Veritas Data Insight Release Notes

6.0

VERITAS™

Documentation version: 6.0.1

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. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email 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 Veritas 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 Veritas 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. Veritas 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 Veritas 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**.

- Content classification

  Data Insight lets you classify content on data sources that it monitors by providing means to define classification rules (policies) that let you specify values (tags) that you can assign to any matching items. The classification feature works in conjunction with the policy framework provided by Veritas Information Classifier to assign tags to files.

  For example, a content scan may search for items whose contents include a credit card number and assign a tag of "PII" (for "personally identifiable information") to any that do.

- 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 Veritas Data Insight

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

Since 6.0

The following features and enhancements are available in Data Insight 6.0

Content classification using Veritas Information Classifier

Today, the need to identify and protect data is elevated. Organizations need to comply with data protection regulations that require them to monitor and locate

sensitive data, protect it against data infringement and loss, and secure it by applying accessibility and usage control. Also, the exponential growth of unstructured data makes taking data management decisions (how long to archive content of business or legal value or what data to delete) a challenge.

Classification helps you improve content analytics by focusing on the relevant data set to perform risk analysis and remediation. It enables you to identify the sensitive data being stored in repositories (for example, Personally Identifiable Information such as Social Security, credit card, and drivers' license numbers) and ensure that the data complies with legal requirements in your organization.

In order to stay in step with the data protection regulations and to deal with the ever growing data, Data Insight operates closely with Veritas Information Classifier 2.0 to create a comprehensive framework to classify content that match the policies defined by your organization. Veritas Information Classifier uses built-in and user-defined policies to assign classification tags based on the content in files in your environment. After the files are classified, users of Data Insight can use the classification tags to filter the files for searches, reviews, and remediation.

For more information about how Data Insight classifies content and how to set up classification, see the *Veritas Data Insight Classification Guide*.

Smart Connect support for EMC Isilon

Data Insight now lets you configure whether you want to use the access zone, SmartConnect zone name, or SmartConnect zone alias to discover shares on an EMC Isilon file server when adding it to Data Insight.

EMC Isilon publishes shares through access zones. The SmartConnect zone hostname and alias is typically used to discover shares instead of the access zone name. Data Insight discovers access zone to SmartConnect zone mapping and uses it to discover shares.

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

Efficient organization of reports with labels

Data Insight now lets you add labels to new and existing reports. The labels enable you to organize and group reports which makes it easier to search through a long list of reports. Reports can be organized under more than one label.

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

Data Insight Query Language (DQL) reports enhancements

DQL reports now include support for the following:

- Parallel execution support for DQL reports
  You can now execute a Data Insight Query (DQL) report using parallel threads on an Indexer node. The global setting that lets you configure the number of

threads responsible for generating the report output database for a single report now also applies to DQL reports.

This setting improves the DQL performance and ensures faster generation of DQL reports.

- New tags tables added.

  Allows you to find all tags that exist globally and to query tags associated with a file path from Veritas Information Classifier. The tags table only has one column - name. It is a string.

  Example query - **from tags get name**

  For more information, see the *Veritas Data Insight Programmer's Reference Guide*.

Ability to purge report outputs and classification data

Data Insight now lets you purge historical report outputs and classification data. Purging frees disk space and keeps data at a manageable size.

You can configure global time and count-based settings that will automatically delete the data. Purging of data is not enabled by default.

For more information about configuring data retention settings, see the *Veritas Data Insight Administrator's Guide*.

Better user management based on last login time

Data Insight now provides information about the time when a Data Insight user last logged into Data Insight. The audit information helps in better user management by allowing you to revoke access to users who have not accessed Data Insight in x number of days.

Since 5.2

The following features and enhancements are available in Data Insight 6.0.

Ability to scan shares using multiple threads in parallel

With large shares, Data Insight takes longer to complete the scan. To overcome this issue, Data Insight provides an option to scan large shares using parallel threads. Scanning shares in a parallel manner significantly reduces the scan time and results in better recency of data.

Depending on the size of the share and the number of processors, Data Insight lets you specify the number of scan threads that you want it to run.

For information on configuring the parallel scans for a share, see *Veritas Data Insight Administrator's Guide*.

New Risk Dossier tab added to user-centric views

Data Insight enables you to monitor malicious activity in your storage environment. It profiles all users by assigning a risk-score to every configured user. The risk score places each user at a relative distance from other users and orders them in accordance with how risky a user is in comparison to other users. Higher the risk score of a user, higher is the perceived risk posed by the user.

A new **Risk Dossier** tab is now added to the user-centric view in Data Insight 6.0. The Risk dossier expands Data Insight's capabilities to analyse risk. It displays visualizations that provide more insight into the risk score and explains why a user is considered risky.

The Risk Dossier also helps you investigate reasons for a spike in the risk score by answering questions such as:

- What is the historical risk landscape for a user?
- Why is risk score high for a user on a given date?
- What contributes to the risk score?
- How can you mitigate the risk?

To navigate to the **Risk Dossier** for a user, from the **Workspace** > **Users** list page, select a user and click **Expand Profile** and then click **Risk Dossier**.

The **Risk Dossier** tab provides the following visualizations for a user's risk score:

- The risk history graph shows the risk score of a user for the last 180 days. The graph gives you an idea of how the risk score for a user is moving. A sudden spike in the risk score may warrant an investigation. You can click on a date on the risk history graph to know the composition of the risk score for each factor - Access, Anomaly, and Alerts.
- The breakup of a user's risk score on a selected date. The chart also lets you compare the risk score parameters for a historical date with the parameters as of the current date.
- The Anomaly factor (attack surface) view display the granular usage deviation for risky users and the potential for damage from a high-risk user.
- Overview of alerts raised against a user.

For detailed information about using the Risk Dossier, see the *Veritas Data Insight User's Guide*.

