Veritas Data Insight Release Notes

6.1.4

November 2019

VERITAS™

Veritas Data Insight Release Notes

Documentation version: .0

PN:

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive.
Santa Clara, CA 95054

http://www.veritas.com

.

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

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

For information about our support offerings, you can visit our website at the following URL:

www.veritas.com/support

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

Contacting Technical Support

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

www.veritas.com/support

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Technical Support
  - Recent software configuration changes and network changes

Licensing and registration

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

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/support

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

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

Support agreement resources

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

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

Contents

Chapter 1

Overview of this release

This chapter includes the following topics:

About 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.

  Data Insight also allows the classification of images. The classification of images is facilitated by a software called Tesseract that is responsible for text extraction from the images. Tesseract needs to be installed on the classification node for classifying contents in an image.

- 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.

See “In 6.1.4” on page 17.

See “In 6.1.2” on page 18.

See “In 6.1.1” on page 18.

See “In 6.1” on page 20.

In 6.1.4

The following features or enhancements are now available in Data Insight 6.1.4.

Support for Optical Character Recognition (OCR) during classification

Data Insight now supports OCR to help you classify image files.

For more information on enabling OCR and initiating classification, see the *Veritas Data Insight Administrator's Guide* and *Veritas Data Insight Classification Guide.*

Support for delete action natively using the Data Insight user interface

Data Insight provides the ability to delete unwanted files from CIFS devices. You can delete old and inactive files from the Data Insight Management console. The delete functionality is disabled by default. You can enable the same from **Settings** > **Remediation** > **Data Management** > **Delete Files**.

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

Enhanced functionality for security auditing

Data Insight now allows enhanced auditing of all important activities from the UI. For example, changes in server or filer configurations, addition of new Data Insight users, and so on.

Customized email notification for reports

You can customize email notifications for reports. For example, if you need to include instructions or company disclaimers on the notification email, Data Insight allows you to change the body or structure of the email.

Enhanced whitelist and blacklist policies

Data Insight now allows you to set real-time alerts to check access and usage of whitelisted and blacklisted users.

Note: Ensure that you update any scripts that you have created containing policy names, to reflect the updated names of the whitelist and blacklist policies - Real-time Data Activity User Whitelist-based policy and Real-time Data Activity User Blacklist-based policy.

Entitlement reporting for SharePoint Online

Data Insight now supports the ability to view the permissions for Microsoft SharePoint Online as a content source and to allow generating permission reports like

Entitlement Review. This in turn helps Admins understand and analyze the access permissions to sensitive data.

Throttling support for parallel scanning

Data Insight now supports throttling for parallel scanning for NetApp 7-mode and NetApp Cluster-mode filers. This helps to avoid overloading the file server during peak sessions.

In 6.1.2

The following features or enhancements are now available in Data Insight 6.1.2.

Support for classification server pool to balance the classification workload

Every data source is associated with a Collector, and every Collector is associated with a Classification server. The mapping of the Collector to the classification server decides, to which classification server the request should be sent. When you submit paths for classification, a Data Insight server with a Collector role fans out the file paths to the assigned classification server which classifies those files. In earlier releases of Data Insight, every classification server is associated to one Collector node. Now with the introduction of classification server pool feature in Data Insight 6.1.2, the master classification server is assigned various slave servers. The master classification server distributes the classification requests to these slaves, which helps to balance the workload on the classification server and increases the overall throughput.

For more information on classification server pool, see the *Veritas Data Insight Administrator's Guide*

Proliferation support in Data Insight 6.1.2

Data Insight 6.1.2 supports the following new versions and features:

- Data Insight minifilter driver is now signed by Microsoft and supports Secure Boot on supported Windows Server operating systems.
- Enterprise Vault 12.3.
- Hitachi NAS 12.x.
- Dell EMC Unity 4.2 or 4.3.

In 6.1.1

The following features and enhancements are available in Data Insight 6.1.1.

Support for gathering analytics for EMC Unity VSA

Data Insight now supports the monitoring of the Dell EMC Unity VSA storage platform and provides visibility, forensics, and the ability to manage data for the data store.

For information on configuring Dell EMC Unity VSA and credentials required to monitor it, see the *Veritas Data Insight Administrator's Guide*.

