Symantec Data Insight Release Notes

4.5.1

October 2014

Symantec Data Insight 4.5.1 Release Notes

Documentation version: 4.5.1 Rev 0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Technical Support 3

Chapter 1 Overview of this release 14

About Symantec Data Insight 14
What's new in Symantec Data Insight 16
Since 4.5.1 16
Since 4.5 19
Since 4.0RP1 25
Since 4.0 31
Since 3.0.1 36

Chapter 2 System requirements 40

System requirements for Symantec Data Insight components 40
List of ports 41
Operating system requirements 43
Supported file servers and platforms 44
Supported browsers 46
Web server version 46

Chapter 3 Software limitations 47

Scanner limitations 47
Windows File Server support 48
Console limitations 48
Expression builder limitation 48
Special characters not supported in NFS paths 48
Size on disk not displayed 48
Filer rename not supported 48
Social Network Map limitation 49
Report configuration limitation in Path Permission reports 49
Known limitations for NetApp Cluster-Mode support 49
Known limitations for Hitachi NAS support 49

Chapter 4 Known Issues 50

Console display issues 50
Changing zoom level in Internet Explorer affects Data Insight interface 50
Incorrect status of scans displayed 50
Scan status not displayed 50
Toolbar error 51
Emailing contents of a table 51
Incorrect status of folder displayed 51
Incorrect information in Inactive Directories report 51
Active Directory scan reporting error 51
Report for deleted paths not supported 51
Error fetching data displayed 51
Unwanted access events displayed 52
Data Insight cannot capture the IP addresses for events on certain platforms 52
Incorrect scale displayed for file activity graph 52
Error displayed on session time out 52
Deleting a DFS server causes error 52
Report includes only physical paths 52
Progress bar display error 53
Error fetching permissions data 53
Inconsistency between permissions view of Windows and Data Insight 53
Error fetching data displayed 53
Sequence of spaces in share names not supported 53
Error in inactive users information 54
Newly added files or shares do not automatically appear in the Folders tab 54
Change in date range not reflected when you navigate to other tabs 54
Renamed file displays in GUI with original name 54
Alphabetical sorting of shares 55
Error when logging in to the Data Insight Management Console 55
Pop-up at site collection level 55
Overlaping tooltips 55
Search bar error 55
Deleted paths visible in the GUI 55
Symantec Data Insight Management Console help issues 55
SharePoint create event displayed incorrectly 56
Custom attribute widget issue 56

Incorrect disk space computation displayed on Workspace tab for NFS shares 56
Share or site collections on disabled filers or Web applications are displayed in charts 56
Disabled share or site collections are reported on scanning dashboard 56
Error displayed while adding a VxFS filer 57
Scan status incorrectly displayed on scanning dashboard 57
Issue regarding the broken search bar 57
Incorrect icon displayed in the reports wizard 57
Audit Logs tab shows incorrect path for CREATE events on SharePoint 2007 server 57
Dashboard tab shows incorrect path for deleted filers and Web applications 58
Issue with Select Resource pop-up for user permissions 58
Newly added Enterprise Vault server are not displayed in the Filer Mapping page 58
Duplicate entry for the Enterprise Vault server is allowed 58
Dashboard report fails, if filers and domains are not configured in Data Insight 58
Access Details for Paths report fails with invalid path 59
Social Network Map fails to render for the shares that have large number of active users 59
Folders with explicit ACEs are not flagged with lock icon 59
Data Insight fails to check user permission on shares 59
Mismatch between permission entries displayed in Windows interface and Data Insight console 59
Incorrect file size may be displayed for archived files in an EMC Celerra file server 60
EVFolderPoint.xml file may be displayed in the Workspace 60
Incorrect recommendation count displayed 60
Permission recommendations for renamed folders may not be accurate 60
The Consumption by File Group report fails 60
Broken membership in case of local groups leads to misleading permissions 60
Built-in groups are not excluded for Path Permissions reports 61
Some filers are not auto-mapped for wrongly configured Enterprise Vault servers 61
Social Network Maps are not displayed when tabs are restored 61

Exception is displayed while trying to archive a batch of file using the Enterprise Vault 61
Domain filter does not work as expected in some cases 62
Add EV Server dialog remains open 62
DFS share mapping and its configuration is not removed when the corresponding physical share is deleted 62
Hidden columns are displayed in reports in the .csv format 62
In Data Inventory reports, the DLP policy names are not displayed against the files 62
Delay in rendering of some views 63
Pagination issue on the Summary pane for permission recommendation 63
Successful partial scan does not change failed consolidated scan status 63
Inconsistency in scan status observed from the Workspace and the Scan History view 63
The inferred owner name in ContextMap view and User Activity summary page do not match 63
The Inactive Subfolders tab displays deleted paths 63
Incorrect product update recommendations may be shown for Indexer nodes 64
The Scan Errors page does not display an error 64
Selected attribute continues to be displayed in drop-down 64
Display name does not appear properly in Firefox browsers 64
Pipe character in share name not supported 64
Display name for users appears blank 64
Default retention category displayed even when data is not selected 65
Enabling or disabling of audits for site collections may take longer time 65
Issue with size filter on the Data Insight dashboard 65
Data Inventory Reports may produce incorrect output in certain cases 65
Custom action with Expand Folder option fails to expand non-CIFS paths 66
Issue with display of active file size in ContextMap 66
ContextMap information may not display in some cases 66
On Internet Explorer 9, the user edge for Social Network map is not highlighted when the user is clicked 66
Users not deleted after deleting Active Directory server 66
Add/Upgrade license succeeds irrespective of the license file type 67
Creating non-domain saved credentials 67

Error message may appear while applying recommendations 67
The End Time column for the audit logs may turn blank, when the page is refreshed 67
The disabled users may be displayed as enabled when you view recommendations on a path 67
Data Insight SharePoint Agent may encounter an exception while fetching attributes 67
Large time gap between the report execution and the report download. 68
Report log displays warning message for step-progress 68
The value of the custodian name variable name may not be displayed correctly 68
Canceling the Ownership Confirmation workflow creation may cause a draft to be saved 68
Sorting by paths or custodians does not work in the Ownership Confirmation workflow creation wizard. 68
A workflow that is in submitted state cannot be canceled. 69
The count of resources to which a custodian is assigned is displayed incorrectly. 69
For Entitlement Review workflows there is no provision to display the excluded users and groups. 69
Custodian assignment may take a long time to complete. 69
Permission remediation emails may display incorrect values for some variables 69
The search filter on the workflow creation wizard may not function 69
The sort functionality does not work for NFS paths in the Self-Service portal. 70
DQL reports fail if the queries contain non-English characters. 70
SharePoint Web applications hierarchies under the Workspace tab may be displayed incorrectly 70
Incorrect positioning of page breaks may appear in the report outputs 70
Exceptions in the webserver logs while running reports with containers 70
Multi-byte characters are incorrectly rendered in the HTML or CSV report outputs 70
Incorrect member count displayed 71
Custodian assignment may fail when the Assign by owner method option is selected 71

Incorrect information may be displayed in the report progress view 71
The custom attribute column name in a DQL query does not ignore case 71
The principal name for a data owner may not be displayed in a DQL report. 71
Custom actions displayed as disabled 72
Email sent for Entitlement Review workflow even for failed paths 72
Issue creating an Ownership Confirmation workflow if custodian is assigned at web application and site collection levels 72
Data management workflows fail in some cases 72
During report configuration the field specifying member count does not accept inputs 72
Activity graph displays incorrect data 73
SID History displayed as parent group 73
Ownership Confirmation workflow does not work for certain NFS paths 73
Column displaying exclude pattern for web applications missing in Health Audit report 73
Management Console may fail to authenticate when you upgrade Data Insight from version 4.5 to 4.5.1 74
Other Issues 74
Capacity Reports are generated for all filers irrespective for RBAC configuration 74
Events display error 74
Error in displaying selected result entry 74
Vfilers wrongly capture open events on folder paths as events on file paths 75
Deletion of a Collector node fails even after disassociating all filers 75
User with Product Administrator role unable to edit share 75
Report creation error 75
Unable to restore tabs 75
Scan resync does not work for certain scenarios 76
Security event not monitored 76
Create event not captured 76
Container and directory service name limitation 76
Incorrect default schedule displayed 76
Special characters in NFS paths cause NFS scanner to fail 76
Error when saving user name, container name, and directory service names 76
Incorrect default schedule displayed 76

Error in deleting report output 77
Custom attributes already selected displayed again for selection 77
Custom attribute discovery does not work in certain scenarios 77
Port number for LDAP directory server required 77
Exclamation mark in user name not supported 77
Duplicate policy name issue 77
A security event does not change last modified by value for a destination folder 78
The job scheduling settings require modification 78
The scan history graph does not display the data as expected 78
Limited support in the Entitlement Review report 78
Issue with launching installer from mapped drive 78
Issue with same NFS export and CIFS share name 78
The scanned shares and the total scan count does not match 79
Access Summary for Paths report displays all active users of a share 79
Limited support for claims-based authenticated Web applications for SharePoint 79
Push-installation on Windows 2003, 64-bit Collectors fails 79
Inactive users view and report does not consider share-level permissions 80
Attempt to archive a file using the Enterprise Vault fails 80
Group Change Analysis report does not report loss of access if users part of built-in groups 80
Filer Mapping page does not reflect the changes in the settings for the Enterprise Vault servers 80
Generic device issue 80
Wildcard support limitation 81
Connection to the Enterprise Vault server fails if host name is used 81
Multi-byte characters not supported 81
Stop DataInsightFPolicy service before shutting down a Collector node 81
Scan-rsync fails to update the folder size 81
Data Insight cannot retrieve retention categories with certain characters 81
Issue with assigning NIS and LDAP users as custodians 82
Disabled icon not displayed 82
Issue with computing custodian for root site collection 82

Size of parent folder is not updated 82
Issue with pagination on Audit Logs view 82
Issue with LHS filter 82
`mxcustodian.exe` is slow in case of large number of paths 83
Certain reports do not honor the global data owner policy 83
Incorrect informaton displayed for migrated user 83
Issue with workflow creation if services on Indexer are down 83
UTF8 characters may not render correctly in report outputs in CSV format 83
Records Classification workflow fails to archive paths using Enterprise Vault for certain devices 84
Unable to get Create event for Hitachi NAS devices in some cases 84
Issue with the new membership object in DQL 85
Empty multi-value column not supported 84
Issue with the new membership object in DQL 85

Chapter 5 Fixed issues in this release 86

Fixed issues in 4.5.1 86

Appendix A Getting help 94

Using the product documentation 94
Contacting Symantec 94
Symantec Data Insight Support 94
Using the support Web site 95
Subscribing to email notification service 95
Accessing telephone support 95

Chapter 1

Overview of this release

This chapter includes the following topics:

- About Symantec Data Insight
- What's new in Symantec Data Insight

About Symantec Data Insight

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

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

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

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

Data Insight provides the following information:

