

Quest[®] NetVault[®] Plug-in *for Malware
Detection* 14.1

User's Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (<https://www.quest.com>) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest Software, Quest, the Quest logo, QoreStor, and NetVault are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

Legend

- **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

- ⚠ **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

- i **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

NetVault Plug-in for *Malware Detection* User's Guide
Updated - April 2026

Software Version - 14.1

Content

Introducing NetVault Plug-in for Malware Detection	4
About NetVault Plug-in for Malware Detection	4
Key benefits	4
Feature summary	4
Target audience	4
Recommended additional reading	5
Installing the plug-in	6
Deployment overview	6
Prerequisites	6
Installing the plug-in	7
Installing the plug-in using the configuration wizard	7
Installing the plug-in from the Manage Clients page	7
Removing the plug-in	8
Scanning the virtual machines	9
Scanning the virtual machines	9
Color codes for savesets	10
Viewing Logs	11
Viewing logs	11
Viewing Reports	12
Viewing reports	12
Troubleshooting	13
Common errors	13
About us	14
Technical support resources	14

Introducing NetVault Plug-in *for Malware Detection*

- [About NetVault Plug-in for Malware Detection](#)
- [Target audience](#)
- [Recommended additional reading](#)

About NetVault Plug-in *for Malware Detection*

Quest NetVault Plug-in *for Malware Detection* (NetVault Plug-in *for Malware Detection*) uses an industry-leading antivirus engine to scan the backup data to proactively identify potential viruses and malware to help avoid reinfection during recovery.

This malware detection feature will work with the VMware plug-in savesets stored on the QoreStor and added as a backup target in NetVault.

Key benefits

- Helps in data recovery by reducing the effort required to find a clean copy of data.
- The user can restore infected data to an isolated environment for analysis.
- Reduce the risk of reinfection during restoration.

Feature summary

- Filesystem plug-in support.
- Supports Malware detection on RHEL 9 and 10.
- Scan performance improvement using multiple threads for VMware and Filesystem scans.
- Scan the disks for malware and report the infected files.

Target audience

This guide is intended for the security analysts or the administrators who are responsible for the managing of NetVault Plug-in *for Malware Detection*.

Familiarity with VMware vCenter and ESXi Server administration and the operating system (OS) under which the virtual machines are running is assumed. Advanced knowledge of VMware would be useful for defining an efficient backup and recovery strategy for the virtual machines.

Recommended additional reading

- **NetVault documentation:**

- *Quest NetVault Installation Guide:* This guide provides information about installing the NetVault Server and Client software.
- *Quest NetVault Administrator's Guide:* This guide provides information about configuring and using NetVault to protect your data. It provides comprehensive information about all NetVault features and functionality.
- *Quest NetVault Command Line Interface Reference Guide:* This guide provides information about using the NetVault command-line utilities.

You can download the complete set of NetVault documentation from <https://support.quest.com/technical-documents>.

- **VMware documentation:** You can download the complete set of VMware documentation from <http://www.vmware.com/support/pubs>. For updated platform-support and vSAN-related information, see the [VMware VDDK Release Notes](#).

Installing the plug-in

- [Deployment overview](#)
- [Prerequisites](#)
- [Installing the plug-in](#)
- [Removing the plug-in](#)

Deployment overview

The NetVault Plug-in *for Malware Detection* is deployable on RHEL 8.x, 9.x and 10.x NetVault clients.

This client acts as the scan proxy. Select either a physical machine or a virtual machine as a scan proxy.

Prerequisites

Before installing the plug-in, verify that the following requirements are met:

- Ensure the plug-in is installed on an Internet-enabled system to install the latest ClamAV malware scanner.
- NetVault Plug-in *for Malware Detection* is supported with NetVault version 14.0 and NetVault Plug-in for VMware version 14.0
- Install the NetVault Client software on the physical or virtual machine on which you want to install the NetVault Plug-in *for Malware Detection*.
- Install applicable libraries on Linux-based clients.
- Ensure that the following hardware and software requirements are fulfilled:
 - RHEL : Version 8, 9 and 10
 - CPU: Minimum 8 CPUs
 - RAM: Minimum 16 GB
- vCenter: 8.0.2 and above
- Register with the subscription manager to access the package manager yum. Ensure the access to EPEL yum repository (For more information, refer to: <https://access.redhat.com/solutions/3358>).
- Add the designated client to the NetVault Server. For more information about adding clients, see the *Quest NetVault Administrator's Guide*.

