Dell EMC Avamar and Data Domain System

Integration Guide

18.1

Dell Inc.

January 2021
Rev. 04

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.

Contents

Figures

Tables

Preface

As part of an effort to improve the product lines, revisions of the software and hardware are periodically released. 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 the 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, configure, administer, and use a Data Domain system as a backup target for Avamar.

Audience

The information in this guide is primarily intended for system administrators who are responsible for configuring and maintaining Avamar and Data Domain system integrated backups.

Revision history

The following table presents the revision history of this document:

Revision	Date	Description
04	January, 2021	Updated the "Preintegration requirements" section.
03	April, 2020	Updated the "Preintegration requirements" section.
02	January, 2020	Added references to Azure and vCenter to Data Domain Cloud Disaster Recovery.
01	July, 2018	GA release of Avamar 18.1

Related documentation

The following Avamar publications provide additional information:

- *Avamar Compatibility and Interoperability Matrix*
- *Avamar Release Notes*
- *Avamar Administration Guide*
- *Avamar Operational Best Practices Guide*
- *Avamar Product Security Guide*
- *Avamar for IBM DB2 User Guide*
- *Avamar for Exchange VSS User Guide*
- *Avamar for Hyper-V VSS 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*
- *Avamar for Oracle User Guide*
- *Avamar for VMware User Guide*

The following Data Domain publications also provide additional information:

- *DD OS Release Notes*
- *DD OS Initial Configuration Guide*
- *DD OS Administration Guide*
- *DD OS Command Reference*
- *DD OS Command Reference Guide*
- *Data Domain Hardware Guide*
- *Avamar Installation and Administration Guide*
- The Data Domain installation and setup guides for each of the supported platforms (for example, DD610, DD690, DD880, and so forth)

Typographical conventions

These type style conventions are used in this document.

Table 1. 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 **Find a Product by Name** box.
3. Select the product from the list that appears.
4. Click the arrow next to the **Find a Product by Name** box.
5. (Optional) Add the product to the **My Products** list by clicking **Add to My Saved Products** in the upper right corner of the **Support by Product** 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, esgxxxxxx) 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.

Please include the following information:

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

1

Introduction

Topics:

Overview

Data Domain deduplication storage systems are typically implemented to back up large high-change rate databases. Avamar is typically implemented to back up file systems, virtual servers, low change rate databases, remote offices, and desktop/laptops.

Avamar and Data Domain system integration enables:

- Data Domain systems to be a backup target for Avamar backups
- One or more Data Domain systems to be managed by Avamar
- Avamar clients to use the Data Domain Boost software option to use Data Domain systems as backup targets
- The target destination of backup data, which is set by a backup policy at the dataset level
- Transparent user interaction to the backup target (Avamar or Data Domain)

Architecture

A Data Domain system performs deduplication through DD OS software. Avamar source based deduplication to a Data Domain system is facilitated through the use of the Data Domain Boost library.

Avamar uses the DD Boost library through API-based integration to access and manipulate directories, files, and so forth. contained on the Data Domain File System. The DD Boost API gives Avamar visibility into some of the properties and capabilities of the Data Domain system. This enables Avamar to control backup images stored on Data Domain systems. It also enables Avamar to manage maintenance activities and to control replication to remote Data Domain systems.

DD Boost is installed on the backup clients and on the Avamar utility node, an Avamar single node system, or on Avamar Virtual Edition.

The following figure depicts a high-level architecture of the combined Avamar and Data Domain solution. With Avamar and Data Domain integration you can specify whether specific datasets in an Avamar backup policy target an Avamar server or a Data Domain system.

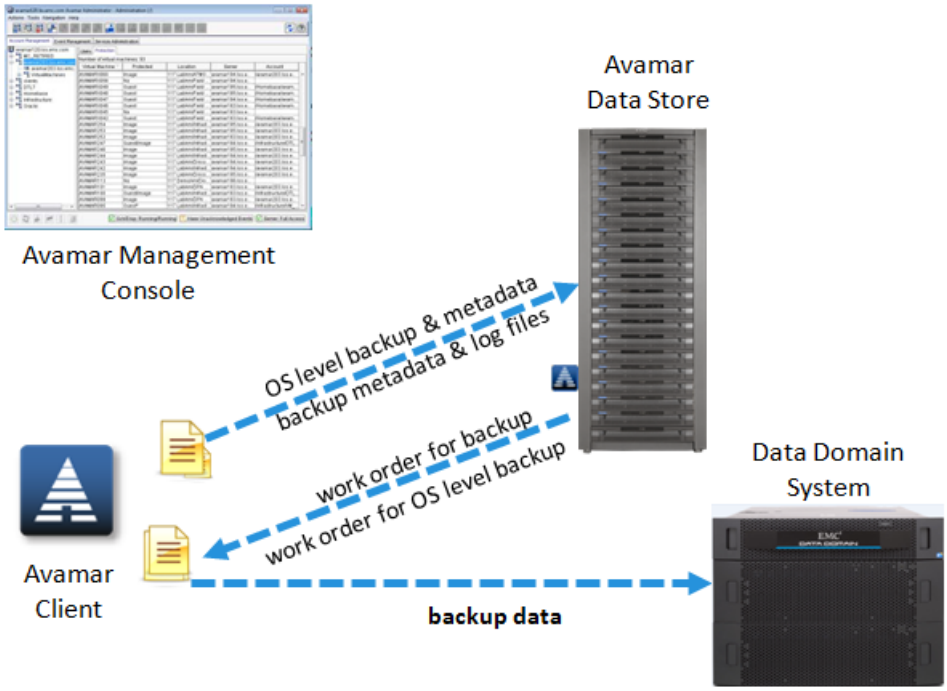

Figure 1. Avamar and Data Domain system workflow

When you select an Avamar server as the backup target, the Avamar client on each host performs deduplication segment processing. Data and metadata are stored on the Avamar server.

When you select a Data Domain system as the backup target, backup data is transferred to the Data Domain system. The related metadata generated by the Avamar client software is simultaneously sent to the Avamar server for storage. The metadata enables the Avamar management system to perform restore operations directly from the Data Domain system without first going through the Avamar server.

Mixed backups are supported. It is possible for backup data to span across both Avamar servers and a Data Domain system within the same backup.

If backups are taking place to an Avamar server and then redirected to a Data Domain system, then subsequent incremental backup data will be stored on the Data Domain system while the original backup data is on the Avamar server. This can affect capacity because the forever incremental data will continue to reside on the Avamar Server while newer/changed incremental data will be stored on the Data Domain system.

If the desire is to ensure backup data is released on the Avamar server and redirect backups to data domain then a full backup must be initiated. This can be achieved by renaming the client's cache files, which will force a full backup. However, note that this will cause the client's backup to take longer and impact performance since it will have to create a new backup on the Data Domain system. If there are many clients that need to be moved to a Data Domain system then it is recommended that the initial full backup be scheduled appropriately to avoid performance impact.

If the capacity on the Avamar server is not a concern then the system will continue to backup incremental backup data to the Data Domain but its prior backup data will remain on the Avamar server until it expires. The implication is that when the last backup containing parts on the Avamar server expire, then a full backup will trigger. The recommendation is to perform a controlled and/or scheduled full backup.

Backup

During a backup, the Avamar server sends a backup request to the Avamar client. If the backup request includes the option to use a Data Domain system as the target, backup data is stored on the Data Domain system. Metadata is stored on the Avamar server.

The following topics provide details on the types of backup data that Avamar can store on a Data Domain system.

Up-to-date client compatibility information is available in the *Avamar Compatibility and Interoperability Matrix* on Avamar Support at http://compatibilityguide.emc.com:8080/CompGuideApp/.

Avamar checkpoints

You can store checkpoints for a single-node Avamar server or Avamar Virtual Edition (AVE) on a Data Domain system. Checkpoints are system-wide backups taken for disaster recovery of the Avamar server.

Storage of checkpoints on a Data Domain system is useful in environments that do not have a secondary Avamar server and Data Domain system for replication, or in environments where most backups are stored on a Data Domain system.

Restore of checkpoints from a Data Domain system requires assistance from Avamar Professional Services.

Restore

The process of data recovery from a Data Domain system is transparent to the backup administrator. The backup administrator uses the same Avamar recovery processes that are native to current Avamar implementations.

VMware Instant Access

VMware Instant Access is used to boot up a lost or corrupted virtual machine almost instantaneously from an image backup stored on a Data Domain system.

VMware Instant Access works through the following processes:

1. A virtual machine image backup is staged to a temporary location on the Data Domain system.
2. The virtual machine is exported to a temporary location as a secure NFS share.
3. The share is mounted as a NFS datastore on an ESX/ESXi host.

When VMware Instant Access is used, the virtual machine should not be left running on the Data Domain system for extended periods. When the virtual machine runs on the Data Domain system, performance might degrade because of the workflow. To move the VMware Instant Access from the Data Domain system to the VMware production environment, use vMotion.

An alternative to VMware Instant Access is to restore a virtual machine back to the production environment. The Avamar software's ability to leverage Changed Block Tracking (CBT) dramatically speeds the recovery process. If performance problems occur when an ISP is hosting multitenancy clients, you can disable instant access. In the `datadomain` section of `mcserver.xml`, set `ddr_instant_access_enabled` to `false`.

The *Avamar for VMware User Guide* provides additional information on VMware Instant Access.

Replication

Replication between primary and replica Data Domain systems is integrated into the Avamar management feature set. This is configured in Avamar Administrator through the Avamar replication policies applied to each dataset.

All typical Avamar replication scenarios are supported for datasets that use a Data Domain system as a target, including:

- Many-to-one, one-to-many, cascading replication
- Extension of data retention times
- Root-to-root

Monitoring and reporting

Avamar can collect and display data for health monitoring, system alerts, and capacity reporting on a Data Domain system by using Simple Network Management Protocol (SNMP).

This enables you to monitor Data Domain activities, events, capacity, and system status in the same way that you monitor activities, events, capacity, and system status for the Avamar server.

You can also run reports to analyze the system.

Security

The connection between the Avamar client and the Data Domain system is encrypted if you use Avamar 7.1 or later clients, Avamar 7.1 or later server(s) and DD OS 5.5.x or later. Previous versions of software do not support data encryption between the client and the Data Domain system. Backups from the Avamar client to the Avamar server are always compressed and encrypted by default.

Use caution when granting users access to the Data Domain system. A user should not be able to directly access the Data Domain system and manually delete data.

Token-based authentication

By using Data Domain Boost token-based authentication, Avamar establishes a secure connection to a Data Domain system running DDOS 5.7 or greater without passing user name and password information.

Two parameters control token-based authentication behavior:

- `use_ddr_auth_token`

  To enable token-based authentication, set the `use_ddr_auth_token` parameter in the `mcserver.xml` file on the Avamar server (`/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml`) to **`true`**. To disable token-based authentication, set `use_ddr_auth_token` to **`false`**. Restart the Management Console server after making this change.

  You can also set the amount of time that an authentication token is valid. Inside the `mcserver.xml` file, the parameter is set to 36000 seconds (10 hours) by default. Some backup and replication jobs, such as NDMP backups, might require a longer duration for the authentication token to remain valid.

- `extend-token-window-sec`

  This parameter controls the interval (in seconds) that is used to call the extend token before it expires. Customize this setting in the `ddrmaint.cmd` file on the Avamar server (`/usr/local/avamar/var/ddrmaint.cmd`). For example,

  `--extend-token-windows-sec=60`

  sets the interval to 60 seconds.

  NOTE: Always set this parameter with a shorter duration value than `ddr_auth_token_duration` to ensure that the token is refreshed before it expires.

  After you set the value for this parameter, restart the service:

  `ddrmaint-service restart`

Configuring a ddboost account for token-based authentication

To configure a ddboost account for token based authentication:

Steps

1. On the Data Domain system, log in as sysadmin and create a user with admin rights and assign the user as a ddboost user:
   a. **`user add newuser role admin`**
   b. **`ddboost user assign newuser`**

   where *newuser* is the user name for the new ddboost user.
2. In the Avamar Administrator, add a new or edit an existing Data Domain to connect with Avamar using the new ddboost user. Adding a Data Domain system on page 24 and Editing a Data Domain system on page 25 provide instructions for adding and editing Data Domain systems.
3. On the Data Domain system, log in as sysadmin and associate the new ddboost user with the Avamar mtree:

   ddboost storage-unit modify *storage-unit* user *newuser*

   where *storage-unit* is the mtree of the Avamar system, usually in a format like `avamar-1234567890`, and *newuser* is the user name for the new ddboost user.

Next steps

Perform a test backup to ensure that the configuration was successful.

SSH authentication for Data Domain systems

When an Avamar system stores backups on a Data Domain system, the Avamar Management Console Server (MCS) issues commands to the Data Domain system using the Secure Shell (SSH) protocol. This protocol provides a secure communication channel for remote command execution.

To permit remote command execution using SSH, Data Domain systems provide an SSH interface named DDSSH. The DDSSH interface requires authentication of the Avamar system. Authentication is accomplished by creating SSH private and public keys on the Avamar system and sharing the public key with the Data Domain system.

The following table describes the attributes of the SSH key pair used with Data Domain systems.

Table 2. Attributes of SSH key pair used with Data Domain systems

Attribute	Description
Bits	3072
Type of key	RSA
Passphrase	Empty
Public key file name	User specified

Providing SSH authentication to Data Domain systems

Enable Avamar Management Console Server (MCS) remote command execution on a Data Domain system by providing SSH authentication to the Data Domain system. To provide SSH authentication, create SSH private and public keys on the Avamar system and share the public key with the Data Domain system.

Prerequisites

Obtain the password of the sysadmin account on the Data Domain system.

Steps

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin.
     b. Load the admin OpenSSH key by typing:

     ```
     ssh-agent bash
     ssh-add ~admin/.ssh/admin_key
     ```

2. Change the current working directory to `/home/admin/.ssh` by typing:

   ```
   cd ~/.ssh
   ```

3. Use the system command `ssh-keygen` to generate an SSH key pair by typing:

   `ssh-keygen -b 3072 -t rsa -N "" -f` *DDR_KEY*

   where *DDR_KEY* is the user-specified base file name for the key pair.