Ability to share reports with other Data Insight users

You can now share reports that you have created with other Data Insight users. This functionality enables you to allow users to run reports that are already created by the Report Administrator and other users, which reduces the overhead of having to create reports for the same resources.

Following conditions apply to reports that are shared among Data Insight users:

- Users with any Data Insight role can configure sharing of their reports. Other users can only view the reports that are created by them and other shared reports.
- You can only run the reports created and shared by other users. Data Insight does not allow you to edit or delete reports shared by other users.
- When you run a shared report, that is created for all configured resources, the report is generated only for the resources (filers/cloud data sources) that you have permissions on.
- If you run a shared report that is created for resources on which you do not have permissions, the instance of the report run will fail.

You can configure sharing of reports when you create a report. For more information, see *Veritas Data Insight User's Guide*.

Proxy support for Microsoft OneDrive and SharePoint Online

You can now configure Microsoft OneDrive and SharePoint Online to use proxy servers to route requests from Data Insight to the cloud data source. You must configure your organization's proxy server to connect to the following destination URLs:

- https://graph.microsoft.com/
- https://login.microsoftonline.com
- https://outlook.office365.com

For information on configuring Microsoft OneDrive and SharePoint Online monitoring, see the *Veritas Data Insight Administrator's Guide*.

Support for classify post-processing action in DQL reports

The classify post-processing action is now supported in DQL reports. You must edit the `report.properties` file to enable classification as the post-processing action.

In 6.1

The following features and enhancements are available in Data Insight 6.1.

Enhanced support for new data sources

With the proliferation of Microsoft Office 365, Data Insight has now widened its support for the following new data sources:

- SharePoint Online
- Microsoft OneDrive cloud accounts
- OpenText Documentum

Support for three new additional data sources provides visibility, forensics, and the ability to manage data on these new data sources. In Release 6.1, Data Insight supports the discovery, scan and audit of these data sources. However, Data Insight does not fetch permissions for these data sources, and audit information for Documentum data sources.

For information on configuring the monitoring of these data sources and for a detailed list of support limitations, see the *Veritas Data Insight Administrator's Guide*.

Ability to customize user roles in Data Insight

Data Insight now provides the ability to have a more granular role-based access control by allowing you to customize user roles to ensure separation of duties for more regulated workloads. The ability to customize roles also ensures that there is a clear separation between users who manage access to the Data Insight application and the users who consume the data.

Data Insight now lets you create the following new user roles to manage user access and do the basic administration tasks:

- User Administrator - This role can add, delete, and modify the roles assigned to Data Insight users. The role has access only to **Settings** > **Data Insight Users** and not to any other tabs.
- Workflow Administrator - This role has access to all sub-tabs under the **Workflows** tab, but does not have access to the other sections of the Data Insight Management Console.

For information on configuring the user roles, see the *Veritas Data Insight Administrator's Guide*.

Licensing changes for cloud data sources

Distribution of a trial cloud license is discontinued from Release 6.1 onwards. You must purchase a cloud license to continue using Data Insight functionality. Contact the Veritas Customer Care for purchase of a cloud license.

An add-on cloud license has been introduced to monitor the data that resides in your cloud environment such as Box, SharePoint Online, and Microsoft OneDrive. On applying a valid cloud license, you can add cloud sources for monitoring, discover and scan data, and view the metadata and audit information.

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

Support for Windows Server 2016

Data Insight now supports the latest Windows Server 2016 operating system for all Data Insight server components and to install the Windows File Server agent.

Support for classification tags in Data Insight policies

Data Insight now supports raising of alerts for activities that are performed on all sensitive data, including the files classified by Veritas Information Classifier (VIC). The enhancement enables you to detect malicious activity and take remediation action to prevent data breaches, as appropriate.

Note that the Real-time Sensitive Data Activity policy does not raise alerts for files classified by VIC.

For more information about configuring real-time polices for raising alerts, see the *Veritas Data Insight Administrator's Guide*.

Support for Enterprise Vault 12.2

Data Insight now integrates with Enterprise Vault 12.2 to enable the archiving of old and inactive data on CIFS shares.

