Veritas Data Insight Installation Guide

6.6.1

December 2023

VERITAS™

Veritas Data Insight Installation Guide

Documentation version: .1

PN:

Legal Notice

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

http://www.veritas.com

.

Technical Support

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

Our support offerings include the following:

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

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

www.veritas.com/support

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

Contacting Technical Support

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

www.veritas.com/support

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

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

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

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

Licensing and registration

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

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/support

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

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

Support agreement resources

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

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

Contents

Technical Support 4

Chapter 1 Understanding the Veritas Data Insight architecture 10

About Veritas Data Insight 10
About the Management Server 13
About the Collector worker node 13
About the Collector 14
About the Scanner 14
About the Indexer worker node 15
About the Classification Server 15
About the Self-Service Portal node 16
About Communication Service 16
About the DataInsightWatchdog service 17
About the DataInsightWorkflow service 18
About Veritas Data Insight installation tiers 18
About three-tier installation 18
About two-tier installation 18
About single-tier installation 18

Chapter 2 Preinstallation 20

Pre-installation steps 20
Minimum system requirements for Data Insight components 22
System requirements for classification components 26

Chapter 3 Installing Veritas Data Insight 28

About installing Veritas Data Insight 28
Federal Information Processing Standards (FIPS) 29
Performing a single-tier installation 30
Performing a two-tier installation 31
Performing a three-tier installation 32
Installing the Management Server 32
Installing the worker node 35
Installing the Classification Server 37

Installing the Self-Service Portal 39
Installing a Linux Indexer worker node 41
Installing Veritas Data Insight in Azure Cloud Environment 46
Installing Veritas Data Insight in AWS Cloud Environment 47

Chapter 4 Upgrading Veritas Data Insight 48

Upgrading Data Insight to 6.6.1 48
Upgrading the product data using the Upgrade Data Wizard 53
Names and locations of cache files 54
Upgrading the Data Insight web service for SharePoint 55

Chapter 5 Post-installation configuration 56

Post-installation configuration 56
Registering the worker node 56
About post-installation security configuration for Management Server 58
About SSL client/server certificates 58
Enabling CA signed certificates for inter-node communication 58
Generating Management Console certificate 59
Configuring your corporate firewall 65

Chapter 6 Installing Windows File Server agent 66

About Windows File Server agent 66
Installing Windows File Server agent manually 67
Configuring the Windows File Server using ConfigureWindowsFileServer.exe 68

Chapter 7 Getting started with Data Insight 71

About the Data Insight Management Console 71
Logging in to the Data Insight Management Console 71
Logging out of the Data Insight Management Console 72
Displaying online help 73

Chapter 8 Uninstalling Veritas Data Insight 74

Uninstalling Veritas Data Insight 74

Appendix A Installing Data Insight using response files 76

About response files 76
Installing Data Insight using response files 76
Sample response files 77

Chapter 1

Understanding the Veritas Data Insight architecture

This chapter includes the following topics:

- About Veritas Data Insight
- About the Management Server
- About the Collector worker node
- About the Indexer worker node
- About the Classification Server
- About the Self-Service Portal node
- About Communication Service
- About the DataInsightWatchdog service
- About the DataInsightWorkflow service
- About Veritas Data Insight installation tiers

About Veritas Data Insight

Veritas Data Insight is a solution for unstructured data governance. It monitors file system activity and helps answer questions such as who is using the data, who owns the data and who has access to the data. Data Insight gives you full visibility into data access, which helps drive security remediation and compliance efforts.

Based on a distributed client-server architecture, a typical Data Insight deployment consists of the following:

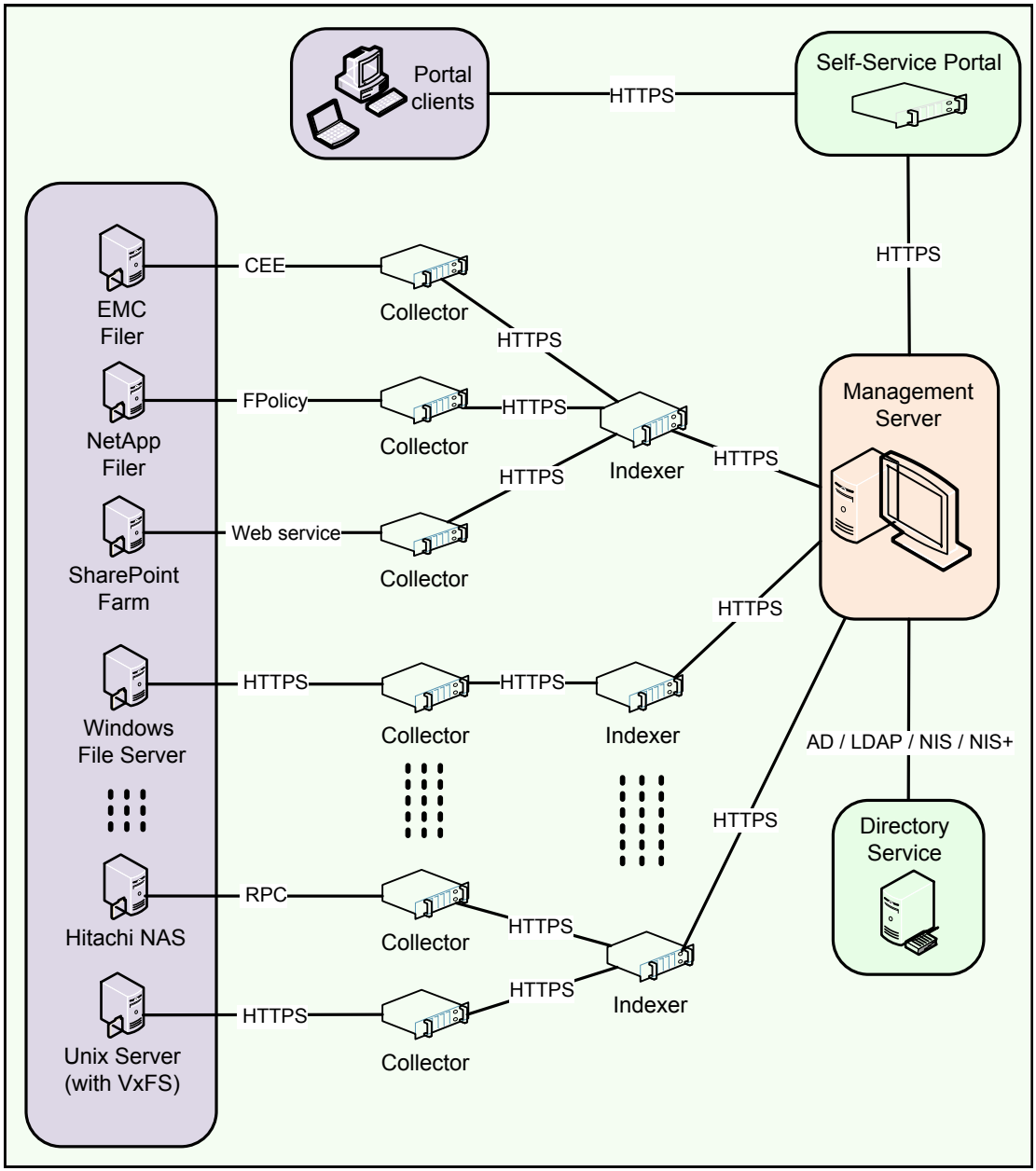
- Management Server
  See “About the Management Server” on page 13.
- Collector worker nodes
  See “About the Collector worker node” on page 13.
- Indexer worker nodes
  See “About the Indexer worker node” on page 15.
- Self-Service Portal nodes
  See “About the Self-Service Portal node” on page 16.

The way you deploy Veritas Data Insight depends on the size of your organization, the geographical distribution of your datacenters, and the number of storage devices that you want Data Insight to monitor.

See “About Veritas Data Insight installation tiers” on page 18.

Figure 1-1 illustrates the Data Insight architecture.

Figure 1-1 Data Insight architecture



About the Management Server

The Management Server is the main component of a Data Insight deployment and hosts the product's web interface. In the single tier deployment, you can also configure the Management Server to connect to multiple storage devices to extract access events and store the extracted data locally to answer queries. Your deployment can only have one Management Server. It also runs the action framework that helps you to take remedial action on your data and enables you to send archiving requests to Enterprise Vault.

The Data Insight Management Server performs the following functions:

- Hosts the Web-based graphical user interface (GUI).
- Scans directory services to obtain information about users in the organization and correlates this information with the access events.
- Ensures that the configuration data on the worker nodes is synchronized with the Management Server's configuration data.
- Authenticates the Data Insight users. It also runs the DataInsightWorkflow service that enables actions on your data.

Users interact with Data Insight primarily through the Data Insight management console. In this interaction, the user connects to the Web server through a Web browser. By default, the Web server runs on HTTPS port 443.

About the Collector worker node

The Collector worker node is a host machine that scans data source hierarchies in your environment and collects access events from data sources such as NAS devices, SharePoint Web Applications, and cloud sources. Data Insight uses this information to perform advanced reporting on the business owners of data and the access history of data. By scanning for file metadata and security descriptors, it reports on the loopholes of permissions on files and folders. The details that are captured by the Collector node also help you find stale and orphan files in the scanned data repositories.

You can have multiple Collector worker nodes attached to the Management Server for load balancing. You can configure each collector node to connect to a subset of storage devices to extract file system metadata and extract access events from these devices. Each data source can have exactly one Collector node associated with it.

Note: Veritas recommends that the Collector worker nodes share a fast network with the storage devices.

A Collector worker node consists of the following components:

- Collector
- Scanner

About the Collector

The Collector (Audit Pre-processor) is a Data Insight process that enables you to collect and parse access events from various storage repositories. The Collector examines the access events available on these storage systems to parse the events that report the read, write, create, delete, and rename activity on files or folders. The access events are processed in batches that consist of several thousand events. Each batch of events that are collected in a cycle is stored in a separate file with appropriate timestamp that indicates the ending time of the last entry in that batch. This data is pruned based on exclude rules or events that are not from the configured shares, site collections or equivalent data sources, and is then segregated on a per-share basis. These files are periodically shipped to the appropriate Indexer node.

Data Insight collects information about access events from various storage repositories through exposed vendor APIs.

For detailed information about which audit service is appropriate for your data source, see the *Veritas Data Insight Administrator's Guide*.

About the Scanner

The Scanner is a Data Insight process that scans enterprise data repositories by mounting CIFS and NFS network shares or accessing SharePoint servers using the Data Insight web service. The Scanner captures the file or folder hierarchy of a shares, site collections or equivalent data sources and helps you collect in-depth information about files and folders.

Note that the Scanner is a scheduled process. Schedule of the scan can be controlled at the worker node level, filer/web application level, or the shares, site collections or equivalent data sources level. For detailed information on administration topics (including how to schedule scanning) see the *Veritas Data Insight Administrator's Guide*.

Depending on how the scans are scheduled, the Scanner stores the collected data in separate database files, with appropriate timestamp. For each subsequent incremental scan, the Scanner only scans the files that are added or modified since the last full scan. In case of a full scan, the Scanner scans the data source hierarchy again. These files are eventually uploaded to the Indexer node using the Communication Service.

See "About the Indexer worker node" on page 15.

The Scanner captures information about the following attributes for each file or directory:

- The size of a file.
- The access time.
- The creation time.
- The modification time.
- The Security ID of the file owner (SID).
- The Access Control Lists (ACLs).

The details the Scanner captures helps in the computation of metadata-based data ownership.

About the Indexer worker node

The access events and filesystem metadata that are collected from the storage repositories are periodically uploaded to the Indexer node. You can choose to have multiple indexers for load balancing purposes. Each storage repository can have exactly one Indexer node associated with it. The indexer performs the following functions:

- Uses the data from the collector process and scanner to create index files.
- Uses the index files to generate report output and service queries from the Management Console.

