

# Veritas Data Insight Software Compatibility List

6.3

# Veritas Data Insight Software Compatibility List

Documentation version: .1

PN:

## Legal Notice

Copyright © 2019 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product and available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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](http://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](http://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](http://www.veritas.com/support)

## Customer service

Customer service information is available at the following URL:

[www.veritas.com/support](http://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
- Non technical 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](mailto:CustomerCare@veritas.com)

Japan

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

# Data Insight Software Compatibility List

This document includes the following topics:

- [Operating system requirements](#)
- [Supported browsers](#)
- [Web server version](#)
- [Java version](#)
- [Minimum system requirements for Data Insight components](#)
- [List of ports](#)
- [Supported data sources](#)
- [Veritas Data Insight integrated solutions](#)

## Operating system requirements

[Table 1-1](#) provides an overview of Veritas Data Insight operating system requirements:

**Table 1-1** Veritas Data Insight operating system requirements

Operating system supported	Notes
Windows Server 2012	Windows Server 2012 (64-bit ) Windows Server 2012 R2 (64-bit )

**Table 1-1** Veritas Data Insight operating system requirements (*continued*)

Operating system supported	Notes
Windows Server 2016	Windows Server 2016 (64-bit ) Supported editions: Standard, Essential, and Data center
Windows Server 2019	Windows Server 2019 (64-bit ) Supported editions: Standard, Essential, and Data center
Red Hat Enterprise Linux	Version 6.0 update 3 or later Version 7 or later Only 64-bit packages are supported.
VMware	64-bit Windows 2012 64-bit Windows 2016 or higher Red Hat Enterprise Linux version 6 update 3 or later Red Hat Enterprise Linux version 7 <b>Note:</b> You must ensure that VMware Tools is installed on VMware virtual machines.

## Supported browsers

[Table 1-2](#) provides an overview of the browser support for Veritas Data Insight

**Table 1-2** Veritas Data Insight Supported browsers

Browser	Versions
Mozilla Firefox	62.0 or higher
Google Chrome	69.0.3497.100 or higher
Microsoft Edge	42.17134.1.0 or higher
Internet Explorer	11

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

## Web server version

Veritas Data Insight uses Apache Tomcat version 9.0.58.

## Java version

Veritas Data Insight uses Amazon Corretto Java version 1.8.0\_292

## Minimum system requirements for Data Insight components

**Table 1-3** Minimum system requirements for Data Insight components

Component	Operating System	Minimum Hardware
Management Server	<ul style="list-style-type: none"><li>■ Windows Server 2012, 2012 R2.</li><li>■ Windows Server 2016.</li><li>■ Windows Server 2019 (supported editions: Standard, Essential, and Data center)</li></ul> <p>The operating system must be 64-bit.</p> <p>VMware ESX virtual machines running supported operating systems. (Recommended - VMware ESX Server version 5.1 or higher)</p>	<ul style="list-style-type: none"><li>■ 32GB RAM</li><li>■ 16 CPUs</li></ul>

**Table 1-3** Minimum system requirements for Data Insight components  
*(continued)*

Component	Operating System	Minimum Hardware
Collector worker node	<ul style="list-style-type: none"> <li>■ Windows Server 2012, 2012 R2.</li> <li>■ Windows Server 2016</li> <li>■ Windows Server 2019 (supported editions: Standard, Essential, and Data center)</li> </ul> <p>The operating system must be 64-bit.</p> <p>VMware ESX virtual machines running supported operating systems.                      (Recommended - VMware ESX Server version 5.1 or higher)</p> <p><b>Note:</b> Enterprise Edition is supported when Windows Server 2012, 2012 R2, or 2016 is being used as the Collector node for NFS exports on devices.</p>	<ul style="list-style-type: none"> <li>■ 8GB RAM</li> <li>■ 4 CPUs</li> </ul>
Indexer worker node	<ul style="list-style-type: none"> <li>■ Windows Server 2012 or 2012 R2.</li> <li>■ Windows Server 2016.</li> <li>■ Windows Server 2019 (supported editions: Standard, Essential, and Data center)</li> <li>■ Red Hat Enterprise Linux version 6.0 or higher and 7.0 or higher.</li> </ul> <p>The operating system must be 64-bit.</p> <p>VMware ESX virtual machines running supported operating systems. (Recommended - VMware ESX Server version 5.1 or higher)</p>	<ul style="list-style-type: none"> <li>■ 32 GB RAM</li> <li>■ 16 CPUs</li> </ul>