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

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

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

- Data owner identification
  Data Insight enables rule-based inference of data owners based on actual usage. Data owner information may not reflect the responsible party. The responsible party or data owner can be a line manager in the business unit, the head of a department, or an information security officer. Symantec Data Insight provides the information to tie the most active user of a file to a manager or responsible party for remediation steps.
- Data custodian identification
  Data Insight enables the assignment of one or more users as custodians of a data repository. Custodian tagging is typically used to determine the person responsible for remediation. The assigned custodian need not have made any accesses on the files and folders. In addition to the physical paths, you can also assign custodians on DFS paths.
- Data leak investigation
  In the event of a data leak, you may want to know who saw a particular file. On the Symantec Data Insight Management Server, you can view detailed information and an audit history of who accessed the data.
- Locate at-risk data
  Data Insight enables organizations to find which shares or folders have overly permissive access rights. Organizations can use this data to prioritize risk-reduction efforts such as the discovery of sensitive data or a review of permissions (or access control rights) to limit access to only those individuals who have a business need.
- Manage inactive data
  Data Insight enables better data governance by letting you archive inactive and orphan data using Symantec 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 recommendations

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

- Remediation using the Self-Service Portal
  Data owners and custodians can take remediation actions using the Self-Service portal. Custodians can log in to the Self-Service Portal to do the following:
  - View Data Loss Prevention (DLP) policy violations and remediate DLP incidents using Smart Response rules.
  - Review permission on resources and make recommendations to allow or revoke user access on resources.
  - Provide confirmation about whether the custodians indeed own the data resources that are assigned to them.
- Raise alerts
  You can configure policies to raise alerts when there is anomalous activity on sensitive data.

What's new in Symantec Data Insight

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

Since 4.5.1

Symantec Data Insight 4.5.1 includes the following new features and enhancements.

Support for Hitachi NAS file servers

Symantec Data Insight now supports monitoring storage devices running Hitachi NAS 12.x. Each Hitachi NAS (HNAS) file server can consist of several Enterprise Virtual Servers (EVS) with own IP addresses and file systems. Data Insight monitors the configured EVS and the shares residing on these virtual servers. For Hitachi NAS, you can monitor only the CIFS shares. Monitoring of NFS shares are not supported.

For information about configuring Hitachi NAS devices in Data Insight and credentials required to monitor them, see the *Symantec Data Insight Administrator's Guide*.

Support for Records Classification workflow

Data Insight introduces a new workflow that lets custodians use the Self-Service portal to mark sensitive documents as Record or No record. When a custodian marks a document as a record, it means that the file is important and must be retained for a legally mandated period. The workflow helps you classify files based on their business value and manage the life cycle of sensitive documents by applying data management rules to the classified data.

You can choose to archive the files marked as record and apply retention categories that define how long the files must be stored before being deleted. The files that are marked as record are retained based on the data classification policies that they violate.

If your organization uses Symantec Enterprise Vault™ to archive data, you can configure Data Insight to trigger automatic archive actions on the files that are marked as Record.

Availability of Data Activity User Blacklist-based policy

The Data Activity User Blacklist policy defines a blacklist of users based on their Active Directory custom attributes who should not access the selected shares or paths. You can create such a policy with multiple conditions with multiple values for the same custom attributes. If users who are included in the blacklist access the selected data Data Insight generates an alert.

For more details, refer *Symantec Data Insight Administrator's Guide* .

Ability to assign Portal role to a Management Server or a Collector node

In case of small deployments or POC environments, you can now use an existing Data Insight Management Server or a Collector node as the Self-Service Portal node. You must add the Portal role to the Data Insight server you want to use as the Portal node. You must ensure that you upgrade the node to which you want to add the Portal node to Release 4.5.1.

For more information about adding a Portal role to an existing server, see the *Symantec Data Insight Administrator's Guide*.

Ability of a Data Insight administrator to log in to the Self-Service Portal on behalf of a custodian

Data Insight now lets a Data Insight administrator log in to the Self-Service Portal on behalf of a custodian.

The administrator can log in to a workflow to debug problems or take actions on the custodian's behalf. The option to log in as custodian is not available if the workflow is complete or if the custodian has submitted his responses for further action for all assigned paths. Once an administrator logs in Data Insight sends a notification to the custodian that the administrator has logged in to a workflow on the behalf of the custodian.

DQL Enhancements

The following enhancements to DQL are available in this release:

- Added the new **Membership** object
  The DQL **Membership** object describes the details of the members of a group. A group member can be a user or another group. Using the membership table, you can write a DQL query to:
  - Get direct member users of a group.
  - Calculate the nested depths of member groups for any top-level group.
  - Calculate the direct parent group of a user or a group with respect to the top group.
- Added the **isdisabled** column to the following objects:
  - **device**
  - **msu**
- Added **odsize** and **file_count** columns to the following objects:
  - **path**
  - **dfspath**

For more details, refer to the *Symantec Data Insight Programmer's Reference Guide*.

Ability to cancel an ongoing filer migration

Data Insight now lets you cancel a filer migration operation which is in progress.

You can cancel only the ongoing migrations. Canceling a migration reverses all the changes affected by the migration operation. You cannot cancel a migration operation which has successfully completed.

New FPolicy safeguard settings provided for NetApp cluster mode file servers

Data Insight now lets you configure FPolicy safeguard settings for NetApp Cluster-mode file servers. Data Insight collects latency information from NetApp file servers. Data Insight can use this information to initiate safeguard mode, if latency of the file server increases above or falls below a certain level. When the safeguard is in effect, Data Insight drops its FPolicy connection to the filer. This ensures event collection does not put additional load on the file server in peak load conditions.

You can configure the FPolicy safeguard settings from the **Settings** > **Scanning and Event monitoring.** of the Management Console.

Ability to specify a pause schedule for auto-delete of audit events from SharePoint server

By default, every 12 hours, Data Insight automatically deletes the audit logs it receives from SharePoint servers.

You can now specify the hours of the day when auto-delete of audit events from SharePoint server should not be allowed. This feature can help you to avoid overloading the SharePoint servers during the peak hours.

Ability to view excluded shares or site collections from the details page of the monitored shares/site collections

You can now view the excluded shares or site collections from the **Monitored Shares**/**Monitored Site Collections** details pages. You can review the exclusion information before you decide to run a scan for a particular filer or a Web Application.

Since 4.5

Symantec Data Insight 4.5 includes the following new features and enhancements.

New Self-Service Portal to streamline the remediation process

The Self-Service Portal enables your central information security team to distribute remediation workflows directly to the custodians and data owners. It helps you engage the business data owners to drive remediation decisions and streamline the process.

You can create remediation workflows that can be submitted for action by custodians via the Portal. Once you start a workflow from the Data Insight console, the custodians receive an email notification with a link to the Self-Service Portal. The custodian can log in to the Portal, choose the configured remediation actions, and

submit the same for execution by the Data Loss Prevention Enforce Server or the Data Insight Management Server, depending on the type of workflow.

You can create workflows for the following remediation tasks.

- Entitlement Review - Review the user permissions on the folders that the custodians own and attest the permissions or suggest changes.
- DLP Incident Management - View policy violations and take action on the files that violate (DLP) policies without requiring access to the DLP Enforce Server administration console. The actions are Smart Response rules defined by DLP administrator. DLP uses the Smart Response rules to remediate the resources that violate configured DLP policies.
- Ownership Confirmation - Confirm the ownership of resources.

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

For information about using the Self-Service Portal, see the *Self-Service Portal Quick Reference Guide*.

Enhanced data governance for new platforms

Data Insight now supports the monitoring of NetApp Cluster-Mode, EMC Isilon, and Windows Server 2012 devices.

Data Insight uses a new Windows service called the DataInsightFpolicyCmode to monitor the NetApp Cluster-Mode ONTAP file servers. The service listens for TCP connections from the filers and receives events from the filers.

Data Insight uses the Common Event Enabler (CEE) version 6.1 or later that is installed on the Data Insight Collector or remote CAVA server to enable Data Insight to fetch access event information from the filer.

See “Supported file servers and platforms” on page 44.

For information about configuring these devices in Data Insight and credentials required to monitor them, see the *Symantec Data Insight Administrator's Guide*.

Analytics and visualization of Data Insight environment from the Console

Data Insight provides enhanced tracking of the topology, data processing, and disk space usage. You can now get a picture of performance of various Data Insight nodes deployed in your environment from the Management Console.

You can do the following:

- View charts that help you visualize backlog of files accumulating on the Data Insight nodes and view other performance statistics, such as the average CPU utilization, the average memory consumption, size of various folders, trends of backlog on nodes.

  You can use these statistics to identify performance issues on the servers, and change the appropriate setting to rectify the problem.
- Run jobs on remote Data Insight nodes from the Management Console. You can also view the status of the job and disable specific jobs from the Console.

For detailed description of the jobs that run as a part of various Data Insight services and configuring the server settings, see the *Symantec Data Insight Administrator's Guide*.

New Health Audit report

Data Insight now runs an automated Health Audit report daily at 5:00 A.M. The report captures high level information about the devices being monitored, the Data Insight servers, the directory services, and various other settings of your deployment and displays that in a consolidated PDF in the logs/health_audit folder on the Management Server. This report allows Symantec Support to quickly to identify and easily troubleshoot any issues in your environment.

Enhanced data owner computation

You can now exclude deleted or disabled users, or SIDs for which corresponding user information is not available in Data Insight (unresolved SIDs) from the computation of the global data owner policy.

Data Insight can still consider an excluded user as the data owner, if the user is the creator of the file, and no other non-excluded users have any access events on the file.

The exclusion of users when calculating the data owner, applies to both the data owner information displayed on the **Workspace** tab and to the Inferred Owner report. However, you can choose to override the exclusion at the time of creating the Inferred Owner report.

You can also assign the data owner computed based on the global policy as a custodian when you configure remediation workflows.

For more information about configuring a data owner policy, see the *Symantec Data Insight Administrator's Guide*.

Automated index migration

You can now migrate your storage devices to to a new Indexer directly from the Data Insight Management Console.

You can use the capability to visualize backlogs on the Indexer node, and if necessary, choose to migrate storage devices to other Indexer to help balance the load on the existing node.

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

Ability to assign a large number of custodians to data resources using the Console

You can now use the Custodian Manager feature to assign custodians to data resources in bulk. You can assign custodians simultaneously to multiple paths in the following two ways:

- Assign by CSV - Use a CSV file that contains the information about the paths and their corresponding custodians.
- Assign by owner method - Specify the criteria for computing the possible owner of the selected paths, and assign the computed owners as the custodians. You can either define the criteria for calculating data owners or use the default data owner policy for the computation.

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

DQL enhancements

The Data Insight Query Language (DQL) interface provides more flexible data extraction including an option to export DQL output as CSV, and a web-service interface for 3rd party and business process integration. The following enhancements to DQL are available in this release:

- Use a DQL query to read the content from a CSV file and use it as input arguments.