Installing the plug-in

The NetVault Plug-in *for Malware Detection* can be simultaneously installed on multiple machines by using the configuration wizard. Alternatively, install it on a single client from the **Manage Clients** page.

The following sections describe the different procedures that you can use to install the plug-in:

- [Installing the plug-in using the configuration wizard](#)
- [Installing the plug-in from the Manage Clients page](#)

Installing the plug-in using the configuration wizard

On Linux-based machines, you can use the configuration wizard to install the plug-in on multiple clients at the same time.

i | **NOTE:** When you use this procedure, verify that the plug-in binary file is compatible with the client OS and platform.

To install the plug-in on Linux based clients:

- 1 In the Navigation pane, click **Guided Configuration**, and then on the **NetVault Configuration Wizard** page, click **Install Plugins**.
- 2 In the **NetVault Clients** table, select the clients on which you want to install the plug-in.
- 3 Click **Choose Plug-in File**, navigate to the location of the “.npk” installation file for the plug-in, for example, on the installation CD or the directory to which the file was downloaded from the website.


Based on the OS in use, the path for this software may vary on the installation CD.

- 4 Select the file entitled “**malwarescanner-w.x.y.z-<platform>.npk**,” where **w.x** represents the version number, **y** represents the patch level, and **z** represents the build number, and click **Next**.

After the plug-in is successfully installed, a message is displayed.

Installing the plug-in from the Manage Clients page

From the **Manage Clients** page, you can install a plug-in on a single client.

- 1 In the Navigation pane, click **Manage Clients**.
- 2 In the **NetVault Clients** table, select the client, and click **Manage**.
- 3 In the lower-right corner of the **Installed Plug-ins** table, click the **Install Plugin** button (.
- 4 Click **Choose Plug-in File**, navigate to the location of the “.npk” installation file for the plug-in, for example, on the installation CD or the directory to which the file was downloaded from the website.

Based on the OS in use, the path for this software may vary on the installation CD.

- 5 Select the file entitled “**malwarescanner-w.x.y.z-<platform>.npk**,” where **w.x** represents the version number, **y** represents the patch level, and **z** represents the build number, and click **Install Plugin**.

After the plug-in is successfully installed, a message is displayed.

Removing the plug-in

- 1 In the Navigation pane, click **Manage Clients**.
- 2 In the **NetVault Clients** list, select the client, and click **Manage**.
- 3 In the **Installed Plug-ins** table, select **NetVault Plug-in for Malware Detection**, and click the **Remove Plugin** button (🗑️).
- 4 In the **Confirm** dialog box, click **Remove**.

Scanning the virtual machines

The NetVault Plug-in *for Malware Detection* helps scan the backed-up savesets of the NetVault Plug-in for VMware.

Scanning the virtual machines

- i** | **NOTE:** The Plug-in *for Malware Detection* will scan the file systems compatible with RHEL 8.x, 9.x and 10.x operating system platforms and the Plug-in for VMware.
- NOTE:** The Plug-in *for Malware Detection* does not support the non-CDP incremental and differential saveset scans.

To scan the savesets of the Plug-in for VMware:

- 1 In the Navigation pane, click **Create Scan Job**. You are redirected to the next page to select savesets.
 - i** | **NOTE:** The savesets backed up with Plug-in for VMware are only displayed.
- 2 Select the desired backed-up saveset from the table. The selected saveset information displays on the right panel of the table.
- 3 Optionally, if “Scan Details” is clicked and the selected saveset has already been scanned, the following information is displayed:
 - Scan Status: Displays selected saveset’s scanned details, e.g., fully scanned, partially scanned, etc.
 - Infected VMs: Displays the infected virtual machines where the saveset resides.
 - VMs Scanned: Displays the total number of virtual machines scanned.
 - Files Scanned: Displays the total number of files scanned on the virtual machines.
 - Infected files: Displays the total infected files on the virtual machine.