About the Classification Server

The Classification Server provides a platform for deploying Veritas Information Classifier service, which lets you author policies and manage classification. The Veritas Information Classifier administration console can be invoked from the Data Insight Management Console.

The Classification Server runs the `DataInsightVICClient` and `DataInsightVICServer` services. This server does not require a separate license. It is functional with the Data Insight base license.

The Classification Server receives file paths for classification in the form of requests from the Indexer nodes. The Classification Server fetches content from the associated data sources. It evaluates content by using any of the enabled policies in the administration console of Veritas Information Classifier. It reads the files to

search for content that matches policies, and assigns tags to files to generate classification results. The tags are sent to the Indexer and displayed on the Data Insight console and are available for querying reports using DQL Reports.

You can also have multiple Classification Servers. Typically, a Classification Server is mapped to a Collector. Note that instead of installing a standalone Classification Server, you can also assign the classification role to a Data Insight server, however this is not a recommended configuration. It is also recommended that a Classification Server should be geographically closer to the data sources that it needs to classify.

For more information about using and configuring the classification feature, see the *Veritas Data Insight Classification Guide*.

About the Self-Service Portal node

The Self-Service portal provides an interface for custodians of data to take remedial actions on the data classified by Symantec Data Loss Prevention. It also lets custodians confirm ownership to folders that they own, and review entitlements to those folders and classify sensitive files for retention based on their business value. Custodians take these actions based on workflows setup by the Data Insight administrator guided by specific business requirements of the organization.

The Portal node is attached to the Management Server and runs the DataInsightWorkflow and DataInsightPortal services. The portal interface, which is separate from the main Data Insight console, can be customized and branded as per customer's requirements.

The Self-Service Portal requires an Add-on license separate from Symantec Data Loss Prevention and Data Insight license. The Portal is available beginning Data Insight version 4.5. You can use the portal for remediating incidents pulled from Data Loss Prevention 12.5 or later.

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

About Communication Service

Each node in a Data Insight deployment runs a process called Communication Service. This service is responsible for all inter-node communication. Communication Service uses Secure Sockets Layer (SSL) to secure communication between the Data Insight nodes. The SSL keys are generated during installation.

By default, Communication Service connects through sever port 8383. This port must be visible to bi-directional HTTPS traffic between all Data Insight nodes. The service is also responsible for scheduling various tasks on a Data Insight node,

which include, scheduling file system scans and uploading files to the Indexer worker node.

About the DataInsightWatchdog service

The DataInsightWatchdog service monitors the disk usage on the Windows File Server agent node and prevents it from running out of disk space by implementing safeguards. When the disk usage crosses the configured threshold, the DataInsightWatchdog service initiates the following safeguards:

- Ensures that the Communication service stops all activities that generate data that can be reconstructed. For example, scanning.
- Deletes all scan snapshot files, files in the `scanner/err` folder, and the volume usage database files in the `outbox` folder. Deleting these files creates additional disk space so that event monitoring can continue.
- If the threshold is crossed again, and there is no other data that can be deleted, the DataInsightWatchdog service stops the DataInsightWinnas service, which in turn stops all event monitoring.
- If the size of the `<DATADIR>/data` folder continues to grow, the DataInsightWatchdog service completely stops the Communication service.

The safeguard mode is reset once the disk space is available over the specified threshold. The DataInsightWinnas service and the Communication service, if stopped, is started, and scanning resumes normally.

When the Windows File Server agent is in the safeguard mode, its status appears as **Failed** on the Data Insight servers listing page on the Management Console.

In addition to enforcing safeguards on the Windows File Server nodes, the DataInsightWatchdog service also runs on each Data Insight server. The service monitors the CPU, disk, and memory on each node. If CPU, disk, and memory are consistently high for a server, the service sends out notifications to configured email recipients.

The node safeguard feature is enabled by default with specific default values. You can configure the thresholds for initiating the safeguard mode from the **Settings** > **Global Settings** > **Scanning and Event Monitoring** page of the Management Console.

For more information about configuring the threshold values for initiating the safeguard mode, see the *Data Insight Administrator's Guide*.

About the DataInsightWorkflow service

The DataInsightWorkflow service is responsible for execution of all actions initiated from the Management Console or the Portal server, such as remediation of Data Loss Prevention (DLP) incidents, handling permission remediation, archiving data, and running custom action scripts to manage data. The service runs on the Management Server and the Portal nodes. By default, the DataInsightWorkflow service runs on port 8686.

The DataInsightWorkflow service is a multi-threaded execution framework which executes actions in parallel.

About Veritas Data Insight installation tiers

Veritas Data Insight supports three different installation types: three-tier, two-tier, and single tier. Your installation type depends on the total number of storage devices that you want Data Insight to scan and their geographical distribution. Single-tier installations are used for Proof of Concept (POC) deployments or smaller setups.

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

About three-tier installation

To implement the three tier installation, you must install the Management server, the Collector worker node, and the Indexer worker node on separate computers. Depending on the size of your organization, you can choose to have multiple Collector and Indexer worker nodes. When your storage repositories span datacenters that are geographically apart, you need multiple Collector worker nodes. When you have a very large number of storage repositories, you need multiple Indexer worker nodes. However, it is recommended that the Management Server and Indexer worker nodes must be co-located on the same network.

About two-tier installation

To implement the two-tier installation, you must install the Management Server and the Collector worker nodes on separate computers. When your storage repositories span datacenters that are geographically apart, you need multiple Collector worker nodes. In this mode, the Management Server also functions as the Indexer.

About single-tier installation

To implement the single-tier installation, you must install only the Management Server. In this mode, the Management Server functions as the Collector as well as the Indexer. Use single-tier installation only for POC deployments or smaller setups.

Note: You can start out with a single-tier deployment and gradually add worker nodes to transition your system to a two-tier or a three-tier setup as the number of sites and storage repositories increase.

Chapter 2

Preinstallation

This chapter includes the following topics:

- Pre-installation steps
- Minimum system requirements for Data Insight components
- System requirements for classification components

Pre-installation steps

Before you install the Veritas Data Insight servers, verify the following:

- Pre-installation steps
- Minimum system requirements for Data Insight components
- System requirements for classification components
- The Data Insight host has a minimum of 10 GB of available disk space.
- If you want to disable NTLM as an authentication method: There should be at least one Active Directory user (non-local), configured in DI, who can authenticate using Kerberos.
- The Management Server node can connect to the domain controller of each domain that needs to be scanned.
- The Data Insight server that hosts the Collector worker node can connect to the filers that it is supposed to monitor.
- A bi-directional network connection on port 8383 exists between the Management Server and the worker node(s), and between the worker node(s).
- The firewall is configured to allow https/http access to the required ports. The Management Server should also be allowed access to *http://sort.veritas.com*, either directly or through a proxy, to get patch notifications.

- The keystore file (commd.keystore) that enables secure communication between the worker node and the Management Server is copied to the worker node from the Management Server.

  Note: Manually copying the commd.keystore file is only necessary if installing the nodes individually. If you are using the push install feature, handling the commd.keystore is part of the feature.

  See "Registering the worker node" on page 56.

- You have obtained the credentials required during software installation. These credentials are required to log into the Data Insight Console after the installation.

  Note: Additional credentials are required when you configure storage repositories and directory services, and for scanning of shares, site collections or equivalent data sources. For a list of these credentials, see the *Veritas Data Insight Administrator's Guide*.

- Prepare for SMTP Alerting. When installing the Management Server, ensure that you have the details of your SMTP server and authentication details, if any, available.
- Prepare for Exclude Rules. Gather a list of paths to be excluded while scanning. For access events, gather a list of IP addresses, user accounts, or file extensions whose access events should be ignored. For more details, see the *Veritas Data Insight Administrator's Guide*.
- If you plan to enable Smart Classification, apply the following Windows updates on the Indexer nodes:
  - For Windows Server 2012 R2 install the update available at: https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows

Note: To allow classification of images, a software called Tesseract is installed on the Management Server, Collector nodes, and Classification server on Windows machines during the installation of Data Insight. The default location for the Tesseract installation is `C:\Program Files (x86)\Tesseract-OCR`. In case the Tesseract installation fails, refer to the Troubleshooting section in the *Veritas Data Insight Administrator's Guide* to manually install the Tesseract software.

Minimum system requirements for Data Insight components

Table 2-1 Minimum system requirements for Data Insight components

Component	Operating System	Minimum Hardware
Management Server	■ Windows Server 2012, 2012 R2 Supported editions: Standard, Essential, and Data center ■ Windows Server 2016. Supported editions: Standard, Essential, and Data center ■ Windows Server 2019. Supported editions: Standard, Essential, and Data center ■ Windows Server 2022 Supported editions: Standard and Data center VMware ESX virtual machines running supported operating systems. (Recommended - VMware ESX Server version 6.7 and 7.0.)	■ 32GB RAM ■ 16 CPUs

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

Component	Operating System	Minimum Hardware
Collector worker node	■ Windows Server 2012, 2012 R2 Supported editions: Standard, Essential, and Data center ■ Windows Server 2016. Supported editions: Standard, Essential, and Data center ■ Windows Server 2019. Supported editions: Standard, Essential, and Data center ■ Windows Server 2022. Supported editions: Standard and Data center VMware ESX virtual machines running supported operating systems. (Recommended - VMware ESX Server version 6.7 and 7.0.) **Note:** Enterprise Edition is supported when Windows Server 2012, 2012 R2, or 2016 is being used as the Collector node for NFS exports on devices.	■ 8GB RAM ■ 4 CPUs

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

Component	Operating System	Minimum Hardware
Indexer worker node	■ Windows Server 2012, 2012 R2 Supported editions: Standard, Essential, and Data center ■ Windows Server 2016. Supported editions: Standard, Essential, and Data center ■ Windows Server 2019. Supported editions: Standard, Essential, and Data center ■ Windows Server 2022. Supported editions: Standard and Data center Red Hat Enterprise Linux 7.x VMware ESX virtual machines running supported operating systems. (Recommended - VMware ESX Server version 6.7 and 7.0.)	■ 32 GB RAM ■ 16 CPUs

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

Component	Operating System	Minimum Hardware
Windows File Server Agent	■ Windows Server 2012, 2012 R2 Supported editions: Standard, Essential, and Data center ■ Windows Server 2016. Supported editions: Standard, Essential, and Data center ■ Windows Server 2019. Supported editions: Standard, Essential, and Data center ■ Windows Server 2022. Supported editions: Standard and Data center VMware ESX virtual machines running supported operating systems. (Recommended - VMware ESX Server version 6.7 and 7.0.)	■ 4 GB RAM ■ 2 CPUs

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

Component	Operating System	Minimum Hardware
Self-Service Portal Node	■ Windows Server 2012, 2012 R2 Supported editions: Standard, Essential, and Data center ■ Windows Server 2016. Supported editions: Standard, Essential, and Data center ■ Windows Server 2019. Supported editions: Standard, Essential, and Data center ■ Windows Server 2022. Supported editions: Standard and Data center VMware ESX virtual machines running supported operating systems. (Recommended - VMware ESX Server version 6.7 and 7.0.)	■ 8 GB RAM ■ 4 CPUs
Data Insight SharePoint Agent	■ Microsoft SharePoint 2013 ■ Microsoft SharePoint 2016 ■ Microsoft SharePoint 2019	Not Applicable

System requirements for classification components

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

Table 2-2 Minimum recommended system requirements for classification components

Component	If classification is enabled	If Smart Classification is enabled
Management Server	■ 32GB RAM ■ 16 CPUs	■ 128GB RAM **Note:** Provision additional 2 MB space per million paths. ■ 32 CPUs ■ 200 GB of free disk space for temporary files which are created during the classification process.
Indexer worker node	■ 32GB RAM ■ 16 CPUs	■ 128GB RAM **Note:** Provision additional 2 MB space per million paths. ■ 32 CPUs ■ 200 GB of free disk space for temporary files which are created during the classification process.
Collector worker node	■ 32GB RAM ■ 16 CPUs	Recommended minimum system configuration is 32GB RAM 16 CPUs
Classification Server	■ 32GB RAM ■ 16 CPUs	■ 32GB RAM ■ 16 CPUs
Windows File Server agent node	■ 8GB RAM ■ 4 CPUs	■ 8GB RAM ■ 4 CPUs

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

Chapter 3

Installing Veritas Data Insight

This chapter includes the following topics:

- About installing Veritas Data Insight
- Federal Information Processing Standards (FIPS)
- Performing a single-tier installation
- Performing a two-tier installation
- Performing a three-tier installation
- Installing the Management Server
- Installing the worker node
- Installing the Classification Server
- Installing the Self-Service Portal
- Installing a Linux Indexer worker node
- Installing Veritas Data Insight in Azure Cloud Environment
- Installing Veritas Data Insight in AWS Cloud Environment

About installing Veritas Data Insight

You can perform a three-tier, two-tier, or single-tier installation of Veritas Data Insight.