  You can now write DQL queries to read a CSV file and use its content as arguments in a query. This technique is useful when you need to specify a host of arguments using any of the list containment operators: IN or NOT IN.

  For example, you can rewrite the following query:

```
FROM device
GET name, id
IF name IN ("device_1", "device_2", "device_3",......"device_N" )
```

  With the query:

```
FROM device
GET name, id
IF name IN FILE("device_names.csv")
```

Where, `device_names.csv` is the CSV file which contains the arguments: "device_1", "device_2", "device_3",·····"device_N".

- Availability of the `iscircular` function.
  You can now use the `iscircular` function to determine if two groups are members of each other, thereby forming a loop.
  Consider the scenario where:
  - Group B is a direct member of Group A
  - Group B and Group C are direct members of each other.

  In this case, iscircular is 0 for Group A, and 1 for Group B and Group C.
- Availability of the web API specification for DQL.
  Data Insight now provides a web API for the DQL to allow third-party applications to submit DQL queries to Data Insight and fetch the results of the submitted query. The third-party web applications request information from Data Insight using HTTPS calls to the Data Insight Management Server.
- Availability of DQL queries templates.
  Data Insight now comes with built-in DQL queries, which you can use as templates. You can modify the content to suit your particular reporting needs. Additionally, you can create your own queries and save them to be used later as templates.
- Ability of DQL reports to generate output in the CSV format.
  You can now specify `.csv` output format for DQL reports.

History of migrated users available in Data Insight

Data Insight now uses the Windows SID-History attribute to store previous SIDs of users who have migrated from another domain. The SID-History feature is used to keep track of all previous SIDs of an object as it migrates from one domain to another.

The SID-History attribute helps Data Insight reduce the number of unresolved SIDs when it scans the directory service domains.

Deleted SIDs displayed in Data Insight

Data Insight can now detect deleted users and groups and it retains their information. This feature helps reduce the number of unresolved SIDs in Data Insight. However, Data Insight does not retain membership information for a deleted user or group.

The deleted users or groups are displayed with a different icon on the views in the **Workspace** tab.

Enhanced user reporting

Data Insight now provides you the following enhancements to help visualize user activity and access permissions:

- Differentiation between direct and indirect membership in **Workspace** views and in reports.
- Two new default domains have been added to improved user search. When Data Insight scans configured domains, it automatically adds the following domains:
  - The Unresolved SIDs domain contains all the SIDs or distinguished names of objects that Data Insight has no information about.
  - The MigratedSIDs domain is used to collect SIDs that are present in the SIDHistory of some user, but do not belong directly to any user in Data Insight.

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

Enhanced filter on user-centric views

The user and group-centric views on the **Workspace** tab have a new share selection filter that helps you effectively search for a selected user's or groups's activity across the environment.

The filter can be used to get an overview of the user's activity or permissions on configured storage devices. For example, on the **Workspace** > **User** > **Permissions** tab, you can view a user's permissions on configured devices in the selected domain.

Ability to view the granular progress of report execution

For certain reports types, you can now view granular progress of a report run.

Granular progress is displayed under the following tabs of the Report progress view panel:

- The **Overview** tab - Gives you the real-time feedback on steps for a report and the speed of execution. This information can help you to estimate the time remaining to generate a report.
- The **Details** tab - Lets you monitor the nodes involved in the execution of a report and the time consumed for executing the steps. This information can help you to identify the bottlenecks of report execution.

Documentation enhancements

- With this release, Symantec Data Insight documentation will be available on the SORT website (https://sort.symantec.com). Publication of the user documents to SORT will give you easy access to up-to-date product information between major releases.
- A new guide, the Self-Service Portal Quick Reference Guide is now part of the documentation set. The guide is aimed at giving an end-to-end workflow of configuring and using the new Self-Service Portal.

Since 4.0RP1

Symantec Data Insight 4.0RP1 includes the following new features and enhancements.

Ability to import sensitive files information through a .csv file

Data Insight pulls information about sensitive files in your storage environment from Symantec™ Data Loss Prevention (DLP).

Data Insight now provides you the ability to identify sensitive files in your storage environment using a .csv file even if you use a third-party application other than DLP. A scheduled Data Insight process reads the .csv file to retrieve the list of sensitive files from Data Insight.

To use a .csv file to classify sensitive files in Data Insight

1. Log in to the Data Insight Management Server.
2. Create a .csv file, in which each line indicates the path of the sensitive file and policy names which that particular file violates.

   For example, you have a file `/foo/bar/info.txt` which violates the policies Personal Information and Hipaa. And another file `/foo/ssn.pdf` which violates the policy “Personal Information” In this case, create .csv file should be as follows:

   data /foo/bar/info.txt,Personal Information, Hipaa /foo/ssn.pdf,Personal Information
3. Edit the dlp_db.conf file to add the following lines:

   ```
   dlp.csv.enabled=true

   external.file.path=<full path to the location of
   .csv file on Management Server>
   ```

   The dlp_db.conf file is located in the installdir\conf directory, where `installdir` is the installation path for Symantec Data Insight.

Note: If the dlp.csv.enabled property is set to true in the dlp_db.conf file, the Data Insight process uses the .csv file to identify sensitive files, even if DLP is configured in Data Insight.

Support for wildcard (*) in exclude rules for SharePoint events

Data Insight now allows you to use the wildcard (*) to exclude events for URLs that contain a specified sting in its name. For example, if you specify <abc>*, events on all URLs that have the string abc anywhere in the path name are excluded.

Auto-complete help for configuring advanced attributes

Configuring advanced attributes for the purpose of sorting users in a Social Network Map or for creating attribute-based filters is now more intuitive. The **Default Attibute** field now supports the auto-complete feature. Data Insight provides suggestion for custom attributes when you enter part of an attribute name in the field.

Archiving support for clustered Windows File Server

Data Insight now supports archiving of files that reside on multiple virtual file servers that are defined as a part of a Windows File Server cluster. The clustered Windows

File Server configured in Data Insight is automatically mapped with the corresponding virtual file server in Enterprise Vault.

However if the filer is configured in Enterprise Vault (EV) using IP address instead of the host name or the Fully Qualified Domain Name (FQDN), Data Insight does not automatically map the clustered Windows File Server to the corresponding file server in Enterprise Vault.

As a workaround to this, you must run the following steps on the Management Server.

To archive paths on filers that are configured on EV using IP address

1. Open a Windows command prompt.
2. Change directory to `<Install_dir/bin>`
3. Run the following command:

   sqlite3.exe `<data_dir>/conf/workflow/steps/ev/EV.db`
4. In the Ev.db file, select the filer, *`ev_server`* from EV_FILERS; check whether the Enterprise Vault file server that you want to map with is present in the query output.

   If the EV server is present, then proceed to the next step. If the EV server is not present in the query output, there is a problem with discovery of the EV server.
5. Insert the following values in the DI_EV_FILER_MAPPING table - ("<*DI_FILER_NAME*>","<*EV_FILER*>","<*EV_SERVER_IP*>");

   Where, <*DI_FILER_NAM*E> should be same as the DFS name discovered by Data Insight <EV_FILER>, and <*EV_SERVER_IP*> should match with result returned in 4.

Ability to search a user or a user group by SID value

You can now search for a user or a group by entering its SID value in the **Go to** bar located under the **Workspace** tab of the Data Insight Management Console.

Ability to implement parallelism for reports

You can now specify the number of instances of the *report.exe* process that are created for running a report. This can speed up the process of report generation by offering you a degree of parallelism.

For a particular product server, the thread count is specified generically for all types of reports. You can specify the number of report threads to run in parallel on the

Report settings panel under the **Advanced Settings** tab of the server details page of any Data Insight server which has an Indexer role.

Once you specify a thread count, you must individually enable report parallelism for each report type. For any report type, you can enable report parallelism, by editing the `type.properties` file that is located under `<INSTALL_DIR>\reports\Types\<report_name>\engine\`. For example for the Access Details for Paths reports this file is located under the following location: `<INSTALL_DIR>\reports\Types\access_details_paths\engine\`.

To enable parallelism, append the following line to the `type.properties` file:

report.run.parallel=<true>

By default, the following types of reports have the value for *report.run.parallel* set to *true*:

- Access Details for Paths
- Access Details for Users / Groups
- Access Summary for Paths
- Access Summary for Users / Groups
- Data Inventory Report
- Path Permissions
- Entitlement Review

Ability to automate the archiving of reports

For all the report types which support archiving actions, you can now enable Data Insight to handle the archiving operations automatically once a report generates successfully. The new **Post Processing Action** tab on the Create Report wizard allows you to specify actions to be taken on the archived data.

The **Post Processing Action** tab lets you configure the following actions for the archived paths:

- Select a retention category on the archived data to indicate how long the data must be stored.

  Note: You must first select the data source from the **Data Selection** tab before you select any retention category.

- Select a post-processing action, such as deleting the original file and replacing it with a shortcut. The shortcut points to the new file location inside the archive.

Archiving is supported for the following types of reports:

- **Access Details** reports.
- **Access Summary** reports.
- **Custom** reports.
- **Data Lifecycle** reports.

For more information about Enterprise Vault retention categories and post-processing action to manage inactive data, see the Symantec Data Insight User's Guide.

Ability to specify the folder depth in the Access Summary Reports

For both the Access Summary reports, you can now configure folder depth to specify folder and subfolders to be included in the report output. This option is useful when you want to limit the total output in the report. By default the folder depth is the **Current Folder**, which is the folder that is specified during the data selection for the report.

Ability to copy report output to a network location

Data Insight now lets you copy the output for your reports to any location on a network that you have access to. While configuring a report, you can specify the network path where you intend to copy your report output. Additionally, you must specify the credentials that are needed to access the network location.

Ability to define a pause schedule for delete operations on SharePoint audit logs

Normally SharePoint audit logs are deleted after they are fetched from the SharePoint server by the Collector node. In some situations, this can lead to an overhead on the SharePoint server. You can now minimize this overhead by specifying a duration for which the delete operation is turned off.

Data Insight has added a node level property *sp.auto_delete.pause.schedule* on the Collector to add a pause schedule for auto-delete of SharePoint audit logs. You can set the property by using `configdb.exe`. For example, you can use the following command to define a pause schedule from 7:00 hours to 19:00 hours, from Monday to Friday:

```
configdb.exe -o -T node -k 1 -J sp.auto_delete.pause.schedule -j "7
0 19 0 2,3,4,5,6"
```

In the command, the parameters for the start time, the end time and the days of the week are mentioned with single space as separator. The days of the week are

mentioned in a comma-separated list of numerical values with the Sunday equals to 1, Monday equals to 2 and so on

To define multiple pause schedules , separate the schedules by a semi-colon (;). For example "7 0 19 0 2,3,4,5,6;10 0 16 0 7". This pauses the scanner from 7:00 A.M. [7 0] to 7:00 P.M. [19 0] on weekdays [2,3,4,5,6;1], and from 10:00 A.M. [10 0] to 4:00 P.M. [16 0] on Saturdays[7].