4. Log in to the Data Domain system by typing:

   `ssh` *AVAMAR_USER*`@`*DD_SYSTEM*

   where:

   - *AVAMAR_USER* is the username assigned to the Avamar system on the Data Domain system.
   - *DD_SYSTEM* is the resolvable hostname or IP address of the Data Domain system.

5. Use `su` to elevate the user to sysadmin on the Data Domain system by typing:

   `su sysadmin`

6. Use the Data Domain command `adminaccess add ssh-keys` to open the keystore on the Data Domain system:

   `adminaccess add ssh-keys user` *AVAMAR_USER*

   where *AVAMAR_USER* is the username assigned to the Avamar system on the Data Domain system.

   The utility prompts for the key.

7. Paste the SSH public key of the Avamar system (*DDR_KEY.pub*) at this prompt, as follows:
   a. Open a second command shell on the utility node of the Avamar system and log in as admin.
   b. Output the contents of the SSH public key by typing:

      `cat ~/.ssh/`*DDR_KEY.pub*

      where *DDR_KEY.pub* is the user-specified file name for the public key.

   c. Select and copy the contents of the SSH public key.
   d. Return to the `adminaccess add ssh-keys` prompt in the first command shell window and paste the SSH public key contents at the prompt.

8. Complete the entry of the key by pressing **Ctrl+D** to send the end-of-transmission character.
   The utility adds the public key to the keystore on the Data Domain system.
9. Exit the sysadmin user and log out of the Data Domain system.
10. Log in to the Avamar utility node as root.
11. Change the current working directory to `/usr/local/avamar/lib`.
12. Copy the private key to the current working directory by typing:

    `cp /home/admin/.ssh/`*DDR_KEY* **`.`**

    where *DDR_KEY* is the user-specified file name for the private key.

13. Change the user and group ownership of the private key to the root user and the admin group by typing:

    `chown root:admin` *DDR_KEY*

    where *DDR_KEY* is the user-specified file name for the private key.

14. Change the permissions for the private key by typing:

    `chmod 440` *DDR_KEY*

    where *DDR_KEY* is the user-specified file name for the private key.

15. Modify the symmetric data-in-flight SSH traffic cipher to use a 128-bit key by typing:

    `ssh -c aes128-cbc` *host_name*`@`*domain_name*

    where:

    - *host_name* is the hostname of the Data Domain system.
    - *domain_name* is the domain name of the Data Domain system.

16. Test that you can log in to the Data Domain system without providing a password by typing:

    `ssh -i` *PATH/DDR_KEY AVAMAR_USER*`@`*DD_SYSTEM*

    where:

    - *PATH/DDR_KEY* is the path and file name of the private key.
    - *AVAMAR_USER* is the name of the Avamar user on the Data Domain system.
    - *DD_SYSTEM* is the resolvable hostname of the Data Domain system.

Data migration to an attached Data Domain system

You cannot migrate backup data directly from the Avamar server to an attached Data Domain system.

To start using the Data Domain system as the backup target for an Avamar client instead of the Avamar server, edit the dataset to use the Data Domain system. Start performing backups to the Data Domain system. When you change the backup target to the Data Domain system, you must perform a full backup.

After you successfully perform a backup to the Data Domain system, you can delete the earlier backups from the Avamar server. The *Avamar Administration Guide* provides details on how to delete backups.

2

Avamar and Data Domain System Integration

Topics:

Preintegration requirements

Ensure that the environment meets all system requirements before you integrate a Data Domain system with Avamar. The integration implies that you have installed the Avamar server and Data Domain systems, and configured them.

NOTE:

- Do not install, configure, or use the Data Domain Retention Lock because Avamar does not support it. Under certain circumstances, using the Data Domain Retention Lock can lead to data loss.
- Do not add more than 8 Data Domain systems to a single Avamar server to avoid performance issues. Ensure that the Data Domain system and the Avamar server has a low latency connection.

Data Domain system requirements

To support Avamar and Data Domain integration, ensure the environment meets the Data Domain system requirements listed in the following table.

Table 3. Data Domain system requirements

Data Domain feature or specification	Requirement for use with Avamar
Data Domain Operating System (DD OS)	Check the Avamar and Data Domain Compatibility Interoperability Matrix for the most current information.
DD Boost	Check the Avamar and Data Domain Compatibility Interoperability Matrix for the most current information DD Boost software enables backup servers to communicate with storage systems without the need for Data Domain systems to emulate tape. There are two components to DD Boost: one component that runs on the backup server and another that runs on the Data Domain system. In the context of Avamar, the component that runs on the backup server (DD Boost libraries) is integrated into the Avamar Client. DD Boost software is an optional product that requires a license to operate on the Data Domain system.
Data Domain device type	Avamar supports any Data Domain system that supports the execution of the required DD OS version.
Data Domain File System	Enable Data Domain File System using either the Data Domain System Manager or CLI.

Table 3. Data Domain system requirements (continued)

Data Domain feature or specification	Requirement for use with Avamar
	After you enable file system operations, it may take up to 10 minutes before Avamar Administrator correctly reflects the status of the Data Domain system, especially if the Data Domain system is using the DD Extended Retention option. Do not perform backups, restores, or system maintenance operations until the status appears correctly in Avamar Administrator. Otherwise, the backups, restores, or system maintenance operations may fail.
DD Boost user account	The DD Boost library uses a unique login account name created on the Data Domain system. This account name is known as the DD Boost account. If the account is renamed and/or the password is changed, these changes must be immediately updated on the Avamar system by editing the Data Domain configuration options. Failure to update the DD Boost account information could potentially yield integrity check errors and/or backup/restore problems. The DD Boost account must have administrator privileges.
DD Cloud Tier	Data Domain cloud storage units must be pre-configured on the Data Domain before being they are configured for cloud tier operations in the Avamar Administrator.
DD Cloud Disaster Recovery	To perform backups from the Avamar with DD Cloud DR support, you must first: 1. Install, deploy, and configure the DD Cloud DR system, including registering the CDRA with Avamar. 2. Add a vCenter client to Avamar and configure proxy-based backup of VMs. 3. Create a dataset with the Store backup on Data Domain system checkbox enabled and a Data Domain system selected.

NOTE: When you enable DD Boost on the Data Domain device, DD Boost becomes the preferred method of connectivity for any clients that are enabled for DD Boost. While this method is acceptable for clients that can take advantage of DD Boost features, it can result in performance degradation for other clients. Proper due diligence and effective data gathering are keys to avoiding such interactions, especially during upgrades.

Network requirements

The following sections list network requirements for Avamar and Data Domain system integration.

Network throughput

Before integrating a Data Domain system with an Avamar server, ensure that enough network bandwidth is available.

To obtain the maximum throughput available on a Data Domain system (for restores, level zero backups, and subsequent incremental backups after a level-zero backup), verify that the network infrastructure provides more bandwidth than the bandwidth required by the maximum throughput of the Data Domain system.

Network configuration

Configure (or verify) the following network configuration:

- Assign a fully qualified domain name (FQDN) to each Data Domain system.
- Do not use IP addresses in place of hostnames when registering a Data Domain system. This can limit the ability to route optimized duplication traffic exclusively through a registered interface.

- Ensure that DNS on the Data Domain system is properly configured.
- Ensure forward and reverse DNS lookups work between the following systems:
  - Avamar server
  - Data Domain system
  - Backup and restore clients
- Use hosts files to resolve hostnames to non-routable IP addresses.
- Do not create secondary hostnames to associate with alternate or local IP interfaces.

Wide area networks not supported

The Avamar server and all Data Domain systems must be on the same local network. Do not connect the Avamar server and Data Domain systems over a Wide Area Network (WAN). Configurations that use a WAN are not supported.

NTP requirements

Configure the Avamar server, all Avamar clients, and the Data Domain system to use the same Network Time Protocol(NTP) server.

Licensing requirements

Ensure that the environment meets the licensing requirements in the following table.

Table 4. Licensing requirements

Product	Licensing requirements
Avamar	Standard Avamar licensing requirements apply.
Data Domain	The DD Boost license must be installed on the Data Domain system. For replication from one Data Domain system to another, a replication license must be installed. For the cloud tier feature, a cloud tier license must be installed.

Data port usage and firewall requirements

To enable communication between Avamar and the Data Domain systems, review and implement the port usage and firewall requirements in the following documents:

- *Avamar Product Security Guide*
- "Port Requirements for Allowing Access to Data Domain System Through a Firewall," on Avamar Support

Capacity requirements

Carefully assess your backup storage needs when evaluating how much data to store on the Data Domain system and the Avamar server. Include estimates from data that is sent to the Data Domain system from any other servers.

Review the capacity management information in the Avamar Administration Guide.

When the Data Domain system reaches its maximum storage capacity, no further backups to the Data Domain system occur until additional capacity is added or old backups are deleted.

Data Domain system streams

Each Data Domain system has a soft limit to the maximum number of connection and data streams that can be sustained simultaneously while maintaining performance. The number of streams varies depending on the Data Domain system model.

For example, the Data Domain DD990 can support 540 backup streams, while the Data Domain DD620 can support 20 backup streams. You configure the maximum number of streams that Avamar can use when you add a Data Domain system to the Avamar server.

The Avamar server uses the backup stream value to limit the number of concurrent backups and restores. If you fully dedicate the Data Domain system to the Avamar server, then you could potentially set the stream value in Avamar Administrator to the maximum supported number of streams. If you share the Data Domain system with other third-party applications or another Avamar server, then you should allocate a subset of the number of streams.

You can configure each Avamar backup client that supports multi-stream backups to use an appropriate number of streams, typically based on the number of databases, through multi-streaming configuration when you configure the Avamar backup job. The streams are released when the backup/restore operation completes. The number of streams you allocate should depend on the number and type of Avamar clients that back up data at about the same time.

NOTE:

Avamar jobs are used for backups, restores, and replication. When integrated with a Data Domain system, Avamar can support up to 336 jobs concurrently. Each job can consist of multiple streams. In this configuration, Avamar supports a maximum of 500 streams (`maxconn`).

The limits of 336 jobs/500 streams are fixed for all Avamar integrations with Data Domain systems, whether you are using Avamar Virtual Edition or an Avamar Data Store. When backing up to an Avamar Data Store, Avamar supports the original number of jobs per node (72) with a maximum 107 streams per node (`maxconn`).

Existing backup products in use with Data Domain

Data Domain systems can use other third-party backup and archiving software. The Avamar server does not assume it has sole ownership of the Data Domain system. Ensure that proper sizing is evaluated if the system is shared with other software products.

The Avamar server makes no use of the native Data Domain system snapshot and replication features. Replication occurs through the DD Boost SDK library by using copying and cloning. However, other third party products may make use of the native Data Domain system snapshot and replication features. In this case, a snapshot of an entire Data Domain system or a replication of an entire Data Domain system includes the Avamar data.

Additional configuration settings when adding a Data Domain to the 8TB or 16 TB AVE

Before adding a Data Domain system to the 8 TB or 16 TB Avamar Virtual Edition (AVE), it is recommended to modify the following Avamar GSAN settings in order to improve system performance.

- avmaint config maxcompdatastripe=20971520 --avamaronly
- avmaint config checkdiratomicrefs=true --avamaronly

Preparing the Data Domain system for Avamar integration

Before you can add a Data Domain system to the Avamar configuration, prepare the Data Domain system by enabling DD Boost and creating a DD Boost user account for the Avamar server to use to access the Data Domain system for backups and restores (and replication, if applicable). Verify the Data Domain system SNMP configuration.

About this task

NOTE: DD OS 5.5 and later supports the use of multiple DD Boost accounts, which can be used for segregation of accounts when multiple backup programs are sharing a common Data Domain system.

Steps

1. Disable DD Boost on the Data Domain system by logging in to the Data Domain CLI as an administrative user and typing **`ddboost disable`**.
2. Create a DD Boost account and password:
   a. Create the user account with admin privileges by typing the following command:
      `user add user role admin`
      where *user* is the username for the new account.
   b. Set the new account as the DD Boost user by typing the following command:
      `ddboost set user-name user`
      where *user* is the username for the account.
3. Enable DD Boost to allow the changes to take effect by typing **`ddboost enable`**.
4. Open the following TCP ports:
   - 161
   - 162
   - 163
5. Enable the NFS and SNMP protocols.
6. In the Data Domain OS CLI, type the following command:
   `snmp show config`
   Output similar to the following appears:

```
General Configuration
---------------------
   SNMP sysLocation:
   SNMP sysContact:
   SNMP sysNotes:

SNMP v2c Configuration
----------------------
   Community   Access       Hosts
   ---------   ----------   -------------
   private     read-only
   public      read-write   1.2.3.4
   ---------   ----------   -------------

   Trap Host              Port      Community
   --------------------   -------   ---------
   2.3.4.5                Default
   avamar.example.com
   --------------------   -------   ---------
```

   Ensure that the following conditions are met:
   - The Avamar server should not be included in the list of community hosts. The hosts column should be empty.
   - The Avamar server should be included in the list of trap hosts without a port or community.

   The Data Domain OS documentation on https://support.emc.com provides more information.

Next steps

- By default encryption is enabled for Data Domain systems through Avamar. If you leave encryption enabled, the `passphrase` command must be set on the Data Domain system. The *Data Domain Operating System Administration Guide* provides additional information on the `passphrase` command.
- If you change the DD Boost account name or password, edit the Data Domain system configuration in Avamar Administrator. Otherwise all backups, restores, and maintenance activities fail.

Configuring IP support

The IP configuration depends on the versions of IP and DD OS in the environment. The following topics provide details.

Configuring dual stack IPv4 and IPv6 support

If you are using IPv4 exclusively, or both IPv4 and IPv6, the configuration can be set through the GUI without any special configuration.

About this task

IPv6 support requires DD OS 5.5.x.

Configuring IPv6 support with DD OS 5.5.1

To add the Data Domain system exclusively with IPv6, edit the `mcserver.xml` file.

Steps

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Stop the MCS by typing **`dpnctl stop mcs`**.
3. Open `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` in a UNIX text editor.
4. Find the `ipv6_only_supported` entry key.
5. Change the `ipv6_only_supported` setting to **`true`**.
   `<entry key="ipv6_only_supported" value="true" />`
6. Close `mcserver.xml` and save the changes.
7. Start the MCS by typing **`dpnctl start mcs`**.