Note the following:

- At the end of the installation process, Data Insight creates a file `install_summary.html` in the `DataInsight\log\install` folder. This file records all the selections that are made on the installation wizard for a particular node.
- Data Insight records the upgrade history for the node in the `install_history.log` file in the `DataInsight\log\install` folder.

Both the files provide information that enable you to troubleshoot errors that may occur during the installation process.

Federal Information Processing Standards (FIPS)

About FIPS 140-2

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The FIPS 140-2 standard specifies the security requirements for cryptographic modules. It describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing. For more information on the FIPS 140-2 standard and its validation program, see the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program website at:
https://csrc.nist.gov/projects/cryptographic-module-validation-program

What does “FIPS 140-2 compliant” mean?

Where the Data Insight documentation states that a version of Data Insight is “FIPS 140-2-compliant”, it means the following:

- Data Insight uses FIPS 140-2-validated instances of algorithms and hashing functions in all instances where data is encrypted or hashed.
- Data Insight manages cryptographic keys and message authentication in a secure manner, as required of FIPS 140-2-validated cryptographic modules.

How Data Insight achieves FIPS 140-2 compliance

To achieve FIPS 140-2 compliance, Data Insight uses a FIPS 140-2-validated cryptographic module to provide the required cryptographic functionality. The Veritas Data Insight Cryptographic Module handles the encryption and decryption of passwords, the hashing of data, and random number generation.

The certificate numbers for the cryptographic modules that are used within the Veritas Data Insight Cryptographic Module are 1012, 1337, and 1894 on the list of validated FIPS 140-2 modules that the NIST publishes. See the following:

- **https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search#1012**
- **http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm#1337**
- **http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#1894**

Using Data Insight in a FIPS 140-2-compliant environment

Note the following points if you want to use Data Insight in a FIPS 140-2-compliant environment:

- FIPS 140-2-compliant versions of Data Insight store data on your storage devices using FIPS-compliant algorithms. However, you may want to check with the storage provider whether your storage devices are FIPS-compliant.
- If you want to run Windows in FIPS 140 compliance mode, you must enable the Windows group policy setting or local policy setting for FIPS-compliant algorithms. This setting restricts the use of non-compliant algorithms in the Microsoft .NET Framework.
  See the Microsoft knowledge base article at
  http://support.microsoft.com/kb/811833
- To use File System Archiving with placeholder shortcuts on an EMC Celerra device, you must configure the Celerra DataMover to use the Secure Sockets Layer (SSL) protocol. Check your Celerra documentation for details of FIPS compliance, if required.

Following modules are not FIPS compliant:

- NetApp Manageability SDK used for supporting NetApp devices
- Box SDK used for supporting Box cloud sources
- Amazon S3 SDK used supported Amazon S3 sources

Performing a single-tier installation

In single-tier mode, the Management Server functions as the Collector and the Indexer for the file servers.

To perform a single-tier installation

1. Perform the pre-installation steps.

   See “Pre-installation steps” on page 20.

2. Install the Management Server.

   See “Installing the Management Server” on page 32.

   Optionally install one or more Portal nodes.

   See “Installing the Self-Service Portal ” on page 39.

3. Perform other post-installation configuration.

   See “Post-installation configuration” on page 56.

Performing a two-tier installation

To perform a two-tier installation

1. Perform the preinstallation steps.

   See “Pre-installation steps” on page 20.

2. Install the Management Server.

   See “Installing the Management Server” on page 32.

   Optionally install one or more Portal nodes.

   See “Installing the Self-Service Portal ” on page 39.

3. Install one or more Collector worker nodes.

   See “Installing the worker node ” on page 35.

4. Register the worker nodes with the Management Server.

   See “Registering the worker node” on page 56.

5. Perform other post-installation configuration.

   See “Post-installation configuration” on page 56.

Note: Choose the two-tier installation mode when your filers are distributed across geographically remote locations that are far away from the Management Server. Install at least one Collector for each remote location. For example, the main data center of your organization is in New York, with additional filers in Singapore and Australia. In this case, the Management Server must be located in New York and there must be at least one Collector each in Singapore and Australia.

Performing a three-tier installation

To perform a three-tier installation

1. Perform the preinstallation steps.

   See “Pre-installation steps” on page 20.

2. Install the Management Server.

   See “Installing the Management Server” on page 32.

   Optionally install one or more Portal nodes.

   See “Installing the Self-Service Portal ” on page 39.

3. Install one or more Collector worker nodes.

   See “Installing the worker node ” on page 35.

4. Install one or more Indexer worker nodes.

   See “Installing the worker node ” on page 35.

   See “Installing a Linux Indexer worker node” on page 41.

5. Register the worker nodes with the Management Server.

   See “Registering the worker node” on page 56.

6. Perform other post-installation configuration.

   See “Post-installation configuration” on page 56.

Installing the Management Server

Data Insight recommends that you disable any anti-virus, pop-up blocker, and registry protection software before you begin the Veritas Data Insight installation process.

Throughout the installation process, the setup wizard displays installation information and options. Use the following options to navigate through the installation process:

To install the Management Server

1. Log on (or remote logon) as Administrator to the computer that is intended for the Management Server.

2. To launch the installer, right-click on the installer and choose the **Run as administrator** option for elevated administrative rights during the installation.

   `Veritas_DataInsight_windows_6_5_0_N_x64.exe,`

   where, `N` is the build number.

3 On the **Welcome to the Veritas Data Insight Setup Wizard** window, click **Next**.

Data Insight recommends that you let the installation process complete once you start it. You can uninstall the software after the installation is complete.

4 In the **License Agreement** window, select **I accept the agreement**, and click **Next**.

5 In the **Select Destination Directory** window, browse to the directory in which you want Data Insight to be installed. By default, the destination directory is `C:\Program Files\DataInsight`.

6 In the **Configure Type of Install** window, select **Management Server**.

Select a location with enough free space and high-performance disks. It is recommended that you choose a location other than the system volume for the `data` directory.

Click **Next**.

7 In the **Configure Data Directory** window, select the location where you want to store the product data.

Click **Next**.

8 In the **Management Server Properties** window, enter the following details:

Management Server Address	The Fully Qualified host name (FQHN) of the current host. The remote worker nodes use this address to communicate with the Management Server
Web Server port	The secure (HTTPS) Web server port on which you can access the Web interface of the Management Server.

The installer validates whether the appropriate ports are free to accept connections.

9 Select the **Add Domain <*Name of domain*> to the list of domains scanned by Data Insight** check box, if you want the Management Server to automatically start scanning the Active Directory domain which the Management Server is a part of. If the Management Server is not part of any Active Directory domain, this option is disabled.

For information on customizing the Active Directory domains to be scanned, see the *Veritas Data Insight Administrator's Guide*.

Click **Next**.

10 In the **Configure Networking** window, enter the following information, and click **Next**:

Communication Service Port	See "About Communication Service" on page 16.
Configuration Service Port	Configuration service is a process that provides interface to configuration and other product data stored on the local system. This service port does not need to be accessible outside the host machine.

11 In the **Configure Product Administrator** window, enter the following information , and click **Next**:

- Name of the user who can log in to Veritas Data Insight with Product Administrator privileges
- Name of the domain to which the user belongs

Note: The product administrator must be a local user or must belong to the same domain as the Management Server.

---

12 Check the box if you want to enable Federal Information Processing Standards (FIPS) mode.

Note: If you enable FIPS mode, you will not be able to change this setting in future.

For more information, See "Federal Information Processing Standards (FIPS) " on page ?.

13 Review the options that you have selected in the installation wizard in **Installation Summary** window.

14 To start the installation process, click **Begin Install**.

15 The Installing window appears and displays a progress bar.

16 The Completing the Veritas Data Insight setup wizard window provides you an option to start Data Insight Services.

Before you start services, Veritas recommends that you check for available patches at *https://sort.veritas.com*. If there is a patch available, install the patch first and then start the services.

The next screen provides you an option to launch the Management Server on exit. Select this option to launch the Console and complete setting up the Management Server.

17 To exit setup, click **Finish**.

Note: Once you install the Management Server, log on to the Management Server to configure the SMTP settings and other product users, as necessary.

Installing the worker node

Throughout the installation process, the setup wizard displays installation information and options. Use the following options to navigate through the installation process:

Installing the worker node

1 Log on (or remote logon) as Administrator to the computer that is intended for the worker node.

2 The **Welcome to the Veritas Data Insight Setup Wizard** window appears. Click **Next**.

3 In the **License Agreement** window, select **I accept the agreement**, and click **Next**.

4 In the **Select Destination Directory** window, browse to the directory in which you want Data Insight to be installed. By default, the destination directory is `C:\Program Files\DataInsight`.

Note: You cannot install the worker node on the same machine as the Management Server.

---

5 Depending on your deployment scenario, in the **Configure Type of Install** window, select **Indexer and Collector**, or **Collector** as the installation option.

6 Click **Next**.

7 In the **Configure Data Directory** window, browse to the location where you want to store the product data.

Select a location with enough free space and high-performance disks. It is recommended that you choose a location other than the system volume for the `data` directory.

8 In the **Worker Node Address** window, enter the Fully Qualified Host Name (FQHN) of the server. This name must be resolvable from the Management Server and the other worker nodes.

9 In the **Configure Networking** window, enter the following information:

Communication Service Port	See "About Communication Service" on page 16.
Configuration Service Port	Configuration service is a process that provides interface to configuration and other product data stored on the local system. This service port does not need to be accessible outside the host machine.
Workflow Service Port	This service is responsible to perform actions like Delete, Set MIP and so on. This service port does not need to be accessible outside the host machine.

Note: The installer validates whether the appropriate ports are free to accept connections.

10 Check the box if you want to enable Federal Information Processing Standards (FIPS) mode.

Note: If you enable FIPS mode, you will not be able to change this setting in future.

For more information, See "Federal Information Processing Standards (FIPS) " on page ?.

11 Review the options that you have selected in the installation wizard in **Installation Summary** window.

12 To start the installation process, click **Begin Install**.

13 To register the worker node with the Management Server after you exit setup, select the **Launch Worker Node Registration Wizard after exit** check box.

See "Registering the worker node" on page 56.

14 To exit setup, click **Finish**.

Installing the Classification Server

The setup wizard displays installation information and options. Use the following options to navigate through the installation process:

Installing the Classification Server

1. Log on (or remote logon) as Administrator to the computer that is intended for the Classification Server.
2. Double-click `Veritas_DataInsight_windows_6_5_0_N_x64.exe` to launch the installer.

   Where, `N` is the build number. If UAC is enabled, right-click on the installer and choose the **Run as administrator** option for elevated administrative rights during the installation.
3. The **Welcome to the Veritas Data Insight Setup Wizard** window appears. Click **Next**.
4. In the **License Agreement** window, select **I accept the agreement**, and click **Next**.
5. In the **Select Destination Directory** window, browse to the directory in which you want Data Insight to be installed. By default, the destination directory is `C:\Program Files\DataInsight`.
6. In the **Configure Type of Install** window, select **Classification Server** as the installation option.
7. Click **Next**.
8. In the **Configure Data Directory** window, browse to the location where you want to store the product data.