Enhancement to the local user scan process for SharePoint site collections

Data Insight has added a node level property *sp.local_users.scan.threads* to run multiple instances of the *sharepoint_users.exe* process in parallel. By defining an optimal count for the threads, you can reduce the time taken to run the local user scan process for a large set of site collections.

You can set the property, by using the `configdb.exe`. For example, to run 5 sharepoint_users.exe processes in parallel on the Collector, use the following command:

```
configdb.exe -o -T node -k 1 -J sp.local_users.scan.threads -j 5
```

Support for SharePoint servers in the Entitlement Review report

With the enhanced Entitlement Review report you can now also view user entitlements on a specified SharePoint path.

Standard templates for configuring node settings

Data Insight now comes bundled with three standard templates which include frequently used settings to help you set up nodes for well known configurations, for example, templates for POC configuration, large Indexer, and large Collector.

The standard node templates are stored in `<INSTALL_DIR>\conf\node_template` folder. You can view the default node templates on Node Templates listing page and apply the templates from the Data Insight Servers list page. However, you cannot edit or delete the standard node templates.

For detailed information about node templates and the procedure to apply templates to configure Data Insight nodes, see the Symantec Data Insight Administrator's Guide.

Default Control Point depth

To enable advanced data analytics, you must configure the depth of the folder hierarchy to be evaluated with respect to the root of the share to compute the control

points within a share. Data Insight displays the information about control points on the **ContextMap** view on the **Workspace** tab of the Management Console.

The default folder depth for computing control points within a share has now been changed to 5. This means that by default Data Insight evaluates the folder hierarchy 5 levels deep to calculate the control points within a share.

For more information about control points, see the Symantec Data Insight User's Guide. For information about configuring advanced analytics, see the Symantec Data Insight Administrator's Guide.

Enhanced Data Loss Prevention (DLP) configuration view

You must configure the settings that allow Data Insight to communicate with Symantec Data Loss Prevention. The DLP settings page has now been enhanced to include three separate text boxes for the user name, domain and Data Loss Prevention role.

Since 4.0

Symantec Data Insight 4.0 includes the following new features and enhancements.

Backward compatibility of Data Insight with lower versions of Windows file server agents

Windows File Server agents are now compatible with one higher version of Data Insight. This backward compatibility provides you enough time to move all the Windows File Server agents to the higher version of Data Insight without having to upgrade the agents along with the Data Insight Collector node. Data Insight 4.0 is compatible with Windows File Server agents with version 3.0RU1 (3.0.1) and 4.0.

Support for wildcard (*) in exclude rules for filesystem events

Data Insight now allows you to use the wildcard (*) with a prefix string to exclude events on paths that contain a specified sting in its path name. For example, if you specify <`abc`>*, events on all paths that have the string `abc` anywhere in the path name are excluded.

Data management using Enterprise Vault and custom scripts

Symantec Data Insight is now integrated with Symantec Enterprise Vault to facilitate archiving and maintenance of data on your storage devices. You can now archive old and inactive data directly from the Data Insight Management Console.

Additionally, you can also perform the following actions for the archived paths:

- Apply a retention category on the archived data to indicate how long the data must be stored.
- Specify a post-archiving operation, such as deleting the original file and replacing it with a shortcut. The shortcut points to the new file location inside the archive.

Data Insight also enables you to use custom scripts to extend the capability to manage your data. For example, you can write scripts to delete or copy selected files and folders. Data Insight lets you invoke these scripts directly from the Management Console.

You can perform the data management operations on the following data:

- Files that are listed under **Workspace** > **Inactive subfolders** sub-tab.
- Files that appear inside the following types of reports:
  - **Access Details** reports.
  - **Access Summary** reports.
  - **Custom** reports.
  - **Data Lifecycle** reports.
- Paths listed in the ContextMap view on the **Workspace** tab.

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

Enhanced permission remediation

Data Insight now identifies inactive users through audit log data and provides you recommendations to revoke permission of such inactive users. Such recommendations are available only to users with the Server Administrator role.

After you receive an automated recommendation, you can perform a what-if analysis to determine the possible consequences of applying the recommendations. Based on this analysis, you can decide whether you want to apply the recommended changes to user and group permissions.

You can remediate permissions by using a third-party ticketing system or directly from the respective views on the Management Console.

For information about configuring Data Insight to handle the permission remediation actions, see the *Symantec Data Insight Administrator's Guide*. For information about viewing the permissions recommendations, see the *Symantec Data Insight User's Guide*.

Ability to visualize the social network of users

The Social Network Map gives a visual representation of collaboration among users in your storage environment. You can use the Social Network Map to identify the following:

- Shares on which users are actively collaborating.
- Shares on which multiple users belonging to multiple organizational units are collaborating.
- Users who appear to be collaborating, but are organizationally unrelated; users whose attributes significantly differ from other active users on the share.

The Social Network Map gives you the ability to visualize large sets of information and enables you to analyze the social network of users. The Social Network Map also enables access risk remediation by helping you identify shares that have excessive permssions.

For more information about using the Social Network Map to analyze the activity pattern of users, see the *Symantec Data Insight User's Guide*.

Support for monitoring of generic device filers

Data Insight now enables you to monitor file servers with varied file systems. You can now configure scanning and auditing of a generic file server in Data Insight.

Data Insight provides a web API to enable third party clients store access events from a generic device filer into an index. This enables partners to add support for devices that are not supported by Data Insight out-of-the-box. For more information on the web API specification for the generic Collector service, refer to the *Symantec Data Insight Programmer's Reference Guide*.

For information about configuring a generic device in Data Insight and credentials required to monitor the device, see the *Symantec Data Insight Administrator's Guide*.

Intelligent upgrade recommendations

Data Insight simplifies the task of installing patches and upgrades by providing you automated suggestions about available patches and upgrades.Data Insight fetches this information from Symantec Operations Readiness Tool (SORT) to help you keep track of the latest rolling patches available for each node.

Data Insight presents the upgrade recommendations as links on the Data Insight Servers page. Click the link to download the patch installer from the SORT website.

Support for custom extensions in file groups

You can now add custom extensions when configuring file groups. Data Insight automatically updates the indexes when new extensions are detected.

Improved usability in configuring node settings

You can now create templates that you can apply to multiple Data Insight nodes. Using node templates to configure servers ensures consistency in the configuration across nodes.

For information about configuring and managing node templates, see the *Symantec Data Insight Administrator's Guide*.

Deployment enhancements

You can remotely deploy installers and patches on the Data Insight worker nodes and Windows file server agents from the Data Insight Management Console. This simplifies the task of upgrading and configuring numerous nodes individually in a large Data Insight deployment.

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

Reports enhancements

The following enhancements have been made to reports in this release:

- Ability to create custom reports.
  You can now create your custom reports if the existing report types are inadequate for your reporting needs. For example, you might want to create a report having the name, size, active data size, openness, and number of active users for each share. You can use the DataInsight Query Language (DQL) to generate such custom reports.
  DQL is a framework that allows you to execute custom DQL queries, and get the results in the form of a relational database. You can create a query for repeated execution from the **Reports** tab of the Management Console.
- Ability to customize the report output.
  You can now rename the default column headers for any reports that you want to generate.
- Availability of two new reports.
  The Duplicate Files report enables you to identify duplicate files residing on the same share. Two files are considered to be duplicates, if they have the same logical file size and the same file extension. Data Insight considers only those file extensions that have been configured to be part of a file group in the configuration database while creating the report.

The Group Change Analysis report enables you to understand the business impact of removing users or child groups from a group. You can either configure the report from the **Reports** tab or initiate the report from the **Workspace** tab to analyze the impact of applying permission changes recommended by Data Insight.

- Ability to truncate the report output.
  Data Insight allows you to truncate the report output for specific reports. This enhancements reduces the overhead on system resources when running large reports. If you want the complete report, Data Insight lets you re-generate the output with additional rows in the output.
- Ability to specify a time filter when configuring reports.
  Data Insight lets you specify a date range as an input parameter when configuring certain reports. Only those files whose access time falls within the date range is part of the output. For example, for a Consumption by File Group report, you can find all `.pst` files older than a year.

For detailed information about these enhancements and about the new reports, see the *Symantec Data Insight User's Guide*.

FPolicy safeguard for NetApp virtual filers

Data Insight now enables you to associate all NetApp virtual filers that are configured in Data Insight to their respective physical file servers and apply the FPolicy safeguard to all virtual filers.

This feature allows Data Insight to disconnect from the physical file server and all the corresponding virtual filers, if the high latency watermark is breached.

For information about configuring the FPolicy safeguard for virtual filers, see the *Symantec Data InsightAdministrator's Guide*.

Supportability enhancements

The new supportability features include the following:

- Data Insight provides the ability to preserve activity on the shares that are marked as under legal hold and override the configured purge and retention settings.
- Data Insight now stores logs for indexer and scanner in separate folders. For example, all of the `index-msu_ID` logs are stored in the `logs/indexer` folder. This feature helps you find the relevant logs faster and reduces the clutter in the `logs` folder.

Since 3.0.1

Symantec Data Insight 3.0.1 included the following new features and enhancements.

Report enhancements

- You can now use the command line to create Data Insight reports.
  Using the command line enables you to create and execute reports without loggging in to the Data Insight Management Console. It also allows you to provide or overide the report input parameters through the properties file. You can also use the command line to run ad-hoc reports to extract required data without having to save a named report.
  For more information about the command-line options required to create and execute reports, see the *Symantec Data Insight Administrator's Guide*.
- Support for `.csv` files in report creation.
  Data Insight now allows you to input parameters such as users, paths, and custodians that you want Data Insight to include in the report though `.csv` files. You can specify the path to the `.csv` file, if creating a report from the command line or you can browse to the location of the input `.csv` file if creating a report from the Management Console.
  Using `.csv` files to input the scope of a report, simplifies the task of creating reports.
- New Reports home page.
  The new Reports home page lists all reports available to the logged in user. You can view the status of the report runs, filter the list of reports, and run specific reports directly from the home page.
- File group and file type information in reports.
  The following three reports allow you to select the file group(s) or the file type(s) that you want to include in the report:
  - Inactive Data by File Group
  - Consumption by File Group
  - Consumption by File Group and Owner

  This enhancement enables you to define the scope of the report more granularly.
- Two new reports have been added to Data Insight in this release.
  - Inferred Data Owner report
    The report provides insight into the inferred owners on specified paths.
  - Entitlement Review report
    The report displays user entitlement on specified paths. It also indicates whether a user is active on path.