New central audit page for remediation workflows

Data Insight now allows you to work with the workflows at a more granular level. The **Workflows** tab now appears as a primary tab long with **Workspace**, **Policies**, **Reports**, and **Settings**. All other functionality related to managing workflow

templates, creating or deleting workflows, and configuring Self-Service Portal settings remains the same.

Data Insight 5.2 introduces a new **Audit** sub-tab that provides a central location to review all paths which have been submitted for action across all workflows.

You can initiate the following remediation actions on workflow paths from the **Workflows** > **Audit** page:

- **Archive**: You can archive the paths that are part of a **Records Classification** workflow.
- **Remove permissions**: You can remove permissions for **Entitlement Review** workflow paths.

For information about remediating workflow paths, see the *Veritas Data Insight User's Guide*.

Support for metadata framework for reporting and classification

You can now add text-based tags to file system objects such as shares, files, and folders. You can import the metadata tags into Data Insight and use DQL reports to retrieve them from the database.

The metadata can then be used for classification and remediation.

For information about adding metadata tags, see the *Veritas Data Insight User's Guide*.

Ability to update encryption keys for saved credentials

Data Insight now lets you rotate the keys that encrypt saved credentials and the communication between Data Insight nodes.

The feature enables you to adhere to your corporate security policies and prevent malicious activity. Updating the encryption keys periodically also mitigates the risk of compromising service accounts.

For information see *Veritas Data Insight User's Guide*.

DQL report enhancements

The following enhancements to DQL are available in this release:

- User risk score querying capability in DQL.
  A new *riskscore* column is now added to DQL that allows you to query the current user risk score for the user.
- New metatagname column added to **path** and **dfspath** tables that let you retrieve metadata tags associated with filesystem objects such as files, folder, or shares. The metadata tags can be used for classification and remediation aids.

- New columns are now added to the **path** and **dfspath** tables that allow you to query Windows file system attributes for CIFS paths.
- The following new Risk Analysis templates are now available when configuring DQL reports:
  - Risky Users Group - Lets you find groups contributing to high level of permissions that are common across users which have risk score > 90.
  - Risky Users Outlier - Lets you find any unusual user with a risk score >90.

Support for Microsoft SharePoint 2016

Data Insight now supports monitoring of data residing on Microsoft SharePoint version 2016.

For the list of supported SharePoint versions, see the *Veritas Data Insight Installation Guide*.

Overcoming spurious read events in Windows File Server

Data Insight now eliminates the issue of seeing spurious read events on Windows file servers. In previous releases of Data Insight, spurious read events were observed when a folder was opened in Windows Explorer.

From Release 5.2, the Windows File Server driver that is responsible for collecting access event information tracks only authentic read events.

The enhancement ensures that analytics and decision making is based on true acitivty.

Note: You can choose to use the previous functionality that did not overcome spurious reads. For the procedure, see the following technical note https://www.veritas.com/support/en_US/article.000114411.

Observations with respect to the new implementation are as follows:

1. If a folder contains executable files, Windows Explorer reads the contents (header and footer) of that executable file when the folder containing it is opened. Hence, even if the executable file has not been opened or executed, the executable show up as a read file when you use this implementation.
2. If the preview pane **Large Icons** is enabled in Windows Explorer, Windows reads the contents of file which shows up in the preview pane. An example is the folder `Pictures`. So, if the preview Large icons is enabled, the files show up as read when you use this implementation.
3. Multiple read events on the same file may not be seen because of caching on windows client and on Linux clients. Once the first read event is cached by the

Windows client, further read events are not seen for at least 3 minutes. In case of Linux clients, once the first read is cached, further read events are not seen until the file is modified or a share is unmounted.

Licensing changes in 5.2

The storage limit-based license framework is revised to alert the user when the storage monitored by Data Insight exceeds the licensed limit. The alert appears on the footer of the Management Console to indicate that the storage monitored by Data Insight is exceeded. With this message, the user is encouraged to review the existing storage resources and if required, procure an appropriate license by contacting the Licensing team.

Upon exceeding the storage limit, Data Insight continues to function with uninterrupted access to all functionality.

For information about the licensing changes, see the *Veritas Data Insight Administrator's Guide*.

Support for reconciling file system hierarchy after the deletion of a site

During a full scan, if Data Insight discovers that a site is missing, it marks the missing site as deleted.

New warning introduced when you attempt to open a large report in PDF or HTML format

On the **Reports** list page, a warning pop-up message appears when you attempt to open a report as a PDF with size more than 100 MB or HTML report with size more than 300 MB (11 MB compressed size). The pop-up indicates that if you continue to view the report, the web browser may become unresponsive. You can choose to view the report in the web browser, cancel the operation, or download the report.

Provision to rename a storage device from the Console

Data Insight now lets you rename a storage device such as a filer and a SharePoint web application from the Management Console. Once the device is renamed, its references are automatically updated with the new name in the Enterprise Vault filer mapping configurations, reports, workflows, audit logs, Data Insight event logs, scan status and history, alerts, policies, exclude rules, and migrations processes.

Note: The cloud-based storage such as Box and certain filer types cannot be renamed from the Console.

For information on renaming a storage device, see *Veritas Data Insight Administrator's Guide*.

Support for Enterprise Vault 12.1

Data Insight now integrates with Enterprise Vault 12.1 to enable the archiving of old and inactive data on CIFS shares.

Inferred owner policy changes

The calculation of the Workspace Data Owner policy was based on various criteria such as Last Accessor, Read+Write Count, and so on. The criterion **Read+Write** is now changed to **All Activity Count** to correctly reflect that all access events are considered if this option is selected. **All Activity Count** includes the cumulative count of read, write, create, delete, security, and rename events. This change is now there in all the reports where the Data Owner Policy tab is supported.