   Select a location with enough free space and high-performance disks. It is recommended that you choose a location other than the system volume for the `data` directory.
9. In the **Worker Node Address** window, enter the Fully Qualified Host Name (FQHN) of the server. This name must be resolvable from the Management Server and the other worker nodes.

10 In the **Configure Networking** window, enter the following information:

Communication Service Port	See "About Communication Service" on page 16.
Configuration Service Port	Configuration service is a process that provides interface to configuration and other product data stored on the local system. This service port does not need to be accessible outside the host machine.

Note: The installer validates whether the appropriate ports are free to accept connections.

---

11 Check the box if you want to enable Federal Information Processing Standards (FIPS) mode.

Note: If you enable FIPS mode, you will not be able to change this setting in future.

For more information, See "Federal Information Processing Standards (FIPS) " on page ?.

12 Review the options that you have selected in the installation wizard in **Installation Summary** window.

13 To start the installation process, click **Begin Install**.

14 To register the Classification Server with the Management Server after you exit setup, select the **Launch Worker Node Registration Wizard after exit** check box.

See "Registering the worker node" on page 56.

15 To exit setup, click **Finish**.

Recommendations:

- XMX specifies maximum memory size for Java virtual machine, which is critical for out of memory issue. If multiple processes are running simultaneously, you might face out of memory issue. To keep the processes running smoothly, you need to allot recommended XMX ratio.
- XMX settings are given primarily in the `.vmoptions` file present at **C:\Program Files\DataInsight\bin** for every service. For example, `WebServerService.vmoptions` file is for DatainsightWeb

CommunicationServerService.vmoptions is for DatainsightComm. In case of VIC, the value has to be changed in the file `VICClientService.vmoptions` at **C:\Program Files\DataInsight\bin**.

- You need to make changes to the XMX values if
  - you get *out of memory* error.
  - If your machine configuration is more than 16 core CPU. To clarify, if your machine is 32 core and you do not change the XMX value, classification will not select better machine resource for computation.
- If the node is used only for Classification, the XMX ratio should be 50% of the available RAM.
- If the node is used as a Management Server or Indexer, do not make any changes. The default XMX value is calculated as per the machine RAM. For example, if RAM >= 8GB, the XMX = 2.5GB (31%). If RAM >= 6GB < 8GB, XMX = 2GB (25% - 33%) and likewise.

Note: You can change the XMX values by navigating to C:\Program Files\DataInsight\bin and making changes to **VICServerService.vmoptions** and **VICServer.vmoptions** files only in case of Classification nodes.

Installing the Self-Service Portal

Installing the Self-Service Portal

1. Log on (or remote logon) as Administrator to the computer that is intended as the Portal.
2. Double-click `Veritas_DataInsight_windows_6_5_0_N_x64.exe` to launch the installer.

   where, `N` is the build number.

   If UAC is enabled, right-click on the installer and choose the **Run as administrator** option for elevated administrative rights during the installation.
3. The **Welcome to the Veritas Data Insight Setup Wizard** window appears. Click **Next**.
4. In the **License Agreement** window, select **I accept the agreement**, and click **Next**.

5 In the **Select Destination Directory** window, browse to the directory in which you want Data Insight to be installed. By default, the destination directory is `C:\Program Files\DataInsight`.

Note: You cannot install the portal node on the same computer as the Management Server.

---

6 Depending on your deployment scenario, in the **Configure Type of Install** window, select **Self-Service Portal** as the installation option.

7 Click **Next**.

8 In the **Configure Data Directory** window, browse to the location where you want to store the product data.

Select a location with enough free space and high-performance disks. It is recommended that you choose a location other than the system volume for the `data` directory.

9 In the **Worker Node Address** window, enter the Fully Qualified Host Name (FQHN) of the host. This host name must be resolvable from the Management Server and the other worker nodes.

10 In the **Configure Networking** window, enter the following information:

Communication Service Port	See "About Communication Service" on page 16.
Configuration Service Port	Configuration service is a process that provides interface to configuration and other product data that is stored on the local system. This service port does not need to be accessible outside the host machine.

11 In the **Configure Self-Service Portal** window, enter the port numbers for the Self-Service Portal service and the Workflow service. By default the port numbers are 443 for the Portal service and 8686 for the Workflow service.

Note: The installer validates whether the appropriate ports are free to accept connections.

---

12 Check the box if you want to enable Federal Information Processing Standards (FIPS) mode.

Note: If you enable FIPS mode, you will not be able to change this setting in future.

For more information, See “Federal Information Processing Standards (FIPS) ” on page ?.

13 Review the options that you have selected in the installation wizard in **Installation Summary** window.

14 To start the installation process, click **Begin Install**.

15 To register the worker node with the Management Server after you exit setup, select the **Launch Worker Node Registration Wizard after exit** check box.

See “Registering the worker node” on page 56.

16 To exit setup, click **Finish**.

Emails for remediation tasks are sent to data owners from the Portal Server. Ensure that you can connect to the configured SMTP server from the Portal server. Similarly, for incident remediation, the Portal node communicates with the DLP server. Ensure that the portal node can connect to the DLP server.

Installing a Linux Indexer worker node

You can choose to install the Indexer on a server installed with Red Hat Enterprise Linux 7.0. The Linux indexer works exactly the same way as the Windows indexer.

Before you install the Indexer on the Linux server, ensure the following:

- The compat-expat1 RPM resource package is installed on the server.
- The firewall is configured to allow access to port 8383 between the Management Server, Indexer, and Collector.
- The worker node should be able to ping itself and other nodes.

SSH to the Linux server where you want to install the worker node . You can install the package either as root or as non-root user. Ensure that you are logged in as that user.

Steps needed for non root users

Installing the worker node

1. Run the following command to launch the installer package:

   ```
   sh Veritas_DataInsight_linux_6_5_N_<RHELVER>_x64.s
   ```

   where *N* is the build number, and RHELVER is RHEL7 depending on the version of your operating system.

2. **The Welcome to the Veritas Data Insight Setup Wizard** window appears. Click **Next**.

3. In the License Agreement window, select **I accept the agreement**, and click **Next**.

4. Enable FIPS Mode? Yes [y], No [n]

   FIPS are standards and guidelines for federal computer systems that are developed by National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce. Choice of FIPS mode should be same for Management server and Worker nodes. You can enable FIPS mode only during fresh product installation or upgrade. You will not be able to make any changes post product installation or upgrade.

5. In the Select Destination Directory window, browse to the directory in which you want the Indexer to be installed. By default, the destination directory is `/opt/DataInsight`.

6. Click **Next**.

7. In the Configure Data Directory window, browse to the location where you want to store the product data.

   Select a location with enough free space and high-performance disks.

8. In the Worker Node address window, enter the Fully Qualified Host Name (FQHN) or IP address of the host. Ensure that the Management Server and the other worker nodes are able to resolve this hostname.

9 In the Configure Networking window, enter the following information:

Communication Service Port	See “About Communication Service” on page 16.
Configuration Service Port	Configuration service is a process that provides interface to configuration and other product data stored on the local system. This service port does not need to be accessible outside the host machine.

Note: The installer validates whether the appropriate ports are free to accept connections.

10 To register the worker node with the Management Server after you exit setup, select the **Launch Worker Node Registration Wizard after exit** checkbox.

See “Registering the worker node” on page 56.

11 To exit setup, click **Finish**.

12 Optionally, to use an alternate location for the log files, edit the following files that are located in the `/opt/DataInsight/conf` directory, to replace `/opt/DataInsight/log` with the new log location:

`cli_logging.properties`

`dscli_logging.properties`

`commd_logging.properties`

`watchdog_logging.properties`

`webserver_logging.properties`

Export the new log directory using the following command:

```
export MATRIX_LOG_DIR=/DataInsight/log
```

Add the export entry to `.bash_profile` file of the user to reflect the change when you restart the system.

Execute the following command to update the profile path:

```
source .bash_profile
```

13 When installing as a non-root user, after you have registered this node with the Management Server, add following entries to `/etc/rc.local` to automatically start the services after you restart the system:

```
su – <name of non-root user>

# export MATRIX_LOG_DIR=/DataInsight/log (Optional)

/opt/DataInsight/bin/DataInsightConfig start

/opt/DataInsight/bin/DataInsightComm start

/opt/DataInsight/bin/DataInsightWatchdog start

logout
```

To stop services during shutdown, add the following entries to `/etc/rc.local.shutdown`:

```
/opt/DataInsight/bin/DataInsightWatchdog stop

/opt/DataInsight/bin/DataInsightComm stop

/opt/DataInsight/bin/DataInsightConfig stop
```

- The compat-expat1 RPM resource package is installed on the server.

- It should be configured to allow access to port 8383 between the Management Server, Indexer, and Collector.
- The worker node should be able to ping itself and other nodes.

Note: The DataInsightConfig service does not start after registration if the `queryd.lock` is present in the /tmp folder. The lock file is present if the installation is done using root, or when the machine is restarted. You must delete the `queryd.lock` file before you restart the DataInsightConfig service.

In case of upgrade:

If previous installation is done using root user and Data Insight is configured for non-root user, perform the following steps:

1. Log in to Data Insightas a root user.
2. Delete the following files

   ```
   rm /tmp/i4jdaemon__DIdata_DataInsight_bin_DataInsightComm
   rm /tmp/i4jdaemon__DIdata_DataInsight_bin_DataInsightWatchdog
   rm /var/run/queryd.pid
   ```

3. Assign execute permissions to the non root user.
4. Stop all services using root user by executing `configcli stop_services` from `/opt/datainsight/bin` folder
5. Navigate to the Data Insight 6.5 installer and assign execute permissions.
6. Log in to Data Insightas a non root user.
7. **The Welcome to the Veritas Data Insight Setup Wizard** window appears. Click **Next**.

8 In the License Agreement window, select **I accept the agreement**, and click **Next**.

9 Enable FIPS Mode? Yes [y], No [n]

FIPS are standards and guidelines for federal computer systems that are developed by National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce. Choice of FIPS mode should be same for Management server and Worker nodes. You can enable FIPS mode only during fresh product installation or upgrade. You will not be able to make any changes post product installation or upgrade.

Note: You need to upgrade product data before services can be enabled. Execute the following command to launch the *Upgrade Data Wizard* after exiting the installer: `/opt/DataInsight/bin/UpgradeData`

Installing Veritas Data Insight in Azure Cloud Environment

You can install Data Insight server on a virtual machine created in Azure environment. You can have following type of deployment:

- All Data Insight components on Azure environment.
- Hybrid deployment, where some components are on-premise and other components on cloud.

Note the following points,

- For hybrid deployment, establish site to site VPN connectivity for secure connection.
- Add appropriate firewall setting.
- Port 135 should be open on Azure Windows File Server.

Veritas doesn't stipulate how a data center is defined. As long as the environment is based on certified technology and meets system requirements the environment will be supported. Veritas Support will diagnose issues in the same manner as they would for on-premise installations unless they can verify that the issue is related to a problem with the underlying cloud infrastructure.

Performance of cloud platforms may vary depending on the cloud infrastructure, factors such as shared storage, network and processing power will all play a role in the performance of the solution. Any published Data Insight performance metrics

are based on dedicated hardware, networking and processing within a single data center (unless specified). Veritas will not accept support calls based on performance unless the issue can be reproduced removing the cloud platform.

Installing Veritas Data Insight in AWS Cloud Environment

You can install Data Insight server on a virtual machine created in AWS environment. You can have following type of deployment:

- All Data Insight components on AWS environment.
- Hybrid deployment, where some components are on-premise and other components on cloud.

Note the following points,

- For hybrid deployment, establish site to site VPN connectivity for secure connection.
- Add appropriate firewall setting.
- Port 135 should be open on AWS File Server.

Veritas doesn't stipulate how a data center is defined. As long as the environment is based on certified technology and meets system requirements the environment will be supported. Veritas Support will diagnose issues in the same manner as they would for on-premise installations unless they can verify that the issue is related to a problem with the underlying cloud infrastructure.

