Dell EMC Avamar

Version 18.2

Product Security Guide

302-005-103

REV 01

DELL EMC

Published December 2018

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

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://support.EMC.com).

Purpose

This publication discusses various aspects of Avamar product security.

Audience

This publication is primarily intended for Field Engineers, contracted representatives, and business partners who are responsible for configuring, troubleshooting, and upgrading Avamar systems at customer sites, as well as system administrators or application integrators who are responsible for installing software, maintaining servers and clients on a network, and ensuring network security.

Revision history

The following table presents the revision history of this document.

Revision	Date	Description
01	December 14, 2018	GA release of Avamar 18.2

Related documentation

The following publications provide additional information:

- *Avamar Release Notes*
- *Avamar Administration Guide*
- *Avamar Operational Best Practices Guide*

The following other publications also provide information:

- *US Department of Defense (DoD) Security Technical Implementation Guide (STIG) for Unix*

Special notice conventions used in this document

These conventions are used for special notices.

DANGER

Indicates a hazardous situation which, if not avoided, results in death or serious injury.

WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Addresses practices that are not related to personal injury.

Note

Presents information that is important, but not hazard-related.

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/home/us/en/19.
2. Type a product name in the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box.
3. Select the product from the list that appears. When you select a product, the **Product Support** page loads automatically.
4. (Optional) Add the product to the **My Products** list by clicking **Add to My Saved Products** in the upper right corner of the **Product Support** page.

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

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

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

To search the Knowledgebase:

1. Go to https://www.dell.com/support/home/us/en/19.
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 http://community.EMC.com 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

CHAPTER 1

Introduction

This chapter includes the following topics:

Security patches

Each Avamar release is available with a set of up-to-date security patches.

Periodic security updates for multiple components

Security updates are periodically provided for components of the Avamar system's host operating system. These periodic updates combine patches and updates that the operating system's company (Red Hat or SUSE) released since the previous Avamar periodic security update. The updates also include relevant kernel-level and OS-level security patches and changes.

The periodic updates are cumulative. Install each periodic update that is issued for the Avamar system in order of release, starting with the first periodic update issued after the release of the Avamar system software.

Each periodic update is announced through a Security Advisory (ESA). The ESA provides details about the contents of the periodic update and installation instructions. Go to https://support.emc.com/products/759_Avamar-Server to view these advisories and to register for email notifications.

Periodic updates are provided as Avamar update packages that can normally be installed through Avamar Installation Manager.

Remedying security patch compatibility issues

If you separately install other security patches or security applications that are found to be incompatible with Avamar:

1. Remove the separately installed patches or applications.
2. Restore the Avamar system to its previous working configuration.
3. File a support case with Avamar Customer Support that includes a specific description of the separately installed patches or applications.

Note

It is the responsibility of the customer to ensure that the Avamar system is configured to protect against unauthorized access. Back up all important files before you apply new security patches, applications, or updates.

Email home notification using ConnectEMC

When configured and enabled, the "email home" feature automatically emails configuration, capacity, and general system information to Avamar Customer Support using ConnectEMC. Summary emails are sent once daily; critical alerts are sent in near-real time on an as needed basis.

The *Avamar Administration Guide* provides details on how to enable the email home feature.

Remote access

If Avamar Customer Support must connect to a customer system to perform analysis or maintenance, the customer can initiate a web conference using a web-based conferencing application such as WebEx.

Additionally, customers can install a Secure Remote Support (ESRS) gateway to allow Customer Support to access their systems without WebEx.

Avamar security features

Installing or upgrading the Avamar server software installs hardening and firewall packages that improve security capabilities on the Avamar server. Installation of the hardening package does not restrict supported server functionality. Installation of the firewall package prevents unencrypted backups from running. These packages cannot be uninstalled.

If you are upgrading from an older version and the scheduled backups are unencrypted, follow the instructions in Permitting unencrypted data-in-flight on page 132 to enable unencrypted backups. For some other tasks, Customer Support provides the steps and tools that are required to complete the task (for instance, FTP capabilities for downloading packages to the server).

