Dell EMC Avamar for Windows Servers

User Guide

19.2

Dell Inc.

June 2021
Rev. 02

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

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

© 2001 - 2021 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Figures **6**

Tables **7**

Preface **8**

Chapter 1: Introduction **11**
Architecture 11
Avamar components 11
How Avamar works in a Windows Server cluster 13
How Avamar works in a Windows Server 2019, 2016, or 2012 cluster with SOFS or SMB 13
Data Domain system support 14
Server virtualization 14
Backup 15
Available backup methods 15
File system backups 15
Developing a backup strategy 16
File system restore 18
File overwrites during restore 19
Parent folder restore scenarios 19
Year 2038 19
Disaster recovery 19
BMR of Windows to physical and virtual machines 19
Active Directory recovery 20
Disaster recovery in a cluster 20
Application restores after BMR 20
Considerations for critical disks and dynamic disks 21
Considerations for HP ProLiant Systems 21

Chapter 2: Installation **22**
Preparing to install the Avamar client software 22
System requirements 22
Windows Server cluster requirements 23
Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster requirements 23
Multi-homed cluster requirements 23
VSS requirements 23
Supported Windows features 25
Hardware requirements 26
Networking requirements 27
Additional software requirements 27
Unsupported configurations and features 27
Preparing a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster 28
Downloading the software 28
Verifying the environment 29
Installing the Avamar client software 29

Installation road maps....30
Installing the Avamar Client for Windows....31
Registering the client....33
Configuring the federated cluster client on Windows Server....33
Configuring the proxy cluster client on Windows Server 2019, 2016, or 2012 for SOFS or SMB clusters....34
Adding permissions for hidden file access in a cluster....35
Adding permissions for non-administrator user access in a cluster....36
Viewing the cluster client configuration....36
Upgrading the Avamar client software....37
Upgrading on a stand-alone server....37
Upgrading in a Windows Server cluster....37
Upgrading in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster....37
Uninstalling the Avamar client software....38
Uninstall road map....38
Uninstalling the federated cluster client in a Windows Server cluster....38
Uninstalling the Avamar Client for Windows....39

Chapter 3: Backup....40
Performing on-demand backups....40
Performing file system backups on a stand-alone server....40
Performing file system backups in a Windows Server cluster....41
Performing file system backups in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster..42
Backing up VHDs with the Windows File System plug-in....43
Performing BMR backups....43
Scheduling backups using the AUI Policy wizard....45
Creating a dataset....46
Creating a backup policy....46
Enabling a scheduled backup for a backup policy....47
Monitoring backups....47
Cancel backups....48
Enforcement of backups to Data Domain....48

Chapter 4: File System Restore....49
Restore requirements....49
Restoring in a cluster....49
Restoring VHD files....49
Restoring SIS volumes on Windows Server 2008....49
Restoring from backups of DFS shares....49
Restoring to the original location....50
Restoring to the original client....50
Restoring to the original location in a Windows Server cluster....51
Restoring to a different location....51
Restoring to a different location on a stand-alone server....51
Restoring to a different location in a Windows Server cluster....52
Restoring to a different location in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster....52
Monitor restores....53
Cancel restores....54

Chapter 5: Bare Metal Recovery **55**
BMR of Windows clients 55
BMR requirements 55
WinPE ISO image preparation 56
Restoring the computer to its original System State 59
Performing post-BMR tasks 62
Viewing Avamar Bare Metal Recovery Wizard log files 63
Active Directory recovery 63
Booting the client into Directory Services Restore Mode 64
Restoring Active Directory 65
Using the System State backup to restore Active Directory 66
BMR of Windows clusters 66
Restoring a cluster node 66
Restoring an entire cluster 67

Appendix A: Plug-in Options **68**
How to set plug-in options 68
Windows File System plug-in backup options 68
Windows File System plug-in restore options 71
Windows VSS plug-in backup options 72
Windows VSS plug-in restore options 74
Windows Cluster File Server plug-in backup options 74
Windows Cluster File Server plug-in restore options 75

Appendix B: Command Line Interface **76**
Overview of the Windows VSS plug-in CLI 76
Command reference 76
Synopsis 76
Operations 76
Options 76
Specifying command line options 79
CLI examples 79

Appendix C: Troubleshooting **80**
Log files 80
Avamar log files 80
Generating log files 81
Backup problems and solutions 82
Restore problems and solutions 83
Bare metal recovery problems and solutions 83

Glossary **85**

Figures

1 Avamar architecture on a stand-alone Windows server....11
2 Avamar architecture in a Windows Server cluster....13
3 Avamar architecture in a Windows Server for SOFS or SMB cluster....14
4 Folders....58
5 Avamar Bare Metal Recovery Wizard....59
6 Avamar Bare Metal Recovery Wizard....61
7 System Configuration window....64

Tables

1 Revision history 8
2 Typographical conventions 9
3 Avamar plug-ins for file system backups 15
4 Files skipped in Windows file system backups 16
5 Supported VSS providers for backups of file system data 23
6 Minimum hardware requirements 26
7 Unsupported configurations 27
8 Windows versions and virtual machine environments supported for P2V BMR 55
9 Windows File System plug-in backup options 68
10 Windows File System plug-in restore options 71
11 Windows VSS plug-in backup options 73
12 Windows VSS plug-in restore options 74
13 Windows Cluster File Server plug-in backup options 74
14 Windows Cluster File Server plug-in restore options 75
15 Common options for the avvss command 77
16 Account options for the avvss command 77
17 Logging options for the avvss command 77
18 Backup options for the avvss command 78
19 Avamar log files 80

Preface

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Therefore, some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact a technical support professional when a product does not function correctly or does not function as described in this document.

NOTE: This document was accurate at publication time. To find the latest version of this document, go to Online Support (https://www.dell.com/support).

Purpose

This guide describes how to install the Avamar client for Microsoft Windows, and how to back up and restore data on a Windows server in both stand-alone and cluster environments.

Audience

The information in this document is primarily intended for system administrators who are responsible for installing software and maintaining servers and clients on a network.

Persons using this document should have administrator permissions in the environment, and current practical experience with administrator functionality on Microsoft Windows servers.

Revision history

The following table presents the revision history of this document.

Table 1. Revision history

Revision	Date	Description
02	June, 2021	Updated 'Restoring the computer to its original System State' section.
01	November 15, 2019	First release of this document for Avamar 19.2.

Related documentation

The following publications provide additional information:

- *Avamar Administration Guide*
- *Avamar Backup Clients User Guide*
- *Avamar Operational Best Practices Guide*
- *Avamar Product Security Guide*
- *Avamar Release Notes*

The Avamar Client for Windows described in this guide is required for Avamar operations and operating system protection on Windows servers. Avamar offers plug-ins to provide protection for the application data, databases, and settings. The following guides provide information on installing and using the application-specific plug-ins:

- *Avamar for Exchange VSS User Guide*
- *Avamar for Hyper-V VSS User Guide*
- *Avamar for IBM DB2 User Guide*
- *Avamar for Lotus Domino User Guide*
- *Avamar for Oracle User Guide*

- *Avamar for SAP with Oracle User Guide*
- *Avamar for SharePoint VSS User Guide*
- *Avamar for SQL Server User Guide*
- *Avamar for Sybase ASE User Guide*

NOTE: Some applications are available on multiple platforms and require the client for the specific operating system. The *Avamar Backup Clients User Guide* provides information about installing and using other operating system clients, such as AIX, HP-UX, Linux, MacOS X, and Solaris.

Typographical conventions

Table 2. Typographical conventions

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications that are referenced in text
`Monospace`	Used for: ● System code ● System output, such as an error message or script ● Pathnames, filenames, prompts, and syntax ● Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means "or"
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information that is omitted from the example

Where to get help

The Avamar support page provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and troubleshooting information. This information may resolve a product issue before contacting Customer Support.

To access the Avamar support page:

1. Go to https://www.dell.com/support.
2. Type a product name in the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box.
3. Select the product from the list that appears. When you select a product, the **Product Support** page loads automatically.
4. (Optional) Add the product to the **My Products** list by clicking **Add to My Saved Products** in the upper right corner of the **Product Support** page.

Documentation

The Avamar product documentation provides a comprehensive set of feature overview, operational task, and technical reference information. To supplement the information in product administration and user guides, review the following documents:

- Release notes provide an overview of new features and known limitations for a release.
- Technical notes provide technical details about specific product features, including step-by-step tasks, where necessary.
- White papers provide an in-depth technical perspective of a product or products as applied to critical business issues or requirements.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to https://www.dell.com/support.
2. Under the **Support** tab, click **Knowledge Base**.
3. Type either the solution number or keywords in the search box. Optionally, you can limit the search to specific products by typing a product name in the search box and then selecting the product from the list that appears.

Online communities

Go to Community Network at https://www.dell.com/community for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all products.

Live chat

To engage Customer Support by using live interactive chat, click **Join Live Chat** on the **Service Center** panel of the Avamar support page.

Service requests

For in-depth help from Customer Support, submit a service request by clicking **Create Service Requests** on the **Service Center** panel of the Avamar support page.

NOTE: To open a service request, you must have a valid support agreement. Contact a sales representative for details about obtaining a valid support agreement or with questions about an account.

To review an open service request, click the **Service Center** link on the **Service Center** panel, and then click **View and manage service requests**.

Enhancing support

It is recommended to enable ConnectEMC and Email Home on all Avamar systems:

- ConnectEMC automatically generates service requests for high priority events.
- Email Home sends configuration, capacity, and general system information to Customer Support.

Comments and suggestions

Comments and suggestions help to continue to improve the accuracy, organization, and overall quality of the user publications. Send comments and suggestions about this document to DPAD.Doc.Feedback@emc.com.

Include the following information:

- Product name and version
- Document name and revision (for example, 01)
- Page numbers
- Other details to help address documentation issues

1

Introduction

Topics:

- Architecture
- Backup
- File system restore
- Disaster recovery

Architecture

Avamar components integrate into the architecture of Microsoft Windows server environments to provide backup and restore on stand-alone computers and clusters.

Avamar components

The following figure illustrates a basic system architecture when you use Avamar to back up a stand-alone Windows server.

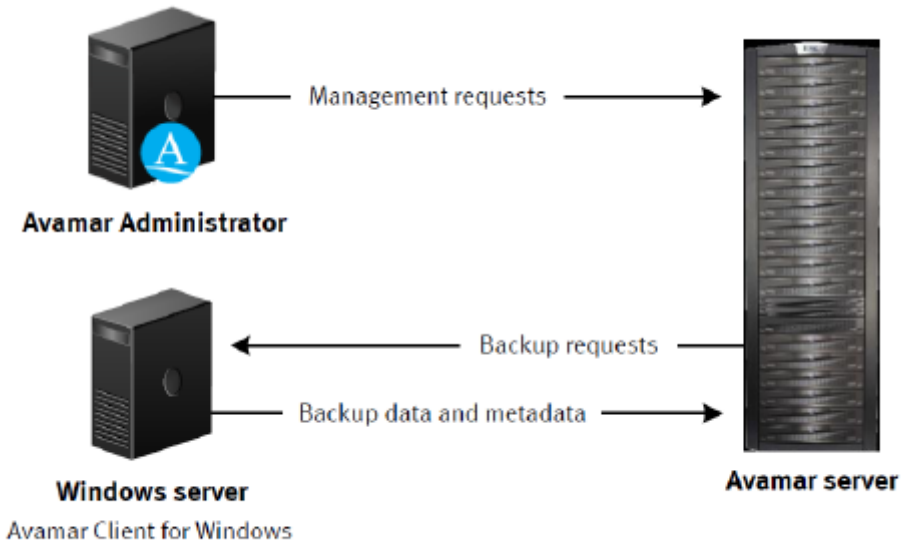

Figure 1. Avamar architecture on a stand-alone Windows server

Avamar components in the environment include the Avamar server, the Avamar Client for Windows, and Avamar Administrator. Additional components are required in cluster environments.

Avamar server

The Avamar server is the server component of the Avamar client/server system. The Avamar server is a fault-tolerant, high-availability system that provides the following services:

- Efficient storage of backups from all protected clients
- Global deduplication across all client computers
- Essential processes and services required for data restores, client access, and remote system administration

Avamar Client for Windows

When you install the Avamar Client for Windows, the installation includes the Avamar agent, the Windows File System plug-in, and the Windows VSS plug-in. In a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster, the installation also includes the Windows Cluster File Server plug-in.

Avamar agent

The Avamar agent is a Windows service that runs on the client computer and communicates with the Avamar server and any plug-ins installed on the client.

Windows File System plug-in

The Windows File System plug-in enables you to back up and restore file system data on a stand-alone Windows computer or on shared storage in a Windows Server cluster.

Windows VSS plug-in

The Windows VSS plug-in enables you to back up the system state and critical disks for bare metal recovery (BMR) of a Windows computer.

The Windows VSS plug-in uses the Microsoft Volume Shadow Copy Service (VSS) technology to create a point-in-time snapshot of a volume, including all open files. Avamar then backs up data from the snapshot instead of directly from the file system. VSS also enables you to back up a single, point-in-time capture of the system state of a Windows computer.

The time required to create a snapshot depends on several factors, including the writer activity during the backup. Once the backup is complete, VSS deletes the snapshot.

Windows Cluster File Server plug-in

The Windows Cluster File Server plug-in enables you to back up and restore file system data on shared storage in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster.

You must manually select the option to install the Windows Cluster File Server plug-in when you install the Avamar Client for Windows on a Windows Server 2019, 2016, or 2012 computer in a cluster.

Install the Windows Cluster File Server plug-in on only the proxy node in the cluster.

Avamar Administrator

Avamar Administrator is a graphical management console software application for remote administration of an Avamar server from a supported Windows or Linux client computer. You can configure, perform, monitor, and manage backups and restores by using Avamar Administrator. The *Avamar Administration Guide* provides complete instructions for installing and using Avamar Administrator.

Application plug-ins

You can install an Avamar application plug-in on a Windows server to protect a specific application, such as Microsoft Exchange, SharePoint, or SQL Server. The application plug-in backs up and restores the specific configuration settings and data types used by that application.

A complete list of supported Windows application plug-ins is available in the *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

Details on how to install each application plug-in and perform backups and restores of application data are available in the user guide for each plug-in.

How Avamar works in a Windows Server cluster

Avamar uses a federated architecture to back up and restore file system data on shared storage in Windows failover cluster or server cluster environments. This is supported on all supported Windows Server platforms.

Avamar supports both active/passive and active/active cluster configurations with two or more nodes.

The following figure illustrates a Windows Server cluster environment with Avamar.

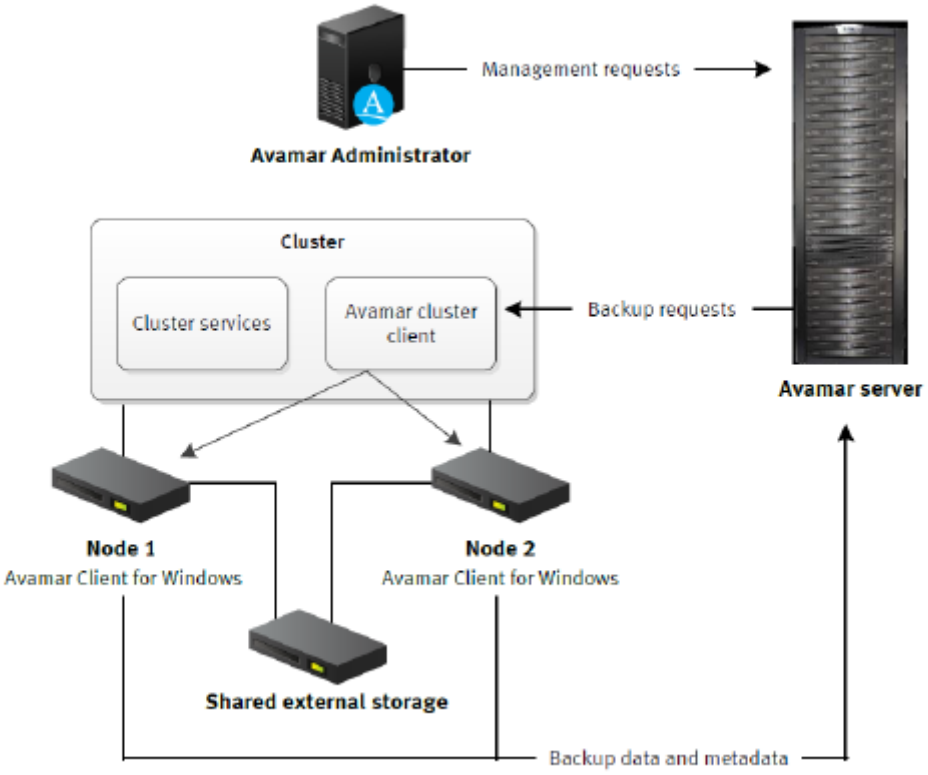

Figure 2. Avamar architecture in a Windows Server cluster

You install the Avamar Client for Windows on each node in the cluster. Then you run the Avamar Cluster Configuration Tool to configure the Avamar federated cluster client. The Avamar federated cluster client serves as a client for the virtual server that provides access to the file system data on the shared failover cluster disk.

When you perform a backup, you select the Avamar federated cluster client as the client to back up. The federated cluster client ensures that Avamar can access the data regardless of which node is managing the data.

You use the Avamar Plug-in for the Windows File System to perform the backup. The Windows File System plug-in is installed when you install the Avamar Client for Windows.

How Avamar works in a Windows Server 2019, 2016, or 2012 cluster with SOFS or SMB

Avamar uses a proxy architecture to back up and restore file system data on shared storage in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster. The shared storage can be a Scale-Out File Server (SOFS) or a clustered file server for general use, or Server Message Block (SMB) 3.0 file shares on a file server.

NOTE: This topic describes a specialized implementation of a Windows Server cluster. How Avamar works in a Windows Server cluster on page 13 describes the support of a standard Windows Server cluster.

The following figure illustrates a Windows Server for SOFS or SMB cluster environment with Avamar.

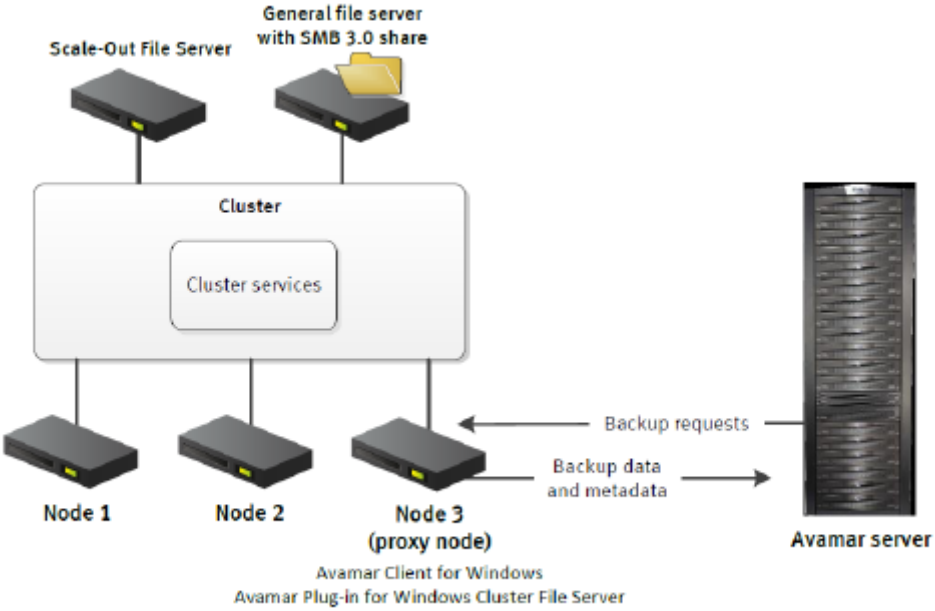

Figure 3. Avamar architecture in a Windows Server for SOFS or SMB cluster

You install the Avamar Client for Windows and the Windows Cluster File Server plug-in on a single node in the cluster. Then you run the Avamar Cluster Configuration Tool to configure the Avamar proxy cluster client on the node.

When you back up or restore file system data on shared storage, you select the Avamar proxy cluster client as the client to back up or restore from. You use the Windows Cluster File Server plug-in to perform the backup or restore.

The Avamar server communicates with the proxy cluster client on the proxy node to back up and restore file system data on shared storage in the cluster, regardless of which node is managing the data.

When you back up data with the Windows Cluster File Server plug-in, you can restore the data either with the Windows Cluster File Server plug-in or the Windows File System plug-in.

Data Domain system support

You can store backups on either the Avamar server or a Data Domain® system. Backup metadata is stored on the Avamar server.

Before you can store backups on a Data Domain system, add the Data Domain system to the Avamar configuration by using Avamar Administrator. Then select the Data Domain system in the plug-in options when you perform an on-demand backup or when you create a dataset for a scheduled backup. You can also use the command line interface (CLI) to perform backups to a Data Domain system.

The steps to restore backups are the same whether you restore from the Avamar server or a Data Domain system. The restore process determines the location of the backup and restores the backup.

Avamar also supports Data Domain Cloud Tier. DD Cloud Tier moves data from Data Domain to the cloud. From the Avamar Administrator, you can configure cloud tiering to move Avamar backups from Data Domain to the cloud, and perform seamless recovery of these backups.

The *Avamar and Data Domain System Integration Guide* provides more information about Data Domain systems in an Avamar environment, including detailed steps to add a Data Domain system to the Avamar configuration.

Server virtualization

You can install Microsoft Windows in a server virtualization environment, such as a VMware or Microsoft Hyper-V environment. There are multiple ways that you can install and use Avamar to back up and restore data in a server virtualization environment.

The following guides provide details on additional system requirements, as well as installation and configuration procedures:

- *Avamar for Hyper-V VSS User Guide*
- *Avamar for VMware User Guide*

Backup

A comprehensive backup strategy includes regular backups of all data in the environment. Avamar provides multiple ways to back up different types of data on a Windows server at different granularity levels, either on-demand or on a scheduled basis. The following topics provide details on how Avamar backs up data on a Windows server.

NOTE: The Avamar AUI is only supported in stand-alone environments.

The following plug-ins provide the ability to include and exclude data from the backup dataset. You can include and exclude data when creating or editing a policy, or when creating or editing a dataset in the **Settings** pane. The *Avamar Administration Guide* provides more information.

- Windows File System
- Windows VSS
- Windows Application Intelligence

Available backup methods

You can perform both on-demand backups and scheduled backups of file system data or the system state and critical disks.

There are three ways to perform Avamar backups:

- Use Avamar Administrator to perform on-demand backups and scheduled backups of file system data or System State and critical disks. Backup on page 40 provides detailed steps to perform backups with Avamar Administrator.
- Use the Avamar client interface on a Windows client computer to perform on-demand backups of file system data. The *Avamar Backup Clients User Guide* provides details on how to use the Avamar client interface to perform on-demand backups.
- Use the `avvss` command line interface on the Windows client computer to perform an on-demand system state backup. Command Line Interface on page 76 provides details on performing backups with the `avvss` command.

File system backups

You can either back up all file system data on a Windows client computer at one time or you can select individual volumes, folders, and files for backup.

The Avamar plug-in that you use for file system backups depends on the operating system and environment as described in the following table.

