When you use the `mxcustodian.exe --assign --csv <path of csv file>`, where the information in the CSV file is in the format - paths, user@domain.

However, if you use a CSV file with information in the format - paths, sID, then NIS and LDAP domain users cannot be assigned as custodians and an error is displayed.

Disabled icon not displayed

If a share is disabled or the filer on which the share resides is disabled, the share is not marked with a disabled share icon. This behaviour is observed only in the left hand side filter of the content pane for the user centric views on the **Workspace** > **Audit Logs** page.

Issue with computing custodian for root site collection

Data Insight is not able to compute custodians for root site collections by using the `mxcustodian.exe --ownermethod` command.

The root site collection has same the URL as the web application. Data Insight considers a web application as a device. The mxcustodian.exe script does not support a device for ownership calculation.

Size of parent folder is not updated

For some files on NFS shares, the changed in the size of the file is not reflected by a change in the size of the parent folder.

Issue with pagination on Audit Logs view

The pagination on the second table on the **Workspace** > **Users** > **Audit Logs** view, freezes intermittently.

Issue with LHS filter

On the **Workspace** > **Users** > **Activity** page, when you select a share in the left-hand side (LHS) filter and click on a bar graph, the selected share under LHS tree view disappears.

`mxcustodian.exe` is slow in case of large number of paths

When you use the `mxcustodian.exe --assign` command to assign custodians to large number of paths, intermittently, while the custodian database for a given index or MSU is being updated (by mxcustodian.exe), you may not see all the inherited custodians on the **Workspace** > **Folders** > **Overview** tab.

Certain reports do not honor the global data owner policy

In case of Consumption by Folder, Data Aging, and Inactive Folders reports, Data Insight does not fetch the data owner based on the global policy defined on the **Settings** > **Workspace Data Owner Policy** tab. These reports return data owner information based on a fixed default owner method order.

Incorrect informaton displayed for migrated user

When a user is migrated from one domain to another, on the user-centric Permissions view, the share-level permissions show the user's SID history as the parent group from which the user inherits the permissions.

Issue with workflow creation if services on Indexer are down

During the creation of a workflow request, under **Data Selection** tab, if you choose **Select paths having Custodians** and if the services on Indexer node are down, you will see rows of data where custodian and custodian email is displayed, but the path column is blank.

This issue is observed for the filers that use remote Indexer,

UTF8 characters may not render correctly in report outputs in CSV format

If the CSV output of a Data Insight report is viewed using Microsoft Excel, UTF8 characters may not render correctly.

Workaround

The CSV file is stored with a byte order mark (BOM) character for UTF-8. You can use Notepad to view the report.

Unable to get Create event for Hitachi NAS devices in some cases

When a CIFS share is mounted on a Linux machine, and a directory is created using the `mkdir` command, the Hitachi NAS device does not generate a Create event.

This is a Hitachi NAS issue, and currently no workaround is available for the same.

Issue with the new membership object in DQL

In case of a circular group, query returns inconsistent results for the depth and directgroup attributes, when the query has topgroup or membergroup in the WHERE condition.

Also, retrieving membergroup.memberusers or membergroup.membergroups will give incosistent results in the depth column in the membership table.

In case a group is in a circular membership, that is, the group becomes a member group of itself, the depth and the directgroup attribute for the the row of that group could be inconsistent depends on the WHERE condition. For example, suppose G1 and G2 are member groups of each other (thus circular), then for G1 row, topgroup = G1, membergroup = G1, depth = either 0 or 2, direct_group = either G2 or NULL. This issue only impacts groups with circular membership.

Empty multi-value column not supported

In DQL, for a multivalue column, there is no way to specify a WHERE condition whether this column is empty or not.

Query with I18N characters may fail to generate Permissions Search Report

If your query for a Permissions Search Report based on criteria that use I18N characters, then the query may fail.

Chapter 5

Fixed issues in this release

This chapter includes the following topics:

Fixed issues in 5.0.2

The following issues were fixed in 5.0.2. The fixed issues are referenced by the Veritas incident number.