Configuring IPv6 with DD OS 5.5.0

DD OS 5.5.0 in an integrated Avamar and Data Domain system configuration requires dual stack IPv4 and IPv6.

Steps

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Stop the MCS by typing **`dpnctl stop mcs`**.
3. Open `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` in a UNIX text editor.
4. Find the `ipv6_only_supported` entry key.
5. Change the `ipv6_only_supported` setting to **`true`**.
   `<entry key="ipv6_only_supported" value="true" />`
6. Close `mcserver.xml` and save the changes.
7. Start the MCS by typing **`dpnctl start mcs`**.

8. Open `/etc/hosts` in a UNIX text editor.
9. Add an extra line for each IPv6 Data Domain system to the `/etc/hosts` file in the dual-stacked Avamar server in the following format:

   ```
   <IPv4 address of DD server> <IPv6 FQDN of DD server> <IPv6 hostname of DD server> <IPv4 FQDN of DD server> <IPv4 hostname of DD server>
   ```

10. Close `/etc/hosts` and save the changes.

Adding a Data Domain system

You can add a Data Domain system to Avamar by authenticating the Data Domain system with credentials, or by key-based SSH. If the login method by providing credentials (username/password) for a Data Domain system is disabled, you must import the SSH public key (/usr/local/avamar/lib/ddr_key.pub) from the Avamar server and add the key to the Data Domain system manually before connecting them. Ensure that you have additional access to log in to the Data Domain system when login method by providing credentials for a Data Domain system is disabled.

Prerequisites

Perform the following steps if you want to authenticate the Data Domain system by key-based SSH:

1. Log in to the Data Domain system either as a sysadmin or with *avamar_ostuser* privileges where *avamar_ostuser* is the name of the DD Boost user for Avamar on the Data Domain system.
2. Add the SSH public key (/usr/local/avamar/lib/ddr_key.pub) from the Avamar server to the SSH authorized keys file on the Data Domain system by typing the command: **`adminaccess add ssh-key user Avamar_ostuser`**.
3. Ensure that the public key is successfully added to the Data Domain system by typing the command: **`adminaccess show ssh-key user Avamar_ostuser`**.

Steps

1. In Avamar Administrator, click the **Server** launcher link.
   The **Server** window appears.
2. Click the **Server Management** tab.
3. Select **Actions** > **Add Data Domain System**.
   The **Add Data Domain System** dialog box appears.
4. On the **System** tab, specify Data Domain system information:
   a. In the **Data Domain System Name** box, type the fully qualified domain name of the Data Domain system.

      NOTE: Do not use an IP address or a secondary hostname that associates with alternative or local IP interfaces. It may limit the ability of Avamar to route optimized deduplication traffic.

   b. In the **DDBoost User Name** box, type the username of the DD Boost account for Avamar to access the Data Domain system for backups, restores, and replication.
   c. In the **Password** box, type the password for the account that Avamar uses to access the Data Domain system for backups, restores, and replication.
   d. In the **Verify Password** box, type the password again for verification.
   e. If you have more than one Data Domain system that is associated with Avamar, you can specify one Data Domain system to be the default replication storage. Select **Use system as default replication storage** if this system is the default replication storage.
   f. To store checkpoints for a single-node Avamar server or Avamar Virtual Edition (AVE) server on the Data Domain system instead of the Avamar server, select the **Use as target for Avamar Checkpoint Backups** checkbox.
   g. Select the **Use certificate authentication for REST communication** checkbox to enable Avamar to use certificate-based authentication while performing an operation with Data Domain system using REST-based communication.

      NOTE: The **Use certificate authentication for REST communication** checkbox is displayed only on the Avamar AUI.

   h. To view the maximum number of streams that the Data Domain system supports, click **Verify**.
   i. Specify the maximum number of streams that Avamar can use at any one time to perform backups and restores:
      - To specify a defined number of streams, type the number in the **Max used by Avamar** box.
      - To specify a maximum number of streams which are based on the percentage of the total number of supported streams:
        i. Type the percentage in the **Max used by Avamar** box.

ii. Select the **As percentage of the max limit** checkbox.

Consider both the maximum number of streams that the Data Domain system supports, as well as whether other applications are using streams to send data to and receive data from the Data Domain system.

If the writing to and reading from the Data Domain system use all available streams, then Avamar queues backup or restore requests until one or more streams become available.

5. To configure SNMP, click the **SNMP** tab.

   SNMP configuration enables Avamar to collect and display data for system health monitoring, system alerts, and capacity reporting.
6. Verify the SNMP configuration:
   - The **Getter/Setter Port Number** box lists the port on the Data Domain system from which to receive and on which to set SNMP objects. The default value is 161.
   - The **SNMP Community String** box lists the community string Avamar uses for read-only access to the Data Domain system.
   - The **Trap Port Number** box lists the trap port on the Avamar server. The default value is 163.
7. To configure the cloud tier feature, click the **Tiering** tab.

   Avamar software uses Cloud tier to move Avamar backup data from a Data Domain system to the cloud.
8. Click **OK**.
   A progress message appears.
9. When the operation completes, click **Close**.

Results

When you add a Data Domain system to the Avamar configuration, Avamar creates an MTree on the Data Domain system for the Avamar server. The MTree refers to the directory created within the DD Boost path. Data Domain systems support a maximum of 100 MTrees. If you reach the limit, you cannot add the Data Domain system to the Avamar configuration.

Editing a Data Domain system

Steps

1. In Avamar Administrator, click the **Server** launcher link.
   The **Server** window appears.
2. Click the **Server Management** tab.
3. Select the Data Domain system to edit.
4. Select **Actions** > **Edit Data Domain System**.

   The **Edit Data Domain System** dialog box appears.
5. Edit the settings for the Data Domain system as necessary.

   The settings are the same as the settings that you specified when you added the Data Domain system to the Avamar configuration.
6. (Optional) If the **Re-add SSH Key** and **Re-add Trap Host** buttons are enabled, then click the buttons to restore the SSH key and trap host values on the Data Domain system.

   When these buttons are enabled, the configuration on the Avamar server is not synchronized with the configuration on the Data Domain system. Clicking the buttons restores the values to the Data Domain system to ensure synchronization.
7. Click **OK**.

   A confirmation message appears.
8. After the edits are complete, click **Close**.

Next steps

If you edited the Data Domain system name, the DD Boost username, or the DD Boost password, then create and validate a new checkpoint. If you perform a rollback to a checkpoint with the outdated Data Domain system name or DD Boost information, then the rollback fails. The *Avamar Administration Guide* provides instructions on creating and validating checkpoints.

Deleting a Data Domain system

You can delete a Data Domain system from the Avamar configuration if the Data Domain system is online and if there are multiple Data Domain systems configured on the Avamar server.

About this task

If you are deleting the only Data Domain system configured on the Avamar server, or if the Data Domain system is offline, then the Avamar server requires advanced service. Contact your Avamar sales representative to purchase this service.

Steps

1. Ensure that no backups are stored on the Data Domain system:
   a. Delete each backup for all clients that use the Data Domain system as a backup target.
   b. Ensure that all backups on the Data Domain system are expired and deleted through the Avamar garbage collection process.
   c. Ensure that there are no checkpoints for the Avamar server that refer to backups on the Data Domain system by using one of the following methods:
      - Wait for all checkpoints that contain backups for the Data Domain system to expire.
      - Perform and validate a new checkpoint after all backups to the Data Domain system are deleted, and then delete all other checkpoints.
2. Ensure that the Data Domain system is not the default replication storage system.
   Setting the default Data Domain destination provides details.
3. In Avamar Administrator, click the **Server** launcher link.
   The **Server** window appears.
4. Click the **Server Management** tab.
5. Select the Data Domain system to delete.
6. Select **Actions** > **Delete Data Domain System**.
   A confirmation message appears.
7. Click **Yes**.
   A dialog box shows the progress of the operation.
8. When the deletion completes, click **Close**.

Next steps

Create and validate a new checkpoint. The *Avamar Administration Guide* provides instructions on creating and validating checkpoints. If you perform a rollback to a checkpoint with the deleted Data Domain system, then the Data Domain system is restored to the configuration

Best practices for WAN backups

Review and implement the best practices in the following topics for environments with DD OS 5.5 or later and backups over a WAN.

Network throttling

The **Network rate throttle setting** in the plug-in options for file system plug-ins controls the rate at which Avamar sends data to the server. When you specify a value in Mbps for this option, the `avtar` process pauses as long as necessary after sending each packet to ensure that network usage does not exceed the specified maximum bandwidth.

Use of this option can improve WAN backups for desktop and laptop clients.

Efficient restore

Enable efficient restore by using the `--ddr-compressed-restore` option in `avtar` for better restore performance over a WAN.

Do not enable efficient restore for clients within the Data Center.

WAN bandwidth guidelines

The WAN use cases in the following table are estimates of typical latencies and bandwidths for the associated use cases. The following network characteristics were tested and are supported for backup over the WAN to an integrated Avamar and Data Domain system. The exact characteristics vary by network type.

Any network characteristics that exceed these requirements (for example, greater than 100ms latency) is not supported.

Table 5. WAN use case bandwidth guidelines

Use case configuration	Speed up/down	Range of latency (in ms)	Jitter	Percentage of bandwidth usable by the integrated Avamar and Data Domain system
Laptop backup from home (DSL line) Home use DSL link shared with other devices	256kbps up / 4000kbps down	20-100	10% normal 25% bad	50-100%
Consumer WAN DSL/Cable Small remote office	683kbps up / 8000kbps down	20-100	10% normal 25% bad	10-100%
Business WAN Use case 1 T1 Remote office / branch office	1000kbps up / 1000kbps down	10-100	10% normal 20% bad	10-100%
Business WAN Use case 2 T1 Remote office / branch office	30Mbps up / 30Mbps down	10-100	10% normal 20% bad	10-100%
High Speed Dedicated T3 to 1GbE	667Mbps up / 667Mbps down	10-100	1% normal 5% bad	10-100%

Encryption in flight

When storing backups on or restoring data from a Data Domain system, you can specify the encryption method for data transfer between the client and the Data Domain system. The **Encryption method to Data Domain system** option appears in the plug-in options during a backup or restore.

The following values are supported:

- **Default**
- **None** (clear text)
- **Medium**
- **High**

The default value is **Default**, which is high encryption. To edit the default value for the option, edit the `mcserver.xml` file.

The following guidelines should be used for encryption best practices:

- For large backups or restores (for example, L0 backups) within the data center, set encryption to **Medium** or **None** to improve performance.

- If you have desktop/laptop clients backing up over a WAN, set encryption to **High.**

NOTE: Use the `--ddr-encrypt-strength` option to specify the encryption method during command line backups and restores. Available values are `none`, `medium`, and `high`.

System upgrades

The Avamar and Data Domain upgrade path is very specific. Failure to upgrade software in the proper order can cause Avamar maintenance functions to fail. If this happens and the GSAN fails, then rollback operations fail.

When you are upgrading the DD OS, ensure that the DD OS version that you upgrade to is compatible with both the current Avamar server version and the next Avamar server version.

Upgrading the DD OS from 5.4.0.8 to 5.5 before you upgrade the Avamar server to release 7.1 is desirable but not required. If you do not upgrade the DD OS to 5.5 before you upgrade the Avamar server to release 7.1, then upgrade the DD OS immediately afterward. Skipping any intermediate steps can create an incompatibility issue that disrupts server operation.

You can upgrade a Data Domain system without product support, but you must open a Service Request with Avamar Support before you upgrade the Avamar server. It is recommended that you open an Avamar Service Request before you upgrade a Data Domain system.

Post-upgrade procedures for Data Domain systems

When the Avamar is connected to a Data Domain system, the following tasks should be performed after the Avamar is upgraded to release 7.3 or greater.

Generating new certificates with Data Domain systems

When the Avamar server is upgraded to release 7.3 or greater and session ticket authentication is enabled during upgrade, the following steps are required for Data Domain systems that are configured for Avamar backup storage. Session tickets are supported with Data Domain systems at release 5.6 or greater.

Steps

1. Wait for the Data Domain server to be aware of the updated certificate.

   The Data Domain server displays a yellow status in Avamar Administrator with the status message `Unable to retrieve ssh key file pair`. This process may take up to 30 minutes.
2. Open the Data Domain server in Avamar Administrator:
   a. In Avamar Administrator, click the **Server** launcher link button.
   The **Server** window appears.
   b. Click the **Server Management** tab.
   c. Select the Data Domain system to edit.
   d. Select **Actions** > **Edit Data Domain System**.
   The **Edit Data Domain System** dialog box appears.
   e. Click **OK**.

   There is no need to change the Data Domain configuration.
3. Restart DD Boost on the Data Domain system:
   a. Log in to the Data Domain System.
   b. Type the following commands in the Data Domain CLI:

   ```
   ddboost disable
   ddboost enable
   ```

Setting the passphrase on Data Domain systems

When the Avamar server is upgraded to release 7.3 or greater, the DDBoost user must have a passphrase enabled.

Steps

1. Log into the Data Domain system.
2. Enter the following command at the Data Domain CLI:
   ```
   system passphrase set
   ```
3. When prompted, enter a passphrase.

   NOTE: The DDBoost user must have admin rights.

3

Backups with Avamar and Data Domain

Topics:

Overview of backups with Avamar and Data Domain

During a backup, the Avamar server sends a backup request to the Avamar client. If the backup request includes the option to use a Data Domain system as the target backup data is stored on the Data Domain system and metadata is stored on the Avamar server.

Where backup data is stored

All data for a backup is stored under a single dedicated MTree on a single Data Domain system.

How Avamar manages backup data

During a backup, Avamar sends the metadata for the backup from the client to the Avamar server. This process enables Avamar to manage the backup even though the data is stored on a Data Domain system.

Avamar does not store the original path and file name for a file on the Data Domain system. Instead, Avamar uses unique file names on the Data Domain system.

Supported backup types

You can perform full backups, incremental backups, and differential backups. Differential backups are only available for select clients or plug-ins when a Data Domain system is the backup target. You can also perform VMware backups with Changed Block Tracking enabled.