To continue scanning the selected saveset, proceed to the next step.

- 4 Click **Scan**.
- 5 Select the desired virtual machine or the containing disk(s) to scan.

The Create Scan Job page will be displayed. Configure the following settings:

 - i** | **NOTE:** Choose one or multiple virtual machines along with one or more disks associated with the chosen virtual machine.
- 6 Enter the scan job name in the Job box.
- 7 Select the **Selection set** from the dropdown or click **+Create New** to create if required.
- 8 Click **Choose** to select the Target client where the NetVault Plug-in *for Malware Detection* is already installed.
- 9 In the **Schedule** list, select an existing Schedule Set or click **Create New**, and configure the schedule type and schedule method.

Choose the scheduling method.






10 Click **Save and Submit** to execute the scan job.

i | **NOTE:** The scan table displays only the status of the most recent successful scan results or job.

Color codes for savesets

The scanned saveset of the Plug-in for VMware reflects the various statuses with the color codes. The following table enlists the same.

Table 1. Saveset status

Color codes/symbol	Description
	Fully scanned and clean.
	Partially scanned and infected.
	Partially scanned and clean.
	Fully scanned and infected.
	Not scanned.

Viewing Logs

Once the scan job completes, the scanned saveset is visible in the logs.

Viewing logs

View the logs generated after the scanning savesets of Plug-in for VMware in the logs section.

To check the logs

- 1 In the navigation page, click **View Logs**.
The recently scanned job/s with NetVault Plug-in for *Malware Detection* is enlisted in the logs along with its severity.
- 2 Click the scanned disk(s) of the virtual machine on the **View Log** page to display more information about the executed scan.

The information displayed here is as per the partition on a disk of a virtual machine in the saveset:

Table 2. Logs parameters

Parameter	Description
VM Name	A virtual machine name that contains the disk with the partition.
Disk Name	A disk within the virtual machine that contains the partition.
Partition	A unique partition ID on the disk.
File System Type	A file system on the partition.
Scan start Time	Initiation time of the scan.
Scan end time	End time of the scan.
Scan time in seconds	Time-span in which the scan process completes.
Virus definition end	Virus database version at the beginning of the scan.
Virus definition begin	Virus database version at the end of the scan.
Scanned file count	Number of files scanned on the partition.
Infected file count	Number of infected files on the partition.
The last 10 infected file paths	The last ten infected files' paths.

Viewing Reports

This section displays a report of all the savesets scanned with Plug-in *for Malware Detection*

Viewing reports

To view the reports

- 1 In the navigation page, click **View Reports**.
- 2 Select the desired filters from the following list:
 - Infected file count: Number of infected files within the virtual machine.
 - VM name: The virtual machine selected for the Malware scan job.
 - Start date: The date selected for the malware scanning.
- 3 Click **Ok** to display the report with selected filters.
A report is displayed.

The generated report has the following fields with one record per partition:

Table 3. Report parameters

Parameter	Description
Job ID	A unique job ID allocated to each scanned job.
Record ID	A unique record ID.
VM Name	A virtual machine name that contains the disk with the partition.
Disk Name	A disk within the virtual machine that contains the partition.
Partition ID	A unique partition ID on the disk.
File System Type	A file system on the partition.
Scan status	Status of the scanned file, e.g. full scan, partial scan, not scanned, etc.
Start date	The date on which the scan started.
Start Time	Initiation time of the scan.
End date	The date on which the scan ends.
End time	End time of the scan.
Scanned file	Number of files scanned on the partition.
Infected file count	Number of infected files on the partition.

Troubleshooting

Common errors

This section describes some common errors and their solutions. It includes the following topics:

Multiple malware scan jobs executing simultaneously might fail with error message “Maximum number of scanners <> reached” if the scan proxy runs out of resources.

Description

The simultaneous executions of Malware scanning may result in failure if the scan proxy goes out of resources.

Symptom

None

Solution

These errors are caused by limited resources on the client. You may try adding more resources or re-run the job.

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.