Avamar firewall hardening

Starting in Avamar 7.2, the Avamar firewall blocks outgoing FTP access. Commands such as `wget` and `curl` fail to reach the target hosts or download any files.

To download hotfixes and other updates from FTP sites, you must disable the Avamar firewall for the duration of the transfer and then re-enable the firewall after the transfer completes.

Procedure

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. Switch user to root by typing the following command:

   ```
   su -
   ```
3. Disable the Avamar firewall by typing the following command:

   ```
   service avfirewall stop
   ```
4. Enable FTP access by typing the following command:

   ```
   /usr/local/avamar/lib/admin/security/ftp_service
   ```
5. Change directory by typing the following command:

   ```
   cd /usr/local/avamar/src/
   ```
6. Download the required file by typing the following command on one line:

   ```
   curl --disable-eprt -P `hostname -i`:35000-35010 -O <url>
   ```

   where *<url>* is the location of the required file.

7. After the transfer completes, enable the Avamar firewall by typing the following command:

   ```
   service avfirewall start
   ```

CHAPTER 2

Authentication

This chapter includes the following topics:

About authentication

The concept of authentication governs the identification of all users who are permitted to take action within an Avamar server. Authentication prescribes certain users as possessing credentials that enable the Avamar server to recognize their identity and, later, grant any authorized permissions.

This chapter describes how users log in to an Avamar server, including means of preventing unauthorized access, and how to manage and configure both user and component authentication.

The *Avamar Administration Guide* provides specific tasks to add, configure, and delete Avamar user accounts, and to configure directory service authentication.

Overview of Avamar user accounts

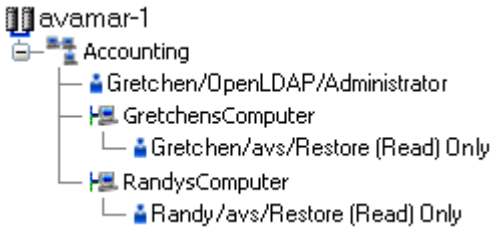
A user account in Avamar can administer a domain or client. The user account defines the authentication system that is used to grant users access to the Avamar server. It also defines the role for the user, which controls the operations that a user can perform.

You can add user accounts to domains or individual clients. When you add a user account to a domain, the account can administer that domain and any subdomains beneath it. When you add a user account to an individual client, the account can perform backups and restores of that client, and access backups belonging to that client in the system.

In Avamar, users are entries in a domain or client access list. When you add a user account to the Avamar system, you are adding an entry to a domain or client user access list.

In the following example, the user “Gretchen” has been added to both the Accounting domain and a computer. However, the authentication system and role are completely separate user accounts that happen to have the same username.

Figure 1 Users in Avamardomains



The following table describes the information that comprises an Avamar user account.

Table 2 Avamar user account information

Information	Description
Username	The username depends on the authentication system and must be in the format that the authentication system accepts. For example, the internal authentication system uses case-sensitive usernames, whereas Windows Active

Table 2 Avamar user account information (continued)

Information	Description
	Directory usernames are case-insensitive. Usernames cannot be longer than 31 characters.
Authentication system	An authentication system is a username/password system that is used to grant users access to the Avamar server.
Role	Roles define the allowable operations for each user account.

Login security settings

The following sections provide information on configuring the login security settings for Avamar.

Login banner configuration

This section provides information on configuring the login banners for Avamar.

STIG requirement GEN005550 requires that the `ssh` protocol support a customer banner. However, the Avamar system is not compliant with this requirement. Custom `ssh` banners are not supported.

Configure login security

This topic provides information about the login behavior for Avamar components.

Most login security configuration options are part of level-2 security hardening features that you can install during Avamar server software installation, or manually after server software installation. Level-2 security features also provide additional behaviors described elsewhere in this guide.