Table 3. Avamar plug-ins for file system backups

Environment	Plug-in for file system backups
Stand-alone computer	Windows File System plug-in
Shared storage in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster	Windows Cluster File Server plug-in
Shared storage in a Windows Server cluster	Windows File System plug-in
Local volumes on a cluster node	Windows File System plug-in

Supported file systems

The Avamar Client for Windows can back up and restore data on the following file systems:

- FAT16
- FAT32
- NTFS
- ReFS

- exFAT

International characters

Avamar generally supports the use of specific international characters in folder names and file names. However, proper display of international language characters depends on the client computer locale and the compatibility of installed system fonts with the original language. Support for international characters on page 22 provides additional details.

Skipped files

The Windows File System plug-in uses Microsoft Volume Shadow Copy Service to perform backups. The backups include open files because Avamar backs up the data from the Shadow Copy volume instead of the original volume. However, according to Microsoft best practices, Avamar skips the files in the following table by default.

Table 4. Files skipped in Windows file system backups

Operating system	Files skipped by default	Comments
All Windows	Files listed in the `FilesNotToBackup` registry for the system and current user	The skipped files include operating system files that are necessary to restore the system.
All Windows	Temporary Internet Files	You can enable backup of these files through special flags.
All Windows	Outlook 2003 temporary cache files	You can enable backup of these files through special flags.
Windows 7 or later	All `Syscache.hve*` files under System Volume information	These additional files do not appear in the `FilesNotToBackup` registry, but Microsoft indicates that backups should skip them.
Windows 7 or later	All `.vhd` and `.vhdx` files for a mounted Virtual Hard Disk (VHD)	Back up the VHD file system, not the `.vhd` file.
Windows Server 2019, 2016, or 2012	All `.vhd` and `.vhdx` files on file shares on clustered file servers	Explicitly select the VHD file for backup, and use the Windows Cluster File Server plug-in. If you select only the parent folder or the file server for the VHD file, then the backup skips the VHD file.

Developing a backup strategy

A comprehensive backup strategy includes ongoing backups of all data in the environment. The Avamar Client for Windows provides multiple ways to back up different types of data at different granularity levels either on-demand or on a scheduled basis.

When to perform backups

You can perform both on-demand and scheduled backups of file system data or the System State and critical disks.

A best practice is to perform an on-demand backup before a system upgrade, installation, or any major change to the server. You may also want to perform an on-demand backup immediately after you install and register the Avamar Client for Windows.

Perform scheduled backups to ensure that there are backups of data on an ongoing basis. You can perform scheduled backups on a daily, weekly, or monthly basis. The *Avamar Operational Best Practices Guide*, available in Online Support at https://support.EMC.com, provides guidance on scheduling backups with other system activities.

File system backups

The Avamar plug-in that you use to back up file system data depends on the operating system and environment.

File system backups on a stand-alone server

Use the Windows File System plug-in to back up file system data on a stand-alone server. You can back up all file system data on a stand-alone Windows client computer at one time, or you can select individual volumes, folders, and files for backup.

File system backups in a Windows Server cluster

Use the Windows File System plug-in to back up file system data on shared storage in a Windows Server cluster. You can back up all file system data at one time, or you can back up individual cluster disks, folders, and files.

To back up data on a local volume of a cluster node, select the physical node as the client to back up, and use the Windows File System plug-in.

Back up shared cluster data separately from file system data on local volumes. You may not be able to restore data from a backup that includes file system data from both shared storage and local volumes. A best practice is to exclude shared cluster data when you back up local file system data, and to exclude local file system data when you back up shared cluster data. Specify the exclusion on the Exclusions tab when you create a dataset for scheduled backups.

Do not include the cluster quorum drive in file system backups. According to Microsoft guidelines, this cluster resource must always remain under exclusive control of the cluster. A best practice is to exclude the quorum drive from backups. To exclude the quorum drive, specify the drive on the Exclusions tab when you create a dataset for scheduled backups of the cluster.

File system backups in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster

Use the Windows Cluster File Server plug-in to back up file system data on shared storage in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster. You can back up all file system data at one time, or you can back up individual clustered file servers, folders, and files.

You can back up both Scale-Out File Servers and clustered file servers for general use in a single on-demand or scheduled backup. However, the backup process creates two different shadow copy sets in the same backup, one for Scale-Out File Servers and one for the general file servers.

To back up data on a local volume of a cluster node, select the physical node as the client to back up, and use the Windows File System plug-in.

File system backups of deduplicated and SIS volumes

Use the Windows File System plug-in to back up Windows deduplicated volumes on Windows Server 2019, 2016, or 2012. You can select to back up optimized files in either an optimized or unoptimized state. This step is done by using the Perform a Windows Optimized Backup of a Windows Deduplicated volume checkbox in the Backup Command Line Options. If you back up files in an optimized state, then you can restore the files in either an optimized or unoptimized state. You must select the entire Windows deduplicated volume for backup. However, you can restore individual folders and files from the volume backup. You can only restore files from a Windows deduplicated volume to the original location or to another Windows Server 2019, 2016, or 2012 computer with Windows deduplicated volumes.

Use the Windows File System plug-in to back up SIS volumes on Windows Storage Server 2008 and Windows Storage Server 2008 R2. Similar to Windows deduplicated volumes, you must select the entire SIS volume for backup. However, you can restore individual folders and files from the volume backup.

VHD file backups

You can use the Avamar Client for Windows to back up and restore Virtual Hard Disk (VHD) files on a Windows server. You also can exclude attached VHDs when you back up a volume on a Windows server.

The Avamar Client for Windows does not support the backup of a VHD configured for native boot.

NOTE: A VHD does not automatically attach when you restart, and is not available after restart until you reattach the VHD. When you reattach the VHD, the previous drive letter mappings reset automatically, unless other drives are using the drive

letters. Because Windows does not automatically reattach VHDs, you must manually check the VHDs on the system, and use consistent drive letter mappings in all subsequent attach and detach operations for backup data consistency.

Bare metal recovery backups

A backup for bare metal recovery (BMR) includes the system state and critical disks. BMR enables you to restore a server without having to rebuild the operating system, and to perform the restore offline. Use the Windows VSS plug-in to back up the system state and critical disks for BMR. For information about BMR support for various versions of Windows, see the *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

NOTE: BMR of Windows Vista computers is not supported. You can back up and restore only file system data for Windows Vista computers.

To prepare for a full disaster recovery of a computer, perform regular backups of all file system data, noncritical disks, and application data.

Maintain a database or spreadsheet of computer names, FQDNs, and IP addresses for each Windows client computer that Avamar backs up. The client information is an important reference in any environment.

If any volume of a dynamic disk pack is critical, then all volumes in the dynamic disk pack become critical. To avoid unnecessarily large System State backups, exclude noncritical dynamic disks by using the `--exclude-non-critical-dynamic-disks=true` option during the backup.

The Windows VSS plug-in does not back up critical disks on shared storage in a cluster. If a shared volume is a critical disk, then use the Windows File System plug-in for the backup.

When a Windows Server role uses SQL Server instances instead of the Windows Internal Database (WID), use the Avamar Plug-in for SQL Server to back up the SQL Server instances for disaster recovery. The *Avamar for SQL Server User Guide* explains how to back up the SQL Server instances.

Active Directory data backups

To back up Active Directory data in preparation for disaster recovery, perform regular System State backups of the domain controllers.

On Windows Server 2008 or newer computer, use the Windows VSS plug-in to perform the backup. When you perform the backup, clear the **Create Disaster Recovery Backup** checkbox on the **Options** tab. When you clear the checkbox, you can only use the backup for online restore, not BMR.

The data that is backed up will differ based on the selection of the **Create Disaster Recovery Backup** checkbox. If this option is selected, the backup will be created for BMR; if the option is not selected, the backup will be created for online restore. Because the backups are for different restore purposes, the two backups may vary.

These backups enable you to perform either authoritative or nonauthoritative restores.

Application data backups

To back up application data, such as Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server, or Microsoft Hyper-V, use an application-specific plug-in.

For example, back up Microsoft Exchange with the Avamar Plug-in for Exchange VSS. The user guide for each plug-in provides details on backup or restore of application data.

File system restore

You can restore file system data from an Avamar backup to the original location or to a different location. If there are multiple items in the backup, you also can restore the items to different locations in the same restore operation.

In most cases, the Avamar plug-in that you use to restore file system data is the same plug-in that you used to perform the backup. However, when you back up data with the Windows Cluster File Server plug-in, you can restore the data with either the Windows Cluster File Server plug-in or the Windows File System plug-in.

NOTE: The Avamar AUI is only supported in stand-alone environments.

File overwrites during restore

If a file with the same name already exists in the restore path, then you can specify whether the restore overwrites the file, even when the file is open. Use the **Overwrite Existing Files and Restoration of open files** options on the **Restore Command Line Options** dialog box to control this behavior.

Parent folder restore scenarios

When you restore a single folder to a different location, Avamar restores only the contents of the folder. Avamar does not restore the original parent folder. However, if you restore two or more folders to a different location, then Avamar restores the original parent folders along with the contents of those folders.

Year 2038

The Avamar subsystem supports backup retention until February 2106. However, for older releases, the Avamar subsystem does not start after January 2038 due to the signed 32-bit integer time format of UNIX and Linux operating systems, and therefore cannot restore backup data after this date.

Newer Avamar releases offer support for longer retention periods:

- For Avamar 19.1 and later, the Avamar server subsystem uses an unsigned 32-bit integer and continues to start until 2106.
- For Avamar 19.1 and earlier, the Avamar client and plug-ins subsystem uses a signed 32-bit integer and retains data until 2038.
- For Avamar 19.2 and later, the Avamar client and plug-ins subsystem uses an unsigned 32-bit integer and retains data until 2106.
- Backup retention after 2038 is successful when all Avamar subsystems use unsigned 32-bit integers.

Therefore, with both Avamar 19.2 and later, and an Avamar 19.2 or later client, backup retention succeeds after 2038.

Avamar 19.2 and later clients also support restoring backups where the retention time is after 2038, and where the local (server and client) time is after 2038. Earlier client releases do not support this.

For backups of Windows or Linux clients, do not assign a retention period for a date after February 7, 2106.

Disaster recovery

The process for disaster recovery of a Windows computer from Avamar backups depends on the operating system.

BMR of Windows to physical and virtual machines

Avamar supports BMR of various versions of Windows to physical and virtual machines: For supported versions, see the *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

- Physical machine to physical machine
- Virtual machine to virtual machine
- Physical machine to virtual machine (P2V): Windows Server only

When a disaster occurs, ensure that the hardware on the target computer is operational, and that the target computer is similar in make, model, and hardware configuration as the source computer to be recovered. You should also review the additional requirements in BMR requirements on page 55.

After you prepare the target computer, download the customized WinPE ISO image for BMR from the Avamar server to a functional Windows computer. The image that you download depends on the operating system and hardware.

The customized WinPE ISO image enables you to recover to the target computer without installing an operating system. Because the local disks are not in use by the booted operating system, you can replace files without conflict.

WinPE enables you to boot with a minimal subset of Windows features. This functionality includes access to network resources, disks, and other features through a command prompt.

You can burn the WinPE ISO image to a CD, DVD, or USB flash drive, and then boot the target computer locally from the media. You also can copy the WinPE ISO image to a Windows Deployment Services (WDS) server, which enables you to perform a network boot of the target computer.

WinPE ISO image preparation on page 56 provides details on downloading and preparing the image.

When you boot with the customized WinPE ISO image, the boot process automatically starts the Avamar Bare Metal Recovery Wizard. The Avamar Bare Metal Recovery Wizard provides a VSS recovery solution that uses the Automated System Recovery (ASR) writer and the customized WinPE ISO image to restore critical volumes and other components of the bootable System State. Restoring the computer to its original System State on page 59 provides details on using the wizard to perform the restore.

Additional steps to recover the computer may be necessary, depending on the environment. Perform the steps in Performing post-BMR tasks on page 62 to complete the restore.

Active Directory recovery

About this task

You can perform system recovery of Active Directory of Windows Server.

Steps

1. Configure the client to boot into Directory Services Restore Mode (DSRM).
2. Boot the computer in DSRM.
3. Restore Active Directory from the System State backup on the Avamar server from the non-disaster recovery System State backup.
4. (Optional) Perform an authoritative restore of Active Directory.

Authoritative and nonauthoritative restores

You can perform either a nonauthoritative or an authoritative restore of Active Directory:

- Use a nonauthoritative restore when Active Directory replication partners can return a domain controller to a known state. You restore the domain controller from a backup. When you restart the domain controller after the restore, other domain controllers replicate changes made after the backup.
- Use an authoritative restore to return a domain controller to a known state as the master copy. The data from the restored domain controller replicates to other domain controllers.

  An authoritative restore also enables you to mark specific organizational units (OUs) so that Active Directory objects replicate to other domain controllers. In addition, replication partners do not overwrite the replicated objects.

The following Microsoft TechNet articles provide details on an authoritative restore:

- “Performing Authoritative Restore of Active Directory Objects” provides general details on an authoritative restore.
- “Mark an Object or Objects as Authoritative” provides details on the command syntax for marking items for an authoritative restore.

NOTE: Microsoft recommends using a nonauthoritative restore or reinstallation to restore a domain controller. The Microsoft TechNet article “Performing Nonauthoritative Restore of Active Directory Domain Services” provides information about reinstating a domain controller with a nonauthoritative restore.

Disaster recovery in a cluster

You can restore an individual cluster node or an entire cluster from a system state backup. BMR of Windows clusters on page 66 provides details.

Application restores after BMR

If you use the Windows VSS plug-in to perform the system state backups, then the backups include binaries for applications that use a Windows service, such as Microsoft Exchange. However, the backups typically exclude application configuration, databases, and files.

When you restore the system state during BMR, these applications are restored to a functional state. If the application binaries are not in the backup, then you must reinstall the application.

If you install an application on a noncritical volume and the volume is destroyed, then you must either restore the noncritical volume from a Windows File System plug-in backup or reinstall the application.

To restore application data, use the application plug-in.

Considerations for critical disks and dynamic disks

A critical disk or volume can contain operating system files and application services.

If a disk contains a mount point for a critical disk, then the disk with the mount point is also a critical disk. For example, if `F:\` is a critical disk and is mounted on `P:\MountPoint_For_F`, then `P:\` becomes a critical disk. Mount critical disks to `C:\`, or another disk that is critical.

If any volume of a dynamic disk pack is critical, then all volumes in the dynamic disk pack become critical. You can exclude noncritical dynamic disks from the system state backups to avoid unnecessarily large the system state backups.

On Windows Server 2019, 2016, 2012, and Windows 8, an application or service may cause a noncritical disk to become critical if you install the application or service on the disk. You can exclude noncritical disks from the backup if the disks become critical from these applications or services.

The BMR process restores all critical disks except for critical disks on shared storage in a cluster. Each critical disk is formatted during BMR, which destroys any existing data. Store application data, such as Exchange or SQL databases, on noncritical disks whenever possible.

Generally, when you restore to the original system, the BMR process does not format noncritical disks. However, when you restore to a different system, BMR sometimes fails if the recovery process cannot format the noncritical disks.

Considerations for HP ProLiant Systems

You cannot use an Avamar BMR backup of an HP ProLiant system for recovery when the system is configured with the HP Intelligent Provisioning Tool (IPT). Configure the tool to use an entire disk for a critical volume, such as the system partition (drive).

Do not use the entire disk for critical volumes when using IPT version 1.4 or 1.5 to configure an HP blade system.

This issue applies to BMR backups and recovery for various versions of Windows. For detailed information about BMR on Windows, see the *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

HP Support advisory ID c03927759, which is available on the HP Support website, addresses IPT, using a full disk for the system partition, and Windows Bare Metal Restore with Windows Server Backup. The advisory also applies to Avamar BMR of critical volumes. Follow the resolution steps that are described in the HP advisory, which are simple and do not require reconfiguration of existing systems except to shrink logical volumes. After you complete the steps, you can use Avamar and the Windows VSS plug-in to perform System State backups.

2

Installation

Topics:

- Preparing to install the Avamar client software
- Installing the Avamar client software
- Upgrading the Avamar client software
- Uninstalling the Avamar client software

Preparing to install the Avamar client software

Review the system requirements for the Avamar client software, and ensure that the environment meets the requirements before you install Avamar client software. The Avamar Config Checker for Microsoft Windows provides an additional automated verification of the environment. You also must download the Avamar Client for Windows installation package from the Avamar server.

System requirements

The environment must meet client compatibility requirements before you install Avamar client software.

Client compatibility requirements are available in the *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection. The requirements in the matrix include supported operating systems and application versions. The Avamar Client for Windows supports most editions of Microsoft Windows.

The Avamar Client for Windows supports backup and restore of only file system data for Windows Vista computers. BMR of Windows Vista computers is not supported.

The Avamar file system client and the plug-ins that you install on the host must have the same version number.

The environment must also meet other requirements, such as file system requirements, cluster requirements, hardware requirements, VSS requirements, networking requirements, Microsoft .NET Framework 4 requirements, and anti-virus requirements.

Supported file systems

The Avamar Client for Windows can back up and restore data on the following file systems:

- FAT16
- FAT32
- NTFS
- ReFS
- exFAT

Support for international characters

Avamar generally supports the use of specific international characters in folder names and file names. However, correct display of international language characters depends on the client computer locale and compatibility of installed system fonts with the original language. If you browse backups with international characters and a compatible font is not installed on the system, then any characters that the system cannot resolve appear as rectangles. The appearance of the rectangle characters does not affect the ability to restore the folders or files. The *Avamar Release Notes* provide additional information about international language support.

Windows Server cluster requirements

The Avamar Client for Windows supports failover cluster or server cluster environments on Windows Server and Windows Storage Server. Avamar can back up and restore shared data on failover cluster disks.

Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster requirements

In Windows Server 2019, 2016, or 2012 for SOFS or SMB clusters, Avamar can back up and restore file system data on both a Scale-Out File Server (SOFS) and a clustered file server for general use.

If a cluster includes file system data on both a SOFS and a clustered file server for general use, then you can include both types of file servers in a single on-demand or scheduled backup. However, the backup process creates two different shadow copy sets in the same backup, one for the SOFS data and one for the general file server data.

NOTE: Backup fails when there are encrypted files and folders on shares on a clustered file server for general use and the proxy node is not the owner node for the file server. Non-encrypted files and folders on the file server are backed up successfully. You can restore the non-encrypted files and folders from the failed backup.

Multi-homed cluster requirements

Plug-ins connect to Avamar services by using the IP address to which the plug-in is bound. If a service is not configured to listen on that IP address, then the plug-in cannot connect.

For example, if the Avamar backup agent on a multi-homed cluster is bound to one IP address, and Exchange or SQL Server is bound to a different IP address, then key Avamar features like browsing, backup, and restore do not work.

Therefore, to correctly configure multi-homed cluster environments for use with Avamar, edit the primary network name to depend on both IP addresses.

VSS requirements

The VSS provider and writer that creates the snapshot for a backup depends on the Avamar plug-in and environment.

Supported VSS providers

The following table lists the VSS providers that Avamar plug-ins use to perform backups of file system data.

Table 5. Supported VSS providers for backups of file system data

Environment	Avamar plug-in	VSS provider
Stand-alone Windows computer, all supported operating system versions	Windows File System	Microsoft Software Shadow Copy Provider
Windows Server 2019, 2016, or 2012 cluster with Scale-Out File Server	Windows Cluster File Server	Microsoft CSV Shadow Copy Provider
Windows Server 2019, 2016, or 2012 with clustered file servers for general use	Windows Cluster File Server	• Microsoft Software Shadow Copy Provider for file servers that the proxy node owns • Microsoft File Share Shadow Copy Provider for file servers that other nodes own
Windows Server	Windows File System	Microsoft Software Shadow Copy Provider

The Avamar Plug-in for Windows VSS uses the Microsoft Software Shadow Copy Provider to perform snapshots for BMR backups in all supported environments.

Hardware providers are not supported.

If you manually install the iSCSI Target VDS or VSS hardware provider, then perform the credential configuration steps in the "iSCSI Target Storage (VDS/VSS) Provider" blog post on the Microsoft TechNet website.

Supported VSS writers

The Avamar Plug-in for Windows VSS uses the following Windows System Component VSS writers for BMR backups:

- Active Directory Domain Services (NTDS) Writer
- Active Directory Federation Services (AD FS) Writer
- Active Directory Rights Management Services (AD RMS) Writer
- Automated System Recovery (ASR) Writer
- Background Intelligent Transfer Service (BITS) Writer
- Certificate Authority Writer
- Cluster Database Writer
- COM+ Class Registration Database Writer
- Distributed File System Replication (DFSR) Writer
- Dynamic Host Configuration Protocol (DHCP) Writer
- File Replication Server (FRS) Writer
- File Server Resource Manager (FSRM) Writer
- IIS Configuration Writer
- IIS Metabase Writer
- MSSearch Service Writer
- Network Policy and Access Service (NPS) Writer
- Performance Counter Writer
- Registry Writer
- Remote Desktop Services (Terminal Services) Gateway VSS Writer
- Remote Desktop Services (Terminal Services) Licensing VSS Writer
- Removable Storage Manager (RSM) Writer
- System Writer
- Task Scheduler Writer
- VSS Metadata Store Writer
- WID Writer
- Windows Deployment Services (WDS) Writer
- WINS (Windows Internet Name Service) Writer

Backups of file system data do not require a VSS writer.

How Avamar works with supported VSS writers

VSS writers provide metadata about what data to back up, and specific methods for correctly handling components and applications during backup and restore. VSS writers also identify the type of application or service in the backup, such as System Boot or System Services.

Writers are only available for active services or applications. If a service or application is present but is not active, then information from its writer is not available. Consequently, a writer can appear or disappear from backup to backup.

During a backup, Avamar checks the following conditions:

- Whether the writer for the application is present and active.
- Whether the writer appears in the list of supported writers.
- Whether a user has disabled the writer.

If the writer is present, active, supported, and enabled, then Avamar backs up the data by using VSS technology. Otherwise, the backup does not include the data that the writer serves.

VSS snapshot volume requirements

The Microsoft VSS framework supports as many as 64 volumes in a VSS snapshot. When you create a dataset or perform an on-demand backup, do not include more than 64 volumes. If you include more than 64 volumes in a snapshot, then the backup fails and the Avamar event log lists the following error:

`VSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHED.`

The VSS framework also limits the number of shadow copies to 64 per volume. If the number of shadow copies in a volume exceeds 64, then the backup fails and the Avamar event log lists the following error:

`VSS_E_MAXIMUM_NUMBER_OF_SNAPSHOTS_REACHED.`

Installing Windows updates for VSS issues

About this task

Backup files from VSS snapshots sometimes contain corrupted files when the size of the volume in the backup is a multiple of 8 GB on one of the following operating systems:

- Windows Server 2008
- Windows Server 2008 R2
- Windows 7
- Windows Vista

Steps

1. Install the Microsoft hotfix at http://support.microsoft.com/kb/2748349.
2. Rename the file cache from `C:\Program Files\avs\var\f_cache.dat` to `C:\Program Files\avs\var\backup_f_cache.dat`.
3. Run the next scheduled backup so that you have a good VSS snapshot.
   The backup may take longer to complete because you removed the file cache and the backup must process all files on the system.