New Data Insight Query Language (DQL) templates to detect ransomware

The newly introduced DQL templates to detect ransomware enable you to detect the files that are exploited by ransomware. In the event of an attack, ransomware uses a vulnerable user account to encrypt and rename files to which the user has access. With timely detection of the ransomware attack, you can take appropriate remediation action to minimize the risk, and respond to the encryptions that might be underway.

Using the ransomware DQL templates in conjunction with your inputs, you can fetch the following information of the files that exist on the monitored data source:

- Collect the count of write and rename activities performed on files in a data source within 24 hours. If the count is higher than the configured threshold, the files are determined as infected and the users are notified. The threshold value is the number of write and rename activities that you permit on a data source within 24 hours.
- Get the count of files that are renamed by per user, and have unique file extensions.
- Fetch the top-level directories in the share or equivalent, and the number of write and rename activities performed in each of these directories by per user.
- List all the files that are created in the last 24 hours by per user. Use this query to identify files created by a risky user.
- List the files that contain a specific string in the file name. For example, when a ransomware appends a unique extension to the encrypted files.
- Enumerate the duplicates of the potentially malicious executables residing on your system.

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

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, 2008 R2, 2012, 2012 R2, or 2016. 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, 2008 R2, 2012, 2012 R2, or 2016. 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. ■ 32GB RAM ■ 16 CPU cores
Collector worker node	■ Windows Server 2008, 2008 R2, 2012, 2012 R2, or 2016. The operating system must be 64-bit. ■ 8GB RAM ■ 4 CPU cores **Note:** For OneDrive, SharePoint Online, and Documentum data sources, the Collector must be running on Windows Server 2012 R2 or 2016.
Self-Service Portal node	■ Windows Server 2008, 2008 R2, 2012, 2012 R2, or 2016. The operating system must be 64-bit. ■ 8GB RAM ■ 4 CPU cores
Windows File Server agent node	■ Windows Server 2008, 2008 R2, 2012, 2012 R2, or 2016. The operating system should be 64-bit ■ 4GB RAM ■ 2 CPU cores
SharePoint web service	Microsoft SharePoint 2010, SharePoint 2013, SharePoint 2016, or SharePoint 2019

See "System requirements for classification components" on page 24.

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 minimum recommended system requirements for classification components.

Table 2-2 Minimum 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, and 2016. The operating system must be 64-bit. ■ 16GB RAM ■ 8 CPU cores	■ Windows Server 2008 or 2008 R2, 2012 or 2012 R2, and 2016. 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 during the classification process.
Indexer worker node	■ Windows Server 2008 or 2008 R2, 2012 or 2012 R2, and 2016. 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 or later. ■ 16GB RAM ■ 8 CPU cores	■ Windows Server 2008 or 2008 R2, 2012 or 2012 R2, and 2016. 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 during the classification process.

Table 2-2 Minimum 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, and 2016. The operating system must be 64-bit. **Note:** If classification role is assigned, then ensure that the operating system is Windows Server 2012 R2 or later. ■ 8GB RAM ■ 4 CPU cores	Same as when classification is enabled.
Classification Server	■ Windows Server 2012 R2, and 2016. The operating system must be 64-bit. ■ 32GB RAM ■ 16 CPU cores	Same as when classification is enabled.
Windows File Server agent node	■ Windows Server 2008, 2008 R2, 2012, 2012 R2, or 2016. The operating system must be 64-bit. ■ 8GB RAM ■ 4 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
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.

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

Component	Default Port
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)
OneDrive	DataInsightOneDrive service, port 9090
Documentum	DataInsightCMIS service, port 9191
SharePoint Online	DataInsightSPOnline service, port 9292
Symantec Data Loss Prevention (DLP)	HTTPS port 443
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)
Windows Server 2016	Windows Server 2016 (64-bit)
Red Hat Enterprise Linux	Version 6.0 update 3 or later Version 7 or later Only 64-bit packages are supported.
VMware	64-bit Windows 2008 64-bit Windows 2012 64-bit Windows 2016 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.

Web server version

Veritas Data Insight uses Apache Tomcat 7.0.90.