Level-2 security hardening
The additional OS hardening package provides the following capabilities that are specific to server logins:

- Setting terminal timeout at 15 minutes
- Removal of unnecessary default accounts and groups

This package satisfies the following STIG requirements that relate to server logins:

Table 3 STIG requirements satisfied by the additional OS hardening package

Requirement ID	Requirement title
GEN000460	Unsuccessful Login Attempts - Account Disabled
GEN000480	Unsuccessful Login Attempts - Fail Delay
GEN000500	Terminal Lockout
GEN000980	Root Console Access

Table 3 STIG requirements satisfied by the additional OS hardening package (continued)

Requirement ID	Requirement title
GEN001000	Remote Consoles Defined
GEN001020	Direct Root Login
GEN001120	Encrypting Root Access

Level-2 additional password hardening

You can configure Avamar servers to provide additional password hardening features, such as:

- Aging — how long a password can be used before it must be changed
- Complexity — required number and type of characters in passwords
- Reuse — number of previously used passwords that can be recycled

Note

Password hardening is not appropriate for all customers. Successful implementation of this feature requires structures and policies that enforce changes to all operating system user accounts every 60 days, and require users to log in to those accounts at least once every 35 days. Failure to implement proper structures and policies before installing the password hardening feature might cause you to be locked out of your Avamar server.

Note

Recent versions of Avamar require the passwords for system user accounts, and the admin and root accounts, to expire every 60 days. The SSH console prompts users to change the password.

You can also change the current complexity configuration and aging rules. User and credential management on page 43 provides more information. However, use the same caution when changing any password configuration details to ensure successful implementation, and perform a backup of the configuration files before making any changes.

Additional password hardening satisfies the following STIG requirements that relate to server logins:

Table 4 STIG requirements satisfied by additional password hardening

Requirement ID	Requirement title
GEN000540	Password Change 24 Hours
GEN000560	Password Protect Enabled Accounts
GEN000580	Password Length
GEN000600	Password Character Mix
GEN000620	Password Character Mix
GEN000640	Password Character Mix
GEN000660	Password Contents

Table 4 STIG requirements satisfied by additional password hardening (continued)

Requirement ID	Requirement title
GEN000680	Password Contents
GEN000700	Password Change Every 60 Days
GEN000740	Password Change Every Year
GEN000760	Inactive Accounts are not locked
GEN000780	Easily Guessed Passwords
GEN000800	Password Reuse
GEN000820	Global Password Configuration Files
GEN000840	Root Account Access

Following successful installation and configuration, the Avamar server enforces the following rules for all local Avamar server operating system user accounts and passwords:

- Password aging
- Password complexity, length, and reuse

Failed login behavior

You can configure the maximum allowed number of failed login attempts for the Avamar server. When a user reaches the failed login attempt threshold, the server locks the user out of the system.

The default threshold value is five failed attempts. The server automatically unlocks after a configurable interval. By default, the interval is 5 minutes, however the admin user can also reset the lock by restarting the MCS.

Configure failed login behavior

Configuring actions on reaching the authentication failure threshold is a level-2 security feature.

The documentation for pam_tally provides more information about parameters and values.

Procedure

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, and then switch user to root by typing **su -**.
   - For a multi-node server, log in to the utility node as admin, and then switch user to root by typing **su -**.
2. Back up the login configuration file by typing the following command:

   cp /etc/pam.d/common-auth /etc/pam.d/common-auth.`date +%s`
3. Using a Linux text editor, such as `vi`, open the file `/etc/pam.d/common-auth`.
4. Locate the line that begins with `auth required pam_tally2.so`.

   For example: `auth required pam_tally2.so deny=3 lock_time=5`

a. If this line does not exist, or is commented out, insert a new line with the necessary parameters after the comment `# BEGIN Avamar modifications`, before the remaining lines.

5. Update the parameters that control the behavior for failed logins.

Parameter	Description
deny	The threshold for failed authentication attempts, after which the operating system locks the user account.
lock_time	The duration for which the operating system prevents login to the user account after each authentication failure. The operating system locks the user account for this duration even if the user has not reached the authentication failure threshold. Use this parameter to rate-limit failed logins.
unlock_time	The interval for which the operating system should wait before re-enabling the specified user account, after a user reaches the authentication failure threshold.
magic_root	Do not track the number of failed authentication attempts for the root user account.
even_deny_root_account	Allow the operating system to disable access to the root user account after reaching the authentication failure threshold. Dell EMC does not recommend using this parameter.