Performance of cloud platforms may vary depending on the cloud infrastructure, factors such as shared storage, network and processing power will all play a role in the performance of the solution. Any published Data Insight performance metrics are based on dedicated hardware, networking and processing within a single data center (unless specified). Veritas will not accept support calls based on performance unless the issue can be reproduced removing the cloud platform.

Chapter 4

Upgrading Veritas Data Insight

This chapter includes the following topics:

- Upgrading Data Insight to 6.6.1
- Upgrading the product data using the Upgrade Data Wizard
- Names and locations of cache files
- Upgrading the Data Insight web service for SharePoint

Upgrading Data Insight to 6.6.1

You can upgrade an existing Data Insight Server with Veritas Data Insight versions 6.4, 6.5 (including their minor releases) to 6.6.1. If the server is installed with a version before 6.4, you must upgrade to at least version 6.4 before you can upgrade to 6.6.1.

All Data Insight worker nodes must be at the same version as the Management Server. Management Server version is compatible with the 5.0, 5.1, 5.2, 6.0, 6.1, 6.2, 6.3 and 6.4 versions of Windows File Server agents in FIPS disable mode.

When you are upgrading to Data Insight, you will get an option to enable FIPS mode. Make sure you read all the information before enabling the FIPS mode.

Note: If you are upgrading to Data Insight 6.6.1 and enabling FIPS mode, make sure Windows File Servers are upgraded to 6.5 version. Management Server 6.5 is not compatible with the 5.0, 5.1, 5.2, 6.0, 6.1, 6.2, 6.3 and 6.4 versions of Windows File Server agents in FIPS enable mode. Also note that if FIPS is enabled, connection to other Data Insight components will be lost until all components are running on same version.

Note that due to security vulnerabilities, Data Insight turned off SSL and TLSv1 protocols. However, Windows File Server agents version 4.5 are not compatible with TLSv1.1 and TLSv1.2 protocols. Thus, Windows File Server agents stop communicating with the collectors that are upgraded to Data Insight 6.6.1. To resume this communication, perform the following on each Windows File Server agent node before or after upgrading the collectors to 6.6.1:

1. Obtain the latest 32-bit Java Runtime Environment (JRE) binaries from the Windows File Server agent version 6.6.1. Typically, they are located in the `jre` folder of the agent 6.6.1 installation. The default location is `C:\Program Files\DataInsight\jre`.
2. Log on to the Windows File Server agent computer with the Administrator privileges.
3. Stop the DataInsightComm and DataInsightWatchdog services on the agent.
4. Replace the old jre binaries on the agent with the ones obtained from the Windows File Server agent node version 6.6.1. By default, the agent version 4.5 JRE is located at `C:\Program Files\Symantec\DataInsight\jre`.
5. Start the DataInsightComm and DataInsightWatchdog services.
6. After few minutes, verify that the node's status is **ONLINE** on the Data Insight console. The status is displayed at **Settings** > **Data Insight Servers** page.

Before you begin to upgrade Data Insight to 6.6.1, note the following:

- As a best-practice measure, Veritas recommends that you take a backup of the server's `data` folder.
- In case of a multi-node setup, the upgrade setup must be run first on the Management Server, then on the Indexer nodes, followed by the Collector nodes. You can upgrade the Windows File Server agent only after upgrading the Collector nodes.
- If you are upgrading the server using a Remote Desktop Connection (RDC), ensure that you do not set automatic log-off for the session.

Ensure that you complete the following tasks after the upgrade:

- Configure the primary attributes that are used to classify users for the purpose of generating advanced analytics data.
- Configure the time period for computing advanced analytics.
- Refresh the Data Insight Dashboard data.
- Verify that the .Net Framework version 4.5 is installed on the following:
  - Collector nodes monitoring the Windows SharePoint servers and the EMC Isilon filers.
  - The Management Server communicating with an Enterprise Vault server.

To upgrade Data Insight to 6.6.1

1. Log in as Administrator to the server that you want to upgrade.
2. When the setup prompts you to upgrade from current version to 6.6.1, click **Yes**.
3. In the **Welcome to the Veritas Data Insight Setup Wizard** window, click **Next**.
4. In the **License Agreement** window, select **I accept the agreement**, and click **Next**.
5. You must upgrade the product data before you start Data Insight services. In the **Completing the Veritas Data Insight 6.6.1 Upgrade Wizard** window, select the **Launch the Upgrade Data Wizard** check box.
6. Check the box if you want to enable Federal Information Processing Standards (FIPS) mode.

   Note: If you enable FIPS mode, you will not be able to change this setting in future.

   For more information, See “Federal Information Processing Standards (FIPS) ” on page ?.
7. Click **Next**
8. Click **Finish** to exit the setup.

Note: After upgrading to 6.5, expect a delay in first index writer run. Data Insight will need extra time to process the incoming scan and audit events.

To upgrade a Linux Indexer

1. In case of a Linux indexer, log in as the appropriate user (root or non-root) configured to run the product.

Note that if you had earlier installed the Linux Indexer as root and later switched to using a non-root user, you must perform the following steps before you start the Linux installer for upgrade. If you do not perform these steps, the installer you launch with non-root credentials cannot detect the previous version of Data Insight on the server.

- Log in to the machine as root user.
- Copy the following file to a temporary location:
  `~/.java/.userPrefs/com/install4j/installations/prefs.xml`.
- Log out and log back in as the non-root user.
- Create the following directory:
  `~/.java/.userPrefs/com/install4j/installations/`
- Change to the directory you have created.
- Take a backup of `prefs.xml`.
- Overwrite `prefs.xml` in this folder with the `prefs.xml` that was copied to the temporary location.

2 When the setup prompts you to upgrade from current version to 6.6.1, click **Yes**.

Note: On Linux, if the installer does not prompt you for upgrade because it does not detect the earlier version of Data Insight on the machine, ensure that you first follow the instructions in 1.

---

3 Enable FIPS Mode? Yes [y], No [n]

FIPS are standards and guidelines for federal computer systems that are developed by National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce. Choice of FIPS mode should be same for Management server and Worker nodes. You can enable FIPS mode only during fresh product installation or upgrade. You will not be able to make any changes post product installation or upgrade.

Note: If you enable FIPS mode, you will not be able to change this setting in future.

See "Upgrading the product data using the Upgrade Data Wizard" on page 53.

Note: After upgrading to 6.5, expect a delay in first index writer run. Data Insight will need extra time to process the incoming scan and audit events.

Note: You can also upgrade the Windows File Server agent and Collector nodes using the Management Console. For more details, see the *Veritas Data Insight Administration Guide*.

Backing-up contents from existing SharePoint Online accounts

After upgrading to 6.6.1, Data Insight does not support Discovery, Scan, and Audits for the SharePoint Online accounts that were added prior to Data Insight 6.1.4. If you want to retain the audit events from existing SharePoint Online accounts, follow the instructions below to take a backup.

Note: You can avoid steps 1 and 2, and directly perform step 3 if you do not want existing audit events.

To back-up contents from existing SharePoint Online accounts

1. Run the following reports on your existing SharePoint Online Account:
   - Activity Details for Path
   - Activity Details for Users/Groups
   - Activity Summary for Paths
   - Activity Summary for Users/Groups
2. Take a backup of the reports folders on the Management Server from the following directory:
   `<data_dir>/console/reports/reportruns/<report_run_id>`.

   You can get the `report_run_id` from **Reports** >**Select Action** > **View** > **Id** (Column).

   After you have a backup, you can delete existing SharePoint Online accounts.
3. Click **Settings** > **Share Point Sources** > *<account* > > **Select Action** > **Delete** to delete existing SharePoint Online accounts.
4. Upgrade to Data Insight 6.6.1. See "Upgrading Data Insight to 6.6.1" on page 48.
5. Add a new Share Point Online Account. See Adding SharePoint Online accounts in the *Veritas Data Insight Administrator's Guide*.

Creating a non-administrator user for an EMC Isilon cluster

While upgrading to 6.2 and above using a non-administrator user for Isilon discovery, run the following command to add the required NFS privilege to the Data Insight role on the Isilon Cluster: `isi auth roles modify dirole --add-priv-ro=ISI_PRIV_NFS`

Upgrading the product data using the Upgrade Data Wizard

Before you upgrade data, Veritas recommends that you check for product updates on https://sort.veritas.com. If updates are available, you must apply the product update, and then proceed to upgrade the data.

To upgrade the product data using the Upgrade Data Wizard

1. Launch the Upgrade Data wizard.
2. On the **Upgrade Product Data** window, select the **Make temporary backup of data before upgrading** check box.

   Veritas recommends that you take a backup of the product data before starting the data upgrade. Taking a backup ensures that the original data can be restored from backup if the upgrade fails. Data Insight deletes the backup after the upgrade completes successfully.
3. Create the backup of the product data. To select a backup location, browse to the location where you want the backup data to be stored.

   Before you begin the upgrade, ensure that there is enough free space available in the target location to take a backup. Data Insight requires that your system must have free space to accommodate your `data` directory and an additional 5% of data size for the upgrade to succeed. If enough free space is not available, the upgrade wizard fails. If the upgrade fails, relaunch the upgrade wizard by executing the command `INSTALL_DIR\bin\UpgradeData.exe` (Windows) or `/opt/DataInsight/bin/UpgradeData` (Linux).
4. Select the following check boxes:
   - **Automatically restore original data from backup if upgrade fails**
   - **Delete backup on successful upgrade**
5. If an index is taking a long time to upgrade, or if the upgrade of an index fails for some unknown reason, you can enter the number of such indexes in the **Skip indexes** field. Specify a comma-separated list of the indexes you want to skip. The wizard skips the specified indexes and continues with the data upgrade process.

6. Specify the number of index upgrade failures after which the installer must exit the data upgrade process.
7. You can upgrade up to 10 indexes in parallel. Select a number from the **Number of indexes to upgrade in parallel drop-down**.

   Just before an index is upgraded, a copy of that index is saved in the same folder where the index resides. This requires additional disk space during the upgrade. Total additional disk space depends on the number of indexes being upgraded in parallel. If you are short on disk space on data volume, you can select the option to **Skip index back up before upgrade**. Selecting this option can also make the upgrade process faster. You should select this option only if you have a backup of your data directory so that indexes that fail to upgrade can be restored at a later time.
8. Click **Upgrade Now** to start the data upgrade process.
9. The Data Upgrade window appears and displays a progress bar while upgrading the product data. The time taken in the upgrade process depends upon the size of the data.
10. On successful completion of the data upgrade, click **OK**.
11. On the **Start Data Insight Services** window, select **Start Data Insight Services now**. Click **Next**.
12. Click **Finish** to exit the wizard.

Names and locations of cache files

Data Insight generates cache files on the Indexer node at the time of installation or upgrade.

Data Insight creates the following persistent activity index files in each index folder for a share:

- `activityidx.info`
- `dir-activity.idx.<timestamp>`
- `file-activity.idx.<timestamp>`

The persistent cache files contain pre-calculated summary information about users and their activity on the files and folders during the time period configured for advanced analytics. The indexer process uses the information in these files to expedite the process of servicing queries related to activity, reports, and Social Network Graph.

Each index folder for a share may also contain the following temporary files:

Table 4-1

Name	Description
file-activity.idx.<*timestamp*>.<*version*> dir-activity.idx.mmap.<*timestamp*>.<*version*>	Uncompressed versions of the file-activity.idx.<timestamp> and dir-activity.idx.<timestamp> files. Since the activity index files are stored in a compressed form on disk, Data Insight creates the uncompressed files when any process attempts to read the activity index. The files remain on disk while the process is reading the files, and are deleted when the process finishes reading the activity index.
rolldir-activity.idx.<*timestamp*>.<*version*>	Temporary file created when Data Insight rolls up the activity count for folders. The file remains on the disk while the process is reading the files, and are deleted when the process finishes reading the activity index.
file-activity.idx.tmp.<*timestamp*>.<*version*> file-activity.idx.attr.<*timestamp*>.<*version*> dir-activity.idx.attr.<*timestamp*>.<*version*>	Temporary files created when Data Insight calculates owners for files and folders. The files remain on disk while the query or report processes the share. Data Insight deletes these files once the share is processed.

