Veritas Data Insight Release Notes

7.1

September 2024

VERITAS™

Contents

Chapter 1

Overview of this release

This chapter includes the following topics:

About Veritas Data Insight

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

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

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

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

Data Insight provides the following information:

- Who owns the data

- Who is responsible for remediation
- Who has seen the data
- Who has access to the data
- What data is most at-risk
- Frequency of usage of data

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

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

Data Insight enables you to analyze the activity on high-risk folders by providing in-depth analysis of usage and collaborative activity. The analysis helps you classify users based on configured attributes to better understand the activity pattern of users in your environment.

- Permission remediation

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

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

- Content classification

  Data Insight lets you classify content on data sources that it monitors by providing means to define classification rules (policies) that let you specify values (tags) that you can assign to any matching items. The classification feature works in conjunction with the policy framework provided by Veritas Information Classifier to assign tags to files. For example, a content scan may search for items whose contents include a credit card number and assign a tag of "PII" (for "personally identifiable information") to any that do.

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

  For more information about setting up classification and initiating classification requests, see the *Veritas Data Insight Classification Guide*.

- 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.

System Requirements

For more information, refer to Veritas Data Insight Software Compatibility List document.

What's new in Veritas Data Insight 7.1

The following features, enhancements, or changes are now available in Data Insight 7.1. or after upgrading to Data Insight 7.0 from previous versions.

New Content Sources

- *Discover, scan and classify CIFS shares on Azure NetApp Files (ANF):* Azure NetApp Files (ANF) is a managed Azure service that provides CIFS and NFS storage volumes. Data Insight provides connector to discover, scan and classify CIFS content from ANF. This provides for a common management pane for managing sensitive content stored in ANF in the Azure cloud.
- *Discover, scan, classify and monitor NFSv4 shares on NetApp clusters:* Data Insight 7.1 introduced support for Linux based collector for NFSv3 shares. In Data Insight 7.1, we are extending support for NFSv4 shares on NetApp.

Better Reporting

- *Data Ex-filtration Report:* Provided an optional configuration which helps capture the number of hits along with classification policy violations. This information helps report the quantum of sensitive hits within a document. It can be used to surface materiality of data breach by reporting on amount of sensitive hits in the potential ex-filtrated data.
- *Executing custom reports (DQLs) on selected indexers:* This feature helps to prioritize the report execution on selected indexers to reduce the overall cycle time of report execution.
- *Performance enhancements on Path Permissions report:* optimized the reporting algorithm to make the report run more efficiently.

Core Product Features

- *Support for Hybrid SVMs on NetApp:* discover, scan, classify and monitor content shared using multiple protocols on the same SVM.
- *Support for Classification server pool for M365 content:* This feature helps to balance out and improve throughput of classification runs by leveraging classification server pools for classifying M365 data.
- *Integration with VIC 4.7.1* providing better stability, performance and access to policy enhancements like authentication policy.

- *Integration with NetApp 9.14.1:* Data Insight now supports NetApp's persistent store volume to decouple the I/O operations with FPolicy audit event processing to reduce client latency.

Usability Enhancements

- *Microsoft Purview (MIP) labeling:* Automate VIC policy creation to read MIP labels from labeled files at source.
- Remove a MIP label from files stored in CIFS sources.
- Support for new Microsoft Purview labeling client.
- Automate retries for scan ingestion failures due to repeatable errors (memory/ disk error, resource contention) to reduce index backlog and manual touch points.

Performance Improvements

- CIFS scanning workflow improvements leveraging V3 scanner, leading to 50% reduced cycle time
- SharePoint Online scanning functional and performance tunings leading to 70% improvement in scanning throughput

Classification Engine upgrade

New classification policies are introduced in every release expanding the compliance and privacy use-cases to newer markets. Data Insight now integrates with version 4.7.1 release of classification engine, which brings in following new enhancements, policies, and patterns for automatic content classification for supported workloads:

Enhancements and fixes

- Classification of emoji-based policy conditions is supported.
- Handling long list of keywords: this feature helps the user in managing long list of keywords by using the Expand option in policies and patterns. The user can perform following additional operations:
  - Search a keyword in the existing list.
  - Sort the existing list alphabetically.
  - Import keywords in CSV format.
  - Export keywords list in CSV format.
- Response time of classification API has been optimized, increasing the overall throughput for classification.
- Regex evaluation failures as part of Sentiment Analysis have been rectified.