Do not modify the configuration values on other lines.

Note that user accounts which reach the authentication failure threshold are permanently locked, unless you specify the `unlock_time` parameter or manually unlock the user account.

6. Save and close the file.

For example:

- To configure a policy that denies login for five seconds after each authentication failure, triggers lockout after six failed attempts, and requires an administrator to manually enable locked user accounts:

```
# BEGIN Avamar modifications
auth    required    pam_tally2.so deny=6 lock_time=5
```

- To configure a policy that denies login for five seconds after each authentication failure, triggers lockout after three failed attempts, and automatically restores access after five minutes:

```
# BEGIN Avamar modifications
auth    required    pam_tally2.so deny=3 lock_time=5
unlock_time=300
```

After you finish

For a multi-node server, repeat this task on all storage nodes.

To manually enable a user account, type the following command as the root user:

```
pam_tally2 -u AccountName --reset
```

Authentication types and setup

An authentication system is a username/password system that is used to grant domain and client users access to the Avamar server.

Avamar supports its own internal authentication system ("Avamar authentication" or "avs"), as well as directory service authentication. Directory service authentication uses an existing LDAP v.3 directory service or an existing Network Information Service (NIS) to provide authentication.

The following topics provide information on the available authentication types and configuration options.

Avamar internal authentication

With Avamar internal authentication, you define the username and password for Avamar user accounts, and Avamar stores the information. Usernames are case-sensitive and cannot be longer than 31 characters.

No additional steps are required to use internal Avamar authentication to authenticate user accounts. You define the username and password for each account when you add the user in Avamar Administrator or the AUI.

Directory service authentication

Use directory service authentication to authenticate and assign roles to Avamar users by using information from an existing directory service. Directory service authentication works with specific LDAP directory services and provides additional functionality when used with an OpenLDAP directory service. Directory service authentication also works with a Network Information Service (NIS), on its own or with one of the supported LDAP directory services.

Avamar products that use directory service authentication

The following Avamar products can use directory service authentication to authenticate and authorize users:

- Avamar Administrator
- Avamar Web Restore
- Avamar client web UI (Avamar Desktop/Laptop)

Avamar product that uses directory service client records

Avamar Client Manager does not use directory service authentication to authenticate and authorize user logins. However, Avamar Client Manager can use the directory service mechanism to obtain information about computers that are potential Avamar clients. Avamar Client Manager queries the directory service to obtain information about clients and, if available, directory service organizational units, such as directory domains, and directory groups.

Directory services types

Directory service authentication supports the following types of directory services:

Table 5 Supported directory service types

Type	Supported implementations
LDAP	• Active Directory for Windows Server 2003 • Active Directory Domain Services for Windows Server 2008 • Active Directory Domain Services for Windows Server 2012 • Active Directory Domain Services for Windows Server 2016 • 389 Directory Server version 1.1.35
OpenLDAP	SUSE OpenLDAP version 2.4
NIS	Network Information Service

Avamar supports encrypted LDAP and OpenLDAP directory service authentication via SSL/TLS. By default, Avamar uses TLS 1.2 if supported by the LDAP or OpenLDAP server. Otherwise, Avamar falls back to a supported version of SSL/TLS. However, the Avamar server does not provide an SSL/TLS certificate to the LDAP or OpenLDAP server for client authentication.

LDAP maps

Directory service authentication uses LDAP maps to form a group of Avamar domain users by using information from a directory service. Link Avamar authorization levels to mapped directory service user accounts to create LDAP maps. The Adding an LDAP map section provides more information.

NOTICE

Deleting an Avamar domain removes the LDAP maps that rely on that Avamar domain for access. However, removing LDAP maps does not affect the directory service groups or the directory service user records that are associated with the removed maps.

Common Access Card and Personal Identity Verification

Avamar supports user authentication by using a Common Access Card (CAC) for United States Department of Defense (DoD) personnel or a Personal Identity Verification (PIV) smart card for US federal government employees and contractors.