Changes to the labels of certain report categories and report types

The following report categories and types are renamed:

- **Access Details** to **Activity Details**
- **Access Details for Paths** to **Activity Details for Paths**
- **Access Details for Users/Groups** to **Activity Details for Users/Groups**
- **Access Summary** to **Activity Summary**
- **Access Summary for Paths** to **Activity Summary for Paths**
- **Access Summary for Users/Groups** to **Activity Summary for Users/Groups**
- **Duplicate Files** to **Potential Duplicate Files**
- **Group Impact Analysis** to **Group Change Impact Analysis**

Changes to reports configuration labels

The **Number of records** field in each report is now modified to ensure clarity. For example, in the **Inactive Data by Owner** report the **Number of records** field is now renamed to **Number of records per owner**.

Adding classification tags while archiving files into Enterprise Vault

Data Insight can add classification tags to a file that is archived. When the file is archived and indexed in Enterprise Vault, this metadata is included in the index of the file. The file can then be searched in Enterprise Vault using these classification

tags. When the archive is searched, the search is carried out on the tags that are attached to the data rather than the entire Enterprise Vault.

As a Server Administrator or a Report Administrator, depending on the property value that you set in Reports, you can carry out the search in Enterprise Vault. If you set the property value as a Text using Data Insight, you can search the property using text-based selection criterion.

This feature is enabled under Data Insight **Reports** where **Archiving** is supported. However, the paths get archived using these tags only when the check box **Add Custom Index Property** is selected. The tag information is added when you archive the data from Reports.

For information on adding classification tags, see the *Veritas Data Insight User's Guide*.

SID History changes

Permission reports like **Inactive Users** report and **Entitlement Review** report make use of SID History now. For more information, see the *Veritas Data Insight User's Guide*

Enhanced Potential Duplicate Files report

Data Insight now considers the modified time of files in addition to the extension and the size of the files when computing duplicate files.

Since 5.1

Veritas Data Insight 5.1 includes the following new features and enhancements.

Licensing changes in 5.1

Until Data Insight 5.0.x, the product functionality operates on Trust and Verify model. A message in the footer indicates whether the base as well as Self-Service portal license has expired, but product features are fully functional if the license has expired or in the absence of a valid license.

From Data Insight 5.1 onwards, if you do not have a valid license or when the license expires, the software continues to run in a restricted mode. The following functionality is disabled on the Management Console:

- The **Workspace**, **Policies**, and **Reports** tab are hidden on the Management Console. Only the Settings tab is visible on the UI.
- The options on the console to add new filers, shares, SharePoint web applications, site collections, cloud storage resources, and directory services are disabled. However, Data Insight lets you edit properties of the resources that are already configured in Data Insight.

- Auto-discovery does not result in discovering new shares or site collections that are created on filer or web application if the license on the Data Insight system is not valid.
- Creation of workflow templates and workflows is disabled, even if portal license is valid but the base license has expired.
- If the Base or Portal license expires the custodians will not be able to access the portal although they will continue to receive reminders for the workflows assigned for their actions. Also, if base license is invalid, the custodians will not be able to access the portal.

Support for cDOT NFS

Data Insight now supports the monitoring of NFS exports on Clustered NetApp Data ONTAP devices. The Data Insight cDOT NFS support works only with NetApp ONTAP Cluster-Mode versions 8.2.3 or higher and ONTAP 8.3.1 or higher.

Veritas recommends that Windows 2008 or Windows 2008 R2 server is used as the Collector node, if you want to monitor NFS exports on NetApp Cluster-Mode.

For information about the prerequisites and procedure for configuring monitoring of NFS exports on NetApp cDOT SVMs in Data Insight, see the *Veritas Data Insight Administrator's Guide*.

Support for Box permissions in Data Insight

Data Insight now enables the visualization and analytics of permissions on Box resources. Visibility into Box permissions enables you to ensure security, minimize the possibility of a data breach, and ensure that the right people have access to the right data.

To understand how Data Insight displays Box permissions and for information on the limitations associated with Box permissions in Data Insight, see the *Veritas Data Insight User's Guide*.

Support for co-admin account for configuring Box resources

You can now use Box co-admin account credentials to configure a Box storage resource in Data Insight. In order to use a co-admin account to monitor Box users and their access events, you must assign certain privileges to the co-admin account.

For information see the *Veritas Data Insight Administrator's Guide*.

Availability of creator owner information in Entitlement Review workflow

For Entitlement Review type of workflows, Data Insight now provides an option to display the creator owner information on the Self-Service Portal. A creator owner

has Full Control permission on the folder. Custodians can use the information to evaluate permissions assigned to the creator owner and take appropriate remediation actions, such as remove creator owner from a path.

You must select the option to display the creator owner information when you create the workflow template.

New Data Insight Query Language (DQL) templates now available

New templates that help you create DQL queries have been added to Data Insight. You can modify the queries in the template to fetch the following information:

- Specific file extensions and the storage capacity occupied by them.
- File extensions that are not configured in Data Insight.
- Duplicate files in a share.
- Stub files that are 4 KB in size.
- Files that are last accesses between 1 and 3 years.
- Box folders owned by a given user.

For information on using templates to create DQL reports, see *Veritas Data Insight User's Guide*

Ability to override certain global scanning and event monitoring settings

Data Insight now enables you to define custom values per Collector node for the following settings:

- Throttling thresholds for NetApp devices
- FPolicy safeguard settings for 7-mode and Cluster-Mode

You can configure the custom settings on the **Data Insight Servers** > **Advance Settings** page on the Management Console.

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

Support for Enterprise Vault 12.0

Data Insight now supports the data management use cases using Enterprise Vault 12.0.

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 *Veritas Data Insight User's Guide*.

Since 5.0

Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 *Veritas 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 Veritas Data Insight components

These requirements are generic and applicable when you do not plan to use the classification feature.