Store the full backup for a client and all subsequent incremental and differential backups on either the Avamar server or a single Data Domain system.

Avamar does not support:

- Full backup on a Data Domain system and incremental or differential backups on the Avamar server
- Full backup on the Avamar server and incremental or differential backups on a Data Domain system
- Full backup on one Data Domain system and incremental or differential backups on another Data Domain system

If you change the device on which backups for a client are stored, then you must perform a full backup before any further incremental or differential backups.

NOTE: When you use the Avamar Plug-in for SQL Server and you perform a tail-log backup during a restore, then the tail-log backup is always stored on the Avamar server.

Canceling and deleting backups

If you cancel a backup while it is in progress, then Avamar deletes the backup data that was written to the Data Domain system during the next cycle of the Avamar garbage collection process.

If you delete a backup in Avamar, then the backup is deleted from the Data Domain system during the next cycle of the Avamar garbage collection process.

The *Avamar Administration Guide* provides instructions on how to cancel or delete a backup.

Selecting a Data Domain target for backups

To select a Data Domain system as the storage for a backup, select the **Store backup on Data Domain system** checkbox in the plug-in options for the backup, and then select the Data Domain system from the list.

Storing Avamar server checkpoints on a Data Domain system

You can store checkpoints for a single-node Avamar server or Avamar Virtual Edition (AVE) on a Data Domain system. Checkpoints are system-wide backups taken for disaster recovery of the Avamar server.

About this task

Restore of checkpoints from a Data Domain system requires assistance from Avamar Professional Services.

The *Avamar Administration Guide* provides details on checkpoints.

Steps

1. In Avamar Administrator, click the **Server** launcher link.
   The **Server** window appears.
2. Click the **Server Management** tab.
3. Select a Data Domain system.
4. Select **Actions** > **Edit Data Domain System**.
   The **Edit Data Domain System** dialog box appears.
5. Click the **System** tab, and then select **Use system as target for Avamar Checkpoint Backups**.
6. Click **OK**.
   A confirmation message appears.
7. After the edits are complete, click **Close**.

Data Domain tab

The **Data Domain** tab in the Server Monitor provides CPU, disk activity, and network activity for each node on the Data Domain system.

The following tables describe the information available on the Data Domain tab.

Table 6. Node details on the Data Domain tab of the Server Monitor

Property	Description
Status indicators	Status of the node. One of the following values: • OK (green)—The Data Domain system is functioning correctly. • Warning (yellow)—There is a problem with the Data Domain system, but backups and restores can continue. • Error (red)—There is a problem with the Data Domain system, and backups and restores are stopped until the problem is resolved. If the status is yellow or red, you can view additional status information to determine and resolve the problem. The

Table 6. Node details on the Data Domain tab of the Server Monitor (continued)

Property	Description
	Avamar and Data Domain System Integration Guide provides details.
Name	Hostname of the Data Domain system as defined in corporate DNS.

Table 7. CPU details on the Data Domain tab of the Server Monitor

Property	Description
Busy Avg.	Average CPU usage as a percentage of total possible CPU usage.
Max	Maximum CPU usage that has occurred as a percentage of total possible CPU usage.

Table 8. Disk (KB/S) details on the Data Domain tab of the Server Monitor

Property	Description
Read	Disk read throughput in kilobytes per second.
Write	Disk write throughput in kilobytes per second.
Busy	Disk I/O usage as a percentage of total possible disk I/O usage.

Table 9. Network (KB/S) details on the Data Domain tab of the Server Monitor

Property [a]	Description
Eth#1	Desc—Description of the network interface. In/Out—Network bandwidth usage in kilobytes per second on network interface 1.
Eth#2	Desc—Description of the network interface. In/Out—Network bandwidth usage in kilobytes per second on network interface 2.
Eth#3	Desc—Description of the network interface. In/Out—Network bandwidth usage in kilobytes per second on network interface 3.
Eth#4	Desc—Description of the network interface. In/Out—Network bandwidth usage in kilobytes per second on network interface 4.

a. The number of Eth# columns depends on the maximum number of network interfaces that the configured Data Domain systems support.

4

Replication

Topics:

Overview of replication

The Avamar replication feature transfers data from a source Avamar server to a destination Avamar server. When you use a Data Domain system with Avamar, then the replication process transfers Avamar data from the source Data Domain system to a destination Data Domain system.

If a Data Domain system is configured with a source Avamar server, then there must be a corresponding Data Domain system configured with a destination server. If there is no destination Data Domain system configured with the destination Avamar server, then replication fails for backups on the source Data Domain system.

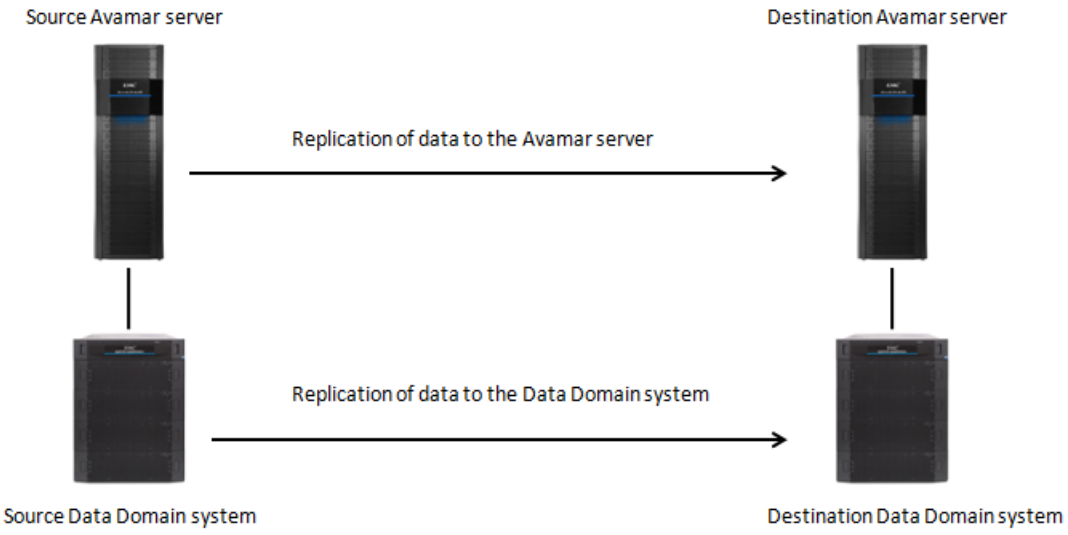

Figure 2. Data Domain basic replication

Replication configurations

If the source Avamar server uses more than one Data Domain system, then you can use either a single destination Data Domain system or multiple destination systems. Also, if the source Avamar server uses a single Data Domain system, then you can use either a single destination Data Domain system or multiple destination systems. All of the data is replicated through DD Boost.

For long-term backup retention requirements on destination Data Domain systems, you can replicate from a source Data Domain system to destination Data Domain system with DD Extended Retention.

Many to one replication

The following figure illustrates a source Avamar server with two source Data Domain systems. Avamar replicates the backup data on the two source Data Domain systems to a single destination Data Domain system.

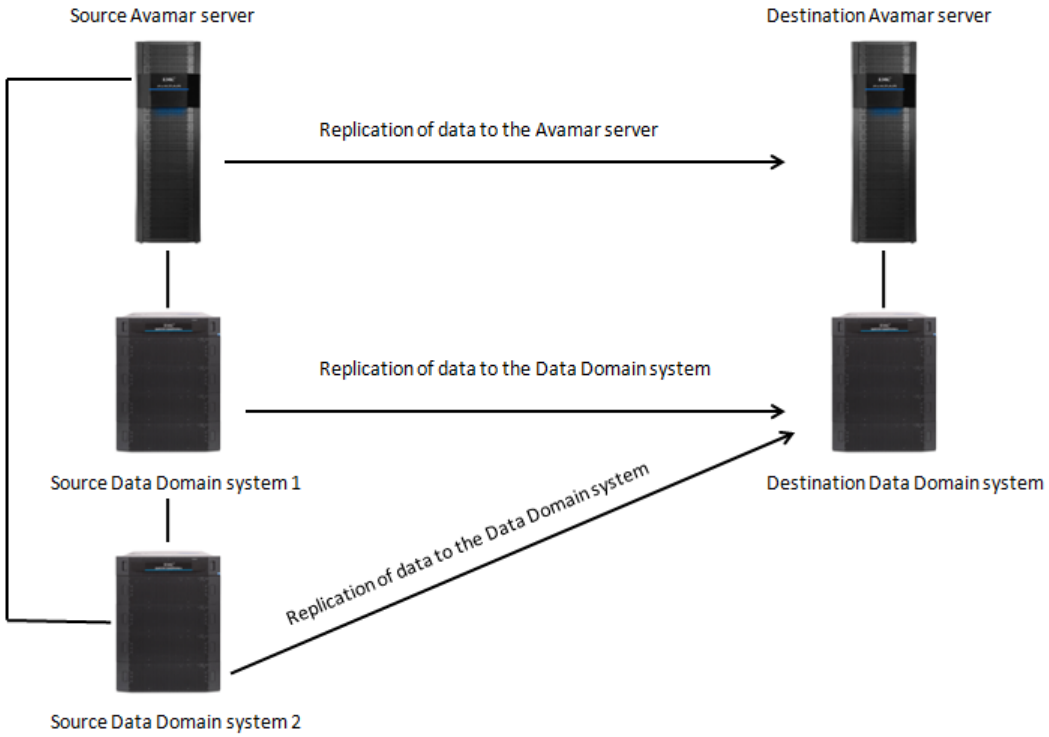

Figure 3. Data Domain system replication many to one configuration

The destination Data Domain system must be able accommodate the replicated data from both source Data Domain systems.

Many to many replication

The following figure illustrates an environment with multiple destination Data Domain systems replicating to multiple destination Data Domain systems.

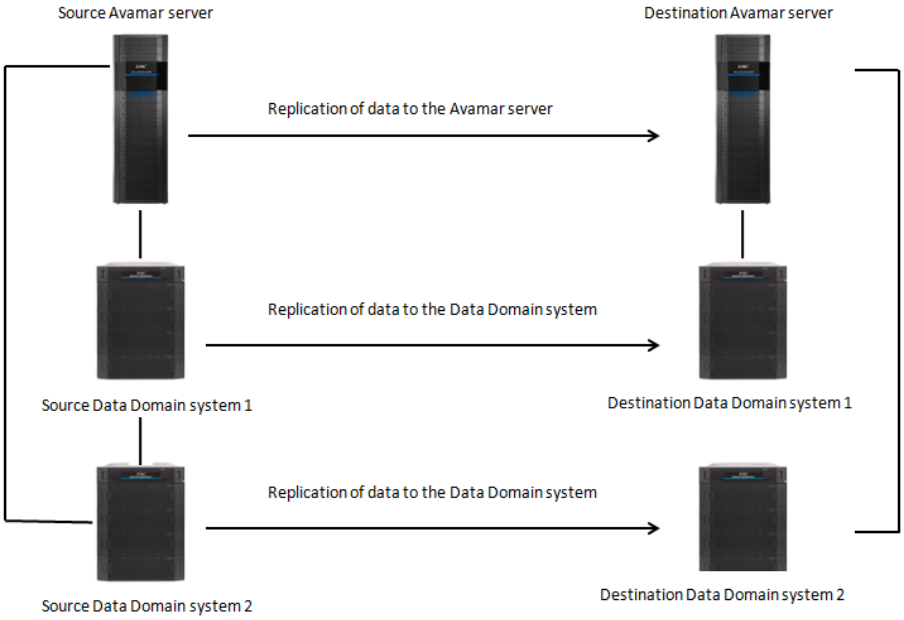

Figure 4. Data Domain system replication many to many configuration

One to many replication

The following figure illustrates an environment where backup data replicates from a single source Data Domain system to multiple destination Data Domain systems.

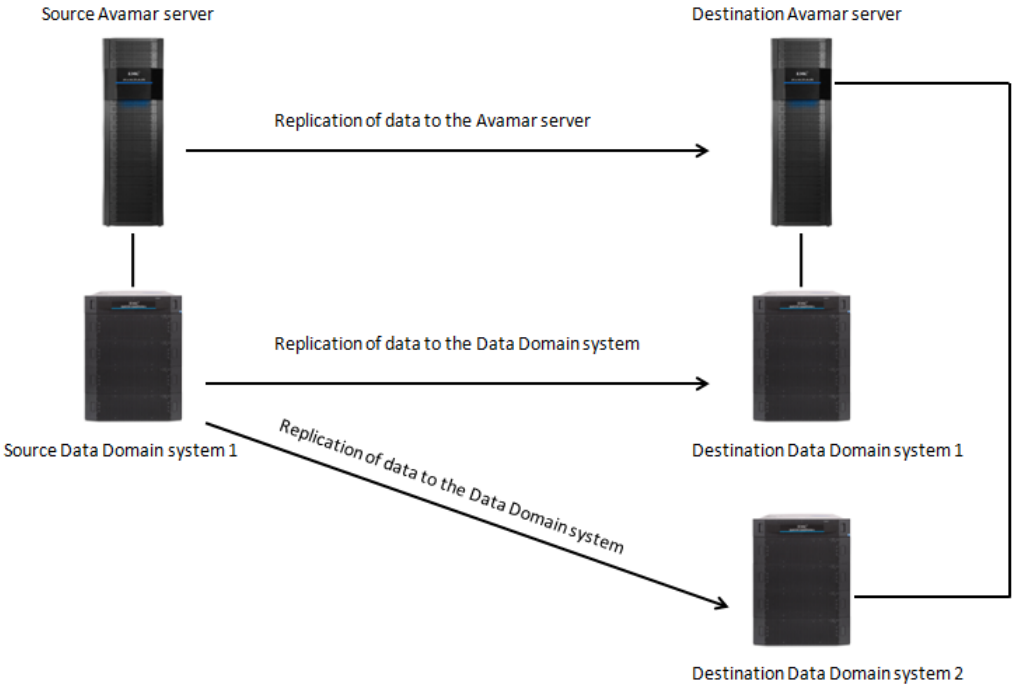

Figure 5. Data Domain system replication one to many configuration

In a configuration with multiple destination Data Domain systems, you can control which system receives the data that replicates from the source Data Domain system by mapping a domain on the source Avamar server to a destination Data Domain system. Mapping a domain to a Data Domain system provides details.