About CAC/PIV authentication

Avamar implements CAC/PIV authentication by presenting alternative login prompts for Avamar Installation Manager and Avamar Administrator. After an administrator configures the Avamar server for CAC/PIV authentication, the following actions occur:

1. The Avamar software displays the CAC/PIV authentication prompts and requires the insertion of a smart card in the smart card reader before proceeding.
2. When prompted, the user supplies a PIN to unlock the list of security certificates that are stored on the smart card.
3. The user selects a security certificate with appropriate authorization.

4. The Avamar software or web browser retrieves the security certificate from the smart card.
5. The validation authority (VA) service verifies the security certificate.
6. Avamar extracts login credentials from the security certificate.
7. An external LDAP server provides the LDAP groups that are associated with the login credentials.
8. Avamar maps these LDAP groups to a corresponding Avamar authorization.

When CAC/PIV authentication is configured, use the login procedures in this appendix whenever a procedure directs you to log in to the Avamar Installation Manager or to Avamar Administrator.

The topics in this appendix assume the following:

- You have a general understanding of the principles of operation for smart cards and LDAP authentication.
- You have configured Avamar for LDAP directory service authentication and the LDAP server contains appropriate users and roles.

  The *Avamar Administration Guide* provides more information.
- You have configured a VA server to validate user security certificates.
- You have the CA issuer certificate that signed the end-user security certificates, in `.pem`, `.cer`, or `.p7b` format.

  You may also optionally supply a CAC/PIV security certificate for the Avamar server, in `.pem`, `.cer`, or `.p7b` format.

  Note

  This optional server-specific CAC/PIV certificate is unique to each Avamar server and signed by the CA issuer.

  Either security certificate can be used to secure communication between the Avamar server and CAC/PIV-enabled clients. However, supplying a server-specific CAC/PIV certificate configures CAC/PIV-enabled clients to trust only communication with this specific Avamar server.

- You know the details of your site implementation of CAC/PIV authentication, including:
  - The hostnames and IP addresses of the LDAP and VA servers.
  - The LDAP search username, password, and filter.

A Microsoft TechNet article provides details about configuring Windows behavior in the event of smart card removal: https://technet.microsoft.com/en-us/library/jj852235(v=ws.11).aspx.

Important information

CAC/PIV authentication presents the following requirements:

- Avamar 7.4.1 or later.
- Microsoft Windows operating system.
- Internet Explorer 8 or later.
- OpenSC libraries, version 0.16 or later.

CAC/PIV authentication is not compatible with Network Information Service (NIS) or Kerberos authentication.

Before you enable or disable CAC/PIV authentication, ensure that the following additional prerequisites are met:

- The Avamar Installation Manager is not configuring or installing workflow packages.
- There are no active or waiting backup jobs.

Some Avamar interfaces do not support CAC/PIV authentication, including:

- The Avamar Installation Manager command line interface.
- The management console command line interface (MCCLI).
- The management console software development kit (MCSDK) interface for simple object access protocol (SOAP) web services.
- The Avamar Downloader Service.
- SSH console access.
- The local console service ports on ADS Gen4S and Gen4T nodes.
- Interfaces for third-party resources, such as vCenter.

Log file locations

The following logs contain information related to CAC/PIV authentication:

- `cac.pl` script:

  `/usr/local/avamar/var/log/cac.log`
- Avamar Installation Manager:

  `/usr/local/avamar/var/avi/server_log/avinstaller.log.0`

  `/usr/local/avamar/var/avi/webserv_log/jetty.log`
- Management console server:

  `/usr/local/avamar/var/mc/server_log/mcserver.log.0`
- Avamar Administrator client:

  `C:\Users\`*`username`*`\.avamardata\var\mc\gui_log\mcclient.log.0`
- VA service:

  `/opt/vas/logs/vas.log`
- Apache:

  `/var/log/apache2/access_log`

  `/var/log/apache2/error_log`

  `/var/log/apache2/ssl_request_log`
- Avamar software upgrade workflows:

  `/usr/local/avamar/var/avi/server_data/package_data/AvamarUpgrade-`*`version`*`/workflow.log`

Enabling CAC/PIV authentication

Enabling CAC/PIV authentication on an Avamar server is a multi-step process that consists of the following tasks:

- Updating the server configuration files.
- Opening the appropriate ports in the Avamar firewall.