**Table 1-3** Minimum system requirements for Data Insight components  
*(continued)*

Component	Operating System	Minimum Hardware
Windows File Server Agent	<ul style="list-style-type: none"> <li>■ Windows Server 2012 or 2012 R2.</li> <li>■ Windows Server 2016.</li> <li>■ Windows Server 2019 (supported editions: Standard, Essential, and Data center)</li> </ul> <p>The operating system must be 64-bit.</p> <p>VMware ESX virtual machines running supported operating systems.                      (Recommended - VMware ESX Server version 5.1 or higher)</p>	<ul style="list-style-type: none"> <li>■ 4 GB RAM</li> <li>■ 2 CPUs</li> </ul>
Self-Service Portal Node	<ul style="list-style-type: none"> <li>■ Windows Server 2012, Windows Server 2012 R2.</li> <li>■ Windows Server 2016.</li> <li>■ Windows Server 2019 (supported editions: Standard, Essential, and Data center)</li> </ul> <p>The operating system must be 64-bit.</p> <p>VMware ESX virtual machines running supported operating systems.                      (Recommended - VMware ESX Server version 5.1 or higher)</p>	<ul style="list-style-type: none"> <li>■ 8 GB RAM</li> <li>■ 4 CPUs</li> </ul>
Data Insight SharePoint Agent	<ul style="list-style-type: none"> <li>■ Microsoft SharePoint 2013</li> <li>■ Microsoft SharePoint 2016</li> <li>■ Microsoft SharePoint 2019</li> </ul>	Not Applicable

## System requirements for classification components

Table 1-4 lists the minimum recommended system requirements for classification components.

**Table 1-4** Minimum recommended system requirements for classification components

Component	If classification is enabled	If Smart Classification is enabled
Management Server	<ul style="list-style-type: none"> <li>■ 32GB RAM</li> <li>■ 16 CPUs</li> </ul>	<ul style="list-style-type: none"> <li>■ 128GB RAM</li> <li><b>Note:</b> Provision additional 2 MB space per million paths.</li> <li>■ 32 CPUs</li> <li>■ 200 GB of free disk space for temporary files which are created during the classification process.</li> </ul>
Indexer worker node	<ul style="list-style-type: none"> <li>■ 32GB RAM</li> <li>■ 16 CPUs</li> </ul>	<ul style="list-style-type: none"> <li>■ 128GB RAM</li> <li><b>Note:</b> Provision additional 2 MB space per million paths.</li> <li>■ 32 CPUs</li> <li>■ 200 GB of free disk space for temporary files which are created during the classification process.</li> </ul>
Collector worker node	<ul style="list-style-type: none"> <li>■ 8GB RAM</li> <li>■ 4 CPUs</li> </ul>	Recommended minimum system configuration is 32GB RAM 16 CPUs
Classification Server	<ul style="list-style-type: none"> <li>■ 32GB RAM</li> <li>■ 16 CPUs</li> </ul>	Same as when classification is enabled.
Windows File Server agent node	<ul style="list-style-type: none"> <li>■ 8GB RAM</li> <li>■ 4 CPUs</li> </ul>	Same as when classification is enabled.

---

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

---

## List of ports

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

**Table 1-5** List of default ports

Component	Default Port
Management Server	Management Console, HTTPS, port 443 Communication service, HTTPS port 8383 DataInsightConfig service, port 8282 Workflow Service, HTTPS, port 8686 Standard RPC, ports 139 and 445
Collector worker node\ Indexer plus Collector worker node	Communication service, HTTPS port 8383 Standard RPC ports 139 and 445 DataInsightConfig service, port 8282 NetApp Cluster-Mode service, TCP port 8787 (configurable) Generic Collector service, HTTPS port 8585 (configurable)
Indexer worker node	Communication service, HTTPS port 8383 DataInsightConfig service, port 8282

**Table 1-5** List of default ports (*continued*)

Component	Default Port
File Server	<p>For NetApp filers - HTTP port 80 (optional), standard RPC ports 139 and 445, 2049 (TCP,UDP) and 111 (TCP,UDP) for NFS</p> <p>For NetApp Cluster-Mode, HTTP port 80</p> <p>On EMC Control Station - HTTP port 80 and HTTPS port 443</p> <p>On Windows File Servers managed without an agent - Standard RPC ports 139 and 445</p> <p>For Veritas File System servers - HTTPS port 5634, 2049 (TCP,UDP) and 111 (TCP,UDP) for NFS</p>
Windows File Server agent node	<p>Communication Service, HTTPS port 8383</p> <p>DataInsightConfig service, port 8282</p> <p>Standard RPC ports 139 and 445</p>
SharePoint web service	SharePoint web service is accessed over the same port as the configured web applications. This port on the SharePoint web servers should be accessible from the Collector node.
LDAP Directory Server	Port 389 or 636 (for TLS)
NIS Server	Ports 111 (TCP,UDP), 714 (TCP), 711 (UDP)
NIS+ Server in NIS compatibility mode	Ports 111 (TCP,UDP), 714 (TCP), 711 (UDP)
OneDrive	DataInsightOneDrive service, port 9090
Documentum	DataInsightCMIS service, port 9191
SharePoint Online	DataInsightSPOnline service, port 9292
Amazon S3	DataInsightAmazonS3 service, port 9393
Symantec Data Loss Prevention (DLP)	HTTPS port 443
Enterprise Vault Server	HTTP port 80 or as configured by Enterprise Vault Server web service.