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

Table 2-1 Minimum system requirements for Veritas 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. ■ 32GB RAM ■ 16 CPU cores

Table 2-1 Minimum system requirements for Veritas 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 6.0 update 3 or higher, or version 7.0. The operating system must be 64- bit. only. ■ 32GB RAM ■ 16 CPU cores
Collector worker node	■ Windows Server 2008, or 2008 R2; 64-bit Windows Server 2012 or 2012 R2. The operating system must be 64-bit. ■ 8GB RAM ■ 4 CPU cores
Self-Service Portal node	■ Windows Server 2008, 2008 R2, 2012, 2012 R2. The operating system must be 64-bit. ■ 8GB RAM ■ 4 CPU cores
Windows File Server agent node	■ Windows Server 2008, 2008 R2, 2012 or 2012 R2. The operating system should be 64-bit ■ 4GB RAM ■ 2 CPU cores **Note:** For Windows 2003 OR 32-bit Windows 2008, use Data Insight Windows File Server Agent version 4.5 in backward compatibility mode.
SharePoint web service	Microsoft SharePoint 2007, SharePoint 2010, SharePoint 2013, or SharePoint 2016

See "System requirements for classification components" on page 33.

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

System requirements for classification components

Table 2-2 lists the recommended system requirements for classification components.

Note: Veritas recommends that you deploy classification service on a standalone server.

Table 2-2 Recommended system requirements for classification components

Component	If classification is enabled	If Smart Classification is enabled
Management Server	■ Windows Server 2008 or 2008 R2, 2012 or 2012 R2. The operating system must be 64-bit. ■ 16GB RAM ■ 8 CPU cores	■ Windows Server 2008 or 2008 R2, 2012 or 2012 R2. The operating system must be 64-bit. ■ 128GB RAM **Note:** Provision additional 2 MB space per million paths. ■ 32 CPU cores ■ 200 GB of free disk space for temporary files which are created and deleted during the classification process.
Indexer worker node	■ Windows Server 2008 or 2008 R2, 2012 or 2012 R2. The operating system must be 64-bit. **Note:** If classification role is assigned to Indexer and Collector node, then ensure that the operating system is Windows Server 2012 R2. ■ 16GB RAM ■ 8 CPU cores	■ Windows Server 2008 or 2008 R2, 2012 or 2012 R2. The operating system must be 64-bit. Red Hat Enterprise Linux version 6.0 update 3 or higher, or version 7.0; 64-bit only. ■ 128GB RAM **Note:** Provision additional 2 MB space per million paths. ■ 32 CPU cores ■ 200 GB of free disk space for temporary files which are created and deleted during the classification process.

Table 2-2 Recommended system requirements for classification components *(continued)*

Component	If classification is enabled	If Smart Classification is enabled
Collector worker node	■ Windows Server 2008, or 2008 R2; 64-bit Windows Server 2012 or 2012 R2. The operating system must be 64-bit. **Note:** If classification role is assigned, then ensure that the operating system is Windows Server 2012 R2. ■ 8GB RAM ■ 4 CPU cores	Same as when classification is enabled.
Classification Server	■ Windows Server 2012 R2. The operating system must be 64-bit. ■ 32GB RAM ■ 16 CPU cores	Same as when classification is enabled.

Note: In case of smaller deployments that have less than 10 million files or folders per share, the Smart Classification functionality requires 32GB RAM and 16 CPU cores. The requirements are determined based on the tests performed on our internal setups.

List of ports

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

Table 2-3 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

Table 2-3 List of default ports *(continued)*

Component	Default Port
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 NetApp 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
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

Table 2-3 List of default ports *(continued)*

Component	Default Port
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
Classification Server	Communication service, HTTPS port 8383 Standard RPC ports 139 and 445 DataInsightConfig, service port 8282 DataInsightVICServer, service port 8989

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

Operating system requirements

Table 2-4 provides an overview of Veritas Data Insight operating system requirements:

Table 2-4 Veritas Data Insight operating system requirements

Operating system supported	Notes
Windows Server 2008	Windows Server 2008 (64-bit) Windows Server 2008 R2 (64-bit)
Windows Server 2012	Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit)
Red Hat Enterprise Linux	Version 6.0 update 3 or later Version 7 Only 64 bit packages are supported.

Table 2-4 Veritas Data Insight operating system requirements *(continued)*

Operating system supported	Notes
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: For 32-bit Windows File Server 2008, install Windows File Server agent version 4.5, which is compatible with Data Insight 6.0. However, due to security considerations, certain manual steps should be performed on the 4.5 agents. This ensures that the agent continues to seamlessly work with the latest Data Insight version. For more information, see the *Veritas Data Insight Installation Guide*.

Web server version

Veritas Data Insight uses Apache Tomcat 7.0.77.

Supported browsers

Table 2-5 provides an overview of the browser support for Veritas Data Insight

Table 2-5 Veritas Data Insight Supported browsers

Browser	Versions
Internet Explorer	Version 11
Mozilla Firefox	Version 45.9 or higher
Google Chrome	Version 58.0.3029.110 or higher
Microsoft Edge	Version 21.10540 or higher

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

Supported file servers and platforms

Table 2-6 lists the Network Attached Storage (NAS) devices and SharePoint platforms that Data Insight supports.