Pool-based replication

Traditional Avamar replication occurs in serial, which can result in a long replication window when the source and targets are both Data Domain systems. Pool-based replication allows for multiple parallel replication backups from a Data Domain source to a Data Domain target.

With traditional Avamar replication, replication is subject to a serial backup queue. This does not guarantee that all backups can be replicated in a single day, if any single backup takes longer to replicate than the desired recovery point objective (RPO). For example, one backup could take 24 hours to replicate, thereby missing an 8 hour RPO.

With pool-based replication, Avamar can start as many backup replication operations as necessary, thereby guaranteeing that the backups eventually reach their destination at the desired RPO . However, due to potential bottlenecks in either replicate throughput of Data Domain systems or the network throughput, it is recommended that replication groups and clients that will be run in parallel should be added one at a time until the desired throughput is achieved.

Pool-based replication is enabled during replication group configuration. Configuring pool-based replication on page 37 provides instructions.

Pool-based replication can also be enabled with the `avrepl` command using the `--use-pool-based` option. Additional options for the `avrepl` command you to determine the order in which backups will be replicated and other information. The *Avamar Administration Guide* contains information about the `--use-pool-based` option with the `avrepl` command and related options.

Replication data flow

Avamar replicates the data directly from one Data Domain system to another. In other words, Avamar does not stage the data on the Avamar server before replicating the data to the destination Data Domain system.

Replication schedule

The replication of Avamar data on a Data Domain system occurs on the Avamar replication schedule. You cannot schedule replication of data on the Data Domain system separately from the replication of data on the Avamar server.

Configuring replication

Steps

1. Configure replication from the source Avamar server to the destination Avamar server by using Avamar Administrator.
   The *Avamar Administration Guide* provides more information on configuring Avamar replication.
2. If there is more than one destination Data Domain system, specify which Data Domain system is the default destination.
3. If there is more than one destination Data Domain system, map the domains on the source Avamar server to a destination Data Domain system.

Setting the default Data Domain destination

In a replication environment with more than one destination Data Domain system, specify which Data Domain system is the default destination. The default destination is the Data Domain system to which Avamar replicates data when a destination Data Domain system is not identified on the **Replication Storage Mapping** tab.

Steps

1. In Avamar Administrator, click the **Server** launcher link.
   The **Server** window appears.
2. Select the destination Data Domain system.
3. Select **Actions** > **Edit Data Domain System**.
   The **Edit Data Domain System** dialog box appears.
4. Click the **System** tab, and then select **Use system as default replication storage**.

5. Click **OK**.
   A confirmation message appears.
6. Click **Close**.

Mapping a domain to a Data Domain system

If there are multiple destination Data Domain systems, you can control which system receives the data that replicates from the source Data Domain system. To specify the destination Data Domain system, map a domain on the source Avamar server to a destination Data Domain system. If you do not provide a mapping, then Avamar replicates the data from the source Data Domain system to the default destination.

About this task

NOTE: You cannot map the domains on the source Avamar server to a destination Data Domain system until after the first replication. During the first replication, the data replicates to the default destination.

Steps

1. In Avamar Administrator, click the **Data Movement Policy** launcher link.
   The **Data Movement Policy** window appears.
2. Click the **Storage Mapping** tab, and then click **Add Domain**.
   The **Select a Domain** dialog box appears.
3. From the **Map to Data Domain System** list, select the Data Domain system to use as the replication target.
4. Click **OK**.

Deleting a domain mapping

When you delete a domain mapping, any data that has already replicated to the destination Data Domain system remains there. However, any new data replicates to the default destination system unless you create a new mapping to a different Data Domain system.

Steps

1. In Avamar Administrator, click the **Data Movement Policy** launcher link.
   The **Data Movement Policy** window appears.
2. Click the **Storage Mapping** tab.
3. Select the mapping and click **Delete**.
   A confirmation message appears.
4. Click **Yes** to confirm the mapping deletion.

Configuring pool-based replication

Pool-based replication, which allows for multiple parallel replication backups from a Data Domain source to a Data Domain target, can be enabled during creation or editing of a replication group.

Steps

1. Follow the instructions for creating or editing a replication group found in the *Avamar Administration Guide*.
2. At the **Order** page of the **New Replication Group** wizard, select **Replicate client backups in parallel** for the mode in which the backups will be processed.
3. Select **Optimize Virtual Synthetic Replication (VSR)** to instruct the replication plug-in to use VSR optimization for plug-ins that support optimization.
   VSR optimization requires that the **Replication order of client backups** must be **Oldest backup to newest backup**. This option is selected by default; to require that all ordering options for pool-based replication are followed, regardless of the plug-in, deselect this option.
4. For the **Replication order of client backups**, select one of the following:

- **Oldest backup to newest backup** begins replication with the oldest backup first.
- **Newest backup to oldest backup** begins replication with the newest backup first.

5. Click **Next**.
6. At the **Overview** page, click **More Options**.
7. Select the **Show Advanced Options** checkbox to specify advanced options.

   The advanced options appear in red on the More Options dialog box.
8. For the **Client list ordering** option, determine the order for client replication.
9. For the **Maximum number of Data Domain Replication Streams** option, enter the maximum number of avtar processes that can be started in parallel.
10. Click **OK** to close the **More Options** dialog.
11. Click **Finish** to complete the configuration of the replication group.

5

Data Domain Cloud Disaster Recovery

Topics:

Overview of Data Domain Cloud Disaster Recovery

The Avamar (DD Cloud DR) solution enables disaster recovery of one or more on-premises virtual machines (VMs) to the cloud. DD Cloud DR integrates with existing on-premises backup software and a Data Domain system to copy the VM backups to the cloud. It can then run a DR test or a failover, which converts a VM to an Amazon Web Services Elastic Compute Cloud (EC2) instance, and then runs this instance in the cloud.

The DD Cloud DR solution supports recovery run books, enabling administrators to create one or more DR plans to recover multiple VMs and preconfigure recovery orchestration, including network and security groups association, VM boot order definition, and EC2 instance type selection. You can manage, recover, and fail back DR plans through the Cloud DR Server (CDRS) UI.

Through the CDRS UI, you can accelerate the recovery process by creating rapid recovery images for protected VMs. Creating a rapid recovery image starts a rehydration process and converts the VMDK files to an Amazon Machine Image (AMI). The recovery process then only needs to launch the recovered instance based on the AMI.

The on-premises Cloud DR Add-on (CDRA) manages deployment of on-premises components, as well as the CDRS, which runs in the cloud. CDRS monitors available copies in the cloud and orchestration activities in AWS.

The CDRS user interface can be used for disaster recovery testing and failover. A DR test enables temporary access to an EC2 instance to retrieve specific data or verify that the recovered VM is working before running a failover. You would start a failover when the on-premises production environment experiences a disaster or the VM is not running.

When the production environment is restored, you can start a failback. This action copies the failover instance from the cloud to a new VM copy in the on-premises vCenter environment. The failback procedure is available only in the CDRS user interface and not from the user interface of the on-premises backup software.

The *Data Domain Cloud Disaster Recovery Installation and Administration Guide* contains information using the cloud-based Cloud DR Server graphical interface.

Protection

VMs are protected with the DD Cloud DR solution within the backup software.

For information about configuring VM protection within the Avamar Administrator user interface, see the *Avamar for VMware User Guide*.

You can also perform DR tests and failover within your on-premises backup software's user interface. Failover refers to moving the data to the cloud when the local instance in the virtual environment fails.

After you backup a VM, you can enable it for rapid recovery in the CDRS user interface. Rapid recovery provides a short RTO of a few minutes when recovering a VM to the cloud. The *Data Domain Cloud Disaster Recovery Installation and Administration Guide* provides detailed information.

Failback is available in the CDRS user interface. A Failback operation is a fully orchestrated creation of a new VM copy in a pre-defined on-premises staging area, and the data is copied from the failed-over EC2 instance.

Configuring Avamar backups to use DD Cloud DR

Prerequisites

To perform backups from the Avamar with DD Cloud DR support, you must first:

- Install, deploy and configure the DD Cloud DR system, including registering the CDRA with Avamar. The *Data Domain Cloud Disaster Recovery Installation and Administration Guide* contains instructions.
- Add a vCenter client to Avamar and configure proxy-based backup of VMs. *Avamar for VMware User Guide* contains instructions.
- Create a dataset with the **Store backup on Data Domain system** checkbox enabled and a Data Domain system selected.

  NOTE: Only policy-based backups can be used with DD Cloud DR. Ad-hoc backups of individual VMs are not supported.

Steps

1. Follow the instructions for creating or editing a backup group found in the *Avamar Administration Guide*.

   NOTE: You must select a dataset that has the **Store backup on Data Domain system** checkbox enabled.

2. At the **Enable DD Cloud DR** page of the **New Group** wizard, select the **Enable DD Cloud DR** checkbox.
3. Select the DD Cloud DR Target.

   The DD Cloud DR Target is configured during CDRA configuration. The *Data Domain Cloud Disaster Recovery Installation and Administration Guide* contains further information.
4. For the **Cloud Retention Policy**, select either:
   - **Copies to keep**, and enter the maximum numbers of copies of the protected VM that will be stored in the cloud for disaster recovery.
   - **Retention period**, and select the amount of time that the copies will be retained in the cloud for disaster recovery.

   NOTE: CDRA will orchestrate the removal of copies from the cloud based on the cloud retention policy entered here.

5. For the **Last backup should not be older than** option, select the maximum interval between two backups that are copied to the cloud.
6. Complete the other information related to the group as described in the *Avamar Administration Guide* and click **Finish**.

Results

After either an ad-hoc or scheduled group backup of the new group has been performed, the copy will be listed as **Remote-CDRA** in the **Restore** tab of the **Backup, Restore and Manage** window.

Performing a DR test or failover of a DD Cloud DR copy

You can perform a DR test or failover of a DD Cloud DR copy from within Avamar Administrator.

About this task

A DR test is designed for temporary access to an EC2 instance, to test that the recovered VM works before performing a failover or to retrieve specific data, whereas a failover should be used when the on-premises production VM has experienced a disaster or is otherwise not running.

You cannot promote a DR test to failover using the Avamar software. To promote a DR test to failover, you must use the Cloud DR Server graphical interface. The *Data Domain Cloud Disaster Recovery Installation and Administration Guide* contains instructions for promoting a DR test to failover.

NOTE: When performing failovers, you must failover VMs in the appropriate order to ensure the proper functioning of servers and applications.

Steps

1. In Avamar Administrator, click the **Backup & Restore** launcher link.

The **Backup, Restore and Manage** window appears.

2. Locate the backup, as described in the *Avamar Administration Guide*.
3. Select **All virtual disks** in the **Contents of Backup** pane.
4. Right-click **All virtual disks** and select **DR Now...**.
   The **Cloud DR Option** dialog displays.
5. Select either **Initiate DR Test** or **Initiate Failover**.
6. Select the cloud network that will be used to launch the recovered instance in AWS or Azure.
7. Click **OK** to begin the DR test or failover operation and click **Yes** to confirm.

Results

The progress of the restore operation can be viewed in the **DR Activity Monitor** tab of the **Activity Monitor** window of Avamar Administrator.

Stop a DR test from the Avamar Administrator

A DD Cloud DR DR test can be stopped from within the Avamar Administrator. Only a DR test activity in the state **READY** can be stopped, and failover activities cannot be stopped.

Steps

1. In Avamar Administrator, click the **Activity** launcher link.
   The **Activity** window appears.
2. Click the **Activity Monitor** tab.
3. Select the **DR Activity Monitor** tab.
4. Right-click an appropriate DR test in state **READY** and select **Stop**.

6

Cloud Tier

Topics:

Overview of Avamar cloud tier

The Avamar cloud tier feature works in tandem with the Data Domain Cloud Tier feature to move Avamar backups from Data Domain systems to the cloud. This provides long-term storage of Avamar backups by seamlessly and securely tiering data to the cloud.

From the Avamar Administrator, you configure cloud tier to move Avamar backups from Data Domain to the cloud, and you can perform seamless recovery of these backups.

Data Domain cloud storage units must be pre-configured on the Data Domain before they are configured for cloud tier in the Avamar Administrator. The *Data Domain Operating System Administration Guide* provides further information.

Avamar cloud tier configuration

Configuring the Avamar server to manage the cloud tier feature on the Data Domain system involves two primary tasks:

- Adding or editing a Data Domain system in the Avamar Administrator to enable cloud tier.

  NOTE: You can switch from one cloud unit to another. Each Avamar server can have only one active cloud unit at the same time. After you switch the cloud unit, Avamar moves the existing backups that have been marked for tiering to the new cloud unit when the Data Domain system triggers data movement. Avamar marks the backups for tiering while the Data Domain system triggers data movement.
- Creating a cloud tier group.

The following sections describe how to perform these tasks.

Adding or editing a Data Domain system with cloud tier support

Use this procedure to add a Data Domain system with cloud tier support.

Steps

1. Follow the instructions at Adding a Data Domain system on page 24 for adding a Data Domain system, or editing an edit Data Domain system in the Avamar Administrator.
2. In the **Add Data Domain System** or **Edit Data Domain System** dialog box, click the **Tiering** tab.
3. Select **Enable Cloud Tier**.
4. For **Cloud Unit**, select the cloud unit that is configured on the Data Domain.

   NOTE: You can switch from one cloud unit to another. Each Avamar server can have only one active cloud unit at the same time. After you switch the cloud unit, Avamar tiers the existing backups that have been marked for tiering, but have not yet been tiered, to the currently-selected cloud unit. Avamar also tiers newly-marked backups to the currently-selected cloud unit.
5. Click **OK**.

A progress message appears.

6. Click **Close** when the operation completes.

Creating a new tier group

Tier groups are used to configure the clients, backups, schedules, and other information that is related to cloud tier configuration.