**Table 1-5** List of default ports (*continued*)

Component	Default Port
Self-Service Portal server	Portal Service, HTTPS port 443 Workflow Service, HTTPS port 8686 DataInsightConfig, service port 8282 Communication service, HTTPS port 8383
Classification Server	Communication service, HTTPS port 8383 Standard RPC ports 139 and 445 DataInsightConfig, service port 8282 DataInsightVICServer, service port 8989
DataInsightVICServer	8989

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

Refer the table below for a different view about the port configuration. Both the tables carry similar information with separate views.

**Table 1-6** List of default ports

Source	Destination Server	Destination Port	Description
Web Browser	Management Server	443	Used for accessing Data Insight UI
Web Browser	Portal UI	443	Used for accessing Data Insight UI
Management Server	Collector	8383	Communication across Data Insight Nodes
Management Server	Indexer	8383	Communication across Data Insight Nodes
Management Server	Classification Server Role	8383	Communication across Data Insight Nodes
Management Server	Windows Agent	8383	Communication across Data Insight Nodes

**Table 1-6** List of default ports (*continued*)

Source	Destination Server	Destination Port	Description
Collector	Management Server	8383	Communication across Data Insight Nodes
Collector	Indexer	8383	Communication across Data Insight Nodes
Collector	Classification Server	8383	Communication across Data Insight Nodes
Collector	Windows Agent	8383	Communication across Data Insight Nodes
Indexer	Management Server	8383	Communication across Data Insight Nodes
Indexer	Collector	8383	Communication across Data Insight Nodes
Indexer	Indexer	8383	Communication across Data Insight Nodes
Indexer	Classification	8383	Communication across Data Insight Nodes
Classification	Indexer	8383	Communication across Data Insight Nodes
Classifier	Management Server	8383	Communication across Data Insight Nodes
Classifier	Collector	8383	Communication across Data Insight Nodes
Classifier	Windows Agent	8383	Communication across Data Insight Nodes
Windows Agent	Management Server	8383	Communication across Data Insight Nodes
Windows Agent	Collector	8383	Communication across Data Insight Nodes
Windows Agent	Classifier	8383	Communication across Data Insight Nodes

**Table 1-6** List of default ports (*continued*)

Source	Destination Server	Destination Port	Description
Present on all Data Insight Nodes	Each Data Insight Nodes accesses its own port 8282 locally. There is no inter-server communication on this port.	8282	Configuration Service
Data Insight Nodes Management Server and Portal Server	Data Insight Nodes Management Server and Portal Server	8686	Workflow Service
Collector	Collector	9090	OneDrive Service (Runs locally)
Collector	Collector	9292	SPOnline Service (Runs locally)
Collector	Collector	9191	CMIS Service: Documentum (Runs locally)
Collector	Collector	9393	Amazon S3 Service (runs locally)
Classifier	Classifier	9393	Amazon S3 Service (runs locally)
Classifier	Classifier	8989	DataInsightVICServer Service (Runs locally)
Collector	Collector	8787	NetApp Cluster-Mode service (Runs locally)
Collector	Collector	8585	Generic Collector service (Runs locally)
Management Server	Symantec Data Loss Prevention (DLP)	443	Used for Communication with Symantec DLP Server

**Table 1-6** List of default ports (*continued*)

Source	Destination Server	Destination Port	Description
Management Server	Enterprise Vault Server	80	Used for Communication with EV Server
Collector	NetApp Filers	HTTP port 80, Standard RPC ports 139 and 445, 2049 (TCP, UDP) and 111 (TCP, UDP) for NFS	Data Insight communicates with NetApp Filers on specified ports
Collector	NetApp Cluster-Management Server	HTTP port 80	Data Insight communicates with NetApp Cluster-Mode Filer on specified port
Collector	EMC Celera/PowerScale	HTTP port 80 and HTTPS port 443	Data Insight communicates with EMC Control Station on specified port
Collector	Windows File Servers managed without an agent	Standard RPC ports 139 and 445	Winnas share and storage discovery
Collector	Veritas File System servers	HTTPS port 5634, and 2049 (TCP, UDP) and 111 (TCP, UDP) for NFS	Data Insight with Veritas File System Server on specified port
Management Server	Active Directory Server	389 or 636 (for TLS)	Data Insight communicates with AD Server on specified port
Management Server	NIS Server	111 (TCP, UDP), 714 (TCP), 711 (UDP)	Data Insight communicates with NIS Server on specified port
Management Server	NIS+ Server in NIS compatibility mode	111 (TCP, UDP), 714 (TCP), 711 (UDP)	Data Insight communicates with NIS+ Server on specified port