Table 5-1 Fixed issues in 5.0.2

Etrack/JIRA IDs	Description
3873661	Keystore password is not encrypted in configuration database.
3865025	NFSUserMappingJob fails while parsing user's entry with no uid/gid fields.
3859874	Ignore file types for events done on streams.
3855646	DQL report is partially successful. The CSV file is blank when using the memberof.name query.

Table 5-1 Fixed issues in 5.0.2 *(continued)*

Etrack/JIRA IDs	Description
3856749	Customer's Administrator user with permissions in Data Insight is unable to render the pages in the GUI.
3852655	Watch listed users are not displayed in report output.
3853919	ADCLI process crash during Active Directory scan.
3870457	Events from HNAS not found in chronological time order.
3863419	DQL Custom Attribute search fails to yield any results.
3855680	idxwriter.exe crashes while trying to process scan metadata files when maximum number of events in memory threshold is reached.
3852650	When "Number of threads for a single report run" is greater than 1, merge_rpt.exe fails to merge report output correctly for Entitlement Review report.
3871500	File size not shown under the Workspace tab for some files on the FAT file system.
3872559	DFS File location in Data Loss Prevention administration console unable to link to file in Data Insightconsole.
3873015	controlpoint.exe crashes on Indexer node's serving SharePoint web application.
3866348	report.exe crashes in scenario where share and its subfolder are added when configuring a Whitelist policy.
3829288	Fixed issue in the User Activity Deviation Policy that causes the Policies report to crash sometimes when a large number of policies are configured.
3853599	Support for internet proxy communication while configuring Box filer.

Table 5-1 Fixed issues in 5.0.2 *(continued)*

Etrack/JIRA IDs	Description
3868944	activityidx.exe process is taking up a large amount of memory
3867200	.xls files are showing up in media files 'Consumption by file group' report.
3865348	Output formats of Box Event API changes to string data type causing exception 'Cannot construct instance of long from String value 'XXXX': not a valid Long value'.
3868034	Entitlement workflow shows paths as failed
3851993	Report fails or completes without formatted output. The user access summary report takes a long time on a big setup.
3860594	Reports run under parallel threads may be empty of data.
3853599	Need to configure Data Insight to connect to internet .
3854794	Data Insight user interface freezes when Users or Groups view is selected
3865199	permchg_cifs* files build up in DATADIR\indexer\err folder on Indexer
3862667	Report.exe crashed with Error 0xc0000409 - The system detected an overrun of a stack-based buffer in this application.
3859874	Need to investigate missing filetypes for cluster mode filers.
3859867	SharePoint scan errors in indexer/err folder when trying to process manually idxwriter.exe is crashing.
DI-1618	When editing a report, if you select the All Physical Resources check box under the Data Selection pane, the User Selection pane hangs.

Table 5-1 Fixed issues in 5.0.2 *(continued)*

Etrack/JIRA IDs	Description
DI-1512	Fixed search filter under the Permissions section of the Workflow Details page of Entitlement Review Workflow.
DI-1503	When a vFiler is added into DI, the latencies of its corresponding physical filer are not fetched if it is not added as a separate physical filer. Hence, safeguard for vFiler does not work correctly.
DI-1489	Filer health for NetApp CMode shows as *needs attention(Event monitoring stopped)*, but actually event monitoring happens as expected.
DI-1487	Fixed multiple occurrences of winnas_util.exe while enabling SACL on HNAS share.
DI-1433	ADCLI process crashes during Active Directory scan
DI-1430	Storage by domain report, does not show dynamic custom attribute in table header Edit Comment Assign More Reopen Export
DI-1381	SharePoint scanner should continue to fetch item list when timeout occurs instead of aborting the scanner process.
DI-1355	Data Aging report for custodians has multiple duplicate rows in output. This duplication happens when the same custodian is assigned explicitly on nested paths.
DI-1338	Access Summary for Paths and Access Summary for Users/Groups show incorrect output for Box for a specific user.
DI-1150	DQL Custom Attribute search fails to yield any results
DI-1187	Extend maximum allowed file extension length to 15 characters so that longer extensions are not ignored by DQL.