Steps

1. In Avamar Administrator, click the **Data Movement Policy** launcher link.
   The **Data Movement Policy** window appears.
2. Select **Action** > **New Group** > **Tier**.
   The **New Tier Group** wizard opens.
3. On the **General** page, perform the following steps:
   a. For **Tier group name**, type the name of the tier group.
   b. Optionally, enable **Undo tiering option** to undo the previous tiering job, and then choose one of the following options:
   - **Unmark backups only**—Unmark the previously marked backups only and perform no actions for backups that have already been moved to the cloud tier.
   - **Unmark and recall backups**—Unmark the previously marked backups and recall backups that have already been moved to the cloud tier.

   NOTE: When **Undo tiering option** is enabled, you cannot attach a schedule to the tier group. To run the tier group manually, right-click the tier group and select **Run Group Now**.
4. On the **Source** page, complete the following information:
   a. For **Membership**, select one of the following:
      - **Tier all client backups**—Selects all clients (except for the clients in the `/REPLICATE` domain) for cloud tier.
      - **Move specific client(s) and/or domain(s) to Tier**:

        Click **Choose Membership** and select the clients that require their backups to be moved to the cloud tier.

   b. For **Filter**, select either to tier all backups or to filter backup tiering by excluding or including backups.
   c. If you select backup filtering, click **Change Filter**.
   The **Tier Filter Options** dialog box opens.
   d. For **Backup Types**, select the type of backup.
   For example, to limit tiering to backups of type monthly only, deselect all the options except **Monthly**.
   e. For **Maximum backups per client**, select how many existing backups to tier to the cloud each time the schedule is run.
   No limit tiers all backups of the type selected in **Backup Types**.
   f. For **Age Threshold**, determine how long the backup resides on the Data Domain before it is tiered to the cloud.
      - The **Older** and **Younger** options allow you to create a range; for example, you can configure tiering for all backups that have been on the Data Domain system for longer than 30 days, but less than one year.

      NOTE: Data Domain requires that data reside on the Data Domain active tier for a minimum of 14 days before being tiered to the cloud.
5. Click **Next**.
   The **Destination** page appears, indicating that the cloud unit that has been configured for the selected Data Domain system.
6. Click **Next**.
   The **Expiration** page appears.
7. On the **Expiration** page, you can choose one of the following options:
   a. **Keep the current backup expiration**.
   b. **Set expiration by backup type**—Updates expiration for backups that are tiered to the cloud tier.

      NOTE: The timeframe for backup expiration must be a minimum of 14 days. The minimum expiration time is dependent on the *Age Threshold* value.

   c. Click **Next**.
   The **Schedule** page appears.
8. On the **Schedule** page, select a schedule, and then click **Next**.

NOTE: The schedule determines when and how often Avamar marks backups on the Data Domain for tiering to the cloud. However, the movement of the data from the Data Domain to the cloud is based on the Data Domain's tier schedule.

The **Overview** page appears.

9. Click **Finish**.

Recall operation for cloud tier

You can do recall operations for cloud tier on backups to cancel the **MARKED** status or move backups from cloud back to active tier of Data Domain. For backups that have been marked, the recall operations for cloud tier cancel the **MARKED** status. For backups that have been tiered to cloud, the recall operation for cloud tier move them from cloud back to active tier of Data Domain.

About this task

Follow the steps to recall backups:

Steps

1. On the Avamar Administrator **Manage** page, select the backup that you want to recall.
2. Right click and select **Recall** operation to trigger recall operation.
3. You can check the logs in Avamar Administrator **Activity** page.

   You can also create a Tier Group with **Undo tier options** enabled to unmark or recall a batch of backups based on your filter settings in Tier Group. Please refer to the Creating a new tier group for detailed procedures.

Restore operations for cloud tier

Restores of backups that have been tiered to the cloud are identical to normal restore operations.

The Avamar software recalls a copy of the backup from the cloud to the active tier of the Data Domain, then performs a restore of the backup from the active tier to the client. The status appears as Cloud. The backup is stored on the Data Domain cloud tier after the restore. The copy of the backup on the Data Domain active tier is used for restore operation and is deleted after 10 days.

To extend the lifetime of the temporary copy on active tier, on the Avamar server, use the following parameter in the `/usr/local/avamar/var/ddrmaint.cmd` command:

```
--cloud-copy-lifetime=days
```

NOTE: The timeframe for backup expiration must be a minimum of 14 days. The minimum expiration time is dependent on the *Age Threshold* value.

How to recover from these restore failures

Follow this procedure to recover from these restore failures:

Steps

1. Find the list of backups required for the restore:

   The Avamar Administrator **Manage** page can be used to locate backups that need to be recalled.

   Use the calendar and the **Date & Time** column to find the full database backup that you intend to restore.

   - For archive log backups required for DB2 restore and roll forward, in addition to the full backup, you will also need all the archive logs from the time of the full backup up to, and including, the archive logs for the point in time to which you are recovering. Use the **Date & Time** column to locate all the required backups.
   - For archive log backups required for SAP CLI restore, there may be additional entries for archive logs that were backed up together with the full backup. Use the **Date & Time** column to locate these entries for the same backup.

For each backup entry in the manage screen that you have located, if the **Tier** column shows **Cloud**, then it will need to be recalled from the cloud tier. Retain the list of the label numbers for all required backups to be used in the next step.

2. To perform a manual recall for the identified label numbers:
   a. On the Avamar Administrator **Manage** page, select the required backup.
   b. Right click and select **Recall** operation to manually trigger recall.
   c. You can check the logs in the Avamar Administrator **Activity** page.

   For backups not listed in Avamar Administrator, use the following procedure to perform a manual recall for the identified label numbers:
   - To perform the recall, log into the Avamar server as admin and run the following command at the command prompt:

     ```
     avtier --operation=restore --hfsaddr=Server-Name --hfsport=27000 --path=/clients/
     Client-Name --labelnum=Label-Num
     ```

     Where:
     - `Server-Name` is the name of the Avamar server.
     - `Client-Name`is the name of the Avamar client whose backups are being recalled.
     - `Label-Num` is the identified label number.

   NOTE: By default, the avtier logs will be generated in the following path: `/usr/local/avamar/var/client/`

3. Verify all required backups are on the active tier:

   Once the recall is complete, the **Tier** column on the Avamar Administrator **Manage** page for each recalled backup will change from **Cloud** to **Active**.
4. Proceed with restore as usual.

File or Granular Level Restore for cloud tier

Avamar support File or Granular Level restore only from the ECS cloud unit. File or Granular Level restore from backup that has been tiered to the ECS cloud unit is identical to normal File or Granular Level restore operations.

To restore a single file or a piece from backup that is in ECS cloud unit, Avamar doesn't need to recall the whole backup from cloud to active tier of the Data Domain. Avamar client directly reads the single file or the piece from the cloud.

Avamar doesn't support File or Granular Level restore from non-ECS cloud unit. Thus, to restore a single file or a piece from backup that is in non-ECS cloud unit, Avamar has to first recall the whole backup from cloud to active tier of Data Domain and then the Avamar client restores the single file or the piece from the active tier of Data Domain.

Avamar cloud tier disaster recovery

Avamar cloud tier disaster recovery supports the recovery of backups from the cloud in case of the loss of a Data Domain server and the recovery of an Avamar server in case of the loss of the Avamar server.

NOTE: If you experience a Data Domain or Avamar data loss, submit a service request to Avamar Support. Support representatives manage the disaster recovery process.

Required Configurations

- To recover backups from the cloud, enable and run the Data Domain cloud tier feature.
- To support recovering an Avamar server from the cloud, configure Data Domain and the tier group so that checkpoint backups are tiered to the cloud. For details on this process, see Configuring an Avamar server for recovery from the cloud on page 46.

Limitations

There are some limitations inherent in the cloud tier disaster recovery feature:

- Data that has resided on the active tier for less than the 14-day minimum is not tiered to the cloud. The data is not available for recovery from the cloud using the cloud tier disaster recovery feature. However, you can recover from a disaster recovery site by using the standard Avamar recovery workflows.
- The Avamar Administrator UI does not display partial or intermediate backups that are not contained in the final snapshot backup. However, these partial or intermediate backups are tiered to or recovered from the cloud.
- Support for this feature is effective with the release of Data Domain OS 6.0.1.
- The feature does not support recovery of a multi-node Avamar server from the cloud.

Configuring an Avamar server for recovery from the cloud

To configure Avamar server for recovery from the cloud, designate the Data Domain system as a target for Avamar Checkpoint backups and edit the Avamar tier group.

Steps

1. In Avamar Administrator, click the **Server** launcher link.
   The **Server** window appears.
2. Select the **Server Management** tab.
3. Select the Data Domain system from the tree in the left pane.
4. Select **Actions** > **Edit Data Domain System**.
   The **Edit Data Domain System** dialog box displays.
5. In the **Misc** section of the dialog box, select **Use as target for Avamar Checkpoint Backups**, then click **OK**.
   The Avamar checkpoint backup can now be stored on the Data Domain system.
6. In Avamar Administrator, click the **Data Movement Policy** launcher link.
   The **Data Movement Policy** window appears.
7. In the **Groups** tab, double-click the tier group that you want to configure, then click **Edit Group**.
   The **Edit Tier Group** window displays.
8. In the left-most pane of the **Edit Tier Group** window, select **Overview** to open the **Overview** page in the right pane.
9. On the **Overview** page, click **More Options** to open the **More Options** dialog box.
10. In the dialog box, select **Tier checkpoint backup**, then click **OK**.
    The Avamar checkpoint backup can now be tiered to the cloud.

Status of cloud tier operations

The Avamar Administrator displays various statuses related to cloud tier operations in the **System Monitor** and the **Backup, Restore, and Manage** window.

Table 10. Status of cloud tier operations

Status	Description
Active	The backup is currently stored on the active tier of the Data Domain and is not stored in the cloud.
Marked	The backup is marked for tiering to the cloud. While the Avamar software marks data for tiering to the cloud, the actual tier operations take place based on the Data Domain tier operations marked schedule. When the backup is marked for tiering but has not yet been tiered, it is listed as Marked in the Avamar Administrator.
Cloud	Avamar can tier the backup to the cloud. The backup is on the cloud tier when the tiering is complete. When the tiering is in progress, and if any part of the backup is tiered to the cloud, Avamar considers the backup to be on the cloud tier.
Indeterminate	When the Avamar server is marking backups for tiering or recalling backups from the cloud, the backup status is Indeterminate. If the backup status remains at Indeterminate, rather than reverting to Marked or Active status, it may indicate that the marking or recall action failed.

Best practices and limitations with cloud tier

This section provides the best practices for using the cloud tier feature, along with its limitations.

Best practices

- Best practices for the cloud tier feature for application plug-in backups:

  The cloud tier feature is for long-term retention of backups that are generally not needed for operational recoveries any longer. It is recommended that the **Age Threshold** be chosen carefully so as to not tier to cloud any backups that may be needed by current backups and restores, particularly for database plug-ins. Some plug-ins create backups in a sequence that are interdependent. Typically, a full backup is followed by incremental and log backups. One backup may be referenced by later backups, and multiple backups may be needed during recovery to bring a database to a specific point in time.

  For plug-in backups, the **Age Threshold** should be chosen based on the frequency of full backups and typical recovery scenarios. At least a single chain of a full backup plus incremental and log backups should be available on the Data Domain active tier to avoid issues. Additional backup chains may need to stay on the active tier depending on your recovery strategy. For example, if you run a full backup once a week and incrementals daily, and you must be able to restore 3-week old data, then you will need the three to four latest chains of full and incremental backups residing on the DD active tier. Data older than four weeks can then be moved to cloud. It is generally also possible to restore older backups from the cloud tier.

- When performing both replication and tiering, replicate the backup first before performing tiering. This will prevent data recalls from the cloud tier, as data can only be replicated from an active tier to active tier.
- Using the Data Domain M-Tree data movement policy to move Avamar backups to the cloud is not supported. Avamar backups should be tiered to the cloud using the Avamar software to configure tier groups and perform tier operations. Otherwise the Avamar software will be unaware of the location of the backups in the cloud and unable to perform recoveries or manage policies for those backups.

Limitations

- Cancelling a tier operation from the Avamar software, once the tier operation has been started, is not supported.
- Cancelling a recall operation from the Avamar software during recovery is not supported.
- Restore operations from the Avamar REST API are not supported.
- When performing a File Level Recovery from non-ecs cloud unit, the entire backup is recalled from the cloud tier to the active tier. Depending on the type of service you have with your cloud provider, this may incur significant egress costs for moving the entire backup from the cloud to the active tier, even if you are only attempting to restore a small number of files.
- Avamar Desktop/Laptop does not currently support the Avamar cloud tier feature.

7

Monitoring and Reporting

Topics:

Monitoring the system with the Avamar Administrator Dashboard

The Avamar Administrator dashboard provides summary information for the Avamar server and any configured Data Domain systems.

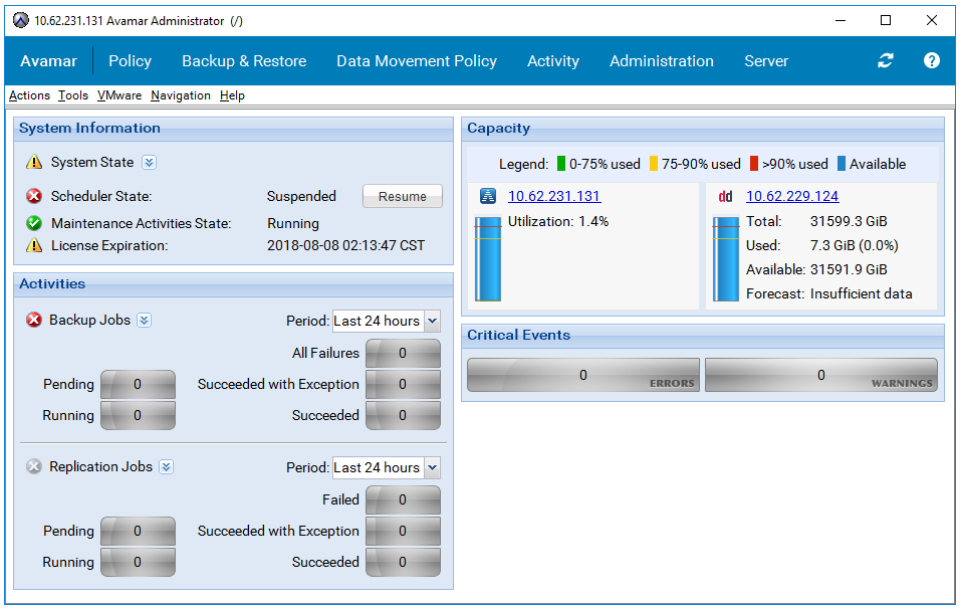

Figure 6. Avamar Administrator Dashboard

The following summary information appears for each server:

- Total amount of storage
- Amount of used storage
- Amount of available storage
- Forecast capacity

Monitoring the system with SNMP

Avamar can collect and display data for health monitoring, system alerts, and capacity reporting on a Data Domain system by using Simple Network Management Protocol (SNMP).