- Data Insight now makes it easy to search for specific report from the Reports home page or from the list page of any report type. You can use either the name of the report or the status of the report run as search key words to filter out specific report(s).
- You can now send a link to a report output via email. Click the link in the email to download the report.
- You can now specify the depth of the subfolders that you want to include in the report output for selected reports. This allows you to limit the the size of the report output and generate more granular data.
- This release of Data Insight includes a technology preview feature called Interactive Reports. This feature lets you view report outputs in an interactive fashion. This feature is hosted by new service called DataInsightHttpd that runs only on the Management Server. For detailed information about the DataInsighHttpd service, see the *Data Insight Installation Guide*.

For details about the reports enhancements, see the *Symantec Data Insight User's Guide*.

Enhanced supportability features

Data Insight has been enhanced with new features that enable you to access relevant information to troubleshoot errors using the Management Console.

The new supportability features include the following dashboards:

- Summary dashboards
  The Data Insight summary dashboards on the **Dashboard** tab provide a snapshot view of the storage, activity, and permissions data pertaining to all the configured storage devices, shares, and site collections.
  You can configure the frequency of running the dashboard report. The dashboard displays a notification if a report run has failed. You can download the logs for that report run directly from the Management Console to help you better troubleshoot the issue.
- System overview dashboard
  The **System Overview** dashboard displays by default on the **Settings** tab. It provides a graphical representation of the health of the storage devices, Data Insight servers, directory services, and the status of scans running in your environment. This dashboard also displays notifications and alerts which help you identify the issues that need attention.
- Scanning dashboard
  The Scanning overview dashboard helps you review the following:
  - The consolidated status of the scans on the configured storage devices.

- The successful full scans that are sorted according to the time elapsed since the scans completed. This data is used to compute the last known good state of a scanned path.
- The number of successful, partially successful, and failed scans for a selected time period.
- The details of the scan errors that occurred in the last 24 hours.

You can use the graphs to drill down to view the details on the **Scan Status** and the **Scan History** tabs.

- Filer statistics
  Graphical representation of the latency, the rate of incoming events, and the total paths for a filer. Latency and event rate is only available for NetApp filers. These statistics help in getting a feel for system performance over the time and lets you plan your resources.
- Data Insight server statistics
  Graphs that provide an overview of the following:
  - CPU, memory, and disk utilization in percentage terms.
  - The number of files in the `inbox`, `outbox`, and `err` folders in the installation directory.
    You can select the time window for which you want to render the graphs.

In addition to the dashboard views, the following enhancements provide insight into the health of the Data Insight servers:

- The **Overview** tab for a server provides details about the health of the selected server and indicates possible causes that have led to the current health status.
- The new **Services** tab enables you to view the status of critical services.

Support for clustered Veritas File System filers

You can now add a VxFS file server which is part of a Veritas Cluster Server configuration to Data Insight.

For details about adding a clustered VxFS server to Data Insight, see the *Symantec Data Insight Administrator's Guide*.

Ability to define open share policy

Data Insight now lets you define the criteria that you can apply to determine whether a share is *open* . You can define the parameters that determine if a share has permissions assigned on it that renders it open. Data Insight uses the open share policy information to flag the shares that have loosely-defined permissions. You

can use the information to do an entitlement review of the shares that are being monitored by Data Insight.

For details about configuring an open share policy, see the *Symantec Data Insight Administrator's Guide*.

Ability to configure file groups

By default, Data Insight sorts files into 18 file groups based on the extension of the files. The file group information is used for reporting on ownership, access pattern, and space consumption on storage devices.

You can now modify the default file groups or add new file groups from the **File Groups** view of the Management Console. At this time you cannot add new extentions to the file groups.

New monitoring service implemented

The new DataInsightWatchdog service monitors disk usage on the Windows File Server agent node and prevents it from running out of disk space by implementing safeguards.

For more information about the DataInsightWatchdog service , see the *Symantec Data Insight Installation Guide*.

For information about configuring the thresholds that initiate the safefguard mode, see the *Symantec Data Insight Administrator's Guide*.

Ability to import additional attributes for users and groups

You can now import additional attributes for users and user groups from other user management systems into Data Insight users database. This attribute information is later included in the report outputs and also sent to Symantec Data Loss Prevention as a part of ownership information.

Chapter 2

System requirements

This chapter includes the following topics:

- System requirements for Symantec Data Insight components
- List of ports
- Operating system requirements
- Supported file servers and platforms
- Supported browsers
- Web server version

System requirements for Symantec Data Insight components

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

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

Component	System requirements
Management Server	■ Windows Server 2003, 2003 R2, 2008 or 2008 R2, 2012 or 2012 R2. The operating system must be 64 bit. ■ 8 GB RAM ■ 4 CPUs

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

Component	System requirements
Indexer worker node	■ Windows Server 2003 or 2008, or 2008 R2, 2012 or 2012 R2. The operating system must be 64 bit. Red Hat Enterprise Linux version 5.0 update 5 or higher or version 6.0 update 3 or higher; 64 bit only. ■ 8 GB RAM ■ 4 CPUs
Collector worker node	■ Windows Server 2003, 2008, or 2008 R2. The operating system can either be 32 bit or 64 bit. Windows Server 2012 or Windows Server 2012 R2. The operating system must be 64 bit. ■ 4 GB RAM ■ 2 CPUs
Self-Service Portal node	■ Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2. The operating system must be 64 bit. ■ 8 GB RAM ■ 4 CPUs
Windows File Server agent node	■ Windows Server 2003 or 2008. The operating system can either be 32 bit or 64 bit. Windows Server 2012 or Windows Server 2012R2. The operating system must be 64 bit. ■ 4 GB RAM ■ 2 CPUs
SharePoint Web Service	Microsoft SharePoint 2007, SharePoint 2010, or SharePoint 2013

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

List of ports

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

Table 2-2 List of default ports

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

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

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

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

Operating system requirements

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

Table 2-3 Symantec Data Insight operating system requirements

Operating system supported	Notes
Windows Server 2003	Windows Server 2003 (32-bit and 64-bit) Standard Edition and Enterprise Edition Windows Server 2003 R2 (32-bit and 64-bit) Standard Edition and Enterprise Edition

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

Operating system supported	Notes
Windows Server 2008	Windows Server 2008 (32-bit and 64-bit) Standard Edition and Enterprise Edition Windows Server 2008 R2 (32-bit and 64-bit) Standard Edition and Enterprise Edition
Windows Server 2012	Windows Server 2012 (64-bit)
Red Hat Enterprise Linux	Version 5.0 update 5 or later Version 6.0 update 3 or later Only 64 bit packages are supported
VMware	32 bit and 64 bit on Windows 2003 32 bit and 64 bit on Windows 2008 64 bit on Windows 2012

Note: You must ensure that VMware Tools is installed on VMware virtual machines.

Supported file servers and platforms

Table 2-4 lists the Network Attached Storage devices and SharePoint platforms that Data Insight supports.

Table 2-4 Supported file servers and platforms

Device	Version
Hitachi NAS file server	Hitachi NAS 12.x.
NetApp ONTAP	From v7.3.5 to v8.1.x ONTAP 8.0.x and ONTAP 8.1.x are supported in 7 mode only. ONTAP 8.2.x is supported in 7-mode and Cluster-Mode.
EMC Celerra	5.6.45 or higher, VNX
EMC Isilon	OneFS version 7.1 or higher

Table 2-4 Supported file servers and platforms *(continued)*

Device	Version
Windows File Server	Windows Server 2003 or 2003 R2, 32 bit, and 64 bit Windows Server 2008, or 2008 R2, 32 bit and 64 bit Windows Server 2012, or 2012 R2 64 bit
Veritas File System (VxFS) server	6.0.1 or higher, configured in standalone or clustered mode using Symantec Cluster Server (VCS) **Note:** For VCS support, Clustered File System (CFS) is not supported.
Microsoft SharePoint	Microsoft Office SharePoint Server 2007 Microsoft SharePoint 2010 Microsoft SharePoint 2013
Symantec Data Loss Prevention (DLP)	Versions 12.0.1 and 12.5
Symantec Enterprise Vault	Versions 10.0.4 and 11.0

Note the following:

- Symantec strongly recommends that you upgrade your NetApp filer to the latest available firmware. Symantec recommends ONTAP 7.3.5 or higher.
- For all supported versions of 7-mode NetApp filers, Data Insight supports CIFS protocol over NTFS and NFS protocol v3. NFS v4 is not supported.
  For supported versions of Cluster-Mode NetApp filers, Data Insight supports only CIFS protocol over NTFS. NFS protocol is not supported.
  Data Insight supports the following volume/qtree styles:
  - NTFS and Mixed for CIFS protocol.
  - UNIX and Mixed for NFS protocol on 7-mode Netapp filers only.
- For all supported versions of EMC Celerra/VNX and EMC Isilon, Data Insight supports only CIFS protocol over NTFS. NFS protocol is not supported. Data Insight supports the latest Common Event Enabler (CEE), version 6.3.1. Data Insight still supports the older version of CEE and VEE, but Symantec recommends that you move to the latest EMC Common Event Enabler, which you can download from the EMC website

- To use the Self-Service Portal to remediate DLP incidents, ensure that Symantec Data Loss Prevention (DLP) version 12.5 or higher is installed. Data Insight uses the DLP Smart Response Rules to remediate incidents, which are introduced in DLP version 12.5.

Supported browsers

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

Table 2-5 Symantec Data Insight Supported browsers

Browser	Versions
Internet Explore	■ Version 9 and version 10
Mozilla Firefox	■ Version 28.0 or higher
Google Chrome	■ Version 33.0.1750.154 or higher

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

Web server version

Symantec Data Insight uses Apache Tomcat 7.0.53.

Chapter 3

Software limitations

This chapter includes the following topics:

- Scanner limitations
- Windows File Server support
- Console limitations
- Expression builder limitation
- Special characters not supported in NFS paths
- Size on disk not displayed
- Filer rename not supported
- Social Network Map limitation
- Report configuration limitation in Path Permission reports
- Known limitations for NetApp Cluster-Mode support
- Known limitations for Hitachi NAS support

Scanner limitations

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

- In case of Windows 2012 Severs used as Windows File Servers, the Scanner does fetch a group having permission based on a condition. For example, "all users who have *xyz* as manager have full access to the share/folder". However, the indexer discards it currently. The console does not display the group as having Dynamic ACL. The other permissions on the path are shown properly.

Resilient File System (ReFS) is supported only for scanning. Auditing is not supported since the drive cannot be attached to the filter driver.

- Scanner does not support share names of more than 200 characters.
- Scanner modifies the access time of directories while traversing the filesystem.

Windows File Server support

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

Console limitations

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

Expression builder limitation

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

Special characters not supported in NFS paths

The following special characters are not supported in NFS paths:

/ \ : * ? " < > |

Size on disk not displayed

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

Filer rename not supported

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

Social Network Map limitation

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

Report configuration limitation in Path Permission reports

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

Known limitations for NetApp Cluster-Mode support

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

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

Known limitations for Hitachi NAS support

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

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

Chapter 4

Known Issues

This chapter includes the following topics:

- Console display issues
- Other Issues

Console display issues

The following issues relate to displays in the Console.