- Enabling the CAC/PIV feature, which includes:
  - Importing the security certificates into the keystore.
  - Enabling two-way client authentication.
  - Configuring the VA service to start automatically on system startup.
  - Configuring the Apache web server.
  - Restarting the AvInstaller, management console, VA, and Apache services.

Note

When you enable CAC/PIV authentication, the **Avamar REST API** and **Avamar User Interface (AUI)** authentication is disabled and you will not be able to log in using these methods.

Updating server configuration files

This task updates two configuration files that provide the Avamar software with access to the VA server.

Procedure

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. Switch user to root by typing the following command:

   su -
3. Copy the CA issuer and optional server-specific CAC/PIV security certificates to `/root`.
4. Edit `mcserver.xml` with a text editor, such as `vi`, by typing the following command:

   vi /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml
5. Search for the `cac` node. The following example shows key/value pairs for an unconfigured server:

```
  <node name="cac">
    <map>
      <entry key="san_index" value="" />
      <entry key="ldap_login_ap" value="" />
      <entry key="ldap_domain_mapping" value="" />
      <entry key="ldap_search_filter" value="userPrincipalName" />
      <entry key="ldap_login_user" value="" />
      <entry key="cac_settings_path" value="/usr/local/
avamar/lib/cac/settings.properties" />
      <entry key="vas_url" value="http://localhost:7480/
validation/cert" />
    </map>
  </node>
```

6. Configure the following keys with appropriate values:

Key name	Value description
ldap_login_user	The username for LDAP authorization.
ldap_login_ap	The password for LDAP authorization.

Key name	Value description
ldap_search_filter	The filter to use when searching for LDAP authorization.
san_index	Specify which Subject Alternative Name (SAN) to use in the certificate if multiple SANs are available. By default, Avamar MCS loops the SANs to discover the first qualified one.
ldap_domain_mapping	If the certificate contains a SAN that ends with a uPNSuffix instead of an actual domain that contains the user, use this key to specify the actual LDAP domain so that the domain that contains the user can be discovered.

When you enable CAC/PIV authentication, Avamar encrypts the plaintext password.

Note

Ensure that the appropriate user entries exist on the LDAP server and that the proper roles are assigned to each user. After validating the security certificate, Avamar consults the LDAP server to determine a role for the user. LDAP directory searches use the value of the security certificate's `subjectAltName` field.

7. Save and close the file.
8. Edit `vas.properties` with a text editor, such as `vi`, by typing the following command:

   `vi /opt/vas/config/vas.properties`

   Output similar to the following appears:

```
# VA server configuration
va.use.https.communication=false
va.http.host=localhost
va.http.port=7080
va.https.port=7043
va.signing.cert.path=/opt/vas/config/va.cer
va.hashing.algorithm.oid=1.2.840.113549.1.1.11
va.ocsp.nonce.ext=true
va.ocsp.response.cache=false
va.max.cache.size=300
va.max.cache.time=3600
va.verify.response.signature=true
va.ssl.cert.path=/opt/vas/config/va_ssl.cer
# Cert configuration
issuer.cert.path=/opt/vas/config/issuer.cer
cert.store.path=/root/.keystore
cert.store.pass=password
crl.repo.url=http://localhost/CRLD/ca_crl.crl
crl.local.path=/opt/vas/config/ca_crl.crl
end.cert.upload.repo=/tmp
# cert validation methods [OCSP, SCVP, CRL]
cert.validation.method=OCSP
```

9. Configure the following properties with appropriate values:

Property name	Value description
va.http.host	The hostname or IP address of the VA server.
va.http.port	The port number of the VA server.
va.signing.cert.path	The local path to the server certificate.
issuer.cert.path	The local path to the CA issuer certificate.

Note the port numbers that you configure for the `va.http.port` and `va.https.port` properties.

10. Save and close the file.

Configuring the Avamar firewall

This task opens two ports in the Avamar firewall for the VA service to communicate with the VA server.