Supported Windows features

Some Windows features supported by Avamar have additional requirements or conditions.

Deduplication and Single Instance Storage support

The Avamar Plug-in for the Windows File System supports backup and restore of both optimized and unoptimized files on Windows deduplicated volumes on Microsoft Windows Server 2019, 2016, or 2012. You can select whether to back up optimized files in either an optimized or unoptimized state. If you back up files in an optimized state, then you can restore the files in either an optimized or unoptimized state. You must select the entire Windows deduplicated volume for backup. However, you can restore individual folders and files from the volume backup. You can only restore files from a Windows deduplicated volume to the original location or to another Windows Server 2019, 2016, or 2012 computer with Windows deduplicated volumes.

Do not perform a System State backup of Windows deduplicated volumes if the volumes are critical volumes. Microsoft does not recommend making a deduplicated volume a critical volume, and Avamar excludes deduplicated volumes from VSS backups.

The Avamar Plug-in for the Windows File System also supports Single Instance Storage (SIS) volumes on Windows Storage Server 2008 and Windows Storage Server 2008 R2. Similar to Windows deduplicated volumes, you must select the entire SIS volume for backup. However, you can restore individual folders and files from the volume backup.

Windows Server Core installation

If you deploy Windows Server by using the Core Installation feature, you do not have access to the traditional full graphical user interface (GUI). Therefore, you must install and maintain the Avamar Client for Windows software from a DOS prompt by using the `msiexec` utility. The installation and registration procedures later in this chapter provide detailed instructions.

User Account Control

The User Account Control (UAC) feature limits application software to standard user privileges. You must provide administrator privileges for certain tasks, such as installing software. UAC is enabled by default.

If you start an Avamar client or plug-in installer without administrator privileges on a computer with UAC enabled, then the software does not install correctly.

You can disable or bypass UAC. The installation procedures in this chapter provide one method to bypass UAC. Other methods and additional information are available in the Microsoft documentation.

NTFS Last Access Time

To correctly back up Windows access control list (ACL) changes, you must leave the NTFS Last Access Time feature enabled. The NTFS Last Access Time feature is enabled by default, but is sometimes disabled for performance purposes.

About this task

If you disable the NTFS Last Access Time feature on a Windows backup client and you have already performed backups, then the Avamar Client for Windows software cannot detect any further ACL changes. This action means that the ACL setting for the file during the original file backup is the ACL setting that applies on all future restores.

Complete the following steps to reestablish proper ACL backup behavior.

Steps

1. Enable the NTFS Last Access Time feature by using one of the following methods:
   - Specify a value of **0** in the following registry entry:

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate.`

     A value of 0 enables Last Access Time, while a value of 1 disables Last Access Time.
   - On Windows 7, Windows Storage Server 2008, Windows Server 2008 R2, Windows Storage Server 2008 R2, Windows Server 2008, and Vista platforms, type the following command from a command prompt:

     `fsutil behavior set disablelastaccess 0`
2. Delete the following local Avamar Client for Windows cache files:
   - `C:\Program Files\avs\var\f_cache.dat`
   - `C:\Program Files\avs\var\p_cache.dat`

   The next backup process for the client re-creates the files.

Symbolic links and directory junctions

File system backups with the Windows File System plug-in or the Windows Cluster File Server plug-in include file system data available through NTFS symbolic links (symlinks), mount points, and directory junctions.

System state backups with the Windows VSS plug-in fail if the path to the system state files includes symbolic links (symlinks) or directory junctions.

Hardware requirements

The client computer on which you install the Avamar Client for Windows software must meet the minimum hardware requirements in the following table.

Table 6. Minimum hardware requirements

Requirement	Minimum
RAM	512 MB
Hard drive space	250 MB permanent hard drive space is required for software installation. 1 GB is recommended. The Avamar client software also requires an additional 12 MB of permanent hard drive space for each 64 MB of physical RAM. Additional disk space might be required by snapshot technology. Backing up the Windows System State requires an additional 1 GB of free disk space.

Up-to-date client compatibility information is available in the *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

Networking requirements

Ensure that the environment meets the following networking requirements:

- The network interface must be 10BaseT or later, coax or optical cable, and configured with the latest drivers for the operating system.
- The Avamar server must be operational and present on the same network as the client computer:
  - To verify that the Avamar server is operational, log in to the Avamar server as admin and run the `dpnctl status` command.

    The *Avamar Administration Guide* provides details on using `dpnctl` commands.
  - To verify that the Avamar server is present on the same network as the client computer, open a command prompt on the client computer and type the following command:

    `ping Avamar_server`

    where *Avamar_server* is the DNS name or IP address of the Avamar server.

    Note the DNS names of the Avamar server and Avamar utility node.

Additional software requirements

Ensure that the environment meets the following additional software requirements for Avamar client software on Windows.

.Net Framework 4

Install Microsoft .NET Framework 4 if you plan to install the Windows client in a cluster or you plan to use the Windows VSS plug-in either on a stand-alone computer or in a cluster.

Microsoft .NET Framework 4 is preinstalled on Windows Server 2019, 2016, or 2012.

For other operating system versions, you can download .NET Framework 4 from the Microsoft Download Center.

Antivirus applications

Some antivirus applications may reduce the performance of Avamar backup operations. Most antivirus applications scan a file for viruses when you open the file. If the antivirus application scans each file during a backup, then the disk and backup program performance is slow.

To reduce backup times and prevent the antivirus application from scanning each file as Avamar backs it up, add the avtar.exe file to the exclusion or safe list for the antivirus application. The settings and steps to do this depend on the antivirus application. For example, McAfee refers to these exceptions as low-risk processes.

Unsupported configurations and features

The following table lists configurations that the Avamar Client for Windows does not support.

Table 7. Unsupported configurations

Unsupported configuration	Description
Microsoft Exchange Server and Microsoft SharePoint Server on the same server	Avamar does not support installation of Microsoft Exchange Server and Microsoft SharePoint Server on the same server. Microsoft does not support this configuration, and Microsoft best practices advise to install these roles on separate servers.
Windows XP Mode on Windows 7	The Avamar Client for Windows does not support backup and recovery of Windows XP Mode components on Windows 7.

Preparing a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster

To ensure successful backup and restore in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster, you must correctly configure roles and permissions in the cluster before you install Avamar client software.

Steps

1. Enable the Remote Management feature on each cluster node.
2. Install the File Server VSS Agent Service server role on each cluster node. Otherwise, backups of clustered file servers for general use fail when the proxy node is not the owner node.
3. To prevent access permissions errors during backup and restore, add the machine accounts for each cluster node to the Backup Operators group on all nodes, and then restart all nodes.

   If the cluster disks use a Scale-Out File Server, then do not manually edit the permissions for a folder or file to remove the machine accounts. If you remove the machine accounts for a folder or file, then Access Denied errors occur for that folder or file during the backup or restore.
4. If you create SMB file shares, then configure the shares so that the machine accounts for each cluster node have access privileges for the shares.
5. Create an account for the Avamar Plug-in Service for Windows, which is the plug-in service that the proxy cluster client uses for backup and restore. The account must have the following privileges:
   - Domain administrator privileges.
   - Access privileges for all file servers and file shares that you plan to back up.

   NOTE: You can use the account for both the Avamar Plug-in Service for Windows and the Backup Agent service, or you can create separate accounts for each service.
6. (Optional) Create a separate account for the Backup Agent service, which is the service for the Avamar agent. The account must have the following privileges:
   - Domain administrator privileges, or privileges to perform WMI queries and copy files to the shared cluster storage during a restore.

     If you do not give domain administrator privileges to the account, then backups include ACL and file attribute information only for file system data on file servers that the proxy node owns. You cannot back up ACL and file attribute information for file system data on file servers that other nodes own.
   - Access privileges for all file servers and file shares that you plan to back up.

Downloading the software

Download the installation packages for the Avamar Client for Windows and the Avamar Config Checker from the Avamar server. Then save the installation packages to a temporary folder.

Steps

1. Log in to the Windows computer as an administrator.
2. Open a web browser and type the following URL:

   `https://Avamar_server`

   where *Avamar_server* is the DNS name or IP address of the Avamar server.

   The **Avamar Web Restore** page appears.
3. Click **Downloads**.
   The **Downloads list** appears.
4. Click **+** next to the operating system headings until the applicable software installation packages appear.
5. Click the appropriate Avamar Client for Windows installation package:
   - `AvamarClient-windows-x86-version.msi (32-bit)`
   - `AvamarClient-windows-x86_64-version.msi (64-bit)`

   where *version* is the Avamar client version.

6. Save the installation package to a temporary folder.
7. Click the appropriate Avamar Config Checker installation package:
   - `Avamar_ConfigChecker_win_x86.zip (32-bit)`
   - `Avamar_ConfigChecker_win_x64.zip (64-bit)`
8. Save the installation package to a temporary folder.

Verifying the environment

Use the Avamar Config Checker for Microsoft Windows to verify that you correctly configured the Windows environment for Avamar backup and recovery. The Config Checker checks the configuration for problems that can lead to installation, backup, or recovery failures. These failures can affect the operating system for the application host or the application itself.

About this task

You can run the Avamar Config Checker either before or after you install Avamar software on the client computer.

The Config Checker supports only English language operating systems.

Steps

1. Unzip the Avamar Config Checker installation package. To install the software, run the setup program.
2. Start the Config Checker:
   a. Open the **Start** screen.
   b. Select **Avamar Config Checker**.
3. Click **Next** on the welcome page.
   The **Avamar Application and User Settings** page appears.
4. Select the version number from the **Avamar version** list.
5. In the application list, select the checkbox next to the applications on the client computer. Specify credentials, if required.
6. Click **Next**.
7. Review the summary information.
8. Click **Run Tests**.
   When the verification completes, the **Config Check Results** window appears.
9. Save or open the results in HTML format.

   NOTE: The Config Checker does not automatically save the results. If you do not save the results, you must rerun the Config Checker to view them.

10. Click **Finish** to exit the Config Checker.
11. Review the HTML result file, and correct all failed checks.
12. Rerun the Config Checker to ensure that all the checks are successful.
    The *Avamar Config Checker for Microsoft Windows Technical Note*, available on Online Support at https://support.EMC.com, provides troubleshooting information and details about the results that appear for each application.

Installing the Avamar client software

To install the Avamar client software, install the Avamar Client for Windows on the client computer. Then register the client with the Avamar server. In a cluster environment, perform these steps on each node, and then configure the cluster client.

Installation road maps

The steps to install the Avamar Client for Windows depend on whether the environment is a stand-alone server or a cluster.

Stand-alone installation road map

About this task

To install the Avamar Client for Windows on a stand-alone server, install the Windows client and then register the client with the Avamar server.

Steps

1. Install the Avamar Client for Windows. Installing the Avamar Client for Windows on page 31 provides instructions.
2. Register the Windows server as a client with the Avamar server. Registering the client on page 33 provides instructions.

Installation road map for Windows Server clusters

About this task

To install the Avamar client software in a cluster, install the Windows client on each node, register each node, and then configure the Avamar cluster client.

Steps

1. Install the Avamar Client for Windows in the same folder on each node in the cluster. Installing the Avamar Client for Windows on page 31 provides instructions.
2. Register each node in the cluster as a client with the Avamar server. Registering the client on page 33 provides instructions.
3. Use the Cluster Configuration Tool to configure the federated cluster client. Configuring the federated cluster client on Windows Server on page 33 provides instructions.

Installation road map for Windows Server active/active clusters

This road map describes how to configure Windows Server active/active clusters.

Prerequisites

In this setup, two cluster groups (for example, G1 and G2) each have a cluster node (for example, N1 and N2).

Steps

1. Create more than one cluster group (for example, G1 and G2).
2. (Optional) Create file shares on the cluster groups.
3. Install the Avamar Client for Windows in the same folder on the cluster nodes, N1 and N2.Installing the Avamar Client for Windows on page 31 provides instructions.

   NOTE: The cluster groups should be owned by a different cluster node. For example, G1 is owned by N1, and G2 is owned by N2.
4. Register each node as a client with the Avamar server. Registering the client on page 33 provides instructions.
5. Run the Cluster Configuration Wizard on the first cluster node N1 to configure the cluster client on the cluster group that is owned by Node 1, G1. Configuring the federated cluster client on Windows Server on page 33 provides instructions.
6. Run the Cluster Configuration Wizard on the second cluster node N2 to configure the cluster client on the cluster group that is owned by Node 2, G2. Configuring the federated cluster client on Windows Server on page 33 provides instructions.

Results

After running the Cluster Configuration Wizard, the network names of the cluster groups should be available in the client list in Avamar Administrator.

Select the names of the cluster groups in the Avamar Administrator client list to perform backups and restores.

Installation road map for Windows Server 2019, 2016, or 2012 clusters with SOFS or SMB

About this task

To install the Avamar client software in a cluster, install the Windows client on the proxy node, register the proxy node, and then configure the Avamar cluster client.

Steps

1. Perform the steps in Preparing a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster on page 28.
2. Install the Avamar Client for Windows on only the proxy node. Installing the Avamar Client for Windows on page 31 provides instructions.
3. Register the proxy node as a client with the Avamar server. Registering the client on page 33 provides instructions.
4. Use the Cluster Configuration Tool to configure the proxy cluster client. Configuring the proxy cluster client on Windows Server 2019, 2016, or 2012 for SOFS or SMB clusters on page 34 provides instructions.

Installation road map for Windows Server 2019, 2016, or 2012 active/active clusters with SOFS or SMB

This road map describes how to configure Windows Server 2019, 2016, or 2012 or 2012 R2 active/active clusters with SOFS or SMB.

Prerequisites

In this setup, two cluster roles (for example, R1 and R2) each have a cluster node (for example, N1 and N2).

Steps

1. Create more than one cluster role (for example, R1 and R2).
2. Create file shares on those cluster roles.
3. Install the Avamar Client for Windows in the same folder on the cluster nodes, N1 and N2. Installing the Avamar Client for Windows on page 31 provides instructions.

   NOTE: The cluster roles can be owned by the same cluster node (N1 or N2), or by a different cluster node (for example, R1 is owned by N1, and R2 is owned by N2.
4. Register each node as a client with the Avamar server. Registering the client on page 33 provides instructions.
5. Run the Cluster Configuration Wizard on the two cluster nodes to create two cluster Proxy nodes (N1 and N2). Configuring the proxy cluster client on Windows Server 2012 provides instructions.

Results

Select the names of the proxy nodes in the Avamar Administrator client list to perform backups on different cluster servers (roles).

Installing the Avamar Client for Windows

The Avamar Client for Windows includes the Avamar agent and the Avamar Plug-in for Windows File System. The Avamar agent is required for backups and restores with application plug-ins. You can use the Windows File System plug-in to back up operating system and application binary files, which are required for disaster recovery.

In a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster, install the Windows client on only the proxy node. In a Windows Server cluster, install the Windows client on each node in the cluster.

Installing the Windows client on full Windows Server installations

About this task

A setup wizard leads you through the steps to install the Windows client. If the User Account Control (UAC) feature is enabled on the client computer, then you must start the setup wizard by using administrator privileges. Otherwise, the software does not install correctly. This procedure provides one method to bypass UAC. The Microsoft documentation provides other methods and additional information.

Steps

1. Log in to the Windows computer as an administrator.
2. Go to the temporary folder that contains the Avamar installation files that you downloaded.
3. Start the setup wizard:
   - If UAC is disabled, double-click the installation file to open it.
   - If UAC is enabled, open a command prompt as an administrator, change directory to the location of the installation package, and then type one of the following commands:

     `msiexec /i AvamarClient-windows-x86-`*`version`*`.msi`

     `msiexec /i AvamarClient-windows-x86_64-`*`version`*`.msi`

     where *version* is the Avamar client version.

   The **Welcome** page appears.
4. Click **Next**.
   The **End-User License Agreement** page appears.
5. Review the license agreement.
6. Select the checkbox to accept the terms in the license agreement, and click **Next**.
   The **Custom Setup** page appears.
7. Ensure that **Avamar Client User Interface** is selected for installation.
8. If you are installing on a proxy node for a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster, enable the **Cluster File Server Plugin** option for installation.
9. (Optional) To specify a folder for the Avamar client installation, click **Browse** and select a location.

   NOTE: Do not rename client installation packages. The Avamar push upgrade mechanisms are incompatible with renamed packages.

10. Click **Next** on the **Custom Setup** page.
    The **Ready to Install Avamar for Windows** page appears.
11. Click **Install**.
12. When the installation completes, click **Finish**.

Installing the Windows client on Windows Server Core installations

About this task

A setup wizard leads you through the steps to install the plug-in. For Windows Server Core installations start the installation wizard at the command line.

Steps

1. Log in to the server as an administrator.
2. Use WinSCP or FTP to copy the Avamar Client for Windows installation package from the download temporary folder to a temporary folder on the Windows Server Core computer.

   Alternatively, use the `net use` command from the Server Core computer to connect to a shared folder with the client install package file.
3. Use the `cd` command to browse to the temporary folder with the client installation package.
4. Start the software installation by typing the following command:

   `msiexec /i AvamarClient-windows-x86_64-`*`version`*`.msi`

   where *version* is the Avamar client version.

The installation wizard appears.

5. Follow the instructions in Installing the Windows client on full Windows Server installations on page 32.

Registering the client

Before you can back up or restore files on a client computer, you must register the server as a client with the Avamar server. You specify the name of the Avamar server, the Avamar domain for the client, and the port on the Avamar server for client/server communication. Avamar domains enable you to group clients and limit backup, restore, and monitoring privileges for the group to certain accounts.

In a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster, register only the proxy node. In a Windows Server cluster, register each node in the cluster.

Registering a full Windows Server client

Steps

1. Log in to the Windows server.
2. Right-click the Avamar client system tray icon and Select **Manage** > **Activate Client**.
   The **Activate Client Setup** dialog box appears.
3. In the **Administrator Server Address** box, type the DNS name of the Avamar server.
4. In the **Administrator Server Port** box, specify the port on the Avamar server for client/server communication.
5. In the **Client Domain** box, type the name of the Avamar domain for the client.
   The default location is `clients`. Do not use a slash (/) as the first character when you type a subdomain. If you use a slash, an error occurs and you cannot register the client.
6. Click **Activate**.
   A confirmation message appears.
7. Click **OK**.

Registering a Windows Server Core client

Steps

1. Open a command prompt on the client computer.
2. Type the following command:
   `C:\Program Files\avs\bin\avregister.bat` ***`MCS_name domain`***

   where:

   - `C:\Program Files\avs\bin\` is the Avamar client installation path.
   - *MCS_name* is the DNS name of the Avamar Management Console Server.
   - *domain* is the Avamar domain for the client. The default domain is `clients`. Do not use a slash (/) as the first character when you type a subdomain. If you use a slash, an error occurs and you cannot register the client.

Configuring the federated cluster client on Windows Server

About this task

The Avamar cluster client enables you to back up and restore Windows data on shared storage in a cluster, regardless of which node is managing the data at the time of the backup or restore. The Cluster Configuration Tool walks you through the steps to configure the Avamar cluster client for the Windows client.

Steps

1. Log in to an active node as a domain administrator.
   a. Ensure that the account is also a member of the local Administrators group on each cluster node.
   b. Ensure that the node on which you logged in, is the owner of the share storage that you want to configure.

NOTE: The account must also be a member of the local Administrators group on each cluster node.

2. Open the Cluster Configuration Tool, by opening a command prompt and typing the following command:

   `C:\Program Files\avs\bin\AvamarClusterConfiguration.exe`

   where `C:\Program Files\avs\bin\` is the Avamar client installation path.

   The wizard opens.
3. Perform the following steps by using the Cluster Configuration Tool:
   a. In the **Choose a group for Install or Update:** field, select the shared storage that you would like to configure.
   b. Click **Configure**.
   c. Ignore the following error message and then click **OK**.

   ```
   No pin files found on local installation path C:\Program Files\avs\bin\. Aborting
   installation!
   ```

   d. Ignore the following error message and then click **OK**.

   ```
   Could not find cid.bin in var folder path(H:\Program Files \Backup Agents for Cluster
   Groups\vm-share16NTFS\var
   \cid.bin). Please check avagent.log file to see if there are problems with client
   registration! Tip: This error can occur
   if provided details for Avamar server are incorrect.
   ```

   e. Ignore the following error message and then click **OK**.

   ```
   Configure of Avamar Cluster Client for cluster group: "vmshare16NTFS" is finished.
   Configured plug-ins:
   ```

   f. Click **Done**.
4. Open the Failover Cluster Manager and perform the following steps:
   a. Select ***<Cluster Name>*** > **Roles** > ***<Shared Storage Name>***..
   b. Click **Resources** at the bottom on the window.
   c. Right-click the **Backup Agent** service that you just configured.
   d. Click **Properties**.
   e. Add the following text to the end of the **Startup parameters**.

   For example:

   ```
   "--service --mcsaddr=a4dpn212d6.asl.lab.emc.com --mcsport=28001 --dpndomain=clients
   --vardir="H:\Program Files\Backup Agents for Cluster Groups\vm-share16NTFS\var"
   --logfile="H:\Program Files\Backup Agents for Cluster Groups\vm-
   share16NTFS\var\avagent.log" --netbind=. --disablegui=true --pin_include=windows.pin
   ```

5. Click **OK**.

Configuring the proxy cluster client on Windows Server 2019, 2016, or 2012 for SOFS or SMB clusters

About this task

The Avamar cluster client enables you to back up and restore Windows data on shared storage in a cluster, regardless of which node is managing the data at the time of the backup or restore. The Cluster Configuration Tool walks you through the steps to configure the Avamar cluster client for the Windows client.

Steps

1. Log in to the proxy node as a domain administrator. The account must also be a member of the local Administrators group on each cluster node.
2. Open the Cluster Configuration Tool:
   - On a full Windows Server 2019, 2016, or 2012 installation, from the Windows Desktop open the **Avamar Windows Cluster Configuration Tool**.

- On a Windows Server 2019, 2016, or 2012 Server Core installation, open a command prompt on the proxy node, and then type the following command:

  `C:\Program Files\avs\bin\av_cluster_config_wizard.exe`

  where `C:\Program Files\avs\bin\` is the Avamar client installation path.

The **Welcome** page appears.

3. Click **Next**.
   The **Plug-Ins** page appears.
4. Select **Windows Proxy Cluster**, and click **Next**.
   The **Operations** page appears.
5. Select **Configure a new proxy cluster client for the proxy node**, and click **Next**.
   The **Prerequisites** page appears. A check mark next to a prerequisite indicates that the environment meets the prerequisite.
6. Ensure that the environment meets all prerequisites on the **Prerequisites** page.

   If the environment does not meet a prerequisite, then exit the wizard, resolve the issue, and restart the wizard.
7. Select the IP version that the environment uses, and then click **Next**.
   The **Summary** page appears.
8. Review the settings that you specified in the wizard, and click **Configure**.
   A dialog box prompts you for credentials.
9. Type the username and password for the service account for the Avamar Plug-in Service for Windows, which is the plug-in service that the proxy cluster client uses for backup and restore.