Table 2-6 Supported file servers and platforms

Device	Version
Hitachi NAS	Hitachi NAS 12.x
NetApp ONTAP 7-Mode	Version 7.3.5 or higher
NetApp ONTAP Cluster-Mode	CIFS - ONTAP 8.2.x or higher NFS - ONTAP 8.2.3 or higher and ONTAP 8.3.1 or higher
EMC	EMC Celerra version 5.6.45 or higher
	EMC Isilon OneFS version 7.1.0.6 or higher
	VNX version 7.1.71.1 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:** For Windows 2008 32-bit, use Data Insight Windows Filer Server Agent version 4.5 in backward compatibility mode.
Veritas File System (VxFS) server	6.0.1 or higher, configured in standalone or clustered mode using Cluster Server (VCS) **Note:** For VCS support, Clustered File System (CFS) is not supported.
Microsoft SharePoint	Microsoft SharePoint Server 2007 Microsoft SharePoint Server 2010 Microsoft SharePoint Server 2013 Microsoft SharePoint Server 2016
Box (Cloud-based content management platform)	-
Symantec Data Loss Prevention (DLP)	Versions 12.0.1, 12.5, 14.0, 14.5, 14.6, and 14.6 MP1 **Note:** Data Insight 6.0 does not support Box integration with DLP 14.6 and 14.6 MP1.

Table 2-6 Supported file servers and platforms *(continued)*

Device	Version
Enterprise Vault	Versions 11.0, 11.0.1, 12.0, and 12.1

Note the following:

- Veritas strongly recommends that you upgrade your NetApp filer to the latest available firmware. Veritas 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 the following volume/qtree styles:

  - NTFS and Mixed for CIFS protocol.
  - UNIX and Mixed for NFS protocol on 7-mode NetApp filers only.
  - NFS exports on the NetApp cluster.
- For all supported versions of EMC Celerra/VNX and EMC Isilon, Data Insight supports only CIFS protocol over NTFS. Data Insight supports Common Event Enabler (CEE), version 8.2 or higher. Data Insight still supports the older version of CEE and VEE, but Veritas 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.

Parallel scanner limitations

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

- Parallel scanner does not support incremental scan. Only full scans are supported.
- Parallel scanner cannot be run for the NFS shares.
- Parallel scanner does not support filtering out shares based on the **Exclude Rules** configuration.
- Parallel scanner does not support throttling of parallel scans for NetApp 7-mode and Cluster-Mode file servers.
- The **Scan History** sub-tab on the **Scanning** dashboard does not display the historical details of a parallel scan.
- The scanning throughput is not displayed for the parallel scanner on the **In-Progress Scans** page.
- For Windows File Server agents version older than 5.2, the parallel scanner cannot be executed. Even if it is configured, the single thread scan runs.

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.

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'.
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

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

Context	Limitation
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.
- If filer is added using data LIF, then scanning of local user on the clustered NetApp cluster is not supported.

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.
- Scanning of local user and groups on Hitachi NAS device 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.

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.

Share or site collections on disabled filers or Web applications are displayed in charts

When a filer or a Web application is disabled, monitoring for all the shares on that filer stops. The shares and site collections on the disabled filers and Web applications are not scanned and not monitored for accesses and should not be included in the calculations for the scanning dashboard.

However, currently the shares and site collections for a disabled filer or Web application are being included in the charts on the **Settings** > **Scanning** > **Overview** page.

Disabled share or site collections are reported on scanning dashboard

When a share or a site collection is deleted from a filer or SharePoint server, a backend process disables that share in Data Insight configuration. The scanning dashboard must not include these shares in the counts shown on the **Settings** > **Scanning** tab. However currently the disabled shares and site collections are reported on the scanning dashboard.

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.

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.

Incorrect icon displayed in the reports wizard

When a SharePoint path is added using *paths.csv*, the report creation wizard shows the directory icon instead of the site icon.

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.

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.

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**.

Domain filter does not work as expected in some cases

If you have configured many domains in Data Insight, the domain filter does not display all configured domains.

Workaround

The domain filter field supports the auto-complete feature. Enter part of the domain name to get a list of matching domains

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.

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.

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.

Display name for users appears blank

If the display name is not specified for a user in the directory service, a blank space is displayed for the user in the tree-view panel and on the Overview page of the **Workspace** tab.

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.

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.

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.

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 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.

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.

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.

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.

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 "\".

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.

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.

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.

When using a CSV file to upload paths to reports, a red cross appears for the paths

Data Insight fails to recognize certain paths in the CSV file, and displays a red cross mark for the paths in the Selected Data panel of the report configuration wizard. However, these paths are successfully uploaded.

Workaround

In the CSV file, specify the pathname with a comma followed by the input type. For example, `http://sharepoint1/sites/Marketing,SiteCollection`. This enables Data Insight to classify the paths based on the input type.

For the supported input types, see the *Veritas Data Insight User's Guide*.

For more information about the issue, see https://www.veritas.com/support/en_US/article.000107668.

Data Insight implicitly adds the groupType Active Directory attribute

If a group custom attribute with name ‘groupType’ is configured, then after upgrade to 5.2, the attribute will be deleted since Data Insightimplicitly adds the groupType Active Directory attribute.

SharePoint paths filtered as a part of Scanner exclude rule are marked as deleted and not displayed on UI

SharePoint paths that are being filtered as a part of a Scanner exclude rule and have any activity on them, appear as expected in the **Audit Logs** view. However, after the activity, on the next scan, these paths are marked as deleted and are no longer displayed on the **Workspace** > **Data Sources** view.

Permission change event missing in Audit Logs after upgrade from 4.5.3

After you upgrade from Data Insight version 4.5.x to 5.2, the permission change event does not appear in the **Audit Logs** view. This is due to an upgrade defect.

This behaviour is only observed if you have migrated from Data Insight version 4.5.x and have indices which were created prior to 5.0. However, all indices that are created in 5.0 or later versions will not be impacted.

Active user count for Ownership Confirmation workflows not displayed on Portal UI

The active user count for Ownership Confirmation workflows is not displayed in case of filers or web application on the Portal UI.

Re-insert variable name when configuring permission remediation after upgrading from version 4.5.x to 5.2

A typo in the variable name **${Recommendation_text}** which is used in the email notification body when configuring permission remediation settings (**Settings** > **Permissions** > **Remediation**) is now fixed.