# Supported data sources

**Table 1-7** Supported data sources

Vendor	Configuration	Version	Supported Protocol	Notes
NetApp	7-mode	Data ONTAP 7.3.5 or higher Data ONTAP 8.x	CIFS over NTFS, NFS version 3	Data Insight supports FabricPool for the ONTAP 9.6 or higher versions.
	Cluster Mode	Data ONTAP 8.2.x or higher	CIFS	
		ONTAP 8.2.3 or higher ONTAP 8.3.1 or higher	NFS version 3	
		ONTAP 9.x	CIFS, NFS version 3	

**Table 1-7** Supported data sources (*continued*)

Vendor	Configuration	Version	Supported Protocol	Notes
EMC	Isilon	7.1.71.1 to 8.x	CIFS over NTFS	NFS protocol is not supported for monitoring and scanning metadata for versions 7.1.71.1 to 8.x
		OneFS 9.x	CIFS over NTFS and NFS	NFS monitoring and scanning metadata is supported only for version 9.x and above.
	Celerra	DART 5.6.45 or higher DART 8.x	CIFS over NTFS	NFS protocol is not supported for monitoring and scanning metadata.
	VNX Operating Environment (OE)	7.1.71.1 to 8.x	CIFS over NTFS	
	PowerScale	OneFS 9.x	CIFS over NTFS	
	Unity VSA	11.x	CIFS	-
	Unity	4.x and 5.x	CIFS	-
OpenText	Documentum	6.x	Cabinets and Repositories	-
Hitachi	Not applicable	Hitachi NAS 12.x Hitachi NAS 13.x	CIFS	NFS protocol is not supported for monitoring and scanning metadata.

**Table 1-7** Supported data sources (*continued*)

Vendor	Configuration	Version	Supported Protocol	Notes
Microsoft SharePoint	Not applicable	2013	Document and Picture libraries.	-
		2016	Document and Picture libraries.	
		2019	Document and Picture libraries.	
Microsoft Windows File Server	Not applicable	2012	CIFS REFS	Windows Server 2012, or 2012 R2 64-bit.
		2016	CIFS REFS	Windows Server 2016, 64-bit.
		2019	CIFS REFS	Windows Server 2019, 64-bit.
Microsoft Office 365	SharePoint Online OneDrive	Not applicable	For SharePoint, Document and Picture libraries.	-
Veritas file server	Unix with Veritas Storage Foundation (VxFS)	6.1 and higher	NFS version 3	Configured in standalone or cluster mode using Veritas Cluster Server (VCS).  For VCS support, Clustered File System (CFS) is not supported.

**Table 1-7** Supported data sources (*continued*)

Vendor	Configuration	Version	Supported Protocol	Notes
Generic devices	Not applicable	Not applicable	CIFS, NFS version 3	Supports collection of events through APIs and automatic share discovery, scanning of metadata, and content classification through Data Insight.
Box (Cloud-based content management platform)	-	Not applicable	-	-
Amazon S3 (Amazon Simple Storage Service is a service offered by Amazon Web Services (AWS) that provides object storage through a web service interface)	-	Not applicable	-	-

Note the following:

- Veritas strongly recommends that you upgrade your NetApp filer to the latest available firmware. Veritas recommends ONTAP 7.3.5 or higher.
- For all supported versions of 7-mode NetApp filers, Data Insight supports the following volume styles:
  - CIFS protocol over NTFS
  - UNIX and Mixed for NFS protocol
  - NFS protocol v3

- For supported versions of Cluster-Mode NetApp filers, Data Insight supports the following volume/qtree styles:
  - NTFS and Mixed for CIFS protocol.
  - UNIX and Mixed for NFS protocol
  - NFS exports on the NetApp cluster
  - NFS protocol v3
- Data Insight supports Common Event Enabler (CEE), version 8.2 or higher. Data Insight still supports the older version of CEE and VEE, but Veritas recommends that you move to the latest EMC Common Event Enabler, which you can download from the EMC website.

## Veritas Data Insight integrated solutions

**Table 1-8** Veritas Data Insight integrated solutions

<b>Product</b>	<b>Certified versions</b>
Symantec Data Loss Prevention (DLP)	15.5, 15.7, and 15.8 MP1
Enterprise Vault	12.0, 12.1, 12.2, 12.3, 12.4, 12.5, 14.0, and 14.2
Veritas Information Classifier (VIC)	3.1.0