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	11
Mozilla Firefox	62.0 or higher
Google Chrome	69.0.3497.100 or higher

Table 2-5 Veritas Data Insight Supported browsers *(continued)*

Browser	Versions
Microsoft Edge	42.17134.1.0 or higher

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

Supported data sources and platforms

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

Table 2-6 Supported data sources and platforms

Device	Version
Hitachi NAS	Hitachi NAS 12.x
NetApp ONTAP 7-Mode	7.3.5 or higher
NetApp ONTAP Cluster-Mode	CIFS - 8.2.x or higher NFS version 3 - ONTAP 8.2.3 or higher and ONTAP 8.3.1 or higher
EMC	EMC Celerra DART version 5.6.45 or higher
	EMC Isilon OneFS version 7.1.0.6 or higher
	VNX version 7.1.71.1 or higher
	Dell EMC Unity 4.2 or 4.3
	Unity VSA 11.0
Windows File Server	Windows Server 2008, or 2008 R2 64-bit Windows Server 2012, or 2012 R2 64 bit Windows Server 2016, 64-bit
Veritas File System (VxFS) server (NFS version 3)	6.1 or higher, configured in standalone or clustered mode using Cluster Server (VCS) **Note:** For VCS support, Clustered File System (CFS) is not supported.

Table 2-6 Supported data sources and platforms *(continued)*

Device	Version
Microsoft SharePoint	Microsoft SharePoint Server 2010 Microsoft SharePoint Server 2013 Microsoft SharePoint Server 2016 Microsoft SharePoint Server 2019
Box (Cloud-based content management platform)	-
Microsoft Office 365	SharePoint Online Microsoft OneDrive
OpenText Documentum	6.7

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.

Veritas Data Insight integrated solutions

Table 2-7 Veritas Data Insight integrated solutions

Product	Certified versions
Symantec Data Loss Prevention (DLP)	12.0.1, 12.5, 14.0, 14.5, 14.6, 14.6 MP1, 14.6 MP2, 15.0, 15.1, 15.1 MP1, and 15.5.
Enterprise Vault	11.0, 11.0.1, 12.0, 12.1, 12.2, and 12.3.
Veritas Information Classifier (VIC)	2.0, 2.1.4.1, 2.1.4.2, 2.1.5, 2.1.6, 2.1.7, 2.2.0, 2.2.1, and 2.2.2

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.
- 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.
- Support for scanning of circular or cyclic symbolic links is not available.
- Support for scanning junction-based paths is not available.

Windows File Server support

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

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.

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.

SharePoint Online and SharePoint On-prem devices not listed under User or Group-centric Permissions view

In the **Workspace** > **Users** or **Groups** > **Permissions** view, the **Devices with permissions** filter will only list those web applications (SharePoint On-prem) and accounts (SharePoint Online) for which the user or group has direct or indirect permissions at the root level of the site collection.

The Activity Pattern Map does not capture the activities performed on folders for cloud sources

In case of cloud sources, the **Workspace** > **Data Source** > **Audit Logs** > **Activity Pattern Map** does not illustrate the activities that are performed at folder level. Although, the table on the Audit log view captures these activities. However, the Activity Pattern Map displays the activities performed at file level.

Data Insight captures audit events only for document library and its child paths

The audit events performed before the document library level in the SharePoint hierarchy are not captured.

Incorrect scan status is displayed for Documentum paths

Even though the repositories are scanned, the Workspace > Shares view incorrectly displays that the repositories are not scanned.

Documentum paths with same names are not considered as different paths

The **Workspace** and **Reports** tab fails to display paths that have same names with different font case. Additionally, in subsequent scans, indexing for these paths also fails.

Broken permission inheritance icon is displayed for Documentum and OneDrive paths

Even though permissions are not supported for Documentum and OneDrive paths, a broken permission inheritance (lock) icon is displayed for certain paths.

Permissions are not supported for certain data sources

As scan does not fetch the permissions for Documentum and OneDrive paths, the permission change events are not captured.

Some data sources do not honor the settings configured under Settings > Scanning and Event monitoring

The SharePoint Online, Documentum, and OneDrive paths do not honor the scan and event monitoring settings.

Security event not monitored for certain devices

The audit logs and report outputs for SharePoint Online and OneDrive paths do not capture the security events.