If the process that creates these temporary files stops unexpectedly, Data Insight deletes these files during the next run of the IndexWriterJob or the ActivityIndexJob processes on the shares.

Upgrading the Data Insight web service for SharePoint

Data Insight does not support an automatic upgrade of the Data Insight web service on the SharePoint server. To upgrade to the latest version, uninstall the previous version from the SharePoint server and install the latest version.

For detailed information on installing the Data Insight SharePoint Web service, see the *Veritas Data Insight Administrator's Guide*.

Chapter 5

Post-installation configuration

This chapter includes the following topics:

- Post-installation configuration
- Registering the worker node
- About post-installation security configuration for Management Server
- Configuring your corporate firewall

Post-installation configuration

You must complete the following configuration after you finish installing Veritas Data Insight:

- Register the worker node with the Management Server.
  See "Registering the worker node" on page 56.
- Configure post-installation security settings.
  See "About post-installation security configuration for Management Server" on page 58.
- Configure your corporate firewall.
  See "Configuring your corporate firewall" on page 65.

Registering the worker node

You must register the worker node with the Management Server to enable communication between them.

You do not need to perform these steps if you have upgraded a worker node.

To register the worker with the Management Server

1. Do one of the following:
   - To launch the Worker Node Registration Wizard immediately after completing the Worker Node installation wizard, select the **Launch Worker Node Registration Wizard after exit** check box.
   - To register the worker node at a later time, execute `RegisterWorkerNode.exe` located in the Data Insight installation bin directory.
2. In the Register Worker Node with Management Server window, enter the following information:
   - Fully Qualified Host Name (FQHN) of the Management Server host
   - Location of the Communication Service keystore file
     The keystore file, `commd.keystore`, enables secure communication between worker nodes and the Management Server. It is present in the `keys` subfolder of the Management Server's data directory. You must manually copy the keystore file from the Management Server machine to a temporary location on the worker node. By default the data directory is located on the Management Server at `C:\DataInsight\data`. It might be different for your setup. You can locate the data directory by reading the file `C:\Program Files\DataInsight\datadir.conf` on the Management Server or by running the `configdb -d` command.
3. Click **Register Now**.
4. After the successful registration of the worker node, delete the `commd.keystore` file from the temporary location.
5. On the Start Data Insight Services window, select **Start Data Insight Services** now.
6. On the Completing the node registration screen, click **Finish**.

   You must log in to the Data Insight Management Server to complete further configuration of the worker node.

About post-installation security configuration for Management Server

Veritas Data Insight secures communications between all Data Insight servers. This task is accomplished by encrypting the transmitted data and requiring servers to authenticate with each other.

The following sections describe the Veritas Data Insight security configuration and how to change the default security configuration.

About SSL client/server certificates

Veritas Data Insight secures all data flowing between the Management Server and the Worker nodes using the Secure Socket Layer/Transport Layer Security (SSL/TLS) protocol. The SSL/TLS protocol not only encrypts the data that is transmitted, Veritas Data Insight also uses it for mutual authentication between servers.

Data Insight implements authentication with the mandatory use of client and server-side certificates or keys. Connections between the Data Insight servers use a single, self-signed certificate. The Management Server generates the certificate at install time and is unique to your deployment. It is present on the Management Server node in the `keys` folder under the `data` folder. The file is called `commd.keystore`. When you configure worker nodes, this file must be manually copied over to the new worker node before installation.

Enabling CA signed certificates for inter-node communication

If you want to opt for CA signed certificates, perform the following steps on the **Management Server**.

On the Management Server,

1. Rename *C:\DataInsight\data\keys\commd.keystore* to *commd-org.keystore*
2. Import *CA Issued Certifcate file* **(pfx)** to the *commd keystore*.
3. Execute the following command `"C:\Program Files\DataInsight\jre\bin\keytool.exe" -importkeystore -srckeystore "c:\<Location of .pfx file>" -destkeystore "C:\DataInsight\data\keys\commd.keystore" -srcalias <certificate unique id> -destalias tomcat -deststoretype jks -destkeypass changeit`
4. Create a backup of the *cacerts keystore*, you can find at *C:\Program Files\DataInsight\jre\lib\security\cacerts*.

5 Rename *C:\Program Files\DataInsight\jre\lib\security\cacerts* to *cacerts-org*.

6 Delete the self-signed certificate from the *cacerts keystore* by executing the following command `"C:\Program Files\DataInsight\jre\bin\keytool.exe" -delete -alias tomcattrustedca -storepass changeit -keystore "C:\Program Files\DataInsight\jre\lib\security\cacerts`

7 Copy *C:\DataInsight\data\keys\commd.keystore* from the **Management Server** to all **Remote Servers** located at *C:\DataInsight\data\keys*.

8 Restart all Data Insight services on the **Management Server** and all remote nodes.

To apply the CA provided certificate to secure web portal communications,

1 Rename *C:\DataInsight\data\keys\webserver.keystore* to *webserver-org.keystore*.

2 Import *CA Issued Certifcate file* **(pfx)** to the *commd keystore*.

3 Execute the following command `"C:\Program Files\DataInsight\jre\bin\keytool.exe" -importkeystore -srckeystore c:\<Location of .pfx file> -destkeystore C:\DataInsight\data\keys\webserver.keystore -srcalias <certificate unique id> -destalias tomcat -deststoretype jks -destkeypass changeit`

To apply the CA provided certificate to secure Self Service portal communications,

1 Rename *C:\DataInsight\data\keys\portal.keystore* to *portal-org.keystore*.

2 Import *CA Issued Certifcate file* **(pfx)** to the webserver portal.

3 Execute the following command `"C:\Program Files\DataInsight\jre\bin\keytool.exe" -importkeystore -srckeystore c:\<Location of .pfx file> -destkeystore C:\DataInsight\data\keys\portal.keystore -srcalias <certificate unique id> -destalias tomcat -deststoretype jks -destkeypass changeit`

Generating Management Console certificate

The Management Server provides a web interface (administration console) for reporting and administration purposes. You access this interface with a web browser. The Management Server and browser communicate through an SSL connection.

To ensure confidentiality, all communication between the Management Server and the browser is encrypted using a symmetric key. To initiate a connection, the

Management Server and browser negotiate the encryption algorithm (algorithm, key size, and encoding) and encryption key to use.

By default, connections between the Management Server and the browser use a single, self-signed certificate. The Management Server generates the certificate at install time and is unique to your deployment. The certificate is present on the Management Server node in a folder called *keys* under the data folder. The file is called `webserver.keystore`. While this certificate is secure, you get a warning message in the browser when accessing the web interface because it is a self-signed certificate. To avoid getting this warning, Veritas recommends that you generate a unique certificate for your organization's installation. This new certificate replaces the default certificate.

To generate a unique Management Console certificate

1 Collect the following information to generate a certificate request:

- Common name
  The fully qualified DNS name of the Management Server. This name must be the actual name of the server that is accessible by all the clients.
- Organization name
  For example, Veritas, Inc.
- Organizational unit (optional)
- City
  For example, San Francisco
- State
  For example, CA
- Country
  For example, US
- Expiration
  Expiration time in days (90)

2 Use `keytool.exe` to create the self-signed certificate (keystore file), which you need to generate the Certificate Signing Request (CSR). `keytool.exe` is a utility for managing keys and certificates. These items are used in self-authentication or data integrity and authentication services, using digital signatures. Certificates also enable users to cache the public keys of their communicating peers.

To create this file, go to the root directory of the Veritas Data Insight installation and perform the following steps in this order:

- From a command window, go to the `installdir\DataInsight\jre\bin` directory, where `installdir` is the directory into which you installed the Management Server.
- Run the following command with the information collected in 1:

```
keytool -genkey -alias tomcat -keyalg RSA -validity 730 -keysize 1024
-keypass changeit -keystore webserver.keystore -storepass changeit
-storetype JKS -dname cn=common_name,o=organization_name,
ou=organization_unit,l=city,s=state,c=US
```

The `-storepass changeit` command sets the password to **changeit**. Enter this password if you are prompted for a password after running the command. This command creates the self-signed certificate (webserver.keystore) in the `<installdir>\jre\bin` directory.

Note: Veritas recommends that you set the password as **changeit**. If you want to use a different password, perform the additional steps mentioned in 11 before you start the DataInsightWeb service.

---

3 Generate the certificate signing request (CSR) file. The CSR file is the request that you submit to the Signature Authority to obtain a signed certificate.

From the `<installdir>\jre\bin` directory and run the following command:

```
keytool -certreq -alias tomcat -keyalg RSA -keystore webserver.keystore
-storetype JKS -storepass changeit -file "DataInsight.csr"
```

If you are prompted for a password, press **Enter**. This command creates a file called `DataInsight.csr`. You submit this file to the Signature Authority.

4 To generate a certificate you send the .CSR file to a Certified Signature Authority (your own or a third party, such as VeriSign).

To obtain a signed certificate from your internal Signature Authority, contact your system administrator for instructions.

For the VeriSign Signature Authority, perform one of the following actions:

- Current Customers
  If you are a current VeriSign customer, go to the following page and buy an additional certificate: http://www.symantec.com /ssl-certificates/?themeid=verisign-ssl-certificates&inid=vrsn_ss_Index
  You need your Common Name, Order Number, or serial number to begin the transaction, as well as the CSR.

- New customers

  If you are not a current customer and want to purchase the signed certificate from VeriSign, go to the following page: http://www.VeriSign.com/products-services/security-services/ssl/buy-ssl-certificates/index.html.

  To purchase the signed certificate, you need the following information, in addition to the CSR:

  - The length of time for the certificate (one year or two years).
  - The number of servers that host a single domain (up to five servers).
  - The server platform.
  - The organization, organizational unit, country, state, or locality (all spelled without abbreviations).
  - Payment information and a billing contact.
  - The common name. This name is the host name and domain name, such as www.company.com or company.com.
  - An email where VeriSign can reach you to validate the information.
  - Documentation to demonstrate that your organization is legitimate.

To obtain signed certificates from other Signature Authorities, go to their web sites and follow the instructions to enroll and obtain a signed certificate. This process is similar to the VeriSign process. However, check with the organization to identify any additional environment information that may be needed for the certificate.

The certified Signature Authority sends you the signed certificate (this process might take 3-5 days). Internal Signature Authorities must return the root certificate along with the signed certificate.

5 Place the signed certificate into the directory (`<installdir>\jre\bin`) with the `webserver.keystore` file. To email the certificate, paste it into a text document exactly as it appears on the screen. Include the top line and bottom line (*-----Begin Certificate----- and -----End Certificate-----*). Make sure that no extra lines, spaces, trailing carriage returns, or characters have been inadvertently added. Save this file in the same directory where the `webserver.keystore` file is located. If the signed certificate is provided as an attachment to an email, copy this file into the same directory where the `webserver.keystore` file is located.

6 Keep a copy of both the `webserver.keystore` file and the signed certificate file in a separate, secure location.

7 Confirm the signed certificate is correct. Open a command prompt and run the following command to view the certificate's fingerprint(s)

```
keytool -printcert -file signed_certificate_filename
```

The following is an example output:

```
Owner: CN=ll, OU=ll, O=ll, L=ll, S=ll, C=ll

Issuer: CN=ll, OU=ll, O=ll, L=ll, S=ll, C=ll

Serial Number: 59092b34

Valid from: Thu Sep 25 18:01:13 PDT 1997 until: Wed Dec 24 17:01:13

PST 1997

Certificate Fingerprints:

MD5: 11:81:AD:92:C8:E5:0E:A2:01:2E:D4:7A:D7:5F:07:6F SHA1:
20:B6:17:FA:EF:E5:55:8A:D0:71:1F:E8:D6:9D:C0:37 37:13:0E:5E:FE
```

8 Call or email the person who sent the certificate and compare the fingerprint(s) you see with the fingerprint(s) they sent you. If the fingerprint(s) are not exactly equivalent, the certificate may have been replaced in transit by an attacker's certificate.