   The account must be a domain administrator or an account that can perform WMI queries and copy files to the shared cluster storage during a restore. The account must also have access privileges for all file servers and file shares that you back up.
10. Click **OK**.
    The **Progress** page provides the status of the configuration. When the configuration is complete, the **Results** page appears.
11. Click **Close**.

Adding permissions for hidden file access in a cluster

To browse, back up, or restore hidden file shares, the machine accounts in a cluster must belong to each other's Backup Operators group. For remote access, the machine accounts must belong to each other's Local Administrator's group.

Steps

1. Add the M2 machine account to the Backup Operators group of machine M1.
2. Add the M1 machine account to the Backup Operators group of machine M2.
3. For remote access to the machines:
   a. Add the M2 machine account to the Local Administrators group of machine M1.
   b. Add the M1 machine account to the Local Administrators group of machine M2.
4. After adding the machine accounts, reboot the machines.

Results

If you get an error similar to the following during restore, add the flag `--ignoreacls` to the plug-in command file, `avwinclusterfs.cmd`. This command file is located in the `\var` directory for the cluster client, in the location specified in the **Cluster client's var** directory when configuring the cluster. You can create this command file with a text editor if it does not already exist.

Error message:

```
File '\\vm-fshv2k12SOHI\restore$\file2.txt' is unable to be restored due to Avamar having
improper permissions to restore the security information for that file. If you wish to
restore the file, either provide proper rights to Avamar or use the --ignoreacls flag.
```

Adding permissions for non-administrator user access in a cluster

To browse, back up, or restore cluster file shares, the user must be added to the Backup Operators and Administrators groups on each cluster node in the same cluster system. For remote access, add the user to the Remote Desktop User group.

Prerequisites

The new user must be in the list of **Users** of the machine's **Domain Controller**.

Steps

1. Log into a cluster node as a **Domain Administrator**.
2. Start **Server Manager**.
3. Select **Tools** > **Computer Management**.
4. Select **Backup Operators** > **Properties** > **Add**.
5. Add the new user.
6. Select **Administrators** > **Properties** > **Add**.
7. Add the new user.
8. To allow the new user remote access to the machine:
   a. Select **Remote Desktop User** > **Properties** > **Add**.
   b. Add the user.
9. Reboot the machine.
10. Repeat the steps for adding the new user to **Backup Operators**, **Administrators**, and **Remote Desktop User** groups on each cluster node in the same cluster.
11. Log in the cluster node using the new user's login account.
12. Uninstall the Avamar base client if it exists.
13. Install the Avamar base client.
14. Run the **Cluster Configuration Tool** to configure the cluster. Enter the new user name and its password in the **Windows Security** dialog box.
15. Reactivate the client to the server.

Results

Once these permissions are set up, the user can do the following:

- Browse, back up, and restore the cluster machine with Avamar Administrator.
- Perform backups and restores from the command line, by right-clicking on the **PowerShell** icon and selecting `Run as Administrator` to open the PowerShell command prompt.

Next steps

Non-administrator users must be added to the permissions list of the `avs` folder in the Avamar client's installation path. This is required to access the `bin` and `var` directories.

Viewing the cluster client configuration

Steps

1. Log in to the node with the cluster client as a domain administrator. The account must also be a member of the local Administrators group on each cluster node.
2. From the Windows Desktop open the **Avamar Windows Cluster Configuration Tool**.
   The wizard opens at the **Welcome to Avamar Windows Cluster Configuration** page.
3. Click **Next**.
   The **Plug-Ins** page appears.
4. Select **Windows Cluster** or **Windows Proxy Cluster**, and click **Next**.
   - If you select **Windows Proxy Cluster**, then the **Operations** page appears. Skip the next step and proceed to the following step.
   - If you select **Windows Cluster**, then the **Cluster Nodes** page appears with a list of nodes and their status.

5. On the **Cluster Nodes** page, ensure that all nodes are in an **Up** status, and click **Next**.
   The **Operations** page appears.
6. On the **Operations** page, select **View the existing cluster client configuration**, and click **Next**.
   The **Summary** page appears with the cluster client configuration.
7. When you finish viewing the configuration, click **Close**.

Upgrading the Avamar client software

The steps to upgrade Avamar client software on a Windows client depend on whether the installation is on a stand-alone server or in a cluster.

Upgrading on a stand-alone server

When you upgrade Avamar client and plug-in software on a stand-alone server, you do not need to uninstall earlier versions before you install a new version. The installation determines that an earlier version is installed, and then prompts you to upgrade to the new version or remove the current version.

Steps

1. Ensure that the environment meets all system requirements for the new version.
2. Upgrade the Avamar Client for Windows by running the Windows client installation wizard for the new version on the Windows server.

Upgrading in a Windows Server cluster

About this task

When you upgrade Avamar client and plug-in software in a cluster, you must uninstall the current Avamar clients and plug-ins from each node, and then install the new versions.

Steps

1. Ensure that the environment meets all system requirements for the new version. Preparing to install the Avamar client software on page 22 provides information.
2. Use the earlier version of the Cluster Configuration Tool to uninstall the earlier version of the Avamar cluster client.
   The *Avamar for Windows Server User Guide* for the earlier version provides instructions.
3. Follow the steps in Installation road map for Windows Server clusters on page 30.

Upgrading in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster

About this task

When you upgrade Avamar client and plug-in software in a cluster, you must uninstall the current Avamar clients and plug-ins, and then install the new versions.

Steps

1. Ensure that the environment meets all system requirements for the new version.
2. Uninstall the earlier version of the Avamar Client for Windows.

   NOTE: You do not need to use the Cluster Configuration Tool to uninstall the proxy cluster client in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster. The proxy cluster client uninstalls automatically when you uninstall the Avamar Client for Windows.

3. Follow the steps in Installation road map for Windows Server 2019, 2016, or 2012 clusters with SOFS or SMB on page 31.

Uninstalling the Avamar client software

When you uninstall Avamar plug-in and client software from a client computer, scheduled backups no longer occur for the client. You cannot restore backups to the client after you uninstall the software.

When you uninstall the Avamar client software, you can keep or delete the backups for the client.

- To keep the backups for the client so that you can restore the backups to a different client, retire the client by using Avamar Administrator.
- To delete the backups for the client, delete the client by using Avamar Administrator.

Retire or delete the client either before or after you uninstall the plug-in. The *Avamar Administration Guide* provides more information.

The steps to uninstall Avamar client software from a Windows client depend on whether the installation is on a stand-alone server or in a cluster, and on a full Windows Server installation or a Windows Server Core installation.

Uninstall road map

About this task

To uninstall Avamar client and plug-in software from a stand-alone server, uninstall the plug-in and Windows client by using standard Windows uninstall features. In a cluster, first uninstall the Avamar cluster client.

Steps

1. (Windows Server cluster only) Uninstall the Avamar cluster client.

   NOTE: You do not need to uninstall the proxy cluster client in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster. The proxy cluster client uninstalls automatically when you uninstall the Avamar Client for Windows.

2. Uninstall the Avamar Client for Windows by using **Programs and Features**.

Uninstalling the federated cluster client in a Windows Server cluster

About this task

To uninstall the Avamar cluster client from a full Windows Server installation, run the Cluster Configuration Tool on an active node in the cluster, and select the removal option.

Steps

1. Log in to the active node with the federated cluster client as a domain administrator. The account must also be a member of the local Administrators group on each cluster node.
2. Start the Cluster Configuration Tool:
   - On Windows Server, on the Windows Desktop open the **Avamar Windows Cluster Configuration Tool**.
   - On Windows Server Core, open a command prompt on the node with the federated cluster client, and then type the following command:

     ```
     C:\Program Files\avs\bin\AvamarClusterConfiguration.exe
     ```

     where `C:\Program Files\avs\bin\` is the Avamar client installation path.

   The welcome page apears.
3. Click **Next**.
   The **Plug-Ins** page appears.
4. Select **Windows Cluster**, and click **Next**.
   The **Cluster Nodes** page appears with a list of nodes and their status.
5. Ensure that the status of each node is **Up**, and click **Next**.
   The **Operations** page appears.
6. Select **Remove the cluster client from all nodes**, and click **Next**.

The **Prerequisites** page appears. A check mark next to a prerequisite indicates that the environment meets the prerequisite.

7. Ensure that the environment meets all prerequisites on the page, and click **Next**.
   The **Select Service** page appears.
8. Select the cluster service from which to detach the cluster plug-in, and click **Next**.
   The **Summary** page appears.
9. Review the settings that you specified in the wizard, and click **Uninstall**.
   The **Progress** page provides the status of the uninstall. When the uninstall is complete, the **Results** page appears.
10. Click **Close**.

Uninstalling the Avamar Client for Windows

About this task

Uninstall the Avamar Client for Windows using Programs and Features for full servers, or with the command line for Windows Server Core.

Steps

1. On Windows Server, use **Programs and Features**.
2. On Windows Server Core, open a command prompt, browse to the folder with the installation file, and type one of the following commands:

   `msiexec /uninstall AvamarClient-windows-x86-`*`version`*`.msi`

   `msiexec /uninstall AvamarClient-windows-x86_64-`*`version`*`.msi`

   where *version* is the version number of the installation package.

   If you do not have the installation file, then complete the following steps:

   a. Download the installation file. Downloading the software on page 28 provides instructions.
   b. Copy the installation file to the client computer. Installing the Windows client on Windows Server Core installations on page 32 to download the file and copy it to the client computer.

3

Backup

Topics:

- Performing on-demand backups
- Scheduling backups using the AUI Policy wizard
- Monitoring backups
- Cancel backups
- Enforcement of backups to Data Domain

Performing on-demand backups

You can use AUI to perform an on-demand file system backup or a BMR backup. The steps to perform an on-demand file system backup or a BMR backup depend on the operating system and whether the environment is a stand-alone server or a cluster.

Performing file system backups on a stand-alone server

About this task

Complete the following procedure to perform an on-demand backup of volumes, folders, and files on a stand-alone Windows server.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain for the client.

   A list of Avamar clients is displayed in the pane below the domains list.
3. In the list of clients, select the Windows computer.

   You can only view clients in the domain for the login account. To view all clients, log in to the root domain.
4. Click **BACKUP**.
   The Backup wizard is displayed. In the **Plugin** pane, a list of plug-ins that are installed is displayed.
5. In the **Plugins** pane, perform the following steps:
   a. Select the *Windows File System* plug-in for the platform.
      A list of volumes on the selected client is displayed.
   b. Browse to and select one or more folder and files for the backup.

      NOTE: If you are backing up SIS-enabled volumes on Windows Storage Server 2008 or 2008 R2, or deduplicated volumes on Windows Server 2019, 2016, or 2012, select the entire volume for backup. However, you can restore individual folders and files from the volume backup.

   c. Click **NEXT**.

   The **Basic Configuration** pane is displayed.
6. In the **Basic Configuration** pane, complete the following fields:
   a. Select the backup retention policy settings:
      - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period**. Specify the number of days, weeks, months, or years for the retention period.
      - To automatically delete this backup from the Avamar server on a specific calendar date, select **End date** and browse to that date on the calendar.
      - To keep this backup for as long as this client remains active in the Avamar server, select **No end date**.

b. In the **Avamar encryption method** list, select the encryption method to use for data transfer between the client and the Avamar server during the backup.

   The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *Avamar Product Security Guide* provides additional information.

c. In the **Optionally select a proxy to perform backup** list, select the proxy.

   The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.

d. Click **NEXT**.

   The **More Options** window is displayed.

7. In the **More Options** pane, set the plug-in options.

   To view advanced options, select **Show Advanced Options**.

   Windows File System plug-in backup options on page 68 provides details on each of the options.

   The **Backup Command Line Options** dialog box is displayed.

8. Click **FINISH**.
   The following status message is displayed:

```
Backup initiated.
```

Performing file system backups in a Windows Server cluster

About this task

Complete the following procedure to perform an on-demand backup of file system data on shared storage in a Windows Server cluster.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain for the federated cluster client.

   A list of Avamar clients is displayed in the pane below the domains list.
3. In the list of clients, select the federated cluster client.

   You can only view clients in the domain for the login account. To view all clients, log in to the root domain.
4. Click **BACKUP**.
   The Backup wizard is displayed. In the **Plugin** pane, a list of plug-ins that are installed is displayed.
5. In the **Plugins** pane, perform the following steps:

   a. Select the *Windows File System* plug-in for the platform.
      A list of shared disks on the selected cluster is displayed.

   b. Browse to and select one or more disks, folders, and files for the backup.

      Keep the following points in mind when you select the data for backup:

      - If you are backing up SIS-enabled volumes on Microsoft Windows Storage Server 2008 or 2008 R2, you must select the entire volume for backup. However, you can restore individual folders and files from the volume backup.
      - Do not select the quorum drive. According to Microsoft guidelines, this cluster resource must always remain under exclusive control of the cluster.
      - Do not select both shared and local file system data. You may not be able to restore data from a backup that includes file system data from both shared storage and local volumes.

   c. Click **NEXT**.

   The **Basic Configuration** pane is displayed.
6. In the **Basic Configuration** pane, complete the following fields:

   a. Select the backup retention policy settings:

      - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period**. Specify the number of days, weeks, months, or years for the retention period.
      - To automatically delete this backup from the Avamar server on a specific calendar date, select **End date** and browse to that date on the calendar.
      - To keep this backup for as long as this client remains active in the Avamar server, select **No end date**.

b. In the **Avamar encryption method** list, select the encryption method to use for data transfer between the client and the Avamar server during the backup.

   The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *Avamar Product Security Guide* provides additional information.

c. In the **Optionally select a proxy to perform backup** list, select the proxy.

   The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.

d. Click **NEXT**.

   The **More Options** window is displayed.

7. In the **More Options** pane, set the plug-in options.

   To view advanced options, select **Show Advanced Options**.

   Windows File System plug-in backup options on page 68 provides details on each of the options.

   The **Backup Command Line Options** dialog box is displayed.

8. Click **FINISH**.
   The following status message is displayed:

```
Backup initiated.
```

Performing file system backups in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster

About this task

Complete the following procedure to perform an on-demand backup of file system data on shared storage in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster.

Steps

1. Ensure that you performed the steps to prepare the cluster in Preparing a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster on page 28.
2. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
   The **Asset Management** window is displayed.
3. In the domain tree, select the domain for the proxy cluster client.

   A list of Avamar clients is displayed in the pane below the domains list.
4. In the list of clients, select the proxy cluster client.

   You can only view clients in the domain for the login account. To view all clients, log in to the root domain.
5. Click **BACKUP**.
   The Backup wizard is displayed. In the **Plugin** pane, a list of plug-ins that are installed is displayed.
6. In the **Plugins** pane, perform the following steps:

   a. Select the *Windows Cluster File Server* plug-in for the platform.
      A list of clustered file servers on the selected cluster is displayed.

   b. Browse to and select one or more clustered file servers, file shares, folders, or files for the backup.

      NOTE: If you are backing up deduplicated volumes, select the entire volume for backup. However, you can restore individual folders and files from the volume backup.

   c. Click **NEXT**.

   The **Basic Configuration** pane is displayed.
7. In the **Basic Configuration** pane, complete the following fields:

   a. Select the backup retention policy settings:

      - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period**. Specify the number of days, weeks, months, or years for the retention period.
      - To automatically delete this backup from the Avamar server on a specific calendar date, select **End date** and browse to that date on the calendar.
      - To keep this backup for as long as this client remains active in the Avamar server, select **No end date**.

b. In the **Avamar encryption method** list, select the encryption method to use for data transfer between the client and the Avamar server during the backup.

   The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *Avamar Product Security Guide* provides additional information.

c. In the **Optionally select a proxy to perform backup** list, select the proxy.

   The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.

d. Click **NEXT**.

   The **More Options** window is displayed.

8. In the **More Options** pane, set the plug-in options.

   To view advanced options, select **Show Advanced Options**.

   Windows File System plug-in backup options on page 68 provides details on each of the options.

   The **Backup Command Line Options** dialog box is displayed.

9. Click **FINISH**.
   The following status message is displayed:

   ```
   Backup initiated.
   ```

Backing up VHDs with the Windows File System plug-in

Use the Windows File System plug-in to back up attached or detached VHDs in the following environments:

- Stand-alone server, all operating system versions
- Windows Server cluster

You must attach the VHD file in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster to back up the VHD file with the Windows File System plug-in.

If the VHD file is attached as a volume and you want to include the VHD in the backup, then select the **Back up Natively Attached Virtual Hard Disks** checkbox in the **Backup Command Line Options** dialog box when you set the options for the backup.

To exclude an attached VHD file from the backup of a volume, clear the **Back up Natively Attached Virtual Hard Disks** checkbox.

The Windows File System plug-in backs up the detached VHD file as a file in the file system with a `.vhd` file name extension. You must select the volume on which the VHD file is located for the backup.

Performing BMR backups

You can perform an on-demand BMR backup of various versions of Windows Server and Windows client computers, including the System State, critical disks, and Active Directory data on a domain controller.

Prerequisites

For details about BMR support, see the *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain for the client.

   A list of Avamar clients is displayed in the pane below the domains list.
3. In the list of clients, select the Windows computer. To back up Active Directory data, select the domain controller.

   You can only view clients in the domain for the login account. To view all clients, log in to the root domain.
4. Click **BACKUP**.
   The Backup wizard is displayed. In the **Plugin** pane, a list of plug-ins that are installed is displayed.
5. In the **Plugins** pane, perform the following steps:

   a. Select the *Windows VSS plug-in* plug-in for the platform.

Do not select individual items in the Windows VSS plug-in, or the backup fails with an error message that you must select all items in the Windows VSS plug-in.

b. Browse to and select one or more folders and files for the backup.

> **NOTE:** If you are backing up SIS-enabled volumes on Windows Storage Server 2008 or 2008 R2, or deduplicated volumes on Windows Server 2019, 2016, or 2012, select the entire volume for backup. However, you can restore individual folders and files from the volume backup.

c. Click **NEXT**.

The **Basic Configuration** pane is displayed.

6. In the **Basic Configuration** pane, complete the following fields:
   a. Select the backup retention policy settings:
      - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period**. Specify the number of days, weeks, months, or years for the retention period.
      - To automatically delete this backup from the Avamar server on a specific calendar date, select **End date** and browse to that date on the calendar.
      - To keep this backup for as long as this client remains active in the Avamar server, select **No end date**.
   b. In the **Avamar encryption method** list, select the encryption method to use for data transfer between the client and the Avamar server during the backup.

      The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *Avamar Product Security Guide* provides additional information.
   c. In the **Optionally select a proxy to perform backup** list, select the proxy.

      The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.
   d. Click **NEXT**.

      The **More Options** window is displayed.
7. In the **More Options** pane, set the plug-in options.
   a. To view advanced options, select **Show Advanced Options**.
   b. (Optional) Type a descriptive label for the backup in the **Snapup label** box.
   c. To perform a BMR backup, select the **Create Disaster Recovery Backup** checkbox.
   d. To perform a nondisaster recovery backup on a domain controller so that you can restore Active Directory data, clear the **Create Disaster Recovery Backup** checkbox.
   e. Specify whether to ignore missing Windows System State files during the backup by selecting or clearing the **When backup detects missing Windows System State files, complete the backup successfully without exceptions** checkbox. When you select the checkbox, warnings appear for the missing files and the backup completes successfully. When you clear the checkbox, errors appear for the missing files and the backup completes with exceptions. On Windows Server 2019, 2016, or 2012 or Windows 8, specify whether to include or exclude a non-critical disk when a service or application is installed on the disk and causes the disk to become critical.
   f. Select the **Ignore third-party services when identifying critical volumes. Applies to Windows 8 (or later)** checkbox to exclude the noncritical disk from the backup, or clear the checkbox to include the noncritical disk in the backup.
   g. To store the backup on a Data Domain system instead of the Avamar server, select the **Store backup on Data Domain system** checkbox, and then select the Data Domain system from the list.
   h. From the **Encryption method to Data Domain system** list, select the encryption method for data transfer between the client and the Data Domain system during the backup.

   Windows VSS plug-in backup options on page 72 provides details on each of the options.
8. To exclude noncritical dynamic disks from the backup, add the following attribute:
   a. Click **More**.
   b. In the **Enter Attribute** box, type **`--exclude-non-critical-dynamic-disks`**.
   c. In the **Enter Attribute Value** box, type **`true`**.
   d. Click **+**.
9. Click **FINISH**.

   The following status message is displayed:

   ```
   Backup initiated.
   ```

BMR backup limitations

Consider the following requirements and limitations of BMR backups:

- BMR backups do not include critical disks on shared storage in a cluster. Perform file system backups of these disks.
- BMR of a UEFI system requires one available drive letter.

Volumes that are considered critical and are included in a Windows BMR backup

Certain volumes are considered critical and are included in a Windows BMR backup.

The following volumes are included in a Windows BMR backup:

- Any volume that contains operating system files.
- Any volume that contains a third-party service.
- A non-critical volume that has a critical volume mounted on it, or a non-critical volume that serves as a parent to a critical volume. In either case, both the parent volume and mounted volume are treated as critical.
- If one of the volumes on a dynamic disk is critical, all volumes on a dynamic disk are critical. Microsoft requires all dynamic disks to be included in the BMR backup if anyone of the dynamic disks is critical.

Excluding a volume from a Windows BMR backup

There are several ways to exclude a volume from a Windows BMR backup depending on the operating system, disk types, configuration, and installation practices.

- Install applications with third-party services on the system disk, or a disk that already has other services installed. Use the `diskshadow` utility command `list writers detailed` to identify the disks that contain third-party services.
- Do not install services on a dynamic disk. This causes all the dynamic disks to be classified as critical volumes, and increases the number of disks included in the BMR backup.
- If a dynamic disk is critical, you can exclude the noncritical dynamic disks by using `--exclude-non-critical-dynamic-disks=true` in `avvss.cmd` or in the dataset definition. When you perform BMR, you must use `--exclude-non-critical-disks=false` in `avvss.cmd`. Create the `avvss.cmd` file in the `var` directory, `C:\Program Files\avs\var`.
- Do not create a mount point on a noncritical disk that points to a critical disk.
- For Windows Server 2008 and 2008 R2 use the `ExcludedBinaryPaths` registry key to exclude third-party services from the System Writer. This prevents the disk where the service is installed from being classified as critical. The *System state backup error in Windows Server 2008, in Windows Vista, in Windows 7 and in Windows Server 2008 R2: "Enumeration of the files failed"* support document on the Microsoft website describes the use of this registry key.
- For Windows Server 2019, 2016, or 2012 and later, use `--dr-exclude-win32-services-files=true` in `avvss.cmd` to exclude disks containing third-party services. The default value is `false` to maintain consistency with older versions of the Windows VSS plug-in. Create the `avvss.cmd` file in the `var` directory, `C:\Program Files\avs\var`.
- For Windows Server 2012 R2, use `--dr-exclude-sync-shares=true` in `avvss.cmd` to ignore Sync Share (Work Folders) data when identifying critical disks. The default value is `false`.

Perform file system backups of any excluded disk so that you can restore files if you need to restore the disk.

Scheduling backups using the AUI Policy wizard

Scheduled backups run automatically to ensure that backups occur on an ongoing basis. You can schedule backups to run daily, weekly, or monthly.

About this task

You can schedule backups by using the Policy wizard to create a backup policy.