Certain paths cannot be uploaded using CSV file

The paths for OneDrive, Documentum, and SharePoint Online data sources cannot be uploaded using a CSV file for creating reports, workflows, and policies.

Audit events are not collected for site collections containing UTF-8 characters

Data Insight does not collect the audit events for site collections in SharePoint Online accounts that contain UTF-8 characters in the site collection's name field.

I18N characters in site collections are not supported

In the **Add New Site Collection** dialog box, site collections having i18N characters in their names are not available for selection.

Incorrect information in report outputs and Workspace tab about Documentum paths

The **Workspace** tab and report output may display Documentum paths even after they are deleted. This is because audit information and reconfirmation scan for Documentum paths is not supported.

The Scan History tab does not display throughput for certain data sources

The **Scan Status** > **Scan History** page does not capture scan data throughput for the OneDrive, SharePoint Online, and Documentum data sources.

Audit events for OneDrive and SharePoint Online data sources take longer to get displayed on the Console

Data Insight collects audit logs from OneDrive and SharePoint Online data sources when audit recording is enabled in the Office 365 Security and Compliance Center. After an event takes place on the data source, it takes up to 30 minutes for the event to get logged in the audit entry log of Office 365. This behavior is emulated in Data Insight, which results in latency.

For more information about how audit logging happens in Office 365, see:

https://support.office.com/en-us/article/Search-the-audit-log-in-the-Office-365-Security-Compliance-Center

The Go-to bar does not return search results for Documentum paths

In case of Documentum data source, the Go-to bar on the Workspace does not honor search strings. Therefore, when you search a Documentum path in the Go-to bar, the associated data fails to get populated on 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.

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.

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. 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.

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.

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.

Newly added Enterprise Vault servers 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.

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.

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.

Attempt to add/upgrade license results in showing success message regardless of validity of the license file

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.

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.

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 “\”.

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.

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 Insight implicitly 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.

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.

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.

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.

No real-time alerts are generated for BOX and OneDrive paths

In case of BOX and OneDrive paths, no alerts are generated for Real-time Data Activity User Whitelist-based and Real-time Data Activity User Blacklist-based policies.

Excel Services Viewers group is displayed as an account level group in Sharepoint Online

Membership information for the group `Excel Services Viewers` of Sharepoint Online is not shown correctly on **Workspace** and **Permission** reports.

License uploading results in an empty file named "upload"

On uploading a license using Google Chrome web browser into Data Insight for the first time, an empty file named `upload` gets downloaded.

Tesseract needs to be uninstalled manually upon Data Insight uninstallation

When Data Insight is uninstalled, Tesseract does not get uninstalled automatically. It has to be uninstalled manually.

Inaccurate Entitlement Review report output for SharePoint Online and SharePoint On-prem devices

For SharePoint Online and SharePoint On-prem devices, when a parent and child group have permissions on the same path the Entitlement Review report output returns inaccurate permissions.

Group Change Impact Analysis report does not work for SharePoint Online and SharePoint On-prem devices

The Group Change Impact Analysis report fails if it is run for SharePoint Online and SharePoint On-prem devices.

The `mxuserwriter.exe` process fails due to over consumption of memory

In Data Insight 6.0 and later versions, the `mxuserwriter.exe` consumes exponential memory when computing user risk score for very large shares. As a result, it runs out of memory and fails.

Workaround

If this issue is experienced frequently and if the User Risk feature for calculating the user risk score is not used, disable the `UserRiskJob` and `UserRiskMergeJob`.

Collector process became unresponsive on rare instances

Rare instances of the Collector process becoming unresponsive were observed, resulting in the audit files incorrectly being moved to the `data/collector/err` folder.

Workaround

Move the audit files from the `data/collector/err` folder back to the `data/collector` folder, and execute the Collector process again.

Scanner infinitely scans circular symlinks

When scanning a share that contains symbolic link that is circular or cyclic in nature, the scanner ends up scanning the share infinitely.

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.

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 < 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.

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.

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 information 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,

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.

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 6.1.4

This section describes the issues fixed in release 6.1.4. The fixed issues are referenced by the Veritas incident number.