If you used an Internal Signing Authority, also view the fingerprint(s) of the root certificate using the same `-printcert` command.

```
keytool -printcert -filename_of_root_certificate_provided
_by_internal_signature_authority
```

Compare the displayed fingerprint with the well-known fingerprint (obtained from a newspaper or the root CA's web page). Contact the certificate's issuer if you have questions.

When you execute the command, the `-importcert` command prints out the certificate information and prompts you to verify it.

9 Return to the `<installdir>jre\bin` directory and update the local `webserver.keystore` file with the signed certificate as follows:

- Internal signature authority
  Use the following command to update the `webserver.keystore` file with the root certificate:

  ```
  <installdir>\jre\bin\keytool.exe -importcert -file
  root_certificate_filename -keystore webserver.keystore
  ```

```
-storepass changeit
```

Use the following command to update the webserver.keystore file with the signed certificate:

```
<installdir>\jre\bin\keytool
-importcert -alias tomcat -keystore webserver.keystore -trustcacerts
-file signed_certificate_filename
```

- VeriSign or third-party signature authority
  Use the following command to update the local webserver .keystore file with the signed certificate:

```
<installdir>\jre\bin\keytool
-importcert -alias tomcat -keystore webserver.keystore -trustcacerts
-file signed_certificate_filename
```

10 Copy the updated `webserver.keystore` file into the `$datadir\keys` directory. By default, `$datadir` is located at `C:\DataInsight\data`. Note that this operation overwrites an existing file of the same name in that location. Rename the existing file if you want to keep it.

11 If you have used a password other than **changeit** in 2, perform the following additional steps:

- Log into the Management Server with Administrator privileges.
- Open a command prompt window, and change to the bin directory in the installation folder for Data Insight. By default, the bin directory is located at `C:\Program Files\DataInsight\bin`.
- Execute the following command:
  `configcli.exe keystore_password webserver <new password>`

12 Restart the Data Insight web service by performing the following steps in the specified order:

- `net stop DataInsightWeb`
- `net start DataInsightWeb`

Note: After generating unique **Management Console certificate**, if you do not wish Data Insight to automatically renew and replace **webserver.keystore** in *<datadir>\keys* folder, add the following global property using command prompt: *<installdir>\bin\configdb -O -J matrix.webserver.keystore.renew -j false*

Configuring your corporate firewall

The instructions in this section assume that the Management Server and Worker nodes are installed inside your corporate LAN behind a firewall. If this is the case, update your corporate firewall settings as follows:

- Allow 2-way connections between the Management Server and the worker nodes and between worker nodes. Configure your firewall to accept connections on the port you entered for the Communication Service when installing the Management Server and worker nodes. By default, the Communication Service communicates over port 8383. You can configure the servers to use any other port. Traffic on this port is HTTPS.

  You should also allow outgoing connection from the Management Server to *https://sort.veritas.com.* Data Insight downloads patch information from the SORT web site to notify you of product updates.
- Allow Windows Remote Desktop Client connections (TCP port 3389). This feature can be useful for setup purposes.
- The web interface of the Management Server runs on port 443 (configurable at the time of installation). Port 443 is also used for the Portal service on the Self-Service Portal server. This port must be opened at the Management Server to allow HTTPS communication between browsers and the Web server and the portal server.
- The DataInsightWorkflow Service runs on HTTPS port 8686. This port must be opened on the Portal server to allow HTTPS communication between Portal server and the Management Server.

Chapter 6

Installing Windows File Server agent

This chapter includes the following topics:

- About Windows File Server agent
- Installing Windows File Server agent manually
- Configuring the Windows File Server using ConfigureWindowsFileServer.exe

About Windows File Server agent

Data Insight requires an agent to be installed on a Windows File Server machine if you want to monitor access events on the file server. Data Insight can automatically install the agent on the Windows File Server when adding the file server using the Console (recommended).

Optionally, you can choose to install the agent manually on the file server.

Note: In case of manual installation, Local system account credentials are used by default. For classification functionality, update the scanner credentials with the user having appropriate privileges for scanning the shares by navigating to Settings > Filers > Windows File Server > Edit and updating scanner credentials.

For detailed information about automatically installing the agent on the Windows File Server, see the *Veritas Data Insight Administrator's Guide*.

To configure a Windows File Server manually

1. Install the Windows File Server agent on the file server machine.

   See "Installing Windows File Server agent manually" on page 67.

2. Register the agent with the Management Server using the `RegisterWorkerNode.exe` utility. During registration, you can specify the address of the worker node that is intended to be the Collector node of this file server. Registration takes place through the Collector worker node. Registering the agent ensures that the file server can communicate with the Collector worker node.

   The procedure to registration of Windows File Server agent is the same as registering a worker node.

   See "Registering the worker node" on page 56.

3. Add the file server to the Management Server using the `ConfigureWindowsFileServer.exe` utility.

   See "Configuring the Windows File Server using ConfigureWindowsFileServer.exe" on page 68.

4. If the file server is clustered using MSCS, do the following:.
   - Install the agent on each node of the cluster.
   - Register each node with the Management Server using its physical host address.
   - Run `ConfigureWindowsFileServer.exe` from each cluster node after registering the node.

Installing Windows File Server agent manually

To install the Windows File Server agent manually

1. Locate the agent installer binary from the agent bundle that ships with the product. The agent bundle is a compressed file that contains the agent installer along with some installation templates. It is called .
2. Unzip it in a temporary location to get the installer binary.
3. Log on (or remote log on) as Administrator to the Windows file server, where you intend to install the agent.
4. Right click the agent and click run as administrator.
5. The Welcome to the Veritas Data Insight Setup Wizard window appears. Click **Next**.

6 In the License Agreement window, select **I accept the agreement**, and click **Next**.

7 In the Select Destination Directory window, browse to the directory in which you want Data Insight to be installed. By default, the destination directory is `C:\Program Files\DataInsight`.

8 In the **Configure Data Directory** window, browse to the location where you want to store the product data. Select a location with enough free space.

9 In the **Configure Networking** window, enter the following information:

- Communication Service Port
  See "About Communication Service" on page 16.
- Configuration Service port
  Configuration service is a process that provides interface to configuration and other product data that is stored on the local system. This service port does not need to be accessible outside the host machine.

Note: The installer validates whether the appropriate ports are free to accept connections.

---

10 To start the installation process, click **Next**.

11 To register the worker node with the Management Server after you exit setup, select the **Launch Worker Node Registration Wizard after exit** checkbox.

See "Registering the worker node" on page 56.

12 To exit setup, click **Finish**.

Configuring the Windows File Server using ConfigureWindowsFileServer.exe

Run the `ConfigureWindowsFileServer.exe` utility to configure the file server from the file server machine. You must run this utility after you have registered the agent node with the Management Server to add the file server to the Management Server configuration. Data Insight starts monitoring this file server after you have completed this step.

To configure the Windows File Server from the file server machine

1. Double-click `ConfigureWindowsFileServer.exe` located in the `bin` folder of the installation.

   The File Server Configuration Wizard appears.

2. Select **This File Server is a part of MSCS cluster** check box if this node is a part of an MSCS cluster. If you select this option, specify name of this cluster in the Cluster Name text box. You must enter the exact same name in this field when you run this utility on all nodes of this cluster.

3. Select the Collector worker node for this file server using the Collector Node drop-down. All communication with this file server happens through the associated Collector node.

4. Select **Automatically discover shares on this filer** check box if you want Data Insight to automatically discover shares on this filer and add them to the configuration.

   Note: If this filer is a Clustered file server, you need to log into the Console later and specify credentials of an Administrative user on this cluster before discovery can happen.

   You can optionally specify shares that need to be ignored during discovery by specifying matching patterns in the adjoining text box.

   ---

5. Select **Scan new shares immediately** check box to add newly added shares to the scan queue immediately without waiting for the normal full scan schedule. However, scanning will still take place only during the times scanning is permitted on the node.

6. Click **Configure Now** button to finish the configuration. The utility will contact the Management Server through the selected Collector node and add the file server to the Management Server. If this is a clustered file server and the filer has already been added through the first node, this step associates this additional cluster node with the existing filer configuration.

Alternately, you can choose to not run this utility post-registration, and configure the Windows File Server agent from the Management Console.

To configure the Windows File Server agent from the Management console

1. Register the Windows File Server agent with the Management Server.

2. Log on to the Management Console.

3 From the **Settings** > **Filers** page, select **Add New Filer** and from the drop-down, select **Windows File Server**.

On the Add New Windows File Server page, clear the **Let Data Insight install the agent automatically** check box.

4 Select this node from the list view control to associate this node with the file server.

Chapter 7

Getting started with Data Insight

This chapter includes the following topics:

- About the Data Insight Management Console
- Logging in to the Data Insight Management Console
- Logging out of the Data Insight Management Console
- Displaying online help

About the Data Insight Management Console

Users interact with Data Insight primarily through the Data Insight Management Console. The Data Insight Console is a graphical user interface that provides a central point to view storage resources that Data Insight monitors, schedule processes, and view reports, among other features. The Console is automatically installed with the Management Server. You access the Console through a Web browser that has a network connection to the Management Server. By default, the Management Server runs on HTTPS port 443.

Logging in to the Data Insight Management Console

To log on to the console from the Management Server or a worker node

1 Do one of the following:

- Click the shortcut created on the Desktop during installation.

- Click **Start** > **Programs** > **Veritas** > **Veritas Data Insight** > **Data Insight Console**.

2. On the Login screen, enter the credentials of a user with privileges to log in to the Management Server.
3. Enter the name of the domain to which the user belongs.
4. Click **Submit**.

   The Management Console appears.

To log on to the console from a machine other than the Management Server or the worker nodes

1. Open a Web browser and enter https://<*ms_hostname/hostip*>:<*ms_port*>. For example, https://datainsight.company.com:443.
2. On the Login screen, enter the credentials of a user with privileges to log in to the Management Server.
3. Enter the name of the domain to which the user belongs.
4. Click **Submit**.

   The Management Console appears.

Configuring single sign-on (SSO) using security assertion markup language (SAML)

Data Insight supports Single Sign On (SSO) for a standard unified login. User authentication is performed through an external Identity Management Server allowing for an increased level of security for user passwords and identity details. To use Single Sign On, setup is required on the Data Insight and an external Identity Provider (IDP).

For more details, refer *Configuring single sign-on (SSO) using security assertion markup language (SAML)* section the Data Insight Administrator's Guide.

Logging out of the Data Insight Management Console

To log out

1. Click logout at the top right of the screen.
2. Click **OK** to go back to the login screen.

Displaying online help

To access online help, click the **Help** button in the upper-right corner of any screen in the Management Console. Veritas Data Insight displays the help in a separate window. The online help shows the table of contents in the left pane and context-sensitive help in the right pane.

Chapter 8

Uninstalling Veritas Data Insight

This chapter includes the following topics:

- Uninstalling Veritas Data Insight

Uninstalling Veritas Data Insight

To uninstall Data Insight

1. If you created shortcuts during the installation, select **Start > All Programs > Veritas Data Insight > Veritas Data Insight Uninstaller**.

   If no shortcuts exist, open the **Add or Remove Programs** control from the **Windows Control Panel**, and select the Veritas Data Insight entry. Then click **Change/Remove**.

   Optionally, you can uninstall Veritas Data Insight using the uninstall.exe file. This file is located in the Data Insight installation folder (for example, `C:\Program Files\DataInsight`). On Linux, execute the script /opt/DataInsight/uninstall to launch the uninstall program.

2. In the Delete Data window, select the **Delete all product data** checkbox to remove all configuration as well as audit log data collected and stored by the product. Do not select this option, if you are attempting to repair the installation by uninstalling and reinstalling the software.