Perform the following steps within the **Policy** wizard. The *Avamar Administration Guide* provides more information about policies, datasets, schedules, and retention settings.

Steps

1. Assign members to the new backup policy.
2. Assign a dataset to the new backup policy.
   To create a dataset, use the Policy wizard or select **Settings** > **Dataset** > **Add**.
3. Assign a schedule to the new backup policy.
   To create a schedule, use the Policy wizard or select **Settings** > **Schedule** > **Add**.
4. Assign a retention policy to the new backup policy.
   To create a retention policy, use the Policy wizard or select **Settings** > **Retention** > **Add**.
5. Enable scheduling for the backup policy.

Creating a dataset

A dataset specifies the data to include in a scheduled backup and the options to use for the backup. Create at least one dataset for scheduled backups on a client or group of clients. Create multiple datasets to segregate client data.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Settings**.
   The **Setting** pane is displayed.
2. Click the **Dataset** tab.
3. Click **ADD**.
   The **Create Dataset** window is displayed.
4. In the **Dataset Name** field, type a name for the dataset.
   The name can include alphanumeric characters (A-Z, a-z, 0–9) and the following special characters: period (.), hyphen (-), and underscore (_). Do not use Unicode characters or the following special characters: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?
5. From the **Plugins** list, select the **Windows File System** plug-in appropriate for your operating system.
   The **Windows File System** plug-in options are displayed.
6. Click the **Options** tab, and then set the plug-in options.

   To view advanced options, select **Show Advanced Options**.

   Windows File System plug-in backup options on page 68 provides details on each of the options.
7. Click the **Source Data** tab, and then set the plug-in options:
   - To include all local Windows file system, select **All local Windows filesystems**. All local Windows filesystems are selected by default. This backs up all file system data.
   - To limit the dataset to specific items, perform the following steps:

   a. In the **File/Folder Path**, type the file path.
   b. Click **ADD**.

   If you are backing up SIS-enabled volumes on Windows Storage Server 2008 or 2008 R2, or deduplicated volumes on Windows Server 2019, 2016, or 2012, type the entire volume for backup. However, you can restore individual folders and files from the volume backup.
8. Click **SUBMIT**.

Creating a backup policy

A backup policy is a collection of Avamar clients that use the same dataset, schedule, and retention settings to implement scheduled backups.

About this task

Member clients must all be in the same Avamar domain. When you create a backup policy, you define the dataset, schedule, and retention settings that apply for scheduled backups. These settings comprise the backup policy, which controls backup behavior for all members of the backup policy unless you override these settings at the client level.

The *Avamar Administration Guide* provides information about creating and editing backup policies, schedules, or retention settings.

Enabling a scheduled backup for a backup policy

Scheduled backups occur only for enabled backup policies. Backup policies are disabled by default unless you select the **Enabled** check box on the first page of the **New Policy** wizard. If you did not enable the backup policy when you created it, use the menu options in the **Policy** window to enable backups.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Backup Policy**.
   The **Policy** page is displayed.
2. In the domain tree, select a domain or subdomain for the backup policy.
   To select a subdomain for the backup policy, toggle the **Include Sub-domain** switch to on.
3. Select a backup policy from the list.
4. To enable a backup policy, click **MORE ACTIONS** > **Enable Policy**.
5. To disable a backup policy, click **MORE ACTIONS** > **Disable Policy**.

Monitoring backups

You can monitor and view status information for backup and restore operations by using the **Activity Monitor**.

About this task

To access the **Activity Monitor**, open the navigation pane, and then click **Activity**. The **Activity Monitor** appears with a list of all activities.

NOTE: The AUI **Activity Monitor** window has been optimized for at least 1366 pixels-wide screens. Display issues might occur for smaller screens. To properly display the AUI, ensure that your display is at least 1366 pixels wide.

The **Activity Monitor** provides you with options to filter the information that appears:

- Filter activities by duration—By default, the **Activity Monitor** displays the most recent 5,000 client activities. To select a different duration, in the **Filter activities by duration** drop-down list, select **Last 24 hours** or **Last 72 hours**.
- Filter activities by domain—By default, the **Activity Monitor** displays all activities regardless of domain. To display only the activities for a specific domain, in the **Filter activities by domain** drop-down list, select a domain or subdomain.
- Filter activities by status—By default, the **Activity Monitor** displays all activities regardless of status.

  To display only activities with a specific status, at the top of the **Activity Monitor**, select one of the following options:

  - Canceled
  - Completed
  - Completed with Exceptions
  - Failed
  - Running
  - Waiting

To filter activities by client, start time, plug-in, or type, click ▼ in their respective column.

The **Activity Monitor** displays the date and time that an activity began, and the total number of bytes examined during an activity.

To view activity details, expand the **Details** pane, by clicking ≪.

Cancel backups

You can cancel a backup any time before it completes. The cancellation might take 5 minutes or longer. The backup might complete before the cancellation finishes.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Activity**.
   The **Activity Monitor** appears with a list of activities.
2. Select the backup from the list.
3. Click **CANCEL**.
   A confirmation dialog box is displayed.
4. Click **YES**.

Enforcement of backups to Data Domain

If the Avamar server is configured to enforce backups to a Data Domain system, the server rejects backups that are not destined for the Data Domain. This enforcement covers backups that you configure through the Avamar Administrator and the AUI, as well as from command-line interfaces and other tools.

These backups must have additional flags that indicate the storage target. The *Avamar and Data Domain System Integration Guide* provides more information about backup enforcement and the related client version requirements. Backup enforcement is disabled by default.

4

File System Restore

Topics:

- Restore requirements
- Restoring to the original location
- Restoring to a different location
- Monitor restores
- Cancel restores

Restore requirements

Review the requirements for your environment before you restore Windows file system data from an Avamar backup.

Restoring in a cluster

When you restore data from a backup of file system data on shared storage in a Windows Server cluster, select the federated cluster client as the client from which to restore. Use the Windows File System plug-in for the restore.

When you restore data from a backup of file system data on shared storage in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster, select the proxy cluster client as the client from which to restore. Use the Windows Cluster File Server plug-in for the restore.

When you restore data from a backup of file system data on a local volume of a node, select the node as the client from which to restore. Use the Windows File System plug-in for the restore.

Restoring VHD files

When you restore VHDs from an Avamar backup, ensure that you meet the following additional requirements:

- When you restore the parent partition and VHDs on a client computer, you must restore the parent partition before you can restore the VHDs on the parent partition.
- When you restore both VHDs and other file types simultaneously, Avamar restores the other file types before the VHDs.
- After you restore the VHDs, reattach the VHDs. Use the same drive letter settings to ensure backup data consistency.

Restoring SIS volumes on Windows Server 2008

When you restore an SIS volume on Windows Server 2008, the SIS Groveler service activity may prevent the restore process from correctly restoring or overwriting some files. Restore problems and solutions on page 83 provides more information about this error and how to correct it.

Restoring from backups of DFS shares

When you restore data from backups of DFS shares, the replication process automatically replicates the restored data to the central DFS hub if the restored data has a newer timestamp.

About this task

NOTE: File system backups include only DFS shares on local volumes on the client computer.

Perform the appropriate steps to prevent automatic replication after a restore:

- Restore specific folders or files from a backup of DFS shares by using the steps in Restoring to a different location on page 51 to restore the data to a location outside of the DFS shared folders.
- Restore all data from a backup of DFS shares:
  1. Disable DFS replication.

     The "Managing DFS Replication" article on the Microsoft TechNet website provides several methods to disable replication.
  2. Follow the steps in Restoring to the original location on page 50 to restore the backup.
  3. Manually run replication to synchronize data with the replication server.

     The "Managing DFS Replication" article on the Microsoft TechNet website provides several methods to synchronize data.

Restoring to the original location

The steps to restore file system data to the original location depend on whether the environment is a stand-alone server or a cluster.

Restoring to the original client

About this task

You can restore a volume, folder, or file to the original location on a stand-alone server. You can also restore file system data to the original location on shared storage in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain that contains the Windows server.

   You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

   A list of Avamar clients is displayed in the pane below the domains list.
3. From the list of clients, select the client that runs the Windows server.
4. (Optional) To locate backups by date:
   a. In the right pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
5. Click the **Restore** tab.

   The **Restore** wizard is displayed and the **Destination Client** pane is displayed on the right.
6. In the **Destination Client** pane, perform the following steps:
   a. Select **Restore to original client**.
   b. Click **NEXT**.

   The **Backup Content** pane is displayed.
7. In the **Backup Content** pane, perform the following steps:
   a. In the left pane, select the folder from the tree.

      The **Backup Content** pane displays a list of databases within the backup.
   b. In the right pane, select the databases that you want to restore.
   c. Click **NEXT**.

   The **Destination Location** pane is displayed.
8. In the **Destination Location** pane, perform the following steps:
   a. Select **Restore everything to its original location**.
   b. Click **Next**.

The **More Options** pane is displayed.

9. In the **More Options** pane, set the plug-in options.

   Windows File System plug-in restore options on page 71 provides additional information about the plug-in options.

   a. To view advanced options, select **Show Advanced Options**.
   b. Click **NEXT**.

   The **Summary** pane is displayed.

10. Review the provided information, and then click **FINISH**.

Restoring to the original location in a Windows Server cluster

When you restore volumes, folders, or files to shared storage in a Windows Server cluster, select the federated cluster client as the client from which to restore. Use the Windows File System plug-in to perform the restore. Restoring to the original client on page 50 provides instructions.

Restoring to a different location

The steps to restore file system data to a different location either on the same client or on a different client depend on the environment:

- Stand-alone server
- Windows Server cluster
- Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster

Restoring to a different location on a stand-alone server

You can restore file system data to a single different location on the same stand-alone server, or to a single location on a different client.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain that contains the Windows server.

   You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

   A list of Avamar clients is displayed in the pane below the domains list.
3. From the list of clients, select the client that runs the Windows server.
4. (Optional) To locate backups by date:
   a. In the right pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
5. Click the **Restore** tab.

   The **Restore** wizard is displayed and the **Destination Client** pane is displayed on the right.
6. In the **Destination Client** pane, perform the following steps:
   a. Select **Restore to original client**.
   b. Click **NEXT**.

   The **Backup Content** pane is displayed.
7. In the **Backup Content** pane, perform the following steps:
   a. In the left pane, select the folder from the tree.

      The **Backup Content** pane displays a list of databases within the backup.

b. In the right pane, select the databases that you want to restore.
c. Click **NEXT**.

The **Destination Location** pane is displayed.

8. In the **Destination Location** pane, perform the following steps:
   a. Select **Restore everything to a different location**.
   b. In the **Restore Location** field, type the file path of the target location where you want to restore the data.

      For example: E:/dbrestore_dir/

      If you type a pathname and the folder does not exist, the restore process creates the folder.

   c. Click **NEXT**.

      The **More Options** pane is displayed.
9. In the **More Options** pane, set the plug-in options.
   a. To view advanced options, select **Show Advanced Options**.

      Windows File System plug-in restore options on page 71 provides additional information about the plug-in options.

      NOTE: If a file with the same name exists in the directory to which you are restoring a file, use the **Overwrite Existing Files** option to control whether the restore process overwrites the file.

   b. Click **NEXT**.

   The **Summary** pane is displayed.
10. Review the provided information, and then click **FINISH**.

Restoring to a different location in a Windows Server cluster

When you restore file system data to a single different location on the same Windows Server cluster, or to a single location on a different client, select the federated cluster client as the client from which to restore. Use the Windows File System plug-in to perform the restore. Restoring to a different location on a stand-alone server provides instructions.

Restoring to a different location in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster

You can restore file system data to a single different location on shared storage in the same Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster, or to a single location on a different client.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain that contains the Windows server.

   You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

   A list of Avamar clients is displayed in the pane below the domains list.
3. From the list of clients, select the client that runs the Windows server.
4. (Optional) To locate backups by date:
   a. In the right pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
5. Click the **Restore** tab.

   The **Restore** wizard is displayed and the **Destination Client** pane is displayed on the right.
6. In the **Destination Client** pane, perform the following steps:
   a. Select **Restore to original client**.

b. Click **NEXT**.

The **Backup Content** pane is displayed.

7. In the **Backup Content** pane, perform the following steps:
   a. In the left pane, select the folder from the tree.

      The **Backup Content** pane displays a list of databases within the backup.

   b. In the right pane, select the clustered file servers, folders, or files to restore.
   c. Click **NEXT**.

   The **Destination Location** pane is displayed.

8. In the **Destination Location** pane, perform the following steps:
   a. Select **Restore everything to a different location**.
   b. In the **Restore Location** field, type the file path of the target location where you want to restore the data.

      For example: E:/dbrestore_dir/

      - To restore to shared storage in a cluster, type the path of the Windows Cluster File Server.
      - To restore to a stand-alone computer, type the path of the Windows File System.

      If you type a pathname and the folder does not already exist, the restore process creates the folder.

      NOTE: When you restore to a different location, Avamar restores only the contents of the folder. Avamar does not restore the original parent folder.

   c. Click **NEXT**.

      The **More Options** pane is displayed.

9. In the **More Options** pane, set the plug-in options.
   a. To view advanced options, select **Show Advanced Options**.

      Windows File System plug-in restore options on page 71 provides additional information about the plug-in options.

      NOTE: If a file with the same name exists in the directory to which you are restoring a file, use the **Overwrite Existing Files** option to control whether the restore process overwrites the file.

   b. Click **NEXT**.
   c. In the **Avamar encryption method** list, select the encryption method for data transfer between the client and the Avamar server during the restore.

      The encryption technology and bit strength for a client/server connection depend on several factors, including the client operating system and Avamar server version. The *Avamar Product Security Guide* provides additional information.

   The **Summary** pane is displayed.

10. Review the provided information, and then click **FINISH**.

Monitor restores

You can monitor and view status information for backup and restore operations in the **Activity Monitor**.

About this task

To access the **Activity Monitor**, open the navigation pane, and then click **Activity**. The **Activity Monitor** appears with a list of all activities.

NOTE: The AUI **Activity Monitor** window has been optimized for at least 1366 pixels-wide screens. Display issues might occur for smaller screens. To properly display the AUI, ensure that your display is at least 1366 pixels wide.

The **Activity Monitor** provides you with options to filter the information that appears:

- Filter activities by duration—By default, the **Activity Monitor** displays the most recent 5,000 client activities. To select a different duration, in the **Filter activities by duration** drop-down list, select **Last 24 hours** or **Last 72 hours**.
- Filter activities by domain—By default, the **Activity Monitor** displays all activities regardless of domain. To display only the activities for a specific domain, in the **Filter activities by domain** drop-down list, select a domain or subdomain.
- Filter activities by status—By default, the **Activity Monitor** displays all activities regardless of status.

  To display only activities with a specific status, at the top of the **Activity Monitor**, select one of the following options:

- Canceled
- Completed
- Completed with Exceptions
- Failed
- Running
- Waiting

To filter activities by client, start time, plug-in, or type, click in their respective column.

The **Activity Monitor** displays the date and time that an activity began, and the total number of bytes examined during an activity.

To view activity details, expand the **Details** pane, by clicking .

Cancel restores

You can cancel a restore any time before it completes. The cancellation might take 5 minutes or longer. The restore might complete before the cancellation finishes.

Steps

1. In the AUI navigation pane on the left, click , and then click **Activity**.
   The **Activity Monitor** appears with a list of activities.
2. Select the restore from the list.
3. Click **CANCEL**.
   A confirmation dialog box is displayed.
4. Click **YES**.

5

Bare Metal Recovery

Topics:

- BMR of Windows clients
- Active Directory recovery
- BMR of Windows clusters

BMR of Windows clients

About this task

You can perform BMR of client computers with a variety of Windows operating systems. For details, see *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

Steps

1. Review the BMR requirements in BMR requirements on page 55.
2. Download and prepare the custom Avamar WinPE ISO image for BMR. WinPE ISO image preparation on page 56 provides details.
3. Test the Avamar Bare Metal Recovery Wizard to ensure that the wizard can run successfully and you have the required drivers:
   a. Complete the steps in Restoring the computer to its original System State on page 59.

      Verify the following requirements as you go through the wizard pages:

      - You can see the network interface that is required to communicate with the Avamar server. If you cannot see the network interface, use the wizard to load the required NIC driver.
      - If DNS is not available, the host can resolve the Avamar server name by some method, such as using a local hosts file.
      - You can see the critical and non-critical local disks for the target host. If you cannot see all of the disks, use the wizard to load the required disk drivers.

   b. When you reach the **Summary** page, click **Exit** to exit the wizard without performing the restore.
      The system automatically restarts.
4. Use the Avamar Bare Metal Recovery Wizard to restore the Windows computer to its original System State. Restoring the computer to its original System State on page 59 provides details.
5. Perform the post-BMR steps in Performing post-BMR tasks on page 62.

BMR requirements

Avamar supports BMR to physical and virtual machines:

- Physical machine to physical machine
- Virtual machine to virtual machine
- Physical to virtual machine (P2V)

The following table lists the Windows versions and virtual machine environments that are supported for P2V BMR.

Table 8. Windows versions and virtual machine environments supported for P2V BMR

Windows versions	Virtual machine environments
• Windows Server 2008 or later • Windows 7 or later	• Microsoft Hyper-V • VMware ESX 5.0, 5.1, and 5.5

NOTE: BMR of a physical Hyper-V server to a VMware virtual machine is not supported. VMware does not support running a nested hypervisor. That means you cannot run a Hyper-V server inside of a VMware virtual machine, and you cannot perform a P2V BMR of a Hyper-V server to a VMware virtual machine. Contact Customer Support for alternatives.

Avamar performs P2V BMR operations on a best-effort basis, and cannot guarantee that all possible combinations of physical hardware can be successfully converted to a virtual machine.

Verify that the environment meets the following requirements before you perform a BMR:

- A valid BMR backup exists. Find the Windows VSS plug-in backup on the Avamar server. If the **BootableSystemState** column in the **Backups** table displays an entry for the ASR writer, then the backup is valid for BMR.
- The hardware on the target host is operational.
- The hardware configuration on the target host is similar to the hardware configuration on the host for which the Windows BMR backup was done (source host). Any hardware, driver, or firmware differences between the source and target host computers might cause the recovery to fail. For example, restore of a 64-bit host to 32-bit hardware is not supported.

  The Microsoft Support article “How to move a Windows installation to different hardware” on the Microsoft website states that Microsoft does not support restoring a System State backup from one computer to a target computer with a different make, model, or hardware configuration.

- The target host has at least 512 MB of RAM.
- The size of the disks on the target host is equal to or greater than the size of the disks on the source host.

  BMR fails to initialize and format the disk when the disk size on the target host is less than the disk size on the source host, even if the target system disk size is sufficient for the BMR backup data.

  After BMR, some unallocated space may remain. You can extend the partition after the recovery to use this extra space.

- There are at least as many disks on the target host as there were on the source host. The disk LUN numbering on the target host must match the disk LUN numbering on the source host.
- If the target host is a Windows 7 computer, then the computer does not use Windows XP Mode components. The Avamar Client for Windows does not support backup and recovery of Windows XP Mode components in Windows 7.
- You have the following information available:
  - The IP address and network name of the target host, and the accounting system pathname of the client computer, for example, `/clients/mycomputer.mycompany.com`.
  - The network name or IP address of the Avamar server to use for the recovery.
  - Account credentials for an Avamar Administrator account on the Avamar server. The credentials enable successful backup of BMR log files.

NOTE: Avamar Windows BMR has not been tested with third-party drive encryption products other than Microsoft's BitLocker. If you use third-party drive encryption products, you should perform a Windows BMR backup and recovery to ensure that a good working system is available. Do the test using the original hardware and new hardware to confirm both scenarios. You will need to determine if any steps are required to reencrypt the drives after a successful restore.

WinPE ISO image preparation

Avamar provides customized WinPE ISO images that enable you to recover the target computer without installing an operating system. Because the local disks are not in use by the booted operating system, the recovery process can replace files without conflict.

NOTE: The Microsoft Windows® Preinstallation Environment software included with this computer or software may be used for boot, diagnostic, setup, restoration, installation, configuration, test, or disaster recovery purposes only. NOTE: THIS SOFTWARE CONTAINS A SECURITY FEATURE THAT WILL CAUSE YOUR COMPUTER SYSTEM TO REBOOT WITHOUT PRIOR NOTIFICATION AFTER 72 HOURS OF CONTINUOUS USE.

NOTE: FOR AUSTRALIA ONLY. References to "Limited Warranty" are references to the warranty provided by the manufacturer or installer. This warranty is given in addition to other rights and remedies you may have under law, including your rights and remedies in accordance with the statutory guarantees under the Australian Consumer Law. Our goods include guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. Goods that are presented for repair may be replaced by refurbished goods of the same type rather than being replaced. Refurbished parts may be used to repair the goods. For further information regarding this warranty and to claim

expenses in relation to the warranty (if applicable), please contact the manufacturer or installer; see the contact information provided in the system packaging.

WinPE supports a minimal subset of Windows features. This functionality includes access to network resources, disks, and other features through a command prompt.

The custom Avamar WinPE ISO image contains the NIC and disk drivers from Microsoft for the Windows versions that the WinPE ISO supports. The custom Avamar WinPE ISO image is based on Windows PE 10.0.

If the WinPE ISO image does not contain the drivers for the NIC or disk devices on the client computer that you are recovering, you can perform one of the following tasks:

- Copy the drivers to a USB flash drive, and then attach the drive after booting with the custom Avamar WinPE ISO image.
- Create a WinPE ISO image that includes the drivers, and reboot from that image. (Optional) Adding NIC or disk drivers to the WinPE ISO file on page 58 provides instructions.

The drivers must meet the following requirements:

- Use 32-bit drivers with 32-bit ISO images and 64-bit drivers with 64-bit ISO images.
- Use drivers that do not require a restart during installation. The WinPE environment loads only in memory, and changes are not persistent across a restart. If a restart prompt appears, you may be able to ignore the prompt. Most NIC drivers are generally plug-and-play.

Preparing the WinPE ISO image for BMR

Download and prepare the WinPE ISO image for BMR of a Windows client computer.

Steps

1. Download the customized WinPE ISO image from the Avamar server. Downloading the custom WinPE ISO image from the Avamar server on page 57 provides instructions.
2. (Optional) If the WinPE ISO image does not contain the drivers for the NIC or disk devices on the client computer that you are recovering, and you do not want to load the drivers from a separate disk during the BMR process, then add the drivers to the WinPE ISO file.

   (Optional) Adding NIC or disk drivers to the WinPE ISO file on page 58 provides instructions.
3. Use one of the following methods to create bootable media from the ISO image:
   - To boot the target computer locally, burn the WinPE ISO image to a CD, DVD, or USB flash drive.
   - To enable a network boot of the target computer, copy the image to a Windows Deployment Services (WDS) server. (Optional) Adding the WinPE ISO boot image to a Windows Deployment Services server on page 58 provides detailed steps.

Downloading the custom WinPE ISO image from the Avamar server

Steps

1. Open a web browser and type the following URL:

   `https://`*`Avamar_server`*

   where *Avamar_server* is the DNS name or IP address of the Avamar server.