About this task

To enable Avamar to collect data, specify the port number to receive traps when you add the Data Domain system to the Avamar configuration.

The Data Domain SNMP service on the Avamar server receives and manages the SNMP traps for all Data Domain systems. You can manage the service in Avamar Administrator.

Steps

1. In Avamar Administrator, click the **Administration** launcher link.
   The **Administration** window appears.
2. Click the **Services Administration** tab.
   The Data Domain SNMP Manager service is the SNMP service for Data Domain.
3. To stop or start the service, right-click the service and select **Stop Data Domain SNMP Manager** or **Start Data Domain SNMP Manager**, respectively.

Monitoring Data Domain system status and statistics

Avamar Administrator provides CPU, disk activity, and network activity for each Data Domain system.

Steps

1. In Avamar Administrator, click the **Server** launcher link.
   The **Server** window appears.
2. Click the **Server Monitor** tab, and then click **Data Domain** tab.
   The data appears on the **Data Domain** tab.

Monitoring system events

When you configure SNMP communication for Avamar and a Data Domain system, the Avamar Event Monitor displays relevant events for the Data Domain system. You can filter the events to display only those events for a Data Domain system.

Steps

1. In Avamar Administrator, click the **Administration** launcher link.
   The **Administration** window appears.
2. Click the **Event Management** tab.
3. Select **Actions** > **Event Management** > **Filter**.
   The **Filter** dialog box appears.
4. Select the Data Domain systems.

Table 11. Data Domain options and descriptions

Option	Description
To view activities for all Data Domain systems	Select **All Systems**.
To view activities for a specific Data Domain system	a. Select **System**. b. Click the **...** . c. Select the Data Domain system in the **Select Data Domain System** dialog box, and then click **OK**.

5. Click **OK** in the **Filter** dialog box.

Monitoring activities

You can monitor recent backup, restore, and validation activities by using the **Activity Monitor** in Avamar Administrator. The **Server** column in the **Activity Monitor** lists the server, either the Avamar server or the Data Domain system, on which the activity occurred.

About this task

The **Activity Monitor** displays the most recent 5,000 client activities during the past 72 hours. You can filter the **Activity Monitor** to view only activities for data on a Data Domain system.

Steps

1. In Avamar Administrator, click the **Activity** launcher link.
   The **Activity** window appears.
2. Click the **Activity Monitor** tab.
3. Select **Actions** > **Filter**.
   The **Filter Activity** dialog box appears
4. Select **Data Domain Systems** from the **Source** list.
5. Select the Data Domain systems.
   - To view activities for all Data Domain systems, select **All Systems**.
   - To view activities for a specific Data Domain system:
     a. Select **System**.
     b. Click the **...** .
     c. Select the Data Domain system in the **Select Data Domain System** dialog box.
     d. Click **OK**.
6. In the **Filter Activity** dialog box, click **OK**.

Monitoring Data Domain system capacity

Avamar checks the capacity of each Data Domain system every 24 hours. Avamar then logs an event in the Event Monitor if the capacity reaches 95 percent full, or if the forecast number of days until the capacity is full is less than or equal to 90 days.

About this task

You can also monitor the capacity of a Data Domain system by using the **Server Management** tab on the **Server** window in Avamar Administrator.

When the Data Domain system reaches its capacity limit, you can reclaim space on the device by using the instructions in Reclaiming storage on a full Data Domain system.

NOTE: When the Data Domain system reaches 99 percent capacity, maintenance operations fail. The best practice recommendation is to limit Data Domain capacity usage to 80 percent.

Steps

1. In Avamar Administrator, click the **Server** launcher link.
   The **Server** window appears.
2. Click the **Server Management** tab.
3. Select the Data Domain system from the tree in the left pane.
   Data Domain system details appear in the right pane.

   The following table provides information on Data Domain system capacity information.

Table 12. Data Domain system capacity details

Field	Description
Total Capacity (post-comp size)	The total capacity for compressed data on the Data Domain system.
Server Utilization (post-comp use%)	The percentage of capacity used on the Data Domain system for any reason after compression of the data.
Bytes Protected	The total number of bytes of data that are protected, or backed up, on the Data Domain system. This value is the number of bytes before the data is compressed.
File System Available (post-comp avail)	The total amount of disk space available for compressed data in the Data Domain File System.
File System Used (post-comp used)	The total amount of disk space used in the Data Domain File System for compressed data.
User Name	The DD Boost user account used for Avamar and Data Domain system integration.
Default Replication Storage System	Specifies if the Data Domain system has been configured as the Default Replication Storage System.
Target for Avamar Checkpoint Backups	Specifies if the Data Domain system is a target for Avamar checkpoint backups. This option is only available for single-node Avamar servers and AVE.
Maximum Streams	Specifies the maximum streams supported by the Data Domain system.
Maximum Stream Limit	The maximum number of Data Domain system streams that Avamar can use at any one time to perform backups and restores.
Instant Access Limit	The maximum number of VMware Instant Access restores allowed. For Avamar 7.4, this number is 32.
DDOS Version	The DD OS version for the Data Domain system.
Serial Number	The serial number for the Data Domain system.
Model Number	The model number for the Data Domain system.
Monitoring Status	The current Avamar monitoring status of the Data Domain system.

Replication monitoring

To monitor replication activity in Avamar, including replication activities associated with a Data Domain system, use either the Activity Monitor or the Replication Report.

Activity Monitor

The Activity Monitor in Avamar Administrator provides a list of recent replication activities. If you select a Replication Source or Replication Destination activity, and then select **Actions** > **View Statistics**, you can view additional statistics about the replication, including:

- A list of backups that were replicated
- The clients associated with the replicated backups
- The scheduled start and end times for the replication
- The actual start and end times for the replication
- A list of any errors that occurred

The *Avamar Administration Guide* provides more information on how to access the Activity Monitor and the available statistics.

Replication Report

The Replication Report in Avamar Administrator also provides details on recent replication activities. You can filter the report to view only replication activities associated with a Data Domain system.

Server maintenance activity monitoring

Avamar performs the system maintenance operations for backup data on the Data Domain system, including HFS checks, checkpoints, rollbacks, garbage collection, and secure backup deletion.

The `ddrmaint` utility implements all required operations on the Data Domain system for the Avamar server. The `ddrmaint` utility is installed on the utility node of a multi-node server, or the single node of a single-node server, during Avamar server installation. The `ddrmaint` utility is not installed on the data nodes of the Avamar server.

The `ddrmaint` utility logs all maintenance activities on the Avamar server in the `ddrmaint.log` file, which is located in the `/usr/local/avamar/var/ddrmaintlogs` directory on the utility node of a multi-node Avamar server. The `ddrmaint.log` file is rotated when it reaches 25 MB in size.

A

Troubleshooting

Topics:

Viewing detailed status information for troubleshooting

Icons on the status bar in Avamar Administrator indicate whether there is a problem either with the Avamar connection to a Data Domain system or with a Data Domain system.

About this task

Table 13. Status bar problem indicators

Status bar icon	Description
	Avamar cannot retrieve information from a Data Domain system. However, backups and restores can continue during this condition.
	Avamar cannot connect to a Data Domain system, or a Data Domain system is disabled in some way. Backups and restores do not occur during this condition.

If one of the icons in the previous table appears in the status bar, you can view more detailed status information for the Data Domain system on the **Server Management** tab in the **Server** window.

Steps

1. In Avamar Administrator, click the **Server** launcher link.
   The **Server** window appears.
2. Select the **Server Management** tab, and then select the Data Domain system in the tree.
   The **Monitoring Status** row in the right pane provides detailed status of the Data Domain system.

Data Domain status and resolutions

The following table lists the available values for the **Monitoring Status** row on the **Server Management** tab in the **Server** window in Avamar Administrator. If the status indicates a problem, a proposed resolution is provided.

Table 14. Monitoring status values and resolutions

Monitoring status	Resolution
OK	No resolution is required.

Table 14. Monitoring status values and resolutions (continued)

Monitoring status	Resolution
`SNMP Getter/Setter disabled`	Use the Data Domain SSH CLI to enable SNMP by typing **`snmp enable`**.
`Unable to get CPU, disk, and network statistics data`	Use the Data Domain SSH CLI to enable SNMP by typing **`snmp enable`**.
`Unable to get CPU and disk statistics data`	Use the Data Domain SSH CLI to enable SNMP by typing **`snmp enable`**.
`Unable to get network statistics data`	Use the Data Domain SSH CLI to enable SNMP by typing **`snmp enable`**.
`Unable to get file system statistics data`	Use the Data Domain SSH CLI to enable SNMP by typing **`snmp enable`**.
`Error invoking ssh cli command`	Review the system log files to determine the cause of the problem. You should also review the *DD OS Command Reference Guide*.
`File system disabled`	Use the Data Domain SSH CLI to enable Data Domain file system operations by typing **`filesys enable`**. When the Data Domain file system is disabled, Avamar cannot perform backups to and restores from the device. After you enable file system operations, it might take as long as 10 minutes before Avamar Administrator correctly reflects the status of the Data Domain system, especially if the Data Domain system is a DD Extended Retention. Do not perform backups, restores, or system maintenance operations until the status appears correctly in Avamar Administrator. Otherwise, the backups, restores, or system maintenance operations might fail.
`Unable to get SNMP file system status`	Verify that the SNMP getter/setter port is valid. This is the port that you specified when you added the Data Domain system to the Avamar configuration.
`Failed to authenticate ssh cli connection with ssh key`	Verify that the SSH public/private key pair was set up correctly on both the Avamar server and the Data Domain system. Re-creating the SSH public/private key pair provides more information.
`Failed to authenticate SSH CLI connection with credentials`	Verify that the DD Boost user credentials are correct. The credentials are the username and password that you specified when you added the Data Domain system to the Avamar configuration.
`Unable to retrieve ssh key file pair`	Verify that the SSH public/private key pair is set up correctly on both the Avamar server and the Data Domain system, and that the public key is copied to the correct location on the Data Domain system. Re-creating the SSH public/private key pair provides more information.
`Unable to retrieve ssh public key file`	Verify that the SSH public/private key pair was set up correctly on both the Avamar server and the Data Domain system, and that the public key was copied to the correct location on the Data Domain system. Re-creating the SSH public/private key pair provides more information.
`Unable to retrieve ssh private key file`	Verify that the SSH public/private key pair was set up correctly on both the Avamar server and the Data Domain system. Re-creating the SSH public/private key pair provides more information.

Table 14. Monitoring status values and resolutions (continued)

Monitoring status	Resolution
DDBoost disabled	Enable DD Boost using either the Data Domain SSH CLI or the web-based Data Domain Enterprise Manager. To enable DD Boost by using the SSH CLI, type **ddboost enable**. When DD Boost is disabled, Avamar cannot perform backups to and restores from the device.
DDBoost user disabled	Use the Data Domain SSH CLI to enable the DD Boost user by typing **user enable *username***, where *username* is the username of the DD Boost user. When the DD Boost user is disabled, Avamar cannot perform backups and restores to and from the device.
DDBoost user changed on Data Domain system	If you edited the DD Boost user account information on the Data Domain system, then you must edit the DD Boost user account information in the Data Domain configuration on the Avamar server. When you edit the DD Boost user account information in Avamar Administrator, the SSH key may fail. To resolve this issue, re-add the SSH key using the instructions in Re-creating the SSH public/private key pair.
DDBoost option disabled	Use the Data Domain SSH CLI to enable DD Boost by typing **ddboost option set distributed-segment-processing enabled**. Backups continue when DD Boost is disabled. However, performance decreases.
DDBoost option not available	No resolution is required. The Data Domain system is in a cluster. DD Boost is not available in a cluster.
DDBoost not licensed	Use the Data Domain SSH CLI to add the license for DD Boost by typing **license add *license***, where *license* is the license code.
Invalid SNMP port	To resolve this issue, use the instructions in Preparing the Data Domain system for Avamar integration on page 22. Verify that you specified the correct getter/setter port when you added the Data Domain system to the Avamar configuration, and ensure that the getter/setter port is open on the Data Domain system by typing **snmp show trap-hosts**.
Invalid SNMP trap host or trap port	To resolve this issue, use the instructions in Preparing the Data Domain system for Avamar integration on page 22. Use the Data Domain SSH CLI to verify that the Avamar server is configured as a trap host on the Data Domain system by typing **snmp show trap-hosts**. If necessary, use the Data Domain SSH CLI to add the Avamar server as a trap host on the Data Domain system by typing **snmp add trap-host *hostname***, where *hostname* is the hostname of the Avamar server. By default, port 163 is used. Verify that you specified the correct trap port when you added the Data Domain system to the Avamar configuration.

Table 14. Monitoring status values and resolutions (continued)

Monitoring status	Resolution
`Invalid SNMP community string`	To resolve this issue, use the instructions in Preparing the Data Domain system for Avamar integration on page 22. Use the Data Domain SSH CLI to verify the SNMP community string by typing **`snmp show ro-communities`**. Verify that you specified the correct SNMP community string when you added the Data Domain system to the Avamar configuration.
`Error getting SNMP objects`	Review the system log files to determine the cause of the problem. Search the Data Domain knowledgebase for the error message.
`SNMP trap manager is not running`	Start the Data Domain SNMP Manager service: 1. In Avamar Administrator, click the **Administration** tab. The **Administration** window appears. 2. Click the **Services Administration** tab. 3. Right-click the **Data Domain SNMP Manager** row in the right pane and select **Start Data Domain SNMP Manager**.
`Unknown Host`	The DNS server cannot resolve the hostname of the Data Domain system. Ensure that the hostname and IP address for the Data Domain system are configured correctly in DNS.
`Host is not reachable`	Avamar cannot connect to the hostname or IP address of the Data Domain system. This may be because the device is powered off, there is a network connection issue, the connection is blocked by the firewall, and so on.
`Invalid host, user name, or password`	Ensure that you specified the hostname or IP address of the Data Domain system, the DD Boost username, and password. Attempt to log in to the Data Domain system with the specified username and password. Verify that the Avamar server can ping the Data Domain system.
`Synchronization of maintenance operations is off`	Avamar cannot synchronize maintenance operations such as checkpoints, HFS checks, and Garbage Collection with the Data Domain system. Avamar Support must enable synchronization of these operations by using the `avmaint config` command to set the `useddr` value to `TRUE`.
`Unknown`	Contact Data Domain Support.