- The content extraction issue in case of CSV file type has been fixed.
- Classification failure in policy conditions using sliding window proximity has been addressed.
- Support for TLS 1.3.

Policies

The following new Policies are added:

- Offensive Terms Policy
- Gifts and Entertainment Policy
- Resumes / CVs Policy
- United States National Institute of Standards and Technology (NIST) 800-171 Policy

The following existing Policies are updated along with the patterns:

- Off Channel Signaling Policy
- High Risk Securities - Complete List Policy
- High Risk Securities - Other Policy
- High Risk Securities - Large CAP Policy
- High Risk Securities - Small CAP Policy
- High Risk Securities - Mid CAP Policy
- Authentication Policy
- Offensive Language

Patterns

The following new Patterns are added:

- Offensive Terms - Low Confidence
- Off Channel X - High Confidence
- Off Channel X - Low Confidence
- Offensive Terms - High Confidence
- Off-Channel Facebook Phrases
- Off-Channel Telegram
- Off-Channel Chomp Phrases
- Off-Channel Discord Phrases

- Off-Channel Weibo Phrases
- Off-Channel Amino
- Off-Channel Skype Phrases
- Off-Channel WeChat
- Off-Channel Telegram Phrases
- Off-Channel IMO phrases
- Off-Channel Threads Phrases
- Off-Channel Kik
- Off-Channel Signal Phrases
- Off-Channel Discord
- Off-Channel Weibo
- Off-Channel Amino Phrases
- Off-Channel BBM phrases
- Off-Channel Substack
- Off-Channel Snapchat Phrases
- Off-Channel Instagram Phrases
- Off-Channel Silence Phrases
- Off-Channel WhatsApp Phrases
- Off-Channel Substack Phrases
- Off-Channel Pulse Phrases
- Off-Channel Element Phrases
- Off-Channel BBM
- Off-Channel Baidu Phrases
- Off-Channel Slack Phrases
- Off-Channel WhatsApp
- Off-Channel Grindr
- Off-Channel Tinder Phrases
- Off-Channel Tango Phrases
- Off-Channel Blink Phrases
- Off-Channel Skype

- Off-Channel Tango
- Off-Channel LinkedIn Phrases
- Off-Channel Reddit Phrases
- Off-Channel Chomp
- Off-Channel Kik Phrases
- Off-Channel Tinder
- Off-Channel Grindr Phrases
- Off-Channel Baidu
- Off-Channel QQ Phrases
- Off-Channel Matrix Phrases
- Off-Channel Dust Phrases
- Off-Channel WeChat Phrases
- Off-Channel Twitter Phrases
- Off-Channel Dropbox Phrases
- Off-Channel Citrix ShareFile Phrases
- Off-Channel Phone
- Off-Channel Email
- Ticket, Tickets or Tix
- Items and Diversions of Value
- North American Major Professional Sports Teams
- Professional Football (Soccer) Teams Lower Confidence
- Professional Football (Soccer) Teams
- Gifts, Donations and Sponsorships
- Sports and Entertainment Events

The following Patterns are updated:

- Off-Channel Low Frequency Channels
- Off Channel X - Low Confidence
- High Risk Securities - Tickers
- High Risk Securities - Tickers Mid CAP
- High Risk Securities - Names Small CAP

- Off-Channel Fileshare Proximity Terms
- High Risk Securities - Names Other
- High Risk Securities - Names Mid CAP
- High Risk Securities - Tickers Large CAP
- Off Channel X - High Confidence
- High Risk Securities - Tickers Small CAP
- High Risk Securities - Names Large CAP
- High Risk Securities - Names
- Programming Language Source Code.
- Australia Postal Address
- Bank Account Number pattern for different countries. For example, Germany Bank Account Number, Greece Bank Account Number and so on.