Table 5-1 Fixed issues in 6.1.4

Incident number	Description
CFT-1458	HNAS audits were throwing errors instead of a warning message. The logging pattern was changed to `INFO`.
CFT-1465	Due to Error code 19, `Queryd.exe` was crashing during some operations, like viewing the data in the **Workspace** or while running a DQL report. There was a fix allocation of 80 characters for domain id in case of a `user-exists` query. This has been fixed now.

Table 5-1 Fixed issues in 6.1.4 *(continued)*

Incident number	Description
CFT-1522	`Queryd.exe` was crashing because of users attempting to delete already-deleted SharePoint Site Collections before the UI was refreshed. There was a fix allocation of 80 characters for domain id in case of a `user-exists` query. This has been fixed now.
CFT-1549	Due to `Queryd.exe` crashing, customers experienced stoppage in the `DataInsightConfig` service and received the message, `error getting data` while attempting to view data in the **Workspace**. There was a fix allocation of 80 characters for domain id in case of a `user-exists` query. This has been fixed now.
CFT-1565	SharePoint sites were not being removed from Data Insight when deleted. This issue is now fixed.
CFT-1618	When a user selected the **Data Modifier** check box, the header of the output column in the **Data Aging** Report was incorrect. This issue is now fixed.
CFT-1620	After an Active Directory scan, users were not visible in the **Workspace** if the `disable.dossier` attribute was set to True. This issue is now fixed.
CFT-1621	When List Permission was given to authenticated users, Data Insight read that as a `Read and Execute and List` Permission under **Effective Permission**. This behaviour resulted misguided information being given to the user. This issue is now fixed.
CFT-1678	Custom DQL reports being run to get list of tagged file came back completely blank as `Queryd.exe` was crashing during the operation. There was a fix allocation of 80 characters for domain id in case of a `user-exists` query. This has been fixed now.
CFT-1693	Excessive logs, for OneDrive, caused the log file to grow beyond the expected space. This issue is now fixed.

Table 5-1 Fixed issues in 6.1.4 *(continued)*

Incident number	Description
CFT-1709	`Queryd.exe` crashed while accessing one share of a Clustered Winnas Filer via **Workspace**. There was a fix allocation of 80 characters for domain id in case of a `user-exists` query. This has been fixed now.
CFT-1759	An update in the `nc_name` using the Edit option resulted in the disappearing of the original name without providing any error message. This issue is now fixed.
CFT-1769	Users were getting email notifications from Box regarding massive data downloaded under Data Insight. This issue is now fixed.
CFT-1778	Data user's `Last Accessed` attribute had an incorrect format in the DLP incident. This issue is now fixed.
CFT-1791	FPolicyCMod service crashed regularly. This issue is now fixed.
CFT-1820	`Queryd.exe` crashed when accessing a share of a Winnas Filer with agent attempts to archive to Enterprise Vault. There was a fix allocation of 80 characters for domain id in case of a `user-exists` query. This has been fixed now.
CFT-1840	Users could not add custodians to Microsoft SharePoint Site's subfolders after deleting existing custodian. This issue is now fixed.
CFT-1854	Classification was hung across a couple of data centers for some specific files. This issue is now fixed.

Fixed issues in 6.1.3

This section describes the issues fixed in release 6.1.3. The fixed issues are referenced by the Veritas incident number.

Table 5-2 Fixed issues in 6.1.3

Incident number	Description
CFT-1215	Share discovery failed on EMC Isilon filers. This issue was caused if the length of the password used for share discovery was greater than or equal to 32; the password was getting decoded and threw a hexadecimal error as it tried to decode a non-encoded password. DecoderException for password usage for share discovery is now fixed.
CFT-1245	Share discovery failed on the NetApp cDOT filer. This issue was caused if the length of the password used for share discovery was greater than or equal to 32; the password was getting decoded and threw a hexadecimal error as it tried to decode a non-encoded password. DecoderException for password usage for share discovery is now fixed.
CFT-1271	Data Aging report fetches data age from last known activity/ events, that is, the last known read/write. The default value for the last known activity date is set to 1/1/2000 when data of the last known activity/ events is not available to Data Insight. Due to this, the Data Aging report indicated that data is older than 42 months. This issue was observed for all SharePoint versions only. This issue is now fixed. The Data Aging report now considers the last modified time to calculate the age if access time doesn't exist. If the access time information is available through audit events, then the report considers the access time only.
CFT-1305	Users with special characters in the login name experienced failure while generating reports. This issue is now fixed.
CFT-1389	Mapping of Box users to Active Directory users failed. This issue is now fixed.
CFT-1400	Box Authorization, in case of proxy, failed after upgrading to Data Insight 6.1.2. This issue is now fixed.
CFT-1422	Box scan throughput dropped post upgrading to 6.1.2 and applying DI6.12HF1 (CFT-1184). This issue is now fixed.