   The **Avamar Web Restore** page appears.
2. Click **Downloads**.
   The **Downloads** list appears.
3. Click **+** next to the correct operating system heading, click **+** next to the **Windows Bare Metal Recovery (BMR) Wizard** heading, and then click the `.iso` file link:
   - **Windows (32 bit) > Windows Bare Metal Recovery (BMR) Wizard > Avamar_Windows_BMR_Wizard_x86_WinPE10-*version*.iso**

     This `.iso` file is for computers with a 32-bit version of Windows Server 2008, Windows 8.1, Windows 8, or Windows 7, and supports only BIOS-based systems.
   - **Windows (64 bit) > Windows Bare Metal Recovery (BMR) Wizard > Avamar_Windows_BMR_Wizard_x64_WinPE10-*version*.iso**

This `.iso` file is for computers with a 64-bit version of Windows operating systems, and supports both BIOS-based and UEFI-based systems.

4. Download the file to a temporary folder.

(Optional) Adding NIC or disk drivers to the WinPE ISO file

Customize the Avamar WinPE ISO image to add NIC or disk device drivers if you do not want to load the drivers from a separate disk during the BMR process.

About this task

NOTE: In general, we do not support changes to the custom Avamar WinPE ISO image. Modify the image at your own risk. One exception, however, is the addition of NIC or disk device drivers that the image does not include.

Steps

1. Open the Avamar WinPE ISO file with a utility like UltraISO or MagicISO.
2. Create a folder for the drivers at the top level of the ISO image, such as `Drivers` in the following example figure.

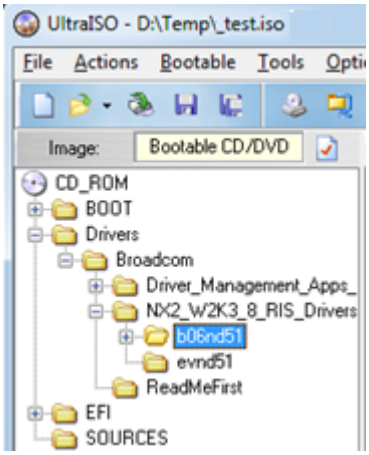

Figure 4. Folders

3. Copy the NIC or disk device drivers to the folder.

   If you have several models of servers that require different NIC or disk device drivers, you can create subfolders for each device, model, or brand.
4. Save the ISO image with a different name.

(Optional) Adding the WinPE ISO boot image to a Windows Deployment Services server

About this task

You can add the WinPE ISO boot image to a Windows Deployment Services (WDS) server to enable a network boot of the target computer. The Microsoft TechNet website provides detailed steps to configure and use WDS.

NOTE: WDS is described here as a known example of how to boot from an ISO boot image over a network. Other network boot technologies may also work.

Steps

1. Configure the WDS server.
2. Add the WinPE ISO boot image to the boot menu.
3. Ensure that PXE booting is enabled on the WDS client.
4. To use the image, perform a network boot of the WinPE ISO boot image, Windows System Recovery, on the WDS client.

Restoring the computer to its original System State

Use the Avamar Bare Metal Recovery Wizard to restore the Windows computer to its original System State.

About this task

For a detailed list of the supported Windows operating systems that are supported, see the *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

Steps

1. Boot the target computer with the WinPE boot disk, or perform a network boot of the WinPE ISO image.

   The Windows Deployment Services documentation on the Microsoft TechNet website provides detailed steps to perform a network boot on the client.

   The **Avamar Bare Metal Recovery Wizard** opens at the **Welcome** page.

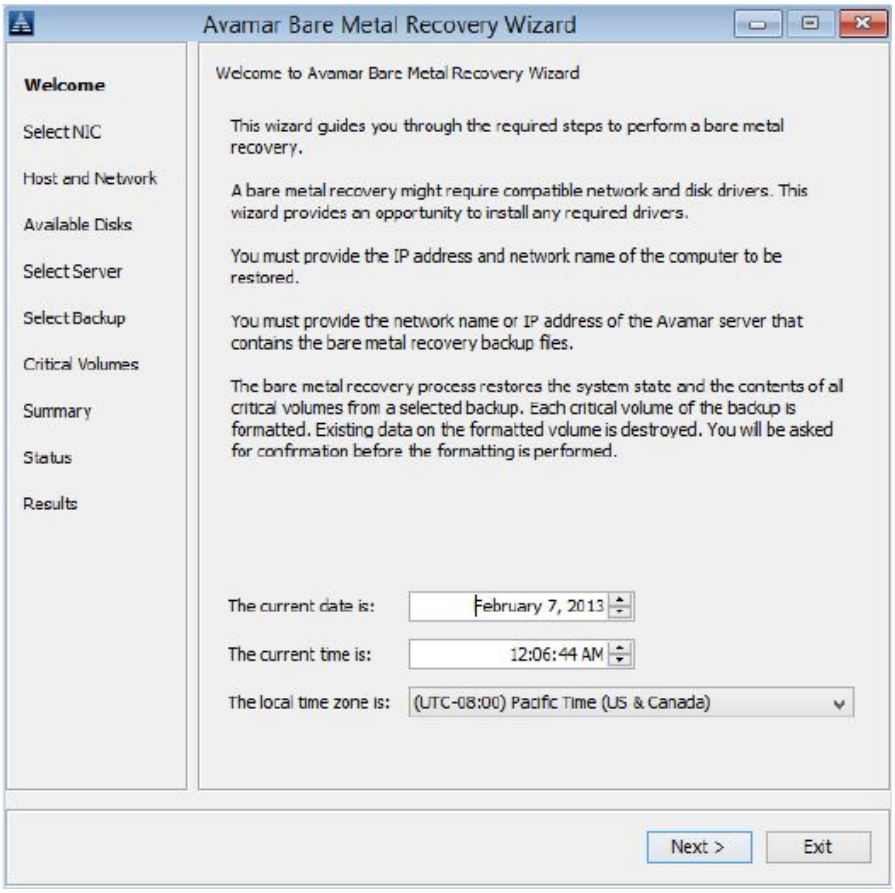

Figure 5. Avamar Bare Metal Recovery Wizard

2. Specify the date, time, and time zone for the computer. The default value is the system date and time of the local computer. You may need to change the date and time if the system date and time are incorrect, or if you are restoring to a computer in a different time zone.

   NOTE: If you specify an invalid date or time, then the wizard attempts to correct the date or time. For example, if you incorrectly specify November 31, then the wizard corrects the date to December 1. Verify that the date and time are correct before you go to the next page of the wizard.

3. If a DNS server is not available on the network, manually edit the hosts file for the WinPE ISO to include the Avamar server:
   a. Return to the WinPE command line.
   b. Open the hosts file, for example `X:\Windows\System32\Drivers\etc\hosts`, and add the IP address and hostname for the Avamar server.
   c. If you exit the wizard, restart the wizard from the *`drive`*`:\Program Files\avs\wizard` folder. For example:

      `X:\Program Files\avs\wizard> javaw -jar WinPEWizard.jar`

d. When the **Avamar Bare Metal Recovery Wizard** appears, click **Next**.

4. On the **Select Network Interface** page, select the network interface for communication with the Avamar server during the restore.

   If the required NIC driver is not in the list, click Load Driver to browse to the required driver.

   NOTE: The driver must not require a restart. The WinPE environment loads only in memory, and changes are not persistent across a restart. If a restart prompt appears, you may be able to ignore the prompt. Most NIC drivers are plug-and-play.

5. Click **Next**.
   The **Configure Hostname and Network** page appears.
6. Type the hostname of the target computer in the **Host name** box.
7. Type the domain name for the host in the **DNS domain** box.

   If the host resides in a workgroup instead of a domain, leave the box blank.
8. Select the tab for **IPv4** or **IPv6** to configure the network to communicate with the Avamar server during BMR.
9. In the **TCP/IP Address** section, specify the IP address information using one of the following methods:
   - If host IP addresses are assigned automatically, then select **Obtain an IP address automatically (DHCP)**. The network must be configured to support DHCP.
   - If the IP address of the target host is static, select **Use the following IP address**, and then specify the IP address and subnet mask (IPv4) or subnet prefix length (IPv6).
   - If the Avamar server is on a different subnet, then type the default gateway in the **Default gateway** box. Otherwise, leave the box blank.
10. In the **DNS Server** section, specify the DNS server information:
    - If you added the Avamar server hostname and IP address to the hosts file, then leave the default values in the **DNS Server** section.
    - If the DNS server name is assigned automatically, select **Obtain DNS server address automatically**.
    - If the DNS server IP address is static, select **Use the following DNS server addresses**, and then specify the IP address of the DNS server and the alternate DNS server, if the environment includes an alternate DNS server.
11. Click **Next**.
    The **Available Disks** page appears with a list of all detected local disks. The list contains all physical disks, but not all physical disks in the list may be critical disks.

    NOTE: If SAN disks appear twice in the list, then WinPE can see multiple paths to the LUN. Temporarily modify the switch configuration so there is only one path to the LUN. You can restore the multi-path configuration after the BMR.
12. If the wizard fails to detect a disk, click **Load Driver** to browse to the driver for the disk, and then click **Refresh List** to update the list of disks.
13. Click **Next**.
14. On the **Select Avamar Server** page, specify the Avamar server settings:
    a. In the **Avamar Server** box, type the fully qualified domain name (FQDN) or IP address for the Avamar server.
    b. In the **Avamar User Name** box, type the name of an Avamar Administrator or Backup/Restore Operator account.

       NOTE: The Avamar Bare Metal Recovery Wizard does not support Legacy LDAP/LDAP map.

    c. In the **Avamar Password** box, type the password for the Avamar administrator account.
    d. In the **Avamar Domain** box, type the domain for the Avamar administrator account. The default value of a forward slash (/) specifies the root domain.
    e. In the **Avamar Account** box, type the pathname of the client on the Avamar server, including the domain and client name.

       For example, if the hostname.example.com client is in the `/clients/MyGroup` domain, then type:

       `/clients/MyGroup/hostname.example.com`

       If you are recovering from a computer in a replication domain, then specify the full client path in the `/REPLICATE` domain, such as:

       `/REPLICATE/orig_server/clients/hostname.example.com`
15. Click **Next**.
16. On the **Select System Recovery Backup** page, select the system backup to restore to the host. System backups appear in the list in descending order from the most recent to the oldest.
17. Click **Next**.

    The **Critical Volumes to Restore** page lists volumes to restore to the host.

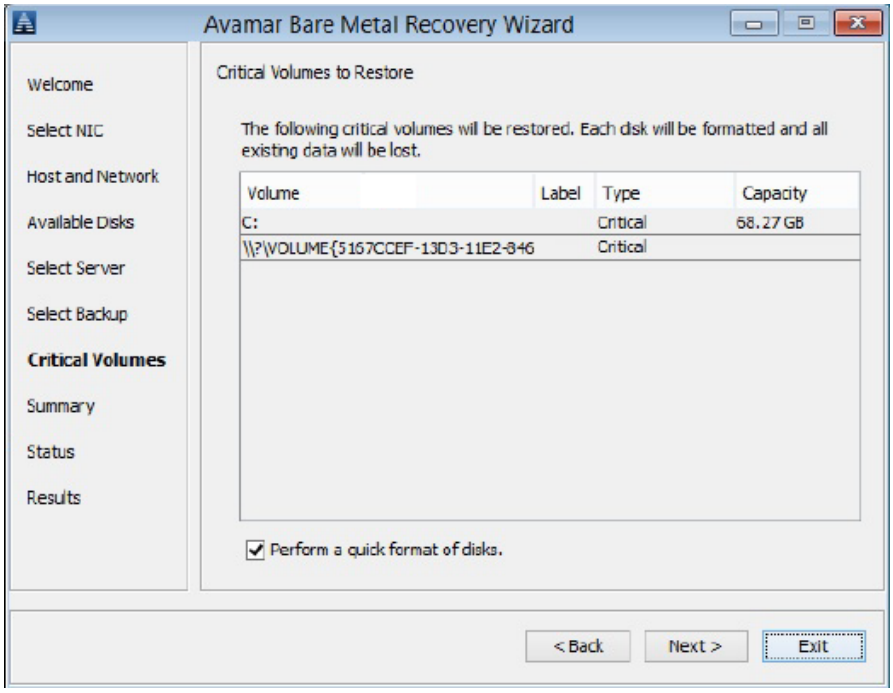

Figure 6. Avamar Bare Metal Recovery Wizard

NOTE: Not all critical volumes appear with a drive letter. For example, the System Reserved partition on Windows Server 2008 R2 and UEFI partitions do not appear with a drive letter. In the preceding figure of the **Critical Volumes to Restore** page, the second volume name, `\\?\VOLUME...`, indicates that a drive letter is not assigned to the volume.

18. (Optional) To perform a quick format of the volumes instead of a full format, select **Perform a quick format of disks**.

    The restore process reformats critical volumes. This process formats non-critical volumes only if the disk signature is different, for example, if you replaced the disk. A quick format is faster than a full format, but a quick format does not verify each sector on the volume.

    NOTE: The BMR process does not recover data on a non-critical volume even if the non-critical volume is reformatted. To recover non-critical volumes, use Avamar Administrator to restore the file system after the wizard completes and the host restarts.

19. Click **Next**.
    The **System Recovery Summary** page lists the selected recovery options.
20. If the original computer was a physical machine and you are restoring to a virtual machine, select the **Physical to Virtual (P2V)** checkbox.

    NOTE: After the P2V restore completes and the machine restarts, you must manually reconfigure networking on the restored machine. The networking reconfiguration is necessary because NIC cards on the new virtual machine are different than the NIC cards on the original physical machine.

21. (Optional) Specify non-default recovery options, which are generally used for troubleshooting with assistance from Customer Support:
    a. Click **Options**.
       The **Non-Default Recover Options** page appears.
    b. Type the options and values in the **Additional Options** box.
    c. Click **OK**.
22. Complete the wizard pages:
    - If you are testing the wizard and do not want to perform a restore, click **Exit** on the **System Recovery Summary** page.

      The wizard closes, and a command prompt appears. You can shut down the computer.
    - To continue with the restore, click **Restore** on the **System Recovery Summary** page.

      A confirmation message appears.

NOTE: All data is lost on volumes that are reformatted.

When the recovery completes, the **System Recovery Results** page appears.

23. (Optional) To view the Avamar Bare Metal Recovery Wizard log files for troubleshooting, click **View Logs**.

    The log files are also stored on the Avamar server. If required, you can restore the log files from the Avamar server after you close the wizard. Viewing Avamar Bare Metal Recovery Wizard log files on page 63 provides instructions.

24. Perform one of the following tasks:
    - If this option is an authoritative restore of Active Directory, click **Exit** to exit the wizard, and then perform the steps in Active Directory recovery on page 63.
    - If you are restoring a Windows Server 2008 or Windows 7 client computer, restart the computer to return to normal operation, and then review Performing post-BMR tasks on page 62.

Performing post-BMR tasks

About this task

After the BMR completes and the system restarts, perform these required tasks:

- If a critical volume was compressed, then reenable compression.
- If you performed a P2V restore, then perform the following steps:
  1. Install VMware tools.
  2. Remove disabled devices.
  3. Configure the virtual NIC.
- Check the disk and volume configuration of the host. All disks and volumes likely appear as they did on the original system. However, if disk signatures do not match the original disks, then non-critical disks may be offline or not mounted. Use Microsoft Disk Manager to bring the disks online or mount the disks. After the disks are online, restart the host to reassign disk drive letters, or assign drive letters to non-critical disks as necessary. Non-critical volumes that are accessed by mount points may have similar issues.
- If required, import disks so that they are known by Windows Storage Manager.
- If required, use the Avamar Plug-in for the Windows File System to restore application data or non-critical disks. If you use an application plug-in, such as the Avamar Plug-in for Exchange VSS or the Avamar Plug-in for SQL Server, then use the application plug-in to restore the application data.
- When a Windows Server 2008 or Windows Server 2019, 2016, or 2012 role uses SQL Server instances instead of the WID, then perform the SQL Server disaster recovery steps:

  1. Complete the SQL Server disaster recovery procedure that Microsoft recommends in the MSDN article “Recovering from a Disaster.”
  2. Install the Avamar Plug-in for SQL Server.
  3. Use the Avamar Plug-in for SQL Server to restore the system databases.
  4. Use the Avamar Plug-in for SQL Server to restore the SQL Server instances.

  The *Avamar for SQL Server User Guide* provides instructions for installing and using the SQL Server plug-in.

- The Active Directory RMS service depends on the Microsoft Message Queuing Service (MSMQ). If an Active Directory service does not restart after BMR, verify whether MSMQ is a service on the system and determine if the service restarted correctly. You can also check the Windows Event Application Log to see if MSMQ recorded Event 2078, `The Message Queuing service cannot start.`

  If MSMQ is enabled but did not start on reboot, then restart the service, as described is the “Event ID 2078 -- Message Queuing Logging and Checkpoint Events” article on the Microsoft TechNet website.

- When you mount a volume on a parent volume and the mounted volume becomes a critical volume, then the BMR restores only the critical volume. Use the Avamar Plug-in for the Windows File System to restore the parent volume after the BMR of the critical volume. File System Restore on page 49 provides instructions.

Recovering encrypted files, folders, and volumes

Avamar supports the backup, recovery, and BMR of files and folders encrypted with Windows Encrypting File System (EFS), and volumes encrypted with BitLocker.

BMR restores EFS encryption attributes on files, but not encryption attributes on folders. After BMR, additional steps are required to fully enable encryption:

- BitLocker services may be running but the BitLocker volumes must be re-encrypted
- EFS encryption attributes on folders must be re-enabled

Consult Microsoft documentation for steps to encrypt with EFS and BitLocker. For EFS, search Help and Support for "Encrypt or decrypt a folder or file." For BitLocker, search Microsoft TechNet for "Windows BitLocker Drive Encryption Step-by-Step Guide." Check with your IT department or Windows administrator for corporate policies governing the use of encryption features on your computer.

Viewing Avamar Bare Metal Recovery Wizard log files

The Avamar Bare Metal Recovery Wizard log files are stored on the Avamar server. You can view the log files when you run the wizard. If required, you also can restore the log files from the Avamar server after you close the wizard.

About this task

Complete the following procedure to restore the Avamar Bare Metal Recovery Wizard log files.

Steps

1. In Avamar Administrator, click the **Backup & Restore** tab.
   The **Backup, Restore and Manage** window appears.
2. In the domain tree, select the domain for the client.
3. In the clients tree, select the client that you used for the recovery.
4. Click the **Restore** tab.
5. Click the **By Date** tab.
6. Select the recovery date from the calendar. This recovery process saved the logs to the Avamar server on that date.
7. In the **Backups** table, select **Offline Restore Logs**.
8. In the **Contents of Backup** pane, expand the WinPE system drive to the location of the Offline Restore Logs backup, `drive:\Program Files\avs\var`.
9. Select the checkboxes next to the `avvss.log`, `winpe_av_support.log`, and `WinPE_Wizard.log` files.
10. Select **Actions** > **Restore Now**.
    The **Restore Options** dialog box appears.
11. Follow the steps in Restoring to a different location on page 51 to restore the log files to a location from which you can open them.

Active Directory recovery

Complete the following procedure to perform system recovery of Windows Server Active Directory.

About this task

NOTE: If the last System State backup of the Windows Server 2008 client is more recent than the last Active Directory backup, then you may want to use the System State backup for the BMR. Using the System State backup to restore Active Directory on page 66 provides details.

Steps

1. Configure the client to boot into Directory Services Restore Mode (DSRM). Booting the client into Directory Services Restore Mode on page 64 provides instructions.
2. Restore Active Directory from the System State backup. Restoring Active Directory on page 65 provides instructions.

Booting the client into Directory Services Restore Mode

Use one of the following methods to boot the client into Directory Services Restore Mode (DSRM) so that you can restore the Active Directory backup.

Manually booting into DSRM with System Configuration

You can use Microsoft Windows System Configuration to manually set the computer to boot directly into DSRM the next time that the computer boots.

Steps

1. From the **Start Menu**, select **Administrative Tools** > **System Configuration**.

   The **System Configuration** dialog box appears.

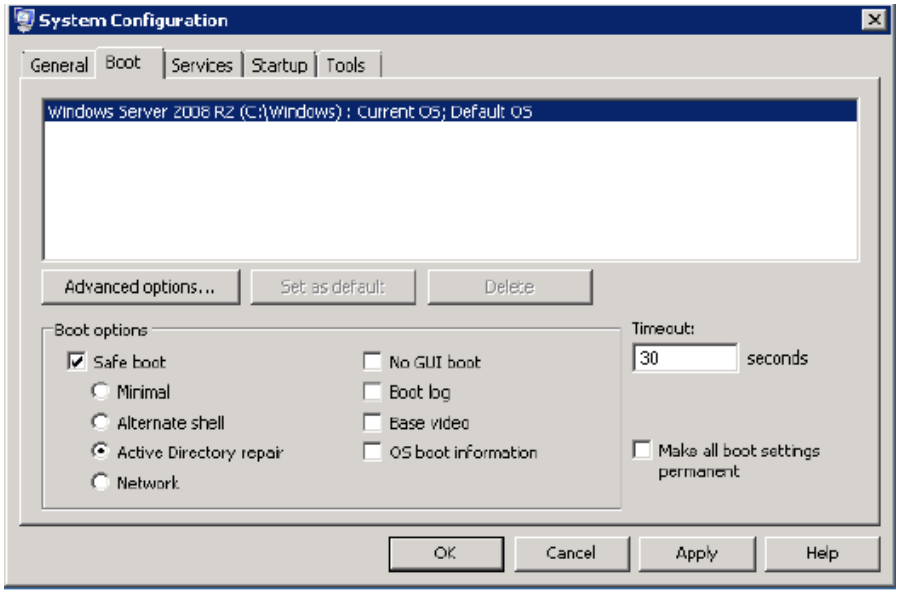

   Figure 7. System Configuration window

2. Click the **Boot** tab.
3. Select the **Safe boot** checkbox, and then select **Active Directory repair**.
4. Click **OK**.
5. Reboot the computer into DSRM.

Adding a Windows bootloader entry for DSRM

About this task

You can add an entry to the Windows bootloader so that the option to boot into DSRM is always available when you start the computer.

Steps

1. Open a command prompt.
2. Copy the DSRM entry from the Boot Configuration Data (BCD) to a GUID by typing the following command:

   `bcdedit /copy {default} /d "Directory Services Restore Mode"`

   A message similar to the following example appears:

   `The entry was successfully copied to {00000000-0000-0000-0000-000000000000}`

   where *00000000-0000-0000-0000-000000000000* is the GUID of the new entry.

3. Set the safeboot option for the bootloader entry in the BCD by typing the following command:

```
bcdedit /set {00000000-0000-0000-0000-000000000000} safeboot dsrepair
```

where *00000000-0000-0000-0000-000000000000* is the GUID.

4. Reboot the computer, and select the option to boot into DSRM.

Restoring Active Directory

About this task

> **NOTE:** If you perform a non-disaster-recovery backup to recover Active Directory data, clear the **Create Disaster Recovery Backup** checkbox before you perform the backup. If you do not clear the checkbox, Avamar cannot recover the individual Active Directory file.