Fixed Issues

List of *Fixed Issues* in this release is as follows:

Table 1-1

Issue Number	Description
CFT-5701	Share Discovery failed for SPOnline.
CFT-5814	Classification is hung up for multiple requests.
CFT-5845	Classification Request ID : 466 is hung
CFT-5856	Post upgrading from 6.5 to 6.6, LocalUserScanJob bugchecked with 0xc0000374 - A heap has been corrupted. Error creating local users database for filer CO-NETAPP-CIFS
CFT-5857	Issues with Set MIP Label creating multiple requests
CFT-5858	MIP Labeling doesn't work due to special characters in the File Path
CFT-5859	Post upgrading to 6.5.1 or 6.6, customers are experiencing NetApp Shares Discovery Failures "Code: Other Message: "Unable to execute a NetAPP API"

Table 1-1 *(continued)*

Issue Number	Description
CFT-5876	Sharepoint Online site scan failing with Exit code -1
CFT-5878	IndexDB copies deleted by idxwriter.
CFT-5880	Deleting share from Isilon is not reflected in Data Insight, causes scans to still be configured and eventually fail.
CFT-5900	Duplicate entries for Access Zone based discovery.
CFT-5908	Unable to perform any filer migration if classification is running
CFT-5993	Reportrun output folder missing using Download Logs
CFT-5994	CIFS share from EMC unity filer failed to add to DI
CFT-5995	DataInsight Console takes a long time to load pages.
CFT-6036	MIP tag not getting updated on UI even after successful MIP labeling
CFT-6037	When fpolicy is disconnected users are unable to write to volume
CFT-6043	Unexpected GUI Behavior, unable to save existing DQL report
CFT-6090	File does not exist or is not accessible.
CFT-6099	Issue in installcli during push install of Hotfix - If incorrect IP/FQDN server name provided in input csv, incorrect message getting displayed

Known Issues

List of *Known Issues* in this release is as follows:

Table 1-2

Issue Number	Description
DI-19013	While migrating Indexer, *In progress* classification requests are not processed. **Workaround** Stop the *In-progress* Classification requests **manually** before initiating Indexer migration.
DI-19588	After classifying NetApp C-mode (NFS), large number of read events are generated.
DI-19602	After migrating Windows collector to Linux collector, only **NFS** shares are supported.

For a list of Known Issues before version 7.0, click here

Chapter 2

Software limitations

This chapter includes the following topics:

Tags

Data Insight considers all files classified by Veritas Information Classifier (VIC) as sensitive files. There can be instances where a VIC policy is created to determine non-sensitive files. Please consider tag information before making any decision based on sensitive flag.

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

Parallel scanner limitations

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

- Parallel scanner does not support incremental scan. Only full scans are supported.
- Parallel scanner cannot be run for the NFS shares.
- Parallel scanner does not support filtering out shares based on the **Exclude Rules** configuration.
- Support for scanning of circular or cyclic symbolic links is not available.
- Support for scanning junction-based paths is not available.

Windows File Server support

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

Report configuration limitation in Path Permission reports

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

Known limitation for NetApp Cluster-Mode support

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

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

Appendix A

Getting help

This appendix includes the following topics:

Using the product documentation

The following guides provide information about Veritas Data Insight:

- *Veritas Data Insight Installation Guide*
- *Veritas Data Insight Administrator's Guide*
- *Veritas Data Insight User's Guide*
- *Data Insight Self-Service Portal Quick Start Guide*
- *Veritas Data Insight Software Compatibility List*

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

Data Insight Support

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

www.veritas.com/support

From there you can:

- Contact the Veritas Support staff and post questions to them.
- Get the latest software patches, upgrades and utilities.
- View updated hardware and software compatibility lists.

- View Frequently Asked Questions (FAQ) pages for the products you are using.
- Search the knowledge base for answers to technical support questions.
- Receive automatic notice of product updates.
- Read current white papers related to Veritas Data Insight.