3. Click **Next** to uninstall.

   The uninstaller removes all Veritas Data Insight components.

4. Click **Finish** to complete the uninstall process.

5 If you uninstall a worker node, log in to the Management Console, click the **Settings** tab.

6 Navigate to the Data Insight Servers page, select the worker node, and click **Delete**.

7 After un-installation, you must remove Data Insight related commands from etc/rc.local and etc/rc.local.shutdown files.

Appendix A

Installing Data Insight using response files

This appendix includes the following topics:

- About response files
- Installing Data Insight using response files
- Sample response files

About response files

The installer or the product installation script generates a response file during any installation, configuration, upgrade, or uninstall procedure. The response file contains the configuration information that you entered during the procedure.

You can use the response file for future installation procedures. The response file passes arguments to the script to automate the installation of that product. You can edit the file to automate installation and configuration of additional systems.

Installing Data Insight using response files

Typically, you can use the response file that the installer generates, after you install Data Insight on a system in order to install Data Insight on other systems.

To install using response files

1. Make sure the systems where you want to install Data Insight meet the installation requirements.

   See "Minimum system requirements for Data Insight components" on page 22.

2. Make sure the pre-installation tasks are completed.

3. Create and copy the response file to the system where you want to install Data Insight.
4. Navigate to the directory that contains the installation program.
5. Start the installation as follows:
6. If installing a worker node, register the worker node using the following command:

```
RegisterWorkerNode.exe –q –console –varfile
<path_to_register_varfile> –wait [timeout in seconds]
```

Note: Before you launch the registration wizard, you must copy `<datadir>/keys/commd.keystore` file to the worker node to a temporary location, for example,`C:\temp\commd.keystore`.

Sample response files

The following example shows a response file for the Management Server:

```
# Installation folder
sys.installationDir=C\:\\Program Files\DataInsight
# Data folder
matrix.datadir=C\:\\DataInsight\\data
# Name for Management Server node
matrix.nodename=host.company.com
matrix.console.name=host.company.com
# Ports for DataInsightWeb, DataInsightComm, DataInsightConfig
matrix.webserver.port$Long=443
matrix.commd.port$Long=8383
matrix.queryd.port$Long=8282
matrix.install.mode=ms
matrix.worker.iswinnas$Boolean=false
# Username/Domain for initial administration
matrix.initial.admin.login=Administrator
matrix.initial.admin.domain=WISDOM
```

```
matrix.initial.admin.isgroup$Boolean=false
```

If the Management Server is part of Active Directory domain, specify if Management Server domain should be scanned.

```
matrix.scan.ad$Boolean=true
```

Specify whether services should be started after installation

```
matrix.ms.startServices$Boolean=true

sys.programGroupAllUsers$Boolean=true

createDesktopLinkAction$Boolean=true

createQuicklaunchIconAction$Boolean=true

sys.programGroupDisabled$Boolean=false

matrix.launch.console$Boolean=false

matrix.fips.enabled$Boolean=${isfips}
```

Sample response file for installing a Collector node

Installation folder

```
sys.installationDir=C\:\\Program Files\DataInsight
```

Data folder

```
matrix.datadir=C\:\\DataInsight\\data
```

#Address for Collector node

```
matrix.nodename=host.company.com

matrix.worker.name=host.company.com
```

Ports for DataInsightComm, DataInsightConfig, DataInsightWorlkflow

```
matrix.commd.port$Long=8383

matrix.queryd.port$Long=8282

matrix.workflow.port=8686

matrix.install.mode=worker

matrix.worker.isindexer$Boolean=true

createQuicklaunchIconAction$Boolean=true

sys.programGroupDisabled$Boolean=true

createDesktopLinkAction$Boolean=true

sys.programGroupAllUsers$Boolean=true
```

```
matrix.launch.register$Boolean=false
```

Sample response file for launching the worker node registration wizard

Address of the Management Server

```
matrix.console.name=<IP address of the Management Server>
```

#Path to commd.keystore

```
matrix.ms.keystore=C\:\\DataInsight\\data\\commd.keystore
```

Whether services should be started after registration

```
matrix.worker.startServices$Boolean=true

matrix.launch.console$Boolean=false

matrix.fips.enabled$Boolean=${isfips}
```

Sample response file for installing a server with the Collector and Indexer roles

Installation folder

```
sys.installationDir=C\:\\Program Files\DataInsight
```

Data folder

```
matrix.datadir=C\:\\DataInsight\\data
```

#Address for Collector node

```
matrix.nodename=host.company.com matrix.worker.name=host.company.com
```

Ports for DataInsightWeb, DataInsightComm, DataInsightConfig

```
matrix.commd.port$Long=8383

matrix.queryd.port$Long=8282 matrix.install.mode=worker

matrix.worker.isindexer$Boolean=false

createQuicklaunchIconAction$Boolean=true

sys.programGroupDisabled$Boolean=true

createDesktopLinkAction$Boolean=true
sys.programGroupAllUsers$Boolean=true

matrix.launch.register$Boolean=false
```

Sample response file for launching the worker node registration wizard

Address of the Management Server

```
matrix.console.name=<IP address of the Management Server>
```

#Path to commd.keystore

```
matrix.ms.keystore=C\:\\DataInsight\\data\\commd.keystore
```

Whether services should be started after registration

```
matrix.worker.startServices$Boolean=true

matrix.launch.console$Boolean=false

matrix.fips.enabled$Boolean=${isfips}
```

Sample response file for installing a Windows File Server node

Run the following command:

Installation folder

```
matrix.upgrade$Boolean=false

sys.installationDir=<INSTALLDIR>
```

#For example, C\:\\Program Files\DataInsight

```
matrix.install.mode=worker

matrix.worker.isindexer$Boolean=false

matrix.worker.iscollector$Boolean=true

matrix.worker.iswinnas$Boolean=true

matrix.datadir=<DATADIR>
```

#For example, C\:\\DataInsight\\data

```
matrix.worker.name=<FILER_FQDN>
```

worker.name property is the name of Windows File Server.

```
matrix.commd.port$Long=8383

matrix.queryd.port$Long=8282

matrix.enable.drwatson$Boolean=true

matrix.launch.register$Boolean=false

matrix.launch.console$Boolean=false
```

```
matrix.fips.enabled$Boolean=${isfips}

#sys.programGroup.name=Veritas Data Insight

#sys.service.selected.114$Boolean=true

#sys.languageId=en

#sys.programGroup.linkDir=/usr/local/bin

#sys.service.startupType.1393=auto

#sys.programGroup.enabled$Boolean=true

#sys.service.selected.1393$Boolean=true

#sys.service.startupType.114=auto

#sys.programGroup.allUsers$Boolean=true
```

Registration properties:

```
#matrix.register.node.during.install$Boolean=true

#matrix.register.node.varfile=<PATH TO VAR FILE>
```

matrix.register.node.varfile can be the path of the varfile. For example, C\:\\Temp\\DataInsight\\winnas.varfile.

```
#matrix.console.name=<COLLECTOR FQDN>:<COMMD PORT>
```

(Default Communication Service port is 8383) For example, DICollector1.win.local:8383

```
#matrix.ms.keystore=<PATH TO KEYSTORE>
```

For example, C\:\\Temp\\DataInsight\\commd.keystore

```
#matrix.shortcuts$Boolean=true

#matrix.worker.startServices$Boolean=true

#matrix.launch.configure.winnas.filer$Boolean=true

#matrix.launch.console$Boolean=false

matrix.fips.enabled$Boolean=${isfips}
```

Sample configuration file for configuring a Windows File Server as a filer

Navigate to `<Data Insight Install directory>\bin` folder and run the following command:

```
Configcli register_filer <Name of configuration file>
```

For example: `Configcli register_filer C:\\tempp\\Registerfiler.conf`

The configuration file contains the following properties:

```
filer.id=11

filer.name=FileServer1.SAMGWIN.local

filer.type=WINNAS

filer.scanNewSharesImmediately$Boolean=true

filer.monitorAllShares$Boolean=true

filer.excludeShares=*$

filer.winnas.clustered$Boolean=false

filer.winnas.with.agent=true

filer.indexer.name=Indexer1.SAMGWIN.local

filer.collector.name=Collector1.SAMGWIN.local
```

Where,

`filer.id` is the ID of the Windows File Server. If adding a new filer, leave this field empty.

`filer.name` is the FQDN of the Windows File Server.

`filer.type` will be WINNAS.

`filer.indexer.name` is the FQDN of the Indexer.

Sample response file for installing the Self-Service Portal node

```
sys.programGroupDisabled$Boolean=false
```

Installation folder

```
sys.installationDir=C\:\\Program Files\DataInsight

sys.languageId=en

matrix.portal.port$Long=443

matrix.worker.iswinnas$Boolean=false

matrix.install.mode=worker

matrix.worker.winnas.plat=WLH

matrix.datadir=C\:\\DataInsight\\data

createQuicklaunchIconAction$Boolean=true

matrix.nodename=testnode.tulip.local
```

```
sys.programGroupName=Veritas Data Insight 6.6.1

matrix.launch.console$Boolean=false

matrix.fips.enabled$Boolean=${isfips}

matrix.launch.register$Boolean=true

matrix.worker.isportal$Boolean=true

matrix.commd.port$Long=8383

sys.programGroupAllUsers$Boolean=true

matrix.worker.name= testnode.tulip.local

createDesktopLinkAction$Boolean=true

matrix.workflowd.port$Long=8686

matrix.queryd.port$Long=8282

sys.adminRights$Boolean=true
```

Sample response file to launch the worker node registration wizard to register the Collector, Indexer, Windows File Server, and the Portal nodes with the Management Console

```
matrix.launch.console$Boolean=false

matrix.fips.enabled$Boolean=${isfips}

sys.languageId=en

sys.adminRights$Boolean=true

matrix.console.name=10.209.109.239

sys.installationDir=C\:\\Program Files\DataInsight

matrix.worker.startServices$Boolean=true

matrix.ms.keystore=C\:\\TempDir\\keys\\commd.keystore
```

Sample response file to upgrade a Collector node

```
matrix.upgrade$Boolean=true
```

# Indicates that upgrade has been requested

```
matrix.upgrade.data.during.install$Boolean=true
```

# Indicates that data be upgraded automatically during the upgrade

```
matrix.upgrade.backup$Boolean=false
```

#Indicates if `data` directory should first be backed up temporarily before the data is upgraded.

`matrix.backup.dir$String=`

#Indicates where data should be backed up. If empty or not defined, %tmp% will be used

`matrix.upgrade.backup.restore$Boolean=true`

#Indicates if old data should be restored back in case upgrade fails. You must set matrix.upgrade.backup to true for this to take effect.

`matrix.upgrade.backup.delete$Boolean=true`

#Indicates if backup copy can be deleted after upgrade is successful. You must set matrix.upgrade.backup to true for this to take effect.

Sample response file to upgrade a Windows File Server Agent

`matrix.upgrade$Boolean=true`

# Indicates that upgrade has been requested.

`matrix.upgrade.data.during.install$Boolean=true`

#Indicates that data be upgraded automatically during the upgrade.

`matrix.upgrade.backup$Boolean=false`

#Response file if any to be passed to `UpgradeData.exe` when `matrix.upgrade.data.during.install` is set to true. This is optional and is generally not needed.

The response file supports following variables:

#Format for `UpgradeData.exe` varfile

Indicates if `data` directory should first be backed up temporarily before the data is upgraded.

`matrix.backup.dir$String=`

#Indicates where data should be backedup. If empty or not defined, %tmp% is used.

`matrix.upgrade.backup.restore$Boolean=true`

#Indicates if the old data should be restored in case upgrade fails. You must set `matrix.upgrade.backup` to true for this to take effect.

`matrix.upgrade.backup.delete$Boolean=true`

#Indicates if backup copy can be deleted after the upgrade is successful. You need to set `matrix.upgrade.backup` to true for this to take effect.