If you have used the variable, you must manually change it after you upgrade from Data Insight 4.5.x to 5.2 to receive permission recommendations .

Sometimes the sensitive file and other columns do not display the correct count

In the **Workspace** > **Data** list page, the **Sensitive File** column and other columns display incorrect information because the classification tags selected in the left-hand side filters are ignored while displaying the counts. However, the list of paths is filtered correctly.

Reports cannot be searched using comma separated labels

When searching for reports, the search does not support the use of comma separated labels.

The classification status of certain paths invariably appears to be in in-progress state

On the **Settings** > **Classification** > **Requests** page, you may observe that for certain classification requests the status continues to appear as in-progress. This issue may occur in the following scenarios:

- When shares or site collections are deleted, after their paths are submitted for classification then the request continues to be in the in-progress state.
- If a Collector responsible for a data source is changed after a classification request is submitted, then the classification is abruptly stalled and the corresponding request continues to remain in the in-progress state.
  To avoid this issue, Veritas recommends that before altering a Collector, ensure that all the requests which the Collector is processing are complete.
- If the Collector associated with a Box account is not serving as a Classification Server for fetching content, then the request status continues to show as in-progress.

Paths with special characters cannot be classified

The classification feature does not support the paths that have angular brackets (<>) as part of their name. Hence, such paths are not classified.

An error is reported during content scan of Box

During the content scan of Box, the following error is reported:

```
User must accept the terms and conditions.
```

Workaround: To override this issue, log on to the owner's user account on https://www.box.com/, and accept the terms and conditions on the license agreement window when prompted.

Status of the classification request invariably remains in the pending state

On Windows 2008, the classification request submitted through on-demand classification approach persists to be in the pending state. This issue is observed

because 64-bit dynamic-link library (DLL) version is incompatible with the system configuration.

Workaround:

To resolve this issue

1. Apply the updates for Visual C++ 2013 and Visual C++ Redistributable Package that is available at:
   - https://connect.microsoft.com/000001d-illegal-instruction-on-msvcr120-log-0x2d3-on-x64
   - https://support.microsoft.com/fix-programs-that-are-built-in-visual-c-2013-crash-with-illegal-instruction-exception
2. From the `%WinDir%\System32` folder on your machine, copy `msvcr120.dll` and `msvcp120.dl` and replace it with the equivalents in the `C:\Program Files\DataInsight\bin`.

Files and folders do not inherit the Custodian assignment

Custodian is assigned at device level. When a device is migrated to another Indexer, then the assignment may not apply to the subfiles and subfolders within that device.

LIF associated with a share is not considered on upgrading Data Insight

If Logical Interface (LIF) is configured after the shares are added, then the configuration does not take effect when Data Insight is upgraded from 5.x to 6.0 version.

Workaround:

To resolve this issue, reconfigure the LIF

1. Log on to Data Insight Management Console.
2. Click **Settings** > **Filers**.
3. Click the filer for which you want to reconfigure LIF.
4. On the filer details page, click **Edit** to open the Edit page.
5. In the **File System Scanning** > **Use CIFS Data LIF hostname for scanning (optional)** field, delete the host name.
6. Click **Save**.
7. Repeat step 3 and 5. In the **Use CIFS Data LIF hostname for scanning (optional)** field, enter the host name and click **Save**.

Discrepancy in the count of paths that failed classification

Sometimes the count of paths that failed classification is different in the **Classification** > **Requests** > **Download failed paths**, and the count displayed in the **Classification** > **Requests** > **Failed Files** column. This issue may occur when the paths are deleted or invalid.

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, Veritas 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.

Paths having double quotes are not added when using CSV method

The workflow and report wizards allow paths on data sources to be uploaded using CSV. But, if any of the paths in the CSV have double quotes (for example, \\filer1\share1\foo\bar”kkk.txt), that path will not be uploaded for the report or workflow configuration.

Empty metadata tag name and value not supported

If the metadata tags have blank name or value in the CSV file, then Data Insight faces issues when parsing the file and can cause the `idxwriter.exe` to fail.

Issue with report output on file group selection when configuring reports

When you select a file group during report configuration and run a report, the report returns data for the specified file group’s name as well as file group names matching substrings within the file group’s name. For example, if you run a report where you have configured the report’s file group as **Email Files**, the report returns data for the file group **Email Files** as well as the file group **Email**.

This happens for the following reports:

- Consumption by File Group
- Consumption by File Group and Owner
- Inactive data by File Group

Chapter 5

Fixed issues

This chapter includes the following topics:

Fixed issues in 6.0

This section describes the issues fixed in release 6.0. The fixed issues are referenced by the Veritas incident number.

Table 5-1 Fixed issues in 6.0

Incident number	Description
DI-3050	The configuration database does not get updated with the Data Loss Protection policy information due to an SQLite error.
DI-3124	The `idxwriter.exe` process becomes unresponsive on Indexer when a blank tag name and tag value are provided in the CSV file.
DI-3136	In the event of no active users, the **Inactive Users** report might become unresponsive.

Table 5-1 Fixed issues in 6.0 *(continued)*

Incident number	Description
DI-3532	Documentation has been updated to reflect the revised label name of a setting **Maximum scans to run in parallel from this collector** that appears on the **Settings** > **Data Insight Servers** > **Advanced settings** page.
DI-3542	Data Insight ignores audit events from the Isilon cluster due to case mismatch between the filer name and the name configured in the Isilon Management console.
DI-3575	The filters on the **Settings** > **Cloud Sources** page are not operational.
SDIOCFT-163	In Data Insight 5.2 version, the Health Audit and Activity reports fail to generate in a CSV format.
SDIOCFT-196	Documentation has been updated to include the `-q` switch to command in the procedure to silently upgrade the Windows File Server Agent using response files.
SDIOCFT-209	On upgrading Data Insight 5.0 to 5.1 version, the **Workspace** > **Dashboard** > **Alerts** list view appears blank.
SDIOCFT-210	When SharePoint with input type as WebApp is configured for anonymous access, the audit data for SharePoint sites fail to get populated.
SDIOCFT-233	Scanning of LDAP takes longer than expected because users and groups without the UidNumber and GidNumber are scanned, and added to the user database.
SDIOCFT-240	Test scanning of NFS shares on cDOT filers fails with error code 53.
SDIOCFT-266	On upgrading to Data Insight 5.2, certain columns in the **msu_summary** table of the dashboard database are not populated.
SDIOCFT-272	The `idxwriter` process becomes unresponsive when the SharePoint site scan is in progress. As a result, the Index database is not updated leading to inaccurate data on the Management Console.
SDIOCFT-275	When SID contains a colon (:), the user index files move to the `indexer/err` folder without being processed.