Changing zoom level in Internet Explorer affects Data Insight interface

In Internet Explorer, changing the zoom level from 100% to a different value causes the Data Insight interface to appear distorted

Incorrect status of scans displayed

If you delete a filer from the Data Insight Management Console, and then add the filer back again, the status of the last full scan of the filer is displayed based on the status before the filer was deleted. For example, The last full scan of the filer before it was deleted from the Data Insight Management Console is displayed as Successful. If you delete this filer and add it back again, the old status continues to be displayed on the Monitored Shares tab, although a full scan of the share under the newly added filer has not been started.

The status of the scan is refreshed after the first full scan of the filer since it is added again.

Scan status not displayed

If you rename a filer, the scan status for the filer is not displayed, although the index is updated with the scan information.

The scan status starts appearing properly after the first full scan of the filer since it is renamed.

Toolbar error

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

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

Emailing contents of a table

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

Incorrect status of folder displayed

The **Workspace** > **Folder Activity** > **Inactive sub-folders** page may display a folder as inactive for a selected time period, even when file(s) within the directory have been deleted in the specified time range and there are no other events on files within the directory This is because a delete event on a file is not considered as activity for the purpose of showing the activity status of the folder.

Incorrect information in Inactive Directories report

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

Active Directory scan reporting error

Even if one domain out of multiple domains is successfully scanned by Data Insight and the scan of all other domains fails, the console Active Directory scan is reported as successful.

Report for deleted paths not supported

Data Insight does not support running a report for paths on deleted data repositories or paths for which the Data Insight user's is permission is revoked.

Error fetching data displayed

If you right-click a user or SID in the tree pane on the **Workspace** > **Users** tab, and this user belongs to an Active Directory domain which is not added to Data Insight or not scanned by it, you will get an error.

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.

Incorrect scale displayed for file activity graph

The graph displaying the access events on a file (**Workspace** > **Folders** > **Folder Activity** tab) shows repeating values for Y-axis scale in some cases.

This occurs due to a limitation in the charting tool.

Error displayed on session time out

On Internet Explorer, if your session times out, when you are on the Workspace tab, instead of redirecting to the login page, the browser may display the message `Error getting children`.

Workaround

Close the browser and log in to the Data Insight Management Console again.

Deleting a DFS server causes error

If you delete the DFS server from a list of filers or delete any of the shares under the DFS server, and this DFS server is part of a container, the container continues to show the folder icon without any text against it in the **Selected Resources** pane. When you move the mouse pointer over the icon, it displays "\\" in the tooltip.

The workaround is to delete the empty path from the data selection.

Report includes only physical paths

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

Progress bar display error

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

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

Error fetching permissions data

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

Inconsistency between permissions view of Windows and Data Insight

On a given path, for example, /foo, if a group, for example, G1, is allowed full control and Everyone is denied full control, then the effective permissions for G1 on the given path, shown through the Windows security permissions view, is **Allow full control**. However, the Data Insight view displays **Deny Full Control**.

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

Error fetching data displayed

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

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

Sequence of spaces in share names not supported

If a share name consists of a sequence of spaces, and no other characters, the scan of such a share fails with the error, `The network path was not found`.

If you try to access the share from the file server, Windows does not list a share with an empty name and displays a list of all shares on the filer.

If you try to view the contents of the share from the Data Insight console, you can only view the list of shares on the filer. Data Insight repetitively displays the list of shares instead of displaying the contents of the share with the empty name.

There is no workaround for this issue.

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.

Newly added files or shares do not automatically appear in the Folders tab

When new files or shares are added to the configuration, they do not automatically appear in the **Workspace** > **Folders** tree view control, while you are logged in.

To make new files and shares appear, right click on the header for the **Folders** tab or in the tree view control, and select **Refresh Tree**.

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

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

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

Renamed file displays in GUI with original name

If a file is renamed during the progress of a scan, the file continues to display with its original name under its parent folder, without any events for it. For example, if you rename a file, abc.txt, to xyz.txt when a scan is in progress, the GUI does not reflect the changed name. The file appears under its parent folder with the name, abc.txt.

Workaround

Create a file with the original name and delete it from the share.

Alphabetical sorting of shares

If you search for shares using a path string, the search result does not display the shares in an alphabetical order.

Error when logging in to the Data Insight Management Console

Logging in to Data Insight may fail when the Web server denies the request. The Web server logs may not display the cause of the failure.

Workaround

Delete the cookies and try logging in again.

Pop-up at site collection level

On the **Workspace** tab, when opening a SharePoint site collection, a pop-up displays the message, This folder does not inherit its parents permissions.

You can safely ignore this message.

Overlaping tooltips

On the **Settings** > **Alerts** page, the tooltips displayed for user SID and reason for alert columns overlap.

Search bar error

The search bar at the bottom of the **Custodian Assignments** panel is grayed out in **Users** > **Custodian** tab.

Deleted paths visible in the GUI

Paths that have already been deleted continue to be displayed in the **Custodian Assignment** panel on the **Users** > **Custodian** tab.

Symantec Data Insight Management Console help issues

The following issues exist in the Management Console help Symantec Data Insight:

- Reports tab: The help text is not displayed.

- Reports listing page: The help text is not displayed.

SharePoint create event displayed incorrectly

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

Custom attribute widget issue

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

Incorrect disk space computation displayed on Workspace tab for NFS shares

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

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

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

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

Disabled share or site collections are reported on scanning dashboard

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

Error displayed while adding a VxFS filer

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

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

Scan status incorrectly displayed on scanning dashboard

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

Issue regarding the broken search bar

The search bar on the upper right corner of the **Workspace** tab displays an incomplete tooltip. But the search for shares and site collections is unaffected.

Incorrect icon displayed in the reports wizard

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

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

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

Workaround

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

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

Dashboard tab shows incorrect path for deleted filers and Web applications

If you delete a filer or Web application, the **Path** column on the **Dashboard** > **Shares/Site Collections** tab shows \\\.

Workaround

Run the dashboard reports again to remove these paths.

Issue with Select Resource pop-up for user permissions

On the **Workspace** > **Users** > **Permissions** tab, if you click **Select Share**, the **Select Resource** pop-up shows all filers/Web applications instead of showing only those that have shares/site collections on which the user has permissions.

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

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

Workaround

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

Duplicate entry for the Enterprise Vault server is allowed

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

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

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

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

Access Details for Paths report fails with invalid path

When no filers or SharePoint web applications are added to Data Insight, the attempt to generate the Access Details for Paths report fails. When no resources are specified, by default the report considers all the available resources for generating a report. Since there are no resources configured in Data Insight, the report fails to generate.

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.

Folders with explicit ACEs are not flagged with lock icon

Folders that do not inherit their parents' permissions, but have explicit ACE applied on them, should be displayed with a lock icon in the tree-view pane. However, such folders are displayed with a regular folder icon.

Data Insight fails to check user permission on shares

A user is allowed to view all shares on a file server, even when he has explicit permission only to view certain shares on the filer.

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

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

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

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

EVFolderPoint.xml file may be displayed in the Workspace

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

Incorrect recommendation count displayed

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

Permission recommendations for renamed folders may not be accurate

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

The Consumption by File Group report fails

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

Broken membership in case of local groups leads to misleading permissions

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

Built-in groups are not excluded for Path Permissions reports

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

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

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

Workaround

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

Social Network Maps are not displayed when tabs are restored

When multiple Social Network Maps are opened in different tabs, and the browser is refreshed and tabs are restored, the Social Network Maps fails to display.

Workaround

Manually reopen the tabs with the Social Network Maps.

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

Add EV Server dialog remains open

The **Add EV Server** dialog remains open even after the session times out or after the user logs out.

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

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

Hidden columns are displayed in reports in the `.csv` format

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

Workaround

Use Microsoft Excel's feature to hide unwanted columns.

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

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

Workaround

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

Delay in rendering of some views

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

Pagination issue on the Summary pane for permission recommendation

You might need to scroll to see the entire list of permission recommendationson on the **Summary** page under the **Settings** > **Permissions** > **Recommendations** tab.

Successful partial scan does not change failed consolidated scan status

In the **Scan Status** page of the **Scanning** dashboard, if a consolidated status displays as *Failed*, a subsequent partial scan cannot change it back to *Partial* or *Successful*. Also, the **Last Known Good State** does not change following a partial or successful.

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

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

The inferred owner name in ContextMap view and User Activity summary page do not match

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

The Inactive Subfolders tab displays deleted paths

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

Incorrect product update recommendations may be shown for Indexer nodes

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

The Scan Errors page does not display an error

The **Scan Errors** page of the Data Insight Management Console does not display an error, if the error occurs while scanning the root of the share or share permissions.

Selected attribute continues to be displayed in drop-down

Data Insight fetches the directory service attributes for all configured domains. These attributes are available for selection when you configure the primary attributes for advanced data analytics. Unless you set a domain-specific attribute the default attribute is assumed to have been set for all configured domains.

If a default attribute (for example, department) is set for all domains, then the next time you want to add an attribute, the attribute *department* should not be available for selection. However, the attribute continues to be displayed in the drop-down list.

Display name does not appear properly in Firefox browsers

When configuring advanced analytics attributes, the display name appears to be slightly cut in Firefox browsers.

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.

Default retention category displayed even when data is not selected

Data Insight now allows you to configure archiving actions automatically on paths in a report after you successfully generate certain types of reports.

Data Insight displays the retention categories configured on the Enterprise Vault server corresponding to the data repository that you have selected. If no data source is selected, then no retention category should be displayed. However, Data Insight displays the default retention category even when you do not select any data when configuring the report.

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.

Issue with size filter on the Data Insight dashboard

The size filter on the Data Insight dashboard does not show any data. When the size filter is used, Data Insight displays the message, *No data matching the criteria*.

Data Inventory Reports may produce incorrect output in certain cases

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

Workaround

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

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

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

Issue with display of active file size in ContextMap

In the ContextMap view, the active size for folders displays as 0 even when there is activity on the underlying files and folders. When the selected activity period is other than 6 months, active data size column in the ContextMap can show an incorrect value.

ContextMap information may not display in some cases

In a large environment, the process that gathers the analytics data for the ContextMap view may take a long time to execute and may eventually timeout. In such cases no data will be displayed on the ContextMap.

In such cases, as a fail back mechanism, Data Insight executes another process that will gather information about the immediate children on filers and this data is displayed on the Workspace tab.

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

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

Workaround

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

Users not deleted after deleting Active Directory server

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

Add/Upgrade license succeeds irrespective of the license file type

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

Creating non-domain saved credentials

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

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.

The End Time column for the audit logs may turn blank, when the page is refreshed

When you navigate to **Workspace**>**Users**>**Audit Logs** and refresh the page using the on-screen refresh button, the **End Time** column turns blank.