Table 5-2 Fixed issues in 6.1.3 *(continued)*

Incident number	Description
CFT-1447	The pop-up dialog box during OneDrive authorization incorrectly showed "Box". This issue is now fixed.
CFT-1454	Data Insight was not able to collect audit events for the Microsoft OneDrive data source. This was caused due to reasons such as the computer locale is set to the one which contains a date separator other than '/'. This issue is now fixed.
CFT-1475	Parallel scanning failed after upgrading to Data Insight 6.1.2.
CFT-1494	Local user scan failed on NetApp C-mode filers if domain user credentials were used to run the job. This issue is now fixed.

Fixed issues in 6.1.2

This section describes the issues fixed in release 6.1.2. The fixed issues are referenced by the Veritas incident number.

Table 5-3 Fixed issues in 6.1.2

Incident number	Description
CFT-776	Data Insight was unable to process the scanned data from Box if the same files or directories were renamed multiple times between the two scans.
CFT-934	The query daemon became unresponsive after the discovery of a large number of site collections
CFT-967	After installing Data Insight 6.1.1, an attempt to add OneDrive as a cloud source failed because OneDrive could not be authorized through proxy.
CFT-1001	The customers using the Hitachi NAS device experience a number of HNAS audit-events-missed errors, which wrongly reflect as errors caused in Data Insight.

Table 5-3 Fixed issues in 6.1.2 *(continued)*

Incident number	Description
CFT-1021	When generating the Entitlement Review Report, the custodians receive emails even if Do not email custodians check-box is selected on the report configuration page.
CFT-1052	Audit consuming failed because the `CollectorJob` wrongfully created a number of 0 kb `Audit_fs` files on the Collector node, which could not be handled properly by the `Pre-IndexerJob` on the Indexer node.
CFT-1075	When Secure Boot was enabled on Windows Server 2016 filer, Data Insight filter driver failed to load, which caused disruption in data monitoring and reporting.
CFT-1117	Scheduled reports in Data Insight were not executing after applying 6.1 RP1.
CFT-1132	After upgrading to Data Insight 6.1.1, the Entitlement Review workflow failed immediately after being submitted.
CFT-1136	Classification content fetching safeguard did not work if the folder containing the classification metadata and the Data Insight data directory were on separate disk drives
CFT-1150	All Data Insight reports failed to generate if the user's login name contained a special character.

Fixed issues in 6.1.1

This section describes the issues fixed in release 6.1.1. The fixed issues are referenced by the Veritas incident number.

Table 5-4 Fixed issues in 6.1.1

Incident number	Description
CFT-347	Scanning the SharePoint environment failed due to timeout issues. This issue is now fixed.
CFT-494	The URL in the alert email generated when a user creates an Activity Deviation Policy was incorrect. This issue is now fixed. The alert email now reflects the correct URL.

Table 5-4 Fixed issues in 6.1.1 *(continued)*

Incident number	Description
CFT-580	Selecting the **Go to Data Insight** option in Data Loss Prevention (DLP) did not open the correct page. This issue is now fixed. The **Go to Data Insight** option now redirects to the Data Insight console as expected.
CFT-626	Upgrading Data Insight from version 5.2 to version 6.1 caused incremental scans to fail with exit code 1. This issue is now fixed.
CFT-675	Running the `execute.exe` binary in interactive mode from the command prompt exposed the password. This issue is now fixed.
CFT-683	The **Time Taken** column on the **Classification Requests** page displayed the duration taken to complete a request that included any pause schedule enabled for the associated classification server. This issue is now fixed. A tool tip to this effect has now been added for clarification.
CFT-693	Upgrading Veritas Information Classifier (VIC) to version 2.1.2 fixes the KVKK/Turkey PII policy false negative issues.
CFT-720	Running the `execute.exe` binary within Data Insight caused the process to hang on Windows 2012 R2 platform. This issue is now fixed.
CFT-753	The `vic_output.log` file kept increasing in size consuming an exorbitant amount of space until all VIC processes were shutdown or the file was removed. This issue is now fixed.
CFT-800	Worker nodes did not display the correct version on the Data Insight console after the Management Server or collector were upgraded to version 6.1. This issue is now fixed.
CFT-836	Apache Tomcat Web server version has been upgraded. Data Insight now uses Apache Tomcat 7.0.82.