Table 5-1 Fixed issues in 6.0 *(continued)*

Incident number	Description
SDIOCFT-298	When a full scan is run on a Box path, negative throughput is displayed.
SDIOCFT-304	The **User/Group Permissions** report displays incorrect permission inheritance for the Administrators group.
SDIOCFT-328	Whenever the **User Activity Deviation** policy is violated, an alert email is sent to the users. However, the hyperlink in this email is not resolvable.

Fixed issues in 5.2

The fixed issues are referenced by the Veritas incident number.

Table 5-2 Fixed issues after 5.2

Incident number	Description
3874079	The keystore file password fails to get encrypted when the `configdb` command is executed.
3870959	On upgrading to Data Insight 5.0, the `idxwriter.exe` process intermittently becomes unresponsive.
3898834	The Portal node observes a low disk space on `C:\` drive because the TEMP folder is populated with MIME files.
3895269	The migration of Indexer is suspended on different shares.
3893886	Data Insight fails to report the permissions assigned to the users who are migrated to a new Windows domain, but still have access to the resources that are present in the old domain.
3880897	When the **Path Permission** report is executed, the report output does not list the members of a group.

Table 5-2 Fixed issues after 5.2 *(continued)*

Incident number	Description
3894788	Data Insight fails to generate report output when the **Number of records** field is set to a number higher than 1000000.
3894042	The DataInsightFPolicyCmod service abruptly terminates on the collectors.
3893121	The help documentation incorrectly states that **Activity Deviation Policy** is configured based on DFS.
3893748	Scan fails for the paths that contain apostrophe or single quotations marks.
3891107	While reassigning filers to a new Collector, the **Test Credentials** field reports an error when the file system is scanned. The error occurs due to a failure while testing the availability of network connection between the Collector worker node and the control station, or the credentials were invalid.
3891339	In the **Inactive Data by File Group** report, the size of all the file groups is displayed as 0 in the **On Disk Size** column.
3889696	The query daemon abruptly terminates due to incomplete Userrisk_Dashboard.db.
3880703	While creating a DLP Incident Remediation Workflow template, Data Insight fails to populate the Smart Response rules that are configured in DLP using the DLP Response Rule Listing Service API.
3879746	Data Insight fails to discover the SharePoint web application on which most of the sites are blocked. This is caused because the `sharepoint_util.exe` is abruptly terminated.
3880179	In the **Path Permission** reports, the **Inherited from path** column displays redundant forward slash (/), which results in incorrect inheritance to directories that do not exist in the path.

Table 5-2 Fixed issues after 5.2 *(continued)*

Incident number	Description
3879491	On upgrading to Data Insight 5.0.2, the **Dashboard** and **Workspace** tab takes longer to display content.
3877576	On Data Insight 5.0.1, the option to configure notifications is not available when **All Physical Resources** is selected to choose all the data resources while configuring a **User Activity Deviation** policy.
3877349	Scan fails for certain large sized SharePoint sites.
3875438	An integration issue was observed during the mapping of file servers on Data Insight and Enterprise Vault because of the mismatch of case in the host names. As a result, the archive option is not available.
3876235	On upgrading to Data Insight 5.0, the index writer process becomes unresponsive when it consumes the scan files.
DI-1813	The **Data Aging** report incorrectly computes the data aging time based on the last accessed timestamp instead of the last modified timestamp. This behavior is observed even when the **Use modified time instead of access time for aging criteria** check box is selected while configuring the report.
3876127	For the **Path Permissions** report with ACL configured, the output report displays incorrect details or duplicate paths without the inheritance details in the **Inherited From Path** column.
3873784	The `Controlpoint.exe` abruptly terminates and fails to create a tag file for the storage device.

Table 5-2 Fixed issues after 5.2 *(continued)*

Incident number	Description
3873757	For certain DFS paths that appear within the DLP Incident Remediation page, the DFS mapping link fails to resolve to the Data Insight Console page.
3871773	The events logged for Hitachi NAS (HNAS) file server are not displayed in the chronological order. As it has to re-open the index.db for every instance and insert an event in the new database.
3811502	For SharePoint paths, the **Remove Permissions** option is not available in the **Workspace** > **Permissions** tab.
DI-1375	The HNAS audit events are not logged chronologically. As a result, the index writer process frequently re-opens the index.db.
DI-1363	Permission change events are not logged for NFS and SharePoint paths.
DI-1361	When the data is exported from the Data Insight Servers list page, the **Updates** column shows incorrect information.
DI-1356	The **Data Aging** report output contains multiple duplicate reports when the same custodian is explicitly assigned the nested paths.
DI-1315	A mismatch is observed between data displayed in the **Inferred Owner** report output and on the **User Activity** > **Summary** sub-tab.
DI-1309	In the Google Chrome web browser, the file group information is lost for the **Consumption by File Group** report and **Inactive Data by File Group** report.
DI-1302	The `CloudDeviceAuditJob` process must not run on the Windows file server node.