The disabled users may be displayed as enabled when you view recommendations on a path

When you navigate to **Workspace**>**Folders**>**Permissions**>**Recommendations** and expand a group, the disabled users are displayed as enabled.

Data Insight SharePoint Agent may encounter an exception while fetching attributes

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

Large time gap between the report execution and the report download.

After report finishes execution on a node, it may take long time to download the report, because the Management Server may be processing other reports that are in the queue. You can get an indication of this problem from the report progress view for report. You will notice a significant gap between the report execution time and the report download time.

Report log displays warning message for step-progress

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

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

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

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

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

Canceling the Ownership Confirmation workflow creation may cause a draft to be saved

When you create an Ownership Confirmation workflow and then close the panel instead of clicking the **Cancel** button, the workflow is saved as a draft.

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

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

A workflow that is in submitted state cannot be canceled.

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

Workaround

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

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

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

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

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

Custodian assignment may take a long time to complete.

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

Permission remediation emails may display incorrect values for some variables

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

The search filter on the workflow creation wizard may not function

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

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

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

DQL reports fail if the queries contain non-English characters.

If a DQL query contains non-English characters the reports fails to generate.

SharePoint Web applications hierarchies under the Workspace tab may be displayed incorrectly

Some of the SharePoint Web applications hierarchies displayed under the **Workspace** tab may not match with the actual hierarchies present in the SharePoint servers. This anomaly is noticed when you select the check box for **Configure resources automatically** while configuring for the Data Loss Prevention settings. When you select this option the resources monitored by DLP but not added to Data Insight are automatically added to Data Insight. But for such added SharePoint resources the wrong hierarchies are displayed by Data Insight.

Incorrect positioning of page breaks may appear in the report outputs

In case of report outputs in the PDF format, sometimes page breaks may appear in wrong places.

Exceptions in the webserver logs while running reports with containers

An exception is observed in the webserver logs while running or editing a report configured with a container. The exception occurs because Data Insight tries to resolve the containers as paths.

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

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

Workaround

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

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

Currently no workaround is available for the HTML outputs.

Incorrect member count displayed

Data Insight considers the count of deleted users, and users belonging to the Migrated SIDs and Unresolved SIDs domains when calculating group memberships.

Custodian assignment may fail when the Assign by owner method option is selected

From the **Custodian Manager**, if the **Assign by owner method** option is selected, sometimes the assignment may not succeed if Data Insight is able to successfully compute the owners only for a subset of all the selected paths.

Incorrect information may be displayed in the report progress view

If a report is run for a group of paths which also includes some DFS paths, Data Insight displays the wrong count in the report progress view. This happens because Data Insight fails to fetch the progress details for the DFS paths.

The custom attribute column name in a DQL query does not ignore case

If a custom attribute is referred in a DQL query, ideally Data Insight is expected to ignore the case used in the custom attribute name. But if the case used in the query does not exactly match with the one used in the directory service, in the report output the column for the corresponding custom attribute fails to display any information.

The principal name for a data owner may not be displayed in a DQL report.

If the method used to compute the data owner is creator and if the creator of a the data resource is Administrator, a DQL report to fetch the principal name of an owner displays the principal name column as blank.

Custom actions displayed as disabled

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

Workaround

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

Email sent for Entitlement Review workflow even for failed paths

In an Entitlement Review workflow, even if some paths fail due to permissions information not being present, the email notification is sent to the custodian.

When the custodian tries to log in to the Portal, the following message is displayed:

"Workflow <workflow name> is completed. No more actions required. Thank you."

Issue creating an Ownership Confirmation workflow if custodian is assigned at web application and site collection levels

When creating an Ownership Confirmation workflow, if a custodian is assigned at the web application and site collection level, and you click **Select All Resources**, only the custodian at the root site collection is assigned correctly. The custodian and custodian email fields for the web application are blank.

On the **Data Selection** panel, if you try to delete the row for the web application, it fails to be deleted, although you see a success message. You can delete the paths only from the Data Selection panel.

You can create the workflow successfully if you select the web application and the site collection individually.

Data management workflows fail in some cases

Data management workflows submitted to Enterprise Vault fail if they are submitted from Data Insight installed on a non-English operating system.

During report configuration the field specifying member count does not accept inputs

In the report creation wizard, under the **Configuration** page, the **Limit number of expanded member users to (Member count)** filed does not accept input, if Internet Explorer 9. The anomaly is observed in the following report types:

- Path Permissions

- Entitlement Review
- User / Group Permissions

Activity graph displays incorrect data

On the user-centric **Activity** view, if you select the Today, Yesterday, or a custom date range for one day, the graph displays data for 48 hours instead of 24 hours. Also, if you click on the hour granule of the bar graph, the graph displays data for all hours.

Similar issue is observed when you cross-launch to the **Audit Logs** tab.

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.

Column displaying exclude pattern for web applications missing in Health Audit report

The column displaying the exclude pattern for SharePoint web applications is missing in the Health Audit report.

Management Console may fail to authenticate when you upgrade Data Insight from version 4.5 to 4.5.1

The Data Insight Management Console may fail to authenticate you when you upgrade from Data Insight from version 4.5 to 4.5.1. This happens in the following scenarios:

1. You have logged off from a Management Console session with Data Insight version 4.5.
2. You have kept the browser open, and once the upgrade is complete, tried to log in using the already open browser-window.
3. Upgraded Data Insight from version 4.5 to 4.5.1.

An error message is displayed indicating the failed authentication.

Workaround

Refresh the browser and log in again.

Other Issues

This sections list some additional issues.

Capacity Reports are generated for all filers irrespective for RBAC configuration

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

Events display error

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

Error in displaying selected result entry

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

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

Workaround

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

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

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

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

Deletion of a Collector node fails even after disassociating all filers

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

User with Product Administrator role unable to edit share

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

Workaround

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

Report creation error

Report creation fails when the report name contains an apostrophe.

Unable to restore tabs

Restoring tabs for DFS and SharePoint paths does not work.

Workaround

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

Scan resync does not work for certain scenarios

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

Security event not monitored

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

Create event not captured

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

Container and directory service name limitation

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

Incorrect default schedule displayed

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

Special characters in NFS paths cause NFS scanner to fail

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

Error when saving user name, container name, and directory service names

User container and directory service names get saved even if they throw an error in GUI while saving.

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.

Custom attributes already selected displayed again for selection

After an upgrade of Data Insight, when you try to add additional custom attributes as a part of the directory service configuration, the custom attributes that have already been added before the upgrade are also available for selection. Ideally, the list of attributes available for selection should exclude the custom attributes that have already been added.

Custom attribute discovery does not work in certain scenarios

Custom attribute discovery for Active Directory domains does not work when Management Server is installed on Windows Server 2003.

Workaround

Add custom attributes manually for Active Directory domains.

Port number for LDAP directory server required

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

Workaround

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

Exclamation mark in user name not supported

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

Duplicate policy name issue

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

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

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

The job scheduling settings require modification

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

The scan history graph does not display the data as expected

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

Limited support in the Entitlement Review report

The Entitlement Review report does not have NFS support.

Issue with launching installer from mapped drive

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

Workaround

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

Issue with same NFS export and CIFS share name

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

The scanned shares and the total scan count does not match

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

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

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

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

Limited support for claims-based authenticated Web applications for SharePoint

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

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

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

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

Workaround

Manually install Data Insight on the Collector.

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

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

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

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

Attempt to archive a file using the Enterprise Vault fails

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

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

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

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

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

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

Generic device issue

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

Wildcard support limitation

Wildcard (*) support in Exclude Rules is not implemented for the following:

- Exclude Rules for scanning.
- Exclude Rules for access events in case of SharePoint.

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.

Multi-byte characters not supported

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

Stop DataInsightFPolicy service before shutting down a Collector node

Symantec 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.

Scan-rsync fails to update the folder size

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

Data Insight cannot retrieve retention categories with certain characters

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

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

Issue with assigning NIS and LDAP users as custodians

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

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

Disabled icon not displayed

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

Issue with computing custodian for root site collection

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

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

Size of parent folder is not updated

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

Issue with pagination on Audit Logs view

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

Issue with LHS filter

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

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

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

Certain reports do not honor the global data owner policy

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

Incorrect informaton displayed for migrated user

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

Issue with workflow creation if services on Indexer are down

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

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

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

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

Workaround

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

Records Classification workflow fails to archive paths using Enterprise Vault for certain devices

Data Insight does not support the archiving of data resources on Hitachi NAS, EMC Isilon, NetApp Cluster-Mode, and generic devices with Symantec Enterprise Vault.

Records classification workflow for paths on these devices will fail when the action is submitted to Enterprise Vault. This happens because the Records Classification workflow enables you to automatically archive data marked as a record with Symantec Enterprise Vault,but Data Insight does not support archiving for these devices.

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

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

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

Issue with the new membership object in DQL

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

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

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

Empty multi-value column not supported

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

Issue with the new membership object in DQL

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

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

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

Chapter 5

Fixed issues in this release

This chapter includes the following topics:

- Fixed issues in 4.5.1

Fixed issues in 4.5.1

Fixed issues are referenced by Symantec incident number and described briefly below for the 4.5.1 release.

Table 5-1 Fixed issues in 4.5.1

Fixed Incidents	Descriptions
3554447	Even though Master report download thread issue is fixed, still, due to incorrect settings for thread queue and core pool size, there is only one report which can download in entire deployment.
3566477	Fix memory leak for queryd in the list_custodian query.
3596849	Events_first/events_next functions not re-entrant causing a dqlexec query to crash.
3618936	'from dfspath get custodians.user.name' crashes because cursor_limit[] was not updated for a newly added table.
3317978	Unable to clear the pending jobs from dashboard run.
3581084	Using top command to compute memory consumption results in showing incorrect value to be shown in statistics for Linux Indexers.
3551787	Memory utilization on Linux indexers will not report high utilization where used memory is greater than what can be reported as XXX KB by java INT.

Table 5-1 Fixed issues in 4.5.1 *(continued)*

Fixed Incidents	Descriptions
3552962	FPolicy service should ignore corrupted `.tmp` file for finalizing and move ahead and start the service, instead of refusing to start.
3365514	Scan resync does not work in scenarios listed in incident.
3553434	Deleted path getting fetched in path_exist query.
3617741	Data Aging report does not honor exclusion of user when the computed user is the last option or the only option for the given owner method.
3526117	In path csv upload with a folder path which exists, but same name file is deleted, the report runs for FILE instead of FOLDER.
3526108	In the report wizard, if a SharePoint folder is selected, on EDIT, the type is shown as unknown and path is displayed as CIFS path style instead of SharePoint path.
3441687	The custom attribute column name in DQL does not ignore case.
3510237	UTF8 characters are encoded using Windows default character encoding in BIRT HTML report output.
3510176	Report: in case of report output (PDF), page breaks inserting incorrectly for certain reports.
3511015	Report: `report.exe` resolves the DFS path and should use the same in the report progress output.
3510539	Upgrading from version 301RP8 to 4.5: archived segments are not asked to restore during upgrade.
3591682	Active Directory scan fails while discovering the domain users if timeout occurs.
3573527	Full scan for share fails with the error code: V-378-1312-102.
3508323	The server statistic page shows overlapping charts in GUI.
3488423	If the IndexWriterJob and the CollectorJob are set to Never then IndexWriterJob_Size & CollectorJob_Size jobs should be set to Never.
3488383	Remove unnecessary stats for the Portal node.
3488183	Remove unnecessary jobs from Portal nodes.
3087723	Active Directory scan fails where there is multi-value custom attribute with hundreds of values.