Steps

1. In Avamar Administrator, click the **Backup & Restore** tab.
   The **Backup, Restore and Manage** window appears.
2. In the domain tree, select the domain for the client.
3. From the list of clients, select the original client.
4. Click the **Restore** tab.
5. Click the **By Date** tab.
6. In the calendar, select the date on which the backup occurred.
7. Select the backup from the **Backups** table to the right of the calendar.
8. In the lower-left pane, expand the tree and select **System State** > **BootableSystemState**.
9. In the lower-right pane, select the checkbox next to **Active Directory**.
10. Select **Actions** > **Restore Now**.
    The **Restore Options** dialog box appears.
11. If you are restoring from a replicate server, select the client for the restore:
    a. Select **Restore everything to a different location**.
    b. In the **Restore Destination Client** dialog box, select **Browse**.
    c. In the **Browse for Restore Client** dialog box, select the client and click **OK**.
    d. In the **Items Marked for Restore** dialog box, click **Set Destination**.
       The **Set Destination** dialog box appears.
    e. Click **Browse**.
    f. In the **Browse for File, Folder, or Directory** dialog box, expand **Windows VSS** and select **System State** as shown in the following figure.
    g. Click **OK** to return to the **Restore Options** dialog box.
12. Click **More Options**.
    The **Restore Command Line Options** dialog box appears.
13. Click **More** to view the attribute data entry fields.
14. In the **Enter Attribute** box, type the following value:
    `--[avvss]allow_partial_system_state`
15. In the **Enter Attribute Value** box, type the following value:
    `true`

    > **NOTE:** Use the `--[avvss]allow_partial_system_state` option only for an online restore of Active Directory. Never use this option for an online restore of other System State components.

16. Click **+** to add the attribute.
17. Click **OK** on the **Restore Command Line Options** dialog box.
18. Click **OK** on the **Restore Options** dialog box.
    The **Restore Request** dialog box indicates that the restore started.
19. Click **Close**.
20. Wait for the restore to complete.
21. Select whether to perform a nonauthoritative restore or an authoritative restore:

- To perform a nonauthoritative restore, restart the client normally after the Active Directory restore completes. Other domain controllers replicate changes to the client after the restart.
- To perform an authoritative restore, continue to the next step. In the authoritative restore, the data from the restored domain controller replicates to other domain controllers.

22. For an authoritative restore only, open a command prompt window and use the `ntdsutil` utility to mark objects for the authoritative restore.

    The objects replicate to other domain controllers during the authoritative restore. In addition, replication partners do not overwrite the replicated objects.

    You can mark a single user object, an entire user subtree, containers, or the entire database.

    You can use Microsoft ADSIEdit to display Distinguished Names for AD objects.

    For example, the following series of commands marks a user with an OU of `CN=Test User,CN=Users,DC=svr1,DC=mydomain,DC=com` for an authoritative restore:

    ```
    ntdsutil
    activate instance NTDS
    authoritative restore
    restore object
    "CN=Test User,CN=Users,DC=svr1,DC=mydomain,DC=com"
    quit
    quit
    ```

    The Microsoft documentation provides details on using the `ntdsutil` utility for an authoritative restore.

23. If you used Windows System Configuration to configure the system to boot into DSRM, use Windows System Configuration again and clear the **Safe boot** checkbox to enable the system to return to normal booting.
24. Restart the client.

Using the System State backup to restore Active Directory

If the last System State backup of the Windows Server client is more recent than the last Active Directory backup, then you may want to use the System State backup for the BMR.

Steps

1. Perform the steps in BMR of Windows clients on page 55 to perform the BMR.
   After you exit the Avamar Bare Metal Recovery Wizard, the WinPE command prompt appears.
2. Perform the steps in Booting the client into Directory Services Restore Mode on page 64 to boot into DSRM.
3. Open a command prompt window and use the ntdsutil utility to mark objects for an authoritative restore. Restoring Active Directory on page 65 provides instructions.
4. If you used Windows System Configuration to configure the system to boot into DSRM, use Windows System Configuration again to configure the system to return to normal booting.
5. Restart the client.

BMR of Windows clusters

You can restore individual nodes in a Windows Server cluster, if the cluster is otherwise functional. This type of restore is a nonauthoritative restore, because cluster replication updates the nodes with existing cluster settings when the nodes rejoin the cluster. Restoring a cluster node on page 66 provides instructions.

To perform BMR of the full cluster, use the steps in Restoring an entire cluster on page 67. This type of restore may be necessary if the entire cluster is down, or if there is a problem with the cluster database.

Restoring a cluster node

Steps

1. Ensure that at least one node in the cluster is still functioning.
2. Shut down the damaged node.

3. Perform an offline BMR of the node. BMR of Windows clients on page 55 provides instructions.
4. Reboot the node.
5. If you applied any Windows service packs or hotfixes to the cluster node after the backup, then reapply the service packs or hotfixes to the restored cluster node to bring the node to the same service pack level as the other nodes in the cluster.
6. If required, rejoin the node to the cluster.

   NOTE: BMR restores the System State and critical disks on cluster nodes. After BMR, use the Windows File System plug-in to restore file system data, non-critical disks, and critical disks on shared storage. Also, use application plug-ins to restore application data.

Restoring an entire cluster

Steps

1. Shut down all cluster nodes.
2. Restore one node in the cluster:
   a. Perform an offline BMR of the node. BMR of Windows clients on page 55 provides instructions.
   b. Reboot the node.
   c. If required, restart the cluster service.
3. Restore the remaining nodes in the cluster:

   NOTE: You must perform an offline BMR of all nodes. If you reboot a node by using the old system disk before you restore the node, then the cluster information from that node replaces the information on all nodes.

   a. Perform an offline BMR of each node. BMR of Windows clients on page 55 provides instructions.
   b. Reboot each node.
   c. If you applied any Windows service packs or hotfixes to the cluster nodes after the backup, then reapply the service packs or hotfixes to the restored cluster nodes to bring them to the same service pack level.
   d. If required, rejoin the nodes to the cluster.

   NOTE: BMR restores the System State and critical disks on the cluster nodes. After BMR, use the Windows File System plug-in to restore file system data, non-critical disks, and critical disks on shared storage. Also, use application plug-ins to restore application data.

A

Plug-in Options

Topics:

- How to set plug-in options
- Windows File System plug-in backup options
- Windows File System plug-in restore options
- Windows VSS plug-in backup options
- Windows VSS plug-in restore options
- Windows Cluster File Server plug-in backup options
- Windows Cluster File Server plug-in restore options

How to set plug-in options

Plug-in options enable you to control specific actions for on-demand backups, restores, and scheduled backups. The available plug-in options depend on the operation type and plug-in type.

Specify plug-in options in the AUI for on-demand backup or restore wizards, or when a dataset for a scheduled backup is created. Set plug-in options with the graphical user interface (GUI) controls (text boxes, check boxes, radio buttons, and so forth). Type an option and its value in the **Key** and **Value** fields.

NOTE: The Avamar software does not check or validate the information that is typed in the **Show Free Form** section of the **More Options** pane. The values in the **Key** and **Value** fields override settings that are specified with the GUI controls for the options.

Windows File System plug-in backup options

Plug-in options enable you to control backup functionality that is specific to the Avamar Plug-in for the Windows File System. You can specify plug-in options for on-demand and scheduled backups.

The following table lists options that are available for the Windows File System plug-in when you perform an on-demand backup or when you configure a dataset for scheduled backups.

Table 9. Windows File System plug-in backup options

Option	Description
Back up Natively Attached Virtual Hard Disks	Backs up natively attached virtual hard disks.
Perform a Windows Optimized Backup of a Windows Deduplicated volume	Specifies whether to back up files in either optimized or unoptimized state on Windows deduplicated volumes on Windows Server 2019, 2016, or 2012. If you back up files in an optimized state, then you can restore the files in either an optimized or unoptimized state. You can only restore files from a Windows deduplicated volume to the original location or to another Windows Server 2019, 2016, or 2012 computer with Windows deduplicated volumes.
Store backup on Data Domain system	To store the backup on a Data Domain system instead of the Avamar server, select the checkbox and then select the Data Domain system from the list. **NOTE:** To enable this option, add a Data Domain system to the Avamar configuration. The *Avamar and Data Domain System Integration Guide* provides instructions.

Table 9. Windows File System plug-in backup options (continued)

Option	Description
Encryption method to Data Domain system	Specifies the encryption method for data transfer between the client and the Data Domain system during the backup.
Backup label	Assigns this descriptive label to the backup.
Logging Options	
List backup contents	Specifies how much information about the backup contents to include in the log files. Select one of the following values: ● No file listing ● List file names ● List files and dates
Informational message level	Specifies how many informational messages to include in the log files. Select one of the following values: ● No informationals — Suppress all informational messages but include errors and warnings. ● Some informationals — Include some informational messages. ● Many informationals — Include additional status information. ● All informationals — Include all informational messages, errors, and warnings.
Report advanced statistics	Includes advanced timing and deduplication statistics in the log files.
Enable debugging messages	Writes maximum information to the log files. The backup process generates very large log files.
File System Traversal	
Do not traverse any mounts	Prevents traversal of mount points during the backup.
Traverse fixed-disk mounts	The backup traverses only fixed-disk file system mount points.
Traverse fixed-disk and remote network mounts	The backup traverses both fixed-disk and NFS network mount points.
File System Traversal Overrides	
Force traversal of specified file system type(s)	Specifies the file system types to traverse during the backup. Use a comma-separated list to specify multiple file system types, for example, nfs, ext2, jfs, xfs.
Force non-traversal of specified file system type(s)	Specifies the file system types that the backup does not traverse. Use a comma-separated list to specify multiple file system types, for example, nfs, ext2, jfs, xfs.
Pre-Script	
Run user-defined script at beginning of backup	Runs a script at the beginning of the backup. The script must be located in the `C:\Program Files\avs\etc\scripts` folder and must have a `.bat`, `.js`, or `.vbs` file name extension.
Abort backup if script fails	Stops the backup if the script returns a non-zero status code.
Script After Freeze	
Run user-defined script after volumes have been frozen	Runs a script after volumes have been frozen. The script must be located in the `C:\Program Files\avs\etc\scripts` folder and must have a `.bat`, `.js`, or `.vbs` file name extension.
Abort backup if script fails	Stops the backup if the script returns a non-zero status code.
Post-script	
Run user-defined script at end of backup	Runs a script at the end of the backup. The script must be located in the `C:\Program Files\avs\etc\scripts` folder and must have a `.bat`, `.js`, or `.vbs` file name extension.

Table 9. Windows File System plug-in backup options (continued)

Option	Description
Exit process with script failure exitcode	If selected, `avtar` exits with the exit code of the script instead of a standard `avtar` exit code.
Volume Freezing Options	
Method to freeze volumes	Uses one of the following values: • Best • Microsoft VSS • OTM • None
OTM freezewait: File activity quiescent time	OTM only: Number of seconds that volumes must be quiescent to establish a freeze.
OTM freezetimeout: Maximum time to wait when trying to freeze volume(s)	OTM only: Maximum number of seconds to wait for volumes to freeze.
OTM freezecachesize: Size in MBs of OTM transaction cache	OTM only: Size of the disk transaction cache. A negative value is a fraction of used disk space. For example, -50 is 1/50th or 2% of used disk space.
OTM freezecachedir: Folder to use for the OTM transaction cache	OTM only: Pathname of the folder for the OTM transaction cache. The default pathname is `C:\Program Files\avs\var`.
Freeze exclude devices	Comma-separated list of devices to exclude from volume freezing, for example, `\Device\mydevice\*`.
Freeze exclude volumes	Comma-separated list of volume names to exclude from freezing, for example, `C:`.
Client Cache Options	
Check client-side caches and report inconsistencies	Performs a validation check of the client-side cache with the Avamar server instead of a backup.
Check and repair client-side caches	Performs a validation check and repairs inconsistences with the client-side cache instead of performing a backup.
Maximum client file cache size (MBs)	Specifies the maximum client file cache size in MB. A negative value indicates a fraction of RAM. For example, -8 specifies that no more than 1/8th of the physical RAM will be allocated to the client file cache.
Maximum client hash cache size (MBs)	Specifies the maximum client hash cache size in MB. A negative value indicates a fraction of RAM. For example, -8 specifies that no more than 1/8th of the physical RAM will be allocated to the client hash cache.
Advanced Options	
Client-side flag file	Specifies the pathname of an option file on the client that contains additional option settings.
Network rate throttle (Mbps)	Reduces network usage to a rate in megabits/second, for example, 0 = unrestricted, 50% of a T1 = 0.772.
Directly connect to all server nodes	Establishes multiple connections to the server, which can improve backup performance in certain circumstances.
Use Last Access Time to detect ACL-only changes	Forces a rescan of any files in which the Access Time changed since the previous backup.
Run as user name	Specifies the username for running the plug-in on the client you are backing up.
Quota limit per backup	
Hard limit size (MBs)	Specify the hard limit size of a backup. If the size of the backup source exceeds the hard limit, the backup fails.

Table 9. Windows File System plug-in backup options (continued)

Option	Description
Soft limit size (MBs)	Specify the soft limit size of a backup. If the size of the backup source exceeds the soft limit, the backup succeeds with a warning. If you specify both the soft and hard limit size, ensure that the soft limit size is smaller than the hard limit size.

Windows File System plug-in restore options

Plug-in options enable you to control restore functionality that is specific to the Avamar Plug-in for the Windows File System. You set restore options manually from the **Restore Command Line Options** dialog box.

The following table lists restore options for the Avamar Plug-in for the Windows File System.

Table 10. Windows File System plug-in restore options

Option	Description
Overwrite existing files	If the file you are restoring already exists, this option specifies whether the restore overwrites the file. Select one of the following values: ● Never — Do not overwrite the file. ● Always — Overwrite the file. ● Generate New Name — Restore the file with a different name. ● If Modified — Restore the file if the existing file has a different timestamp. ● If Newer — Restore the file if the existing file is newer.
Restoration of open files	If the file you are restoring already exists and is open, this option specifies whether the restore overwrites the file. Select one of the following values: ● Never — Never restore. ● Defer until reboot — Replace the open file after a restart. ● Generate New Name — Restore the file with a different name. ● If newer defer until reboot — Replace the open file after a restart if the restored file is newer than the open file.
Restore the system profile	Restores the Windows system profile.
Restore Reparse Points as	Specifies how to restore reparse points. Select one of the following values: ● Links and targets—Restore both the links and the targets for the links. ● Links only—Restore only the links, not the targets. ● Links as files and folders (don't create links)—Restore the links as files or folders, depending on the type of reparse point. If the reparse point points to a folder, then the reparse point restores as a folder. If the reparse point points to a file, then the reparse point restores as a file
Encryption method from Data Domain system	Specifies the encryption method for data transfer from the Data Domain system to the client during the restore.
Logging	
List backup contents	Specifies how much information about the backup contents to include in the log files. Select one of the following values: ● No file listing ● List file names ● List files and dates
Informational message level	Specifies how many informational messages to include in the log files. Select one of the following values: ● No informationals — Suppress all informational messages but include errors and warnings.

Table 10. Windows File System plug-in restore options (continued)

Option	Description
	• Some informationals — Include some informational messages. • Many informationals — Include additional status information. • All informationals — Include all informational messages, errors, and warnings.
Report advanced statistics	Includes advanced timing and deduplication statistics in the log files.
Enable debugging messages	Writes maximum information to the log files. The restore process generates very large log files.
Pre-Script	
Run user-defined script at beginning of restore	Runs a script at the beginning of the restore. The script must be located in the `C:\Program Files\avs\etc\scripts` folder and must have a `.bat`, `.js`, or `.vbs` file name extension.
Abort restore if script fails	Stops the restore if the script returns a non-zero status code.
Post-Script	
Run user-defined script at end of restore	Runs a script at the end of the restore. The script must be located in the `C:\Program Files\avs\etc\scripts` folder and must have a `.bat`, `.js`, or `.vbs` file name extension.
Exit process with script failure exitcode	If selected, `avtar` exits with the exit code of the script instead of a standard `avtar` exit code.
Client Cache and Repair Options	
Check client-side caches and report inconsistencies	Performs a validation check of the client-side cache with the Avamar server instead of a restore.
Check and repair client-side caches	Performs a validation check and repairs inconsistences with the client-side cache instead of performing a restore.
Rebuild client-side caches from most recent backup	Re-creates the client-side file cache by using the contents of the last backup, but does not restore data.
Advanced Options	
Do not descend into subdirectories	Restores only the top-level folder, not any subfolders.
Recreate original path beneath target directory	Re-creates the original path names of files and folders in the target folder. For example, if you restore `F:\Temp\MyFile.txt` to `C:\Temp` and you select this option, then the full path name of the restored file is `C:\Temp\F\Temp\MyFile.txt`.
Restore hidden folders and files	Restores folders and files with the HIDDEN attribute.
Restore folders and files with SYSTEM attribute	Restores folders and files with the SYSTEM attribute.
Directly connect to all server nodes	Establishes multiple connections to the server, which can improve restore performance in certain circumstances.
Run as user name	Specifies the username for running the plug-in on the client to which you are restoring.

Windows VSS plug-in backup options

Plug-in options enable you to control backup functionality that is specific to the Avamar Plug-in for the Windows VSS. You can specify plug-in options for on-demand and scheduled backups.

The following table lists options that are available for the Avamar Plug-in for Windows VSS when you perform an on-demand backup in Avamar Administrator or when you configure a dataset for scheduled backups.

Table 11. Windows VSS plug-in backup options

Option	Description
Backup type	Sets the backup level. Full is the only supported backup level for the Avamar Plug-in for Windows VSS.
Backup label	Assigns this descriptive label to the backup.
Create Disaster Recovery Backup	Specifies whether to perform a BMR backup with the System State backup. Select the checkbox to perform a BMR backup except when you are backing up Active Directory data. If you clear the checkbox, the backup is not valid for BMR.
When backup detects missing Windows System State files, complete the backup successfully without exceptions	Specifies whether to ignore missing Windows System State files during the backup. Select the checkbox to report the missing files as warnings and allow the backup to complete successfully. Clear the checkbox to report the missing files as errors and to allow the backup to complete with exceptions.
Ignore third-party services when identifying critical volumes. Applies to Windows 8 (or later).	Specifies whether to include or exclude a noncritical disk on Windows Server 2012 or Windows 8 when a service or application is installed on the disk and causes the disk to become critical. Select the checkbox to exclude the noncritical disk from the backup. Clear the checkbox to include the noncritical disk in the backup.
Store backup on Data Domain system	To store the backup on a Data Domain system instead of the Avamar server, select the checkbox and then select the Data Domain system from the list. **NOTE:** To enable this option, add a Data Domain system to the Avamar configuration. The *Avamar and Data Domain System Integration Guide* provides instructions.
Encryption method to Data Domain system	Specifies the encryption method for data transfer between the client and the Data Domain system during the backup.
Advanced Options	
Temporary directory for the plug-in	Temporary folder.
Enable debugging messages	Writes maximum information to the log files. The backup process generates very large log files.
Command line flags[a]	
`--exclude-non-critical-dynamic-disks={true | false}`	Set this option to true to exclude noncritical disks from system restore preparation to avoid reformatting the disks. The default value is `true`. According to Microsoft Best Practices, if any dynamic disk is critical, then the entire dynamic disk pack should be treated as critical and included in the backup. If you specify this option, then you may need to use the `--exclude_non_critical_disks` option during the offline disaster recovery.
`--vss-ignore-missing-windows- files={true | false}`	Set this option to `true` to ignore any missing VSS writer files during the backup. Backups may fail if VSS writers contain files that do not exist on the computer.

a. Specify command line flags using the **Enter Attribute** and **Enter Attribute Value** fields on the **Backup Command Line Options** dialog box or the **Options** tab for a dataset. You can also specify command line flags in the `avvss.cmd` file in the `C:\Program Files\avs\var` folder.

Windows VSS plug-in restore options

Plug-in options enable you to control restore functionality that is specific to the Avamar Plug-in for Windows VSS. You set restore options manually from the **Restore Command Line Options** dialog box.

The following table lists options are available when you perform a restore using the Avamar Plug-in for Windows VSS.

Table 12. Windows VSS plug-in restore options

Option	Description
Encryption method from Data Domain system	Specifies the encryption method for data transfer from the Data Domain system to the client during the restore.
Advanced Options	
Temporary directory for the plug-in	Temporary folder.
Enable debugging messages	Writes maximum information to the log files. The restore process generates very large log files.
Command line flags	
`--allow_partial_system_state`	Allows partial System State to be restored online. Supported only for Active Directory. Specify this option by using the **Enter Attribute** and **Enter Attribute Value** fields on the **Restore Command Line Options** dialog box.
`--exclude-non-critical-disks= {true | false}`	Excludes noncritical disks from disaster recovery preparation so that the disks do not reformat. Set this flag to `false` to work around a disaster recovery failure from configuration changes, such as changes to the dynamic disk configuration. Use this flag only during offline disaster recovery. You can specify this option in the Avamar Bare Metal Recovery Wizard by clicking **Options** on the **System Recovery Summary** page.

Windows Cluster File Server plug-in backup options

Plug-in options enable you to control backup functionality that is specific to the Windows Cluster File Server plug-in. You can specify plug-in options for on-demand and scheduled backups.

The following table lists options that are available for the Windows Cluster File Server plug-in when you perform an on-demand backup or when you configure a dataset for scheduled backups.

Table 13. Windows Cluster File Server plug-in backup options

Option	Description
Store backup on Data Domain system	To store the backup on a Data Domain system instead of the Avamar server, select the checkbox and then select the Data Domain system from the list. **NOTE:** To enable this option, add a Data Domain system to the Avamar configuration. The *Avamar and Data Domain System Integration Guide* provides instructions.
Encryption method to Data Domain system	Specifies the encryption method for data transfer between the client and the Data Domain system during the backup.
Advanced Options	
Enable debugging messages	Writes maximum information to the log files. The backup process generates very large log files.

Windows Cluster File Server plug-in restore options

Plug-in options enable you to control restore functionality that is specific to the Windows Cluster File Server plug-in. You set restore options manually from the **Restore Command Line Options** dialog box.

The following table lists the options that are available when you perform a restore by using the Windows Cluster File Server plug-in.

Table 14. Windows Cluster File Server plug-in restore options

Option	Description
Encryption method from Data Domain system	Specifies the encryption method for data transfer from the Data Domain system to the client during the restore.
Advanced Options	
Enable debugging messages	Writes maximum information to the log files. The restore process generates very large log files.

B

Command Line Interface

Topics:

- Overview of the Windows VSS plug-in CLI
- Command reference
- CLI examples

Overview of the Windows VSS plug-in CLI

The Windows VSS plug-in enables you to use a command line interface (CLI) with the avvss command instead of Avamar Administrator to back up and restore Windows VSS data. You can use the CLI from all operating systems that the plug-in_name supports.

When you use the CLI to perform a backup, you specify the options for the Windows VSS plug-in binary on the command line. The plug-in interacts with the `avtar` process to write backup data to or read backup data from the Avamar server or a Data Domain system.

The `avvss` binary is available in the `C:\Program Files\avs\bin` folder, where `C:\Program Files\avs` is the Avamar client installation folder.

To use the CLI, open a command prompt and change directory to the bin folder of the Avamar client installation folder. Then type the command at the command prompt.

Command reference

The `avvss` command enables you to perform a System State backup. You can specify command options to control the backup behavior.