Fixed issues in 6.1

This section describes the issues fixed in release 6.1. The fixed issues are referenced by the Veritas incident number.

Table 5-5 Fixed issues in 6.1

Incident number	Description
CFT-359	The `LocalUserScanJob` job failed to fetch local user or group information for cluster mode NetApp devices. As a result, incorrect user information is displayed on the Data Insight Console and in report outputs.
CFT-369	On upgrading from Data Insight 5.0 RP2 to 5.2 using silent upgrade method, certain Windows File Server devices did not get upgraded. To resolve this issue, users had to manually run the UpgradeData.exe.
CFT-372	Due to a security vulnerability, non-administrator users were able to view data sources that Data Insight monitors. Ideally, the data source listing page should only be visible to users having administrative permissions.
CFT-377	Processing of large set of parameters specified in the exclude rules field utilizes high amount of resources. Due to this, a delay is observed when a user attempts to log on to the Data Insight Console. Even the **Settings** tab took longer time to populate content.
CFT-390	On upgrading to Data Insight 5.2, user cannot import paths and assign custodians while creating a DLP Incident Remediation Workflow using the sample CSV template.
CFT-392	The Data Loss Prevention (DLP) Console displayed incorrect inferred owner information as it fetched most active users along with the excluded users. With 6.1, this issue has been fixed such that the DLP Console now displays the inferred owner similar to Data InsightConsole and ignores the excluded user.
CFT-423	In Windows 2008 R2, on applying security update (KB3139914), the report output could not be copied to a network share.
CFT-433	Scanning of a SharePoint web application failed due to an invalid character present in the site's name, title, or description field.
CFT-436	The error logging codes have been revised to ensure that user receives email notifications only for genuinely severe issues.

Table 5-5 Fixed issues in 6.1 *(continued)*

Incident number	Description
CFT-441	Data Insight 6.0 documentation has been updated to describe privileges required for automatic discovery of CIFS shares on EMC Isilon clusters.
CFT-466	Importing of custodians using the sample CSV fails as Data Insight could not parse the first row in the CSV file. This is because the first row consists of the column headers which Data Insight incorrectly assumes to be user names.
CFT-468	Data Insight Console becomes unresponsive when a user attempts to delete or disable a SharePoint web application or site collection that includes an invalid character. This issue is caused because Data Insight is not able to parse the character.

Appendix A

Documentation errata

This appendix includes the following topics:

Errata for the Data Insight Admin Guide

The Description column of Table 22-2 in the *Add/Edit OneDrive Account* section of the *Veritas Data Insight 6.1.2 Administrator's Guide* reads:

Select this check box to enable event monitoring on the OneDrive account. You must manually enable auditing in the Office 365 Admin Center to enable Data Insight to collect audit logs for the OneDrive account.

From the OneDrive Credentials drop-down, select the credentials of a user with SharePoint administrator role which has been assigned the View-Only Audit Logs privilege.

It should instead read:

Select this check box to enable event monitoring on the OneDrive account. You must manually enable auditing in the Office 365 Admin Center to enable Data Insight to collect audit logs for the OneDrive account.

From the OneDrive Credentials drop-down, select the credentials of a user with SharePoint administrator role which has been assigned the View-Only Audit Logs and Audit Logs privilege.

Note: The user used for auditing of the OneDrive account should be set to **username@DOMAIN.com** instead of **DOMAIN\username**. Microsoft supports the User Principal Name (UPN) for connecting to a remote Exchange server.

Appendix B

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*
- *Veritas Data Insight Software Compatibility List*

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.

Data Insight Support

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

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.