Table 5-1 Fixed issues in 4.5.1 *(continued)*

Fixed Incidents	Descriptions
3601287	Active Directory scan fails while discovering the domain users.
3389526	On the Portal node the FileTransferJob failed to transfer file from inbox\tmp to workflow\inbox
3583328	Share name is wrongly getting added in Data Insight when the share name contains the characters: ' and &.
3549344	ContextMap save table data contains "-1" for lot of field, where as GUI shows null.
3508639	Entries having comma (,) in the CSV files fails for CSV upload functionality throughout the product.
3478876	Deletion of msu/device should delete .lst file under <datadir>\scanner\lst of Collector or Windows File Server node.
3547499	For the non-existing users/groups in `customattr.csv` file, attribute value should not get added in attr and textvalue tables.
3585607	While executing workflows, temporary reports for Entitlement Review are stored under `installdir/bin/null` folder which occupies too much disk space.
3551120	Custom action with the expand folder option fails to expand non-CIFS folders and hence generated workflow status remains in-progress as the workflow_paths table is empty.
3548112	In the Management Console, the Attribute query (**Workspace** > **Users**) should show the edit option for existing queries.
3597995	Sorting on saved credential page not working.
3502504	Entitlement Review workflow: There is no way to know which users and groups that are excluded under the Exclusion List tab.
3506279	Workflows: Data Selection tab - Select Paths having Custodian - Search for DFS paths does not work properly.
3513398	In Entitlement Review workflow, email is sent even when the paths are failed.
3513291	Ownership Confirmation workflow: Data Selection pane (Select Resources having Custodians)does not work as expected if you have custodian assigned at web application and site collection levels and you click Select All Resources.

Table 5-1 Fixed issues in 4.5.1 *(continued)*

Fixed Incidents	Descriptions
3521333	Ownership Confirmation workflow: Clearing the selected action for some paths in certain situations still results in submitting all paths instead of submitting only the paths which have actions associated with them.
3528789	Windows File Server fails to scan. Both the credential tests fail in Data Insight Console.
3586006	Exclude rules do not work - First exclude rule contains the criteria for user, IP address, and prefix. The second exclude rule contains the file extension.
3612194	Maximum kernel ring buffer size changes to 0 when a node template is used.
3441387	Workflow template creation: if you choose a different font for custodian name variable, the value of the variable name is not displayed in the mail. This issue is resolved when you apply the style to the entire variable including $ and {}.
3602705	Indexer fails to process a SharePoint audit file, stating: Path '/' can not be a file - Unable to add event to index. error=203.
3526657	report.exe crashes for non-existing paths or for paths with no activity..
3524480	Add pagination to SharePoint web service during enabling of event handler feature to SharePoint.
3463724	EMC Celerra and Isilon: When filer is disabled, raw audit files should not be generated.
3507610	In the Folder-centric view for **Permissions**>**Recommendations**: When a group is expanded, a disabled user is displayed as an enabled user.
3547163	Inactive Data By File Group report may crash.
3544968	DQL- query returns incomplete data for permissions query for msu.
3537652	queryd crash- get_analytics is crashing on 4.5GA build.
3525526	In SharePoint if the Path Permissions report is configured to run on unique paths, the report shows paths with non-unique permissions.
3540130	Custodian report is failing that involves direct and inherited custodians coming from the same device/share.

Table 5-1 Fixed issues in 4.5.1 *(continued)*

Fixed Incidents	Descriptions
3543888	DQL- msu query that references device object crashes.
3543883	DQL- syntax check does not work in case of query that involves nested objects.
3501122	PORTAL- If remote communication service is down, Data Insight still shows paths coming from remote indexer under '**Show paths having custodian**' panel.
3496942	DQL- In case of invalid syntax query returns nothing, this causes blank popup on console.
3514519	Portal: Ownership Confirmation- DLP policy filter is not working.
3493231	DQL- root level site collection not printed in path table if its absname is specified in IF condition.
3507740	Entitlement report for SharePoint - Report returns wrong permissions if group G1 and its parent group PG1 has permission on same path.
3489596	Inactive Data By File Group Report- report ran against any folder within share returns share level data
3487464	Portal Delegation: delegation trail column in workflow details panel needs to be provided.
3375457	Report-Custodian report: Setting up keep intermediate DBs true results in report failure.
3605262	DQL Query does not return values for multivalued attribute such as dlp_policies if you prefix the attribute name with object, and do not provide FORMAT specifier.
3588184	DQL- Presence of same column twice in Get clause results in merge failure.
3600369	Under Services panel, DataInsightWorkflow service should not be shown for Collector, Collector+Indexer node. Also DataInsightGenericCollector,DataInsightWorkflowservice should be hidden for Linux Indexer.
3593331	DQL- Global MSU query returns wrong last_activity_time.
3570945	`dqlexec` may crash if large number of values are present in IF condition.

Table 5-1 Fixed issues in 4.5.1 *(continued)*

Fixed Incidents	Descriptions
3575288	list_custodian query is executed for each custodian, instead of executing just once through report framework, when data is selected using custodians.
3568072	Reports- Send latest copy of email does not work with email id ends with .local.
3548614	DQL- MSU query that involves permission computation does not work for MSU type NFSv3.
3538893	DQL- The database link provided in report email notification does not work.
3538735	Portal Entitlement Review- Console fails to assign custodian to shares, even though custodian already exists in Data Insight.
3240597	Unable to read property for log rollover for sharepoint and Enterprise Vault clients.
3547793	Workflow should also process sensitive files which do not have any incident associated with them.
3535186	Database locking issues if a single workflow db is accessed by over 100 users simultaneously.
3596074	The msu_summary table in dashboard database fails to populate with data.
3510996	Report: If report is run on DFS paths, incorrect count is displayed in View Report progress > report execution on node.
3526315	Fix SharePoint inherited permissions flag in the Dashboard summary report.
3430460	If using IE 9, you cannot edit the Member count field in Entitlement Review report.
3586907	DataInsightFPolicy should not disconnect from filer due to crossing threshold for NFS latency when only CIFS shares are being monitored from Data Insight.
3612865	Indexwriter crashes while processing audit files.
3581623	Data Insight FPolicy service trying to connect to a NetApp filer that is no longer configured.
3519318	cel_util crashes when no command is provided while invoking it.

Table 5-1 Fixed issues in 4.5.1 *(continued)*

Fixed Incidents	Descriptions
3561296	cel_util.exe should not discover NFS exports.
3510980	Provide an additional logging under fpolicycmod logs if events database is locked.
3587664	root directory "/" may not get listed in DQL output when there are no other directories in the share.
3536600	The segment file mismatch with segment size in database is more than on disk size should not crash segment read.
3630066	Rolling Patch upgrade is disabled for Indexer+Collector node.
3523967	If a file is selected in report creation wizard under data selection, on edit, it is displayed as a folder.
3510446	mxcustodian crashes on Linux Indexer when input csv contains i18n paths.
3620906	Multibyte characters are not handled for encoding or decoding URL for portal.
3577068	Login administrator as custodian feature - improvements.
3462848	Entitlement Review report generates incorrect output in case of nested groups, resulting in showing blank rows in Entitlement Review portal.
3508654	Reports- Report framework maps invalid path to any random device then triggers and executes report successfully.
3573534	Need to handle 4.5.1(i.e 4.5.1.build number) in the SORT code.
3507761	Need to add action "view migration status" for SharePoint web applications.
3228192	Show output on GUI even though report fails at copy output to stage.
3455300	We need to enhance DlpImportSensitiveFilesJob to map DFS share with actual physical share.
3508392	FURTHER consolidate DO policy across ContextMap and get_data_owner() and mxcustodian.
3591005	dqlexec membership 'group.iscircular' may mess up with 'depth'.
3599519	DQL- Global MSU query is returning wrong last_activity_time.

Table 5-1 Fixed issues in 4.5.1 *(continued)*

Fixed Incidents	Descriptions
3341634	During the creation of Incident Remediation workflow, re-selecting **path with custodian** does not work.
3381820	Remove options which are not related to Portal node from Download Logs list wizard.
3628337	GUI does not show correct schedule when filer's scan schedule is edited.
3601169	Report: Edit icons are not showing correctly. Issue observed for SharePoint sites only.
3534151	1) Report footer should accept UTF-8 characters. 2) report header cannot be changes to utf-8 characters. 3) html output via BIRT report does not support UTF-8 characters.
3629122	Show appropriate message when web-app addition fails because of adding duplicate web application.
3509902	Report: Getting exception in Webserver logs while running a report with container. It appears when a container is added to a report and the report is edited or run. It tries to resolve all container as path and throws exception.
3554645	CEE supports only one Auditing connector for Isilon and not multiple.
3533663	Avoid IndexWriterJob and ActivityIndexJob on the index only in case it is migrating out of the current node.
3632817	path:device.capacity is slow and cause memory leak.
3627353	Security event should not change last access timestamp for file and folders because lot of times it does not get updated on file system.
3602443	ChangelogJob throws exception when it fails to merge a pathdb file and tries to publish an event.
3604947	After upgrading a deployment to 4.5.1, the GUI in all browsers using version 4.5 on that deployment should refresh post-upgrade automatically on next login.

Appendix A

Getting help

This appendix includes the following topics:

- Using the product documentation
- Contacting Symantec
- Symantec Data Insight Support
- Using the support Web site
- Subscribing to email notification service
- Accessing telephone support

Using the product documentation

The following guides provide information about Symantec Data Insight:

- *Symantec Data Insight Installation Guide*
- *Symantec Data Insight Administrator's Guide*
- *Symantec Data Insight User's Guide*

Contacting Symantec

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

Symantec Data Insight Support

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

http://www.symantec.com/business/support/overview.jsp?pid=58588

Using the support Web site

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

http://www.symantec.com/enterprise/support/assistance_care.jsp

From there you can:

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

Subscribing to email notification service

Subscribe to the Symantec Email notification service to be informed of software alerts, newly published documentation, Beta programs, and other services.

http://www.symantec.com/enterprise/support/assistance_care.jsp

Select a product and click E-mail Support at the bottom of the page. Your customer profile ensures that you receive the latest Symantec technical information pertaining to your specific interests.

Accessing telephone support

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