Table 5-2 Fixed issues after 5.2 *(continued)*

Incident number	Description
3750376	When the inheritance flag of a SharePoint web application path is modified, the permission change event is not logged for that path.
3829816	Data Insight does not monitor filers with longer file extensions.
3874613	The health check of NetApp filers fails despite of the filer being healthy.
DI-1340	The filer heath for NetApp C-Mode falsely displays a warning message stating that the event monitoring has stopped. However, the event monitoring works as expected.
3867218	For certain files, the file size is not displayed in the Workspace views.
3872038	The `activityidx.exe` and `idxwriter.exe` processes utilize a high amount of memory.
3872325	An error was reported while generating the report output file. This error may have occurred due to insufficient disk space.
3872924	In the Entitlement Review workflow, certain paths incorrectly display the status as failed.
3873076	In the **Consumption by file group** report, the files with extension as .xls are incorrectly grouped as media files.
3873854	On upgrading to Data Insight 5.1, certain NetApp C-Mode filers are not discovered.
3877155	Entitlement Review workflow or report does not allow a concurrent selection of a folder and a subfolder in the same report or workflow.
3877555	Migration process failed due to duplicate records in the idx_migration.db.

Table 5-2 Fixed issues after 5.2 *(continued)*

Incident number	Description
3877686	The help documentation does not contain instructions to install the SSL certificates on NetApp C-Mode.
3877854	Users with limited access are able to access other restricted shares by navigating through the breadcrumbs.
3879807	The **Overview** page does not display the latest access information leading to a mismatch of information in the **Overview** page and the **Workspace** > **Audit Logs** tab.
3880172	When using a CSV file to upload SharePoint subsites, a red cross (x) mark appears on the data elements.
3882132	The audit files that are not indexed are stored in the `$data/inbox` folder on the Indexer. When the number of these files grows, they get accumulated in the Indexer's backlog affecting its performance.
3891346	The `userindex.exe` abruptly terminates when parsing large number of `usermaps.txt` files.
3894787	Data Insight remediation process and Enterprise Vault File System Archiving (FSA) integration for a DFS path fails due to a mismatch in the file name format exercised by both the products.
3895473	For certain NetApp CIFS with UNIX protocols, the scan fails with system error 1003.
3896408	On the **Monitored Shares** list page for a filer, a message displays the number of shares that are excluded in the share discovery. However, the message does not provide the recent list of excluded shares. It includes shares that were excluded in the past but are now monitored.

Table 5-2 Fixed issues after 5.2 *(continued)*

Incident number	Description
3898395	On NetApp OnTap 9.0, Data Insight fails to establish a communication with Clustered Data ONTAP (cDOT) filers. The failure occurs because by default, the HTTP mode is turned off in NetApp OnTap 9.0.
DI-2913	When the `UserRiskJob` process fails, the **Users** tab does not show any user.
DI-2328	During the computation of the risk score, the total MSU count does not include the site collections.
DI-3037	When most of the shares or site collections have same names, the **Data Custodian Summary** report may become unresponsive.

Fixed issues in 5.1.1

This section describes the issues fixed in Release 5.1.1. The fixed issues are referenced by the Veritas incident number.

Table 5-3 Fixed issues in 5.1.1

Incident number	Description
3853590	The health check up for the newly added NetApp Filers shows that the Fpolicy service is not running.
3863476	SharePoint site collection scan fails for large sites due to timeout.
3870958	Index Writer process crashes while trying to process scan metadata files when maximum amount of events in memory threshold is reached.
3871772	Events from HNAS are not found in a chronological time order.
3871843	The file size is not displayed in the workspace for some files.

Table 5-3 Fixed issues in 5.1.1 *(continued)*

Incident number	Description
3871922	When the Path Permissions report is generated to get the Access Control list, it contains incorrect values for **Inherited From Path** column.
3872037	The `activityidx.exe` process is taking up a large amount of memory.
3872523	`USERINDEX.exe` process crashes under some scenarios.
3872923	The Entitlement workflow shows paths as failed in case of DFS paths if the prefix of a path is a repetition.
3873053	The Path Permissions report output incorrectly contains a forward slash in the **Inherited from path** field.
3873075	Files with .xls extension (Microsoft Excel files) are displayed in the media files category in a **Consumption for File Group** report.
3873719	Data Insight fails to discover NetApp Cluster-Mode Storage Virtual Machines (SVMs) in scenarios when no logical interfaces (LIFs) are configured.
3873756	DFS File location in Data Leak Prevention console unable to link to file in Data Insight console. Non-DFS file paths work properly.
3873783	`Controlpoint.exe` crashes and does not generate a tag file.
3875069	Filer mappings are case sensitive in Data Insight 5.1 which cause issues with Enterprise Vault integration.
3875457	Steps on configuring SSL on NetAPP cluster mode filer are missing from the Administration Guide.
3875843	The notification configuration is missing when you select **All Physical Resources** on the **Data Selection** tab of the User Activity Deviation Policy wizard.
3876153	Migration inserted duplicate record into the idx_migration database causing it to fail.
3878299	The GUI response on the **Workspace** tab is slow after upgrading to Data Insight 5.0.2.

Table 5-3 Fixed issues in 5.1.1 *(continued)*

Incident number	Description
3878876	When creating a DLP Incident Remediation Workflow template, Data Insight fails to fetch the DLP Smart Response list.
3879745	Sharepoint discovery fails as `sharepoint_uticlient.exe` crashes when a high number of sites are blocked.

Fixed issues in 5.0.1

The fixed issues are referenced by the Veritas incident number.

Table 5-4 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.

Table 5-4 Fixed issues after 5.0 *(continued)*

Incident number	Description
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.
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 5-5 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.
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 Veritas Data Insight:

- *Veritas Data Insight Installation Guide*
- *Veritas Data Insight Administrator's Guide*
- *Veritas 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 Veritas 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.