Monitoring status

When the monitoring status on the **Server Management** tab in the **Server** window in Avamar Administrator is a value other than `OK`, additional information appears in a list below the **Monitoring Status**.

The following table describes status messages and provides resolutions if the status indicates a problem.

Table 15. Server Management monitoring status details

Monitoring status	Description
• `DDBoost Licensed` • `DDBoost not Licensed`	DD Boost licensing status.

Table 15. Server Management monitoring status details (continued)

Monitoring status	Description
	If the value is `DDBoost not licensed`, then use the Data Domain SSH CLI to add the license for DD Boost by typing **`license add license`**, where *license* is the license code.
• `DDBoost Enabled` • `DDBoost Disabled`	DD Boost status. If the value is `DDBoost Disabled`, then enable DD Boost by using either the Data Domain SSH CLI or the web-based Data Domain Enterprise Manager. To enable DD Boost by using the SSH CLI, type **`ddboost enable`**. When DD Boost is disabled, Avamar cannot perform backups to and restores from the device.
• `DDBoost User Enabled` • `DDBoost User Disabled`	DD Boost user status. If the value is `DDBoost User Disabled`, then use the Data Domain SSH CLI to enable the DD Boost user by typing **`user enable username`**, where *username* is the username of the DD Boost user. When the DD Boost user is disabled, Avamar cannot perform backups to and restores from the device.
• `DDBoost User Valid` • `DDBoost User Changed`	DD Boost user status. If the value is `DDBoost User Changed` and you edited the DD Boost user account information on the Data Domain system, then you must edit the DD Boost user account information in the Data Domain configuration on the Avamar server. When you edit the DD Boost user account information in Avamar Administrator, the SSH key may fail. To resolve this issue, re-add the SSH key using the instructions in Re-creating the SSH public/private key pair.
• `DDBoost Option Enabled` • `DDBoost Option Disabled` • `DDBoost Option not Available`	DD Boost option status. If the value is `DDBoost Option Disabled`, then use the Data Domain SSH CLI to enable DD Boost by typing **`ddboost option set distributed-segment-processing enabled`**. Backups continue when DD Boost is disabled. However, performance decreases. If the value is `DDBoost Option not Available`, then the Data Domain system is in a cluster, and DD Boost is not available in a cluster.
• `SNMP Enabled` • `SNMP Disabled`	SNMP status. If the value is `SNMP Disabled`, then use the Data Domain SSH CLI to enable SNMP by typing **`snmp enable`**.
• `File System Running` • `File System Enabled` • `File System Disabled` • `File System Unknown` • `File system status unknown since SNMP is disabled`	Status of the Data Domain file system. When the Data Domain file system is disabled, Avamar cannot perform backups to and restores from the device. If the value is `File System Disabled`, then use the Data Domain SSH CLI to enable Data Domain file system operations by typing **`filesys enable`**.

Table 15. Server Management monitoring status details (continued)

Monitoring status	Description
	If the value is `File system status unknown since SNMP is disabled`, then use the Data Domain SSH CLI to enable SNMP by typing **`snmp enable`**. If the value is `File System Unknown`, then verify that the SNMP getter/setter port is valid. This is the port that you specified when you added the Data Domain system to the Avamar configuration. If you enable file system operations, it may take as many as 10 minutes before Avamar Administrator correctly reflects the status of the Data Domain system, especially if the Data Domain system is a DD Extended Retention. Do not perform backups, restores, or system maintenance operations until the status appears correctly in Avamar Administrator. Otherwise, the backups, restores, or system maintenance operations may fail.
• `Synchronization of maintenance operations is off` • `Synchronization of maintenance operations is on`	Synchronization status of maintenance operations, such as checkpoints, HFS checks, and Garbage Collection, between the Avamar server and the Data Domain system. If the value is `Synchronization of maintenance operations is off`, then Avamar Support must enable synchronization of these operations by using the `avmaint config` command to set the `useddr value` to `TRUE`.

Common problems and solutions

This topic lists common problems and solutions when you store Avamar backups on a Data Domain system.

Backups to Data Domain storage corrupted due to client NIC configuration

If the Network Interface Card on client machines does not have ECC memory enabled, backups to the Data Domain system might result in silent corruption of data.

Backup fails if the Data Domain system is offline

If the Data Domain system is offline when a backup starts, then the backup may take five minutes or more before it fails. The failure occurs because there is a minimum timeout period of five minutes for almost all DD Boost operations.

To resolve the failed backup, set the Data Domain system online and then retry the backup.

Tail-log backup restrictions with DD Extended Retention

If you are restoring SQL Server data from either the target archive or sealed archive tiers on a DD Extended Retention, then you must clear the **Tail-log backup** checkbox to disable tail-log backups. The **Use SQL Replace** checkbox must be selected. Otherwise, the restore fails. Tail-log backups are supported only when restoring data from the active tier of a Data Domain system.

Level 1 Oracle backups to a DD Extended Retention may time out

When performing a Level 1 backup from an Oracle client to a DD Extended Retention, the backup may time out and fail in the process of creating a snapview. To work around this issue, increase the timeout limit by adding the following flag to the `avoracle.cmd` file:

`--[avoracle]subprocesstimeoutsecs=`*n*

where *n* is the number of seconds before the timeout occurs. The default value is 150. A value of 200 or greater is recommended.

Rollback includes deleted Data Domain system

If you roll back to a checkpoint that contains a configured Data Domain system that you deleted from the configuration after the checkpoint, then the Data Domain system is restored to the configuration.

If you do not want the Data Domain system, then delete it from the configuration after the rollback completes. However, if you want to restore the Data Domain system to the configuration, then you must re-add the SSH key and trap host to the Data Domain system. These values are deleted when you delete the Data Domain system and cannot be restored on the Data Domain system during a rollback of the Avamar server. To restore these values, open the **Edit Data Domain System** dialog box in Avamar Administrator and click the **Re-add SSH Key** and **Re-add Trap Host** buttons.

Backend capacity reports fail

Do not run a backend capacity report for a client with backups on a Data Domain system. Otherwise, the report fails. Backend capacity reports cannot include data on a Data Domain system.

Reclaiming storage on a full Data Domain system

About this task

If you use all of the storage space on a Data Domain system, the following issues may occur:

- Backups do not succeed and may not start.
- Operations that change information on the Data Domain system fail, including the deletion of checkpoints, active backups, and expired backups during Garbage Collection. These operations may fail because they involve directory renames, which are not allowed on a full Data Domain system.

Steps

1. Determine the source of the data that is using the storage. The data may be from a specific client, a group of clients associated with a specific Avamar server, or a different backup product that stores data on the Data Domain system.
2. Cancel any backups that are in progress:
   a. In Avamar Administrator, click the **Activity** launcher button.
   b. In the **Activity** window, click the **Activity Monitor** tab.
   c. Select the backups, and then select **Actions** > **Cancel Activity**.
   d. Click **Yes** on the confirmation message.
3. Suspend backups and restores:
   a. In Avamar Administrator, click the **Server** launcher button.
   b. In the **Server** window, click the **Server Management** tab.
   c. In the tree pane, select the Avamar server node of the tree.
   d. Select **Actions** > **Suspend Backups/Restores**.
   e. Click **Yes** on the confirmation message.
4. Suspend server maintenance operations on the Avamar server:
   a. In Avamar Administrator, select **Tools** > **Manage Schedules**.
   b. In the **Manage All Schedules** window, click **Suspend All**.
5. On the Data Domain system, manually delete the existing `STAGING`, `DELETED`, or `cur/DELETED` directories for the Avamar server.

6. Use Data Domain Enterprise Manager to initiate the Data Domain file system cleaning operation.

   This process should free enough space to enable Avamar server maintenance operations to successfully complete.
7. Restart server maintenance operations on the Avamar server:
   a. In Avamar Administrator, select **Tools** > **Manage Schedules**.
   b. In the **Manage All Schedules** window, click **Resume All**.
8. Restart backups and restores:
   a. In Avamar Administrator, click the **Server** launcher button.
   b. In the **Server** window, click the **Server Management** tab.
   c. In the tree pane, select the Avamar server node of the tree.
   d. Select **Actions** > **Resume Backups/Restores**.
   e. Click **Yes** on the confirmation message.
9. After server maintenance operations completes, you might need to perform the following tasks to reclaim storage space on the Data Domain system:
   - Delete backups.
   - Delete checkpoints.
   - Run Avamar Garbage Collection.
   - Run the Data Domain file system cleaning operation.

Re-creating the SSH public/private key pair

When you add a Data Domain system to the Avamar configuration, the system automatically creates and exchanges the public/private keys that the Avamar Management Console Server (MCS) needs to enable a secure connection with the Data Domain Secure Shell (DDSSH) interface.

About this task

However, in some unlikely circumstances, such as if you edit the DD Boost account that Avamar uses to connect to the Data Domain system, then the SSH key may fail. If this occurs, you must re-create and re-add the key on the Data Domain system.

Steps

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Change to the `.ssh` directory by typing **`cd ~/.ssh`**.
3. Generate a public/private key pair by typing the following command:

   `ssh-keygen -t rsa -N "" -f ddr_key`

   This command sets `ddr_key` as the file name for the key. There is no passphrase for the key.
4. Log in to the Data Domain system by typing the following command:

   `ssh Avamar_ostuser@dd_system`

   where *Avamar_ostuser* is the name of the DD Boost user for Avamar on the Data Domain system, and *dd_system* is the name of the Data Domain system.
5. Add the SSH public key to the SSH authorized keys file on the Data Domain system by typing the following command:

   `adminaccess add ssh-keys user Avamar_ostuser`
6. Copy and paste the public key, which is the contents of the file `ddr_key.pub`, in `/home/admin/.ssh`:
   a. Open a second command shell and log in to the utility node of the Avamar server as admin.
   b. Change to the `.ssh` directory by typing **`cd ~/.ssh`**.
   c. Display the ddr_key.pub file by typing **`cat ddr_key.pub`**.
   d. Select and copy the contents of the file.
   e. Return to the first command shell window.
   f. Paste the contents of the file in `/home/admin/.ssh`.
7. Enter the key by pressing **`Ctrl`**+**`D`**.
8. Switch user to root by typing **`su -`**.
9. Change directory to `/usr/local/avamar/lib` by typing the following command:

cd /usr/local/avamar/lib/

10. Copy the private key to `/home/admin/.ssh/ddr_key`, which is the path and name specified by `ddr_ssh_key_path_name` in the `mcserver.xml` file, by typing the following command:

    cp /home/admin/.ssh/*ddr_key* .

    where *ddr_key* is the file name for the key.

11. Change the ownership of the key to the admin group by typing the following command:

    chown root:admin *ddr_key*

    where *ddr_key* is the file name for the key.

12. Change the permissions for the key to 440 by typing the following command:

    chmod 440 *ddr_key*

    where *ddr_key* is the file name for the key.

13. Test that you can log in to the Data Domain system without providing a password by typing the following command:

    ssh -i *path/ddr_key Avamar_ostuser*@*dd_system*

    where:

    - *path/ddr_key* is the path and filename of the key.
    - *Avamar_ostuser* is the name of the DD Boost user for Avamar on the Data Domain system.
    - *dd_system* is the name of the Data Domain system.

Using legacy certificate authentication with Data Domain requires command line flags

When performing a backup to Data Domain using the `--encrypt=tls-sa` command line flag to indicate legacy certificate authentication, metadata backups to the Avamar server will succeed but backups to the Data Domain will fail. For successful backup, you must specify the following flags:

```
--ddr-auth-enabled=false
--ddr-auth-mode=3
```

This will force certificate authentication for metadata backups to the Avamar server while allowing backups to the Data Domain to succeed.

Glossary

A

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 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*.

Avamar server
The server component of the Avamar client/server system. Avamar server is a fault-tolerant, high-availability system that efficiently stores the backups from all protected clients. It also provides essential processes and services required for data restores, client access, and remote system administration. Avamar server runs as a distributed application across multiple networked storage nodes.

B

backup
A point-in-time copy of client data that can be restored as individual files, selected data, or as an entire backup.

C

checkpoint
A server backup taken for the express purpose of assisting with disaster recovery of the Avamar server.

client
A computer or workstation that runs Avamar software and accesses the Avamar server over a network connection. Avamar client software consists of a client agent and one or more plug-ins.

D

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.

DD Boost
DD Boost is the API that Avamar clients use to access a Data Domain system. The DD Boost API is installed automatically on the client computer when you install the Avamar client. It is also installed automatically on the Avamar server when you install Avamar.

DD OS
Data Domain Operating System (DD OS) is the internal operating system on the Data Domain system. The DD OS provides both a command line interface (CLI) for performing all system operations and the Enterprise Manager (a graphical user interface, or GUI) for some configuration operations, management, and monitoring.

ddrmaint utility

Installed on the utility node of a multi-node server (or the single node of a single-node server), this utility implements all required operations on the Data Domain system on behalf of the Avamar server. It is not installed on the storage nodes of the Avamar server.

The `ddrmaint` utility also uses the DD Boost to connect to a Data Domain system. The DD Boost is installed with the `ddrmaint` utility automatically when you install Avamar.

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*.

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.

R

replication
Replication is an optional feature that enables an Avamar system to store read-only copies of its data on a remote system. The replicated data can be replicas of client backups and copies of Avamar system data. Replication supports disaster recovery of the Avamar system.

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

SNMP
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.