Synopsis

```
avvss --operation=backup [options]
```

Operations

The only available operation for the `avvss` command is backup. The backup operation performs an on-demand System State backup. To specify the operation, use the `--operation=backup` option on the `avvss` command line.

Options

The options that you specify with the `avvss` command control the backup behavior.

Common options

The following common options are available for the `avvss` command.

Table 15. Common options for the avvss command

Option	Description
`--label=`*label*	Specifies a label for the backup.
`--version`	Displays the build version of the Windows VSS plug-in.

Account options

The following account options are available for the `avvss` command.

Table 16. Account options for the avvss command

Option	Description
`--account=`*domain/client* `--path=`*domain/client* `--acnt=`*domain/client*	Specifies the Avamar domain and the client computer for the backup.
`--ap=`*password* `--password=`*password* `--pswd=`*password*	Specifies the password for the account that you specify with the `--id` option.
`--id=`*user@domain/client*	Required. Specifies the Avamar username for authentication, where: ● *user* is the username. ● *domain* is the Avamar domain for the user. ● *client* is the name of the client computer.
`--server=`*Avamar_server*	Required. Specifies the hostname or IP address of the Avamar server.

Logging options

The following logging options are available for the `avvss` command.

Table 17. Logging options for the avvss command

Option	Description
`--informationals=`*n*	Sets the informational level for status messages, where *n* is a number, such as 0, 1, 2, and so on.
`--log` `--logfile=`*file*	Specifies the full path name and file name of the `avvss` plug-in log file. **NOTE:** The Activity Monitor in Avamar Administrator displays only `avtar` logs for backups with the command line interface. To create a plug-in log for CLI activities, you must specify the `--log` or `--logfile` option on the command line.
`--noinformationals`	Disables all status messages.
`--nostdout`	Disables output to standard output (stdout). However, if you supply `--log` or `--logfile=`*file*, then output still goes to the log file.
`--nowarnings`	Disables warning messages.
`--quiet`	Suppresses all debugging messages.

Table 17. Logging options for the avvss command (continued)

Option	Description
--verbose=*n* --v	Enables all messages, including status and warning messages. To set the level of verbosity, specify --verbose=*n*, where *n* is the level of verbosity.

Backup options

The following avvss options are available for the backup operation.

Table 18. Backup options for the avvss command

Option	Description
--ddr={true | false}	Specify true to store the backup on a Data Domain system instead of the Avamar server.
--ddr-index=*n*	Specifies the index number of the Data Domain system. The index is the order in which the Data Domain systems were added to the Avamar server configuration.
--dr-cluster-disk-warning={true | false}	Specify true to complete the backup with exceptions if components are on cluster disks. Specify false to disable the warning. The default value is true.
--dr-exclude-win32-services-files={true | false}	Specify true to ignore third-party services when identifying critical volumes. This feature is supported if the System Writer contains the Win32 Services Files component.
--exclude-non-critical-dynamic-disks={true | false}	Specify true to exclude noncritical disks from system restore preparation to avoid reformatting the disks. The default value is true. According to Microsoft Best Practices, if any dynamic disk is critical, then the entire dynamic disk pack should be treated as critical and included in the backup. If you specify this option, then you may need to use the --exclude_non_critical_disks option during the offline disaster recovery.
--expires={*days* | *timestamp*}	Specifies backup expiration as a number of *days* from today or an absolute *timestamp*.
--perform_dr_backup={true | false}	Specifies whether to create a BMR backup. The default value is true.
--retention-type=*type* --retentiontype=*type*	Assigns advanced retention to the backup. Specify one of the following values: • none — Do not explicitly assign any retention type to this backup. That is, treat the backup as a normal on-demand backup. • daily — Explicitly designate this backup as a daily backup. • weekly — Explicitly designate this backup as a weekly backup. • monthly — Explicitly designate this backup as a monthly backup. • yearly — Explicitly designate this backup as a yearly backup.
--vss-ignore-missing-windows-files={true | false}	Set this option to true to ignore any missing VSS writer files during the backup. Backups fail if VSS writers contain files that do not exist on the computer.

Help option

To view command line help output, use the `--help` option. The `--help` option displays a list of available operations and options for the `avvss` command. You can view all help output for `avvss`, or only the options for a specific operation.

The following command displays all help output for the `avvss` command:

```
avvss --help
```

Specifying command line options

The method that you use to specify options for the `avvss` command depends on the complexity of the command value and the frequency with which you use the options.

Type options directly on the command line when you perform command line operations on an occasional basis or you are using a limited set of simple options. Use a command file, option file, or environment variables when you frequently perform command line operations or you are using a complex set of options.

The following methods are available for specifying options for the `avvss` command:

- Type the individual options on the command line.
- List the options in the `avvss.cmd` file, which is located in the `C:\Program Files\avs\var` folder, where `C:\Program Files\avs` is the Avamar client installation folder. List each option on its own line, as shown in the following example:

  ```
  --debug
  --logfile=avamarclient.log
  --verbose=5
  ```

CLI examples

These command examples illustrate how to use options to perform different types of backups with the `avvss` command.

The following command performs a backup of System State and critical disks for BMR of the computer named `Windows1` in the `Clients` domain, stores the backup on the Avamar server with an IP address of `12.34.56.78`, and writes `avvss` logging information to the `avvss.log` file in the `C:\Program Files\avs\var` folder:

```
avvss --operation=backup --server=12.34.56.78 --id=AvamarAdmin
--password=password -path=/Clients/Windows1
--perform_dr_backup=true --log=C:\Program Files\avs\var\avvss.log
```

The following command performs a non-BMR backup for restoring Active Directory online of the computer named `Windows1` in the `Clients` domain, stores the backup on the Avamar server with an IP address of `12.34.56.78`, and writes `avvss` logging information to the `avvss.log` file in the `C:\Program Files\avs\var` folder:

```
avvss --operation=backup --server=12.34.56.78 --id=AvamarAdmin
--password=password -path=/Clients/Windows1
--perform_dr_backup=false --log=C:\Program Files\avs\var\avvss.log
```

The following command performs a Windows VSS backup of the computer named `Windows1` in the `Clients` domain, and stores the backup on the Data Domain system indexed as 1 on the Avamar server with the path `red-avsn100.corp.example.com`:

```
avvss --server=red-avsn100.corp.example.com --id=MCUser@/ --ap=pwd
--path=/clients/Windows1 --ddr=true --ddr-index=1
--operation=backup
```

C

Troubleshooting

Topics:

- Log files
- Backup problems and solutions
- Restore problems and solutions
- Bare metal recovery problems and solutions

Log files

During backup and restore operations, log files are created for troubleshooting problems.

There are log files in both Avamar and Windows that can be useful in troubleshooting restores. An example of a useful Windows log file for monitoring Windows-related activities is the Windows Application Event log. Check Windows documentation for information about viewing the Windows Application Event log.

Avamar log files

Avamar log files capture Avamar, VSS, and service events and are available in the `var` directory, whic h is typically `C:\Program Files\avs\var`. The following table describes each log file.

Table 19. Avamar log files

Log file	Description	Command file	Debugging flags
`avagent.log`	Avamar agent log	`avagent.cmd`	`--debug`
`MOD-`*`timestamp`*`-3001-Windows.log` `MOD-1379109227779-3001-Windows.log`	Contains information about the Windows File System plug-in backup. ● On demand backups run from Avamar Administrator are prefixed with `MOD`. ● Command line backups are prefixed with `COD`. ● Scheduled backups are prefixed with the group name. ● `3001-Windows` at the end of the file name identifies it as a Windows VSS plug-in log file.	`avtar.cmd`	`--debug` `--verbose`

`COD-`*`timestamp`*`-3015-VSS.log`
`MOD-`*`timestamp`*`-3015-VSS.log`
`group-timestamp``-3015-VSS.log`
	Contains information about the Windows VSS plug-in backup.
	● On demand backups run from Avamar Administrator are prefixed with `MOD`.
	● Command line backups are prefixed with `COD`.
		`avvss.cmd`	`--debug`
			`--verbose`

Table 19. Avamar log files (continued)

Log file	Description	Command file	Debugging flags
	• Scheduled backups are prefixed with the group name. • `3015-VSS` at the end of the file name identifies it as a Windows VSS plug-in log file.		

`COD-`*`group`*`-3036-winclusterfs.log`
`MOD-`*`group`*`-3036-winclusterfs.log`
`group``-`*`group`*`-3036-winclusterfs.log`
	Contains information about the Windows Cluster File Server backup.
	• On demand backups run from Avamar Administrator are prefixed with `MOD`.
	• Command line backups are prefixed with `COD`.
	• Scheduled backups are prefixed with the group name.
	• `3036-winclusterfs` at the end of the file name identifies it as a Windows Cluster File Server plug-in log file.
		`avwinclusterfs.cmd`
		`avtar.cmd`
			`--debug`
			`--verbose`

`WinPEWizard.log`	Contains information about the pages loaded or displayed by the wizard.	None	
`avvss.log`	Contains information about BMR operations.	`avvss.cmd`	`--debug` `--verbose`
`winpe_av_support.log`	Contains information about Avamar-related data displayed in the wizard. For example, the list of BMR backups.	None	
`winpe_os_support.log`	Contains information about the WinPE environment. For example, NIC settings, available disks, or registry values.	None	

Generating log files

You can generate log files by creating a command file with debugging flags before you perform a backup or restore operation.

1. Create the `.cmd` file in the `var` directory, which is typically `C:\Program Files\avs\var`.
2. In the `.cmd` file, add debugging flags as listed in Avamar log files on page 80.

Backup problems and solutions

The following sections describe common backup problems and solutions.

System State backups of offline dynamic critical disks fail in Windows Server 2008

A known problem with the ASR writer on Windows Server 2008 may cause System State backups of offline dynamic critical disks to fail. The failure may occur with an ASR writer error code (0x800423f4). If this error occurs, set the dynamic critical disks online, and rerun the backup. The error does not occur on Windows Server 2008 R2, or Windows Server 2012 or later.

Backup fails when Windows deletes the Shadow Volume during backup

Windows sometimes deletes the Shadow Volume although Avamar is running the backup service. This is a known Microsoft issue that affects all backup products. When this backup failure occurs, the Windows Event Viewer System log may contain an error similar to the following:

```
The shadow copies of volume H: were deleted because the shadow copy storage could not grow
in time. Consider reducing the IO load on the system or choose a shadow copy storage volume
that is not being shadow copied.
```

If this issue occurs, try one or both of the following workarounds:

- Leave more space on the drive.
- Perform the backup when the drive is less busy.

System State backups of dynamic critical volumes on storage spaces are not supported

System State backups of dynamic critical volumes on storage spaces in Windows Server 2012 fail. When storage spaces are on a dynamic critical disk, a System State backup cannot detect the storage spaces because of API incompatibility. The backup includes the storage spaces because they contain critical volumes, but you cannot restore the configuration for the storage spaces during BMR.

Use the following guidelines to ensure that backups protect both storage spaces and dynamic critical volumes:

- Do not create storage spaces on dynamic disks.
- Place dynamic critical volumes on basic disks.

Windows Server Core 2012 backup completes with exceptions

An exception may occur when backing up Windows Server Core 2012, with an error similar to the following:

```
Unable to open directory "c:\Users\Default\PrintHood" (code 3: The system cannot find the
path specified).
```

To avoid the exception, add an exclude attribute and value in the plug-in options for the backup.

System State backups exclude Windows Server 2012 deduplicated volumes

Do not perform a System State backup of Windows Server 2012 deduplicated volumes if the volumes are critical volumes. Microsoft does not recommend making a deduplicated volume a critical volume, and Avamar excludes deduplicated volumes from VSS backups.

Restore problems and solutions

The following topics describe common restore problems and solutions.

Restoring over corrupted SIS links

An SIS volume restore may fail because the SIS Groveler service is running and prevents the restore process from correctly restoring some files. In the log file for the restore, the error for the failed restore appears similar to the following example, and the size of the restored file is set to zero:

```
Error "avtar Error <5737>: I/O error: Unable to write(4) "path to file" (code 38: Reached
the end of the file)."
```

To correct this error, delete the corrupted SIS links from the restored server, and then use Avamar to select and restore the links from the backup set.

Restore of folders or files with many Access Control Entries may fail

Restore of folders or files with 1,820 Access Control Entries (ACEs) may fail with one of the following error messages:

- `File '%s' is unable to be restored due to Avamar having improper permissions to restore the security information for that file. If you wish to restore the file, either provide proper rights to Avamar or use the --ignoreacls flag.`
- `I/O error: Unable to BackupWrite(4) ...(code 87: The parameter is incorrect).`

Perform one of the following steps to resolve this issue:

- Add the `--ignoreacls` attribute to the **Restore Command Line Options** dialog box before you restore.
- Remove ACEs from the folders and the files so that there are fewer than 1,820 entries.

Office XML files may need special flag to restore correctly

If you back up an Office XML file (.docx, .xlsx), then an error message similar to the following may appear when you restore the file and open it:

```
Excel cannot open the file 'Spreadsheet.xlsx' because the file format or file extension
is not valid...
```

or

```
The Office Open XML file filename.docx cannot be opened because there are problems with
the contents, Word found unreadable content in documentfile.docx. Do you want to recover
the contents of this document? If you trust the source, click Yes.
```

If you open the file anyway, the file may be empty or unusable. When this occurs, rerun the restore using the `--deflateofficexml=false` flag in the **Restore Command Line Options** dialog box. After restore, when you open the file you may get the same MS Office error message, but if you click **OK** to open the file anyway, the file should open correctly.

Bare metal recovery problems and solutions

The following topics describe common BMR problems and solutions.

UEFI machine fails to boot after BMR

After a successful BMR, a UEFI machine may fail to boot. This can occur if the EFI boot manager does not have a valid Boot Order entry. For example, if the Boot Order was deleted or the BMR was performed to different hardware. In those situations the operating system recreates the Boot Order entry when the machine is rebooted, and it may not use the same path.

To correct this issue, use the computer manufacturer instructions to set the EFI boot order. Follow the instructions for setting the `Boot from a file` option. The target file path is `EFI\Microsoft\Boot\bootmgfw.efi`.

Re-creating 8dot3 file names after BMR may fail

During BMR, 8dot3 names are temporarily enabled for all volumes. This allows 8dot3 names to be created when files are restored. After the machine is rebooted, the system uses the following registry value to determine where 8dot3 names are created:

`HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation`

The default value of `NtfsDisable8dot3NameCreation` is `per-volume` for volumes that have 8dot3 names enabled by `fsutil`. The "NtfsDisable8dot3NameCreation" article on the Microsoft TechNet website provides details.

After BMR, decide how to manage 8dot3 names.

Windows Server 2008, Windows 7, and later do not automatically create 8dot3 file names. This is because it is increasingly unlikely that 8dot3 names are actually needed. The use of 8dot3 names also has significant performance penalties for the file system. Microsoft recommends using the `fsutil` program to strip 8dot3 names from the file system if they are not needed.

You can enable 8dot3 file names on all volumes or on a per volume basis using the `fsutil` program. The values to enable or disable 8dot3 for all volumes or on a per volume basis are described in the "Fsutil 8dot3name" article on the Microsoft TechNet website.

Glossary

Special Terms

A

activation
The process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

See also client activation

Active Directory
A directory service for network administration and security in Microsoft Windows domain networks.

administrator
Person who normally installs, configures, and maintains software on network computers, and who adds users and defines user privileges.

avagent
The name of the *client agent* process.

Avamar Administrator
A graphical management console software application that is used to remotely administer an Avamar system from a supported Windows or Linux client computer.

Avamar Bare Metal Recovery Wizard
A wizard that uses the Automated System Recovery (ASR) writer and the customized WinPE ISO image to restore critical volumes and other components of the bootable System State as part of BMR for Windows computers.

Avamar client
A computer or workstation that runs Avamar software and accesses the Avamar server over a network connection. Avamar client software comprises a *client agent* and one or more *plug-ins*.

avtar
The Avamar process that performs backups and restores.

B

backup
A point-in-time copy of client data that can be restored as individual files, selected data, or as an entire backup.

backup policy
In the AUI, a backup policy specifies a dataset, schedule, and retention settings that are applied to a client or a group of clients. A backup policy must contain at least one Avamar client. If the backup policy contains two or more clients, the clients must belong to the same Avamar domain. You can override backup policy settings at the client level.

bare metal recovery (BMR)
The process of restoring data from a backup to recover a computer system from “bare metal,” or without previously installed software or operating system.

browse
The process of viewing data that is available for backup on a client computer or restore from the Avamar server.

C

client activation
The process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

See also activation

client agent
A platform-specific software process that runs on the client and communicates with the Management Console Server (MCS) and with any plug-ins installed on that client.

client registration
The process of establishing an identity with the Avamar server. When Avamar recognizes the client, it assigns a unique client ID (CID), which it passes back to the client during *client activation*.

See also registration

cluster
Two or more independent network servers, usually with exact copies of the same software and data, that operate and appear to clients as if they are a single unit. A cluster configuration enables work to be shifted from one server to another, providing high availability, which allows application services to continue despite most hardware or software failures.

Cluster Configuration Tool
Avamar configuration wizard to configure the cluster client.

clustered file server for general use
A type of clustered file server where the file server, and therefore all shares associated with the file server, are online on one node at a time. File shares associated with this type of clustered file server are called clustered file shares.

cluster shared volumes (CSV)
A shared disk that contains an NTFS volume that is accessible for read and write operations by all nodes in the cluster.

critical disk
A volume on a Windows computer that stores system components. Also called a critical volume.

D

database
A collection of data arranged for ease and speed of update, search, and retrieval by computer software.

Data Domain system
Disk-based deduplication appliances and gateways that provide data protection and disaster recovery (DR) in the enterprise environment.

dataset
A policy that defines a set of files, directories, and file systems for each supported platform that are included or excluded in backups across a group of clients. A dataset is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

Directory Services Restore Mode (DSRM)
A mode on a Microsoft Windows domain controller to take the Active Directory on that computer offline so that you can restore Active Directory data.

disaster recovery
Recovery from any disruptive situation, such as hardware failure or software corruption, in which ordinary data recovery procedures are not sufficient to restore a system and its data to normal day-to-day operations. A disaster recovery can be a *bare metal recovery*.

DNS
Domain Name Server. A dynamic and distributed directory service for assigning domain names to specific IP addresses.

domain
A feature in Avamar Administrator that is used to organize large numbers of clients into named areas of control and management.

F

federated cluster client
A virtual client that runs on a cluster node in a Windows Server cluster. The federated cluster client communicates with the Avamar server to perform backups and restores of file system data in the cluster, regardless of which node is managing the data at the time of the operation.

file system
Software interface used to save, retrieve, and manage files on storage media by providing directory structures, data transfer methods, and file association.

G

group
A level of organization in Avamar Administrator for one or more Avamar clients. All clients in an Avamar group use the same group policies, which include the *dataset*, *schedule*, and *retention policy*.

group policy
In Avamar Administration, a group policy is defined as a *dataset*, *schedule*, and *retention policy* for all clients in an Avamar group.

L

LAN
Local Area Network.

M

MCS
Management console server. The server subsystem that provides centralized administration (scheduling, monitoring, and management) for the Avamar server. The MCS also runs the server-side processes used by *Avamar Administrator*.

metadata
Data about the backup, including information about the original database files, the backup types, the date and time of the backup, and other information necessary for restore.

N

nonauthoritative restore
A type of Active Directory restore where Active Directory replication partners can return a domain controller to a known state. When you restart the domain controller after you restore the computer from a backup, other domain controllers replicate changes made after the backup.

noncritical disk
A volume on a Windows computer that stores only file system data. System components are not installed on the volume. Also called a noncritical volume.

P

plug-in
Avamar client software that recognizes a particular kind of data resident on that client.

plug-in options
Options that you specify during backup or restore to control backup or restore functionality.

policy
A set of rules for client backups that can be named and applied to multiple groups. Groups have dataset, schedule, and retention policies.

proxy cluster client
A virtual client that runs on a single node (the proxy node) in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster. The proxy cluster client communicates with the Avamar server to perform backups and restores of file system data on shared storage in the cluster, regardless of which node is managing the file system data at the time of the operation.

proxy node
The node with the proxy cluster client in a Windows Server 2019, 2016, or 2012 for SOFS or SMB cluster.

R

redirected restore
The process of restoring a backup to a different location than the original location where the backup occurred.

registration
The process of establishing an identity with the Avamar server. When Avamar recognizes the client, it assigns a unique client ID (CID), which it passes back to the client during *client activation*.

See also client registration

restore
An operation that retrieves one or more file systems, directories, files, or data objects from a backup and writes the data to a designated location.

retention
The time setting to automatically delete backups on an Avamar server. Retention can be set to permanent for backups that should not be deleted from an Avamar server. Retention is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

S

Scale-Out File Server (SOFS)
A type of clustered file server in Windows Server 2019, 2016, or 2012 that allows you to store server application data, such as Hyper-V virtual machine files, on file shares. All file shares are online on all nodes simultaneously. File shares associated with this type of clustered file server are called scale-out file shares.

schedule
The ability to control the frequency and the start and end time each day for backups of clients in a group. A schedule is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

Server Core
A scaled-back version of Windows Server, where no Windows Explorer shell is installed. All configuration and maintenance occurs by using a command prompt, or by connecting to the computer remotely through Microsoft Management Console.

Server Message Block (SMB) 3.0 file shares
File shares that use the SMB 3.0 protocol. You can store shared file system data on SMB 3.0 file shares in a Windows Server 2019, 2016, or 2012 cluster.

shadow copy volume
A backup volume that VSS creates.

System State
A term that refers to key configuration files for the Windows operating system, such as boot files and the Windows Registry.

V

virtual hard disk (VHD) files

The file format for a virtual hard disk, the storage medium for a virtual machine. VHD files can reside on any storage topology that the management operating system can access, including external devices, storage area networks, and network-attached storage. The file name extension is `.vhd`.

virtual machine (VM)
A computer that is a software implementation of a computer. Virtual machines are used to run different operating systems at the same time on one physical computer. Each operating system runs in its own isolated execution environment.

Volume Shadow Copy Service (VSS)

A technology in Microsoft Windows that enables manual or automatic backup copies or snapshots of data, even if there is a lock on the data, on a specific volume at a specific point-in-time over regular intervals. VSS is implemented as a Windows service called the Volume Shadow Copy service.

VSS provider
A software or hardware-based process that links the VSS service to the storage hardware and creates a snapshot for backup on the storage hardware. Avamar supports only software providers.

VSS requestor
A backup application that uses the VSS API to request the services of VSS to create and manage shadow copy volumes. The Avamar Plug-in for Windows VSS is a VSS requestor.

VSS writer
A process that provides metadata about application data for backup, and specific methods for correctly handling components and applications during backup and restore. A VSS writer also identifies the type of application or service in the backup, such as System Boot or System Services. A VSS writer does not play a role in backing up the file system.

W

Windows Deployment Services (WDS)
A Microsoft technology for network-based installation of Windows operating systems.

WinPE ISO image
A Windows Preinstallation Environment (WinPE) package with a lightweight version of Windows used for the deployment of workstations and servers or troubleshooting an operating system while it is offline. The Avamar WinPE ISO images are used for BMR.