Fixed issues in 5.0.1

The fixed issues are referenced by the Veritas incident number.

Table 5-2 Fixed issues after 5.0

Incident number	Description
3764098	Box Scan does not capture "created_by_user" information for file and folder.
3821579	Permissions Search report > **Select Action** > **Remove Permissions** view is not rendered correctly in case of large number of paths in the report output database.
3829226	In the Self-Service Portal, the Ownership Confirmation workflow has been in grace period for 5 days.
3831463	On the **System Overview** page, the device pie-chart for SharePoint slice shows 25.00 instead of 25% (percentage).
3831766	In the **Workspace**, a cross launch always opens in the **Overview** tab, instead of opening in previously opened tab.
3831770	For certain pages like **Inactive Folders** etc., the profile page is truncated at the bottom.
3834541	When trying to launch a group name having the equal sign "=", the Dashboard displays an error message.
3838166	Some events are lost when audit data is collected for Hitachi NAS device.
3838301	SharePoint scanner goes in a loop generating huge scan database files.
3839168	In case of Box devices, LocalUserScanJob executes successfully first time, but fails from second time onwards.
3839638	For SharePoint server 2013, few SharePoint groups are not rendered in the management console for site collections.

Table 5-2 Fixed issues after 5.0 *(continued)*

Incident number	Description
3840406	Addition of filers of type Isilon, Hitachi NAS, and NetApp cluster-mode should also add filer entry under the **Data Management** > **Add Filer Mappings** page.
3841498	Add **Show permissions** and **Show activity status** checkboxes in the Entitlement Review workflow template under portal options.
3842792	In case of Permissions Search report, add horizontal scroll bars for the **Remove Permissions** pop-up.
3843963	During Indexer migration, all Indexer data for the destination Indexer appears to be missing.
3845062	Email notification in Data Insight does not work if the SMTP port number is set to a value other than 25.
3850401	Due to timing issue, the **Export** option is not consistently available in the Workspace.
3854596	Entitlement Review Reports run under parallel threads and return no data.

Fixed issues in 5.0

The fixed issues are referenced by the Veritas incident number.

Table 5-3 Fixed issues after 4.5.3

Incident number	Description
3791005	If Permission Remediation (Email for raising ticket) is configured in the Entitlement Review workflow, and you submit a path without making any changes to the permissions, the mail is not sent. Also, the status for that path always remains "Executing Action".
3798450	Extended workflow date is not used. Workflow moves to completed date after the end_date specified during workflow creation.

Table 5-3 Fixed issues after 4.5.3 *(continued)*

Incident number	Description
3793823	Usermaps file size is too large.
3778465	Indexing of certain shares is too slow.
3771762	SharePoint scanner creates large temp files (hundreds of MB).

Appendix A

Getting help

This appendix includes the following topics:

Using the product documentation

The following guides provide information about Symantec Data Insight:

- *Symantec Data Insight Installation Guide*
- *Symantec Data Insight Administrator's Guide*
- *Symantec Data Insight User's Guide*
- *Data Insight Self-Service Portal Quick Start Guide*

The Data Insight documentation is updated, if required after the product release. Refer to the documentation on the Support site for the most current version.

Contacting Veritas

You can contact Veritas on the Web, by email, or by telephone.

Data Insight Support

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

www.veritas.com/support

Using the Support web site

For technical assistance with any Veritas product, visit the Veritas Support Web site:

www.veritas.com/support

From there you can:

- Contact the Veritas Support staff and post questions to them.
- Get the latest software patches, upgrades and utilities.
- View updated hardware and software compatibility lists.
- View Frequently Asked Questions (FAQ) pages for the products you are using.
- Search the knowledge base for answers to technical support questions.
- Receive automatic notice of product updates.
- Read current white papers related to Symantec Data Insight.

Accessing telephone support

Telephone support is available with a valid support contract. To contact Veritas for technical support, dial the appropriate phone number listed on the Support Guide included in the product box and have your product license information ready for quick navigation to the proper support group.