Procedure

1. Change directory by typing the following command:

   `cd /usr/local/avamar/lib/admin/security`

2. Run the firewall rules script by typing the following command:

   `./edit-firewall-rules.sh`

   The following output appears:

   ```
   Choose an Action
   ----------------
   1) Add a custom rule
   2) Remove a custom rule
   3) List Current Custom Rules
   4) Exit
   5) Save & Exit
   Enter desired action:
   ```

3. Type `1` to add a custom rule and press **Enter**.

   The following output appears:

   ```
   Firewall Rule Types
   -------------------
   1) IPv4 Rule
   2) IPv6 Rule
   Enter Firewall Rule Type:
   ```

4. Type the number that corresponds to the addressing system in use and press **Enter**.

   The following output appears:

   ```
   Firewall Chains
   ---------------
   1) OUTPUT
   2) INPUT
   3) LOGDROP
   4) FORWARD
   Select Chain:
   ```

5. Type `1` to add an output rule and press **Enter**.

   The following output appears:

   ```
   Protocol
   --------
   1) TCP
   ```

```
2) UDP
3) ICMP
Enter Protocol:
```

6. Type `1` to select TCP and press **Enter**.

   The following output appears:

   ```
   Enter source IP (leave blank for none):
   ```

7. Type the IP address of this Avamar server and press **Enter**.

   The following output appears:

   ```
   Enter source port (leave blank for none):
   ```

8. Leave this field blank and press **Enter**.

   The following output appears:

   ```
   Enter Destination IP Address (leave blank for none):
   ```

9. Type the IP address of the VA server that you specified in the `va.http.host` property for `vas.properties` and press **Enter**.

   If you specified a hostname for the `va.http.host` property, type the corresponding IP address in this field.

   The following output appears:

   ```
   Enter Destination Port (leave blank for none):
   ```

10. Type the VA server port number that you specified in the `va.http.port` property for `vas.properties` and press **Enter**.

    The following output appears:

    ```
    Targets
    -------
    1) ACCEPT
    2) REJECT
    3) DROP
    4) LOGDROP
    Select Target:
    ```

11. Type `1` to allow packets that are destined for the VA server and press **Enter**.

    The following output appears:

    ```
    Node Types
    ----------
    1) ALL
    2) DATA
    3) UTILITY
    4) ACCELERATOR
    Select node type to apply rule to:
    ```

12. Type `3` to select the utility node and press **Enter**.

    Output similar to the following appears:

    ```
    Add rule |7080|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY to
    file? (Y/N):
    ```

13. Type `Y` to save the new rule and press **Enter**.

    The script writes the new rule to `avfwb_custom_config.txt`.

    Output similar to the following appears:

    ```
    Adding |7080|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY to file...
    Add another rule? (Y/N):
    ```

14. Repeat the preceding steps to add another new rule for the same VA server and the `va.https.port` property.

    At the completion of the process, output similar to the following appears:

```
Adding |7043|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY to file...
Add another rule? (Y/N):
```

15. Type **N** and press **Enter**.

    The following output appears:

    ```
    Return to main menu? (Y/N):
    ```

16. Type **N** and press **Enter**.

    The following output appears:

    ```
    Save and execute rules now? (Y/N):
    ```

17. Type **Y** to save the new firewall rules and press **Enter**.

    The script saves the new rules to the system firewall tables and automatically restarts the Avamar firewall, then exits.

    Output similar to the following appears:

    ```
    Rules have been saved to /usr/local/avamar/lib/admin/security/
    avfwb_custom_config.txt
    |7080|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY will be applied
    |7043|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY will be applied
    Applying rule /usr/sbin/iptables -A OUTPUT -p tcp --dport 7080 -
    d 10.6.197.105 -j ACCEPT
    Applying rule /usr/sbin/iptables -A OUTPUT -p tcp --dport 7043 -
    d 10.6.197.105 -j ACCEPT
    ```

Enabling the CAC/PIV feature

This task imports the security certificates and enables CAC/PIV authentication prompts.

Before you begin

Ensure that you are still logged in as the root user.

It is recommended but not required to import the optional server-specific CAC/PIV security certificate into the keystore.

Procedure

1. Change directory by typing the following command:

   cd /root

2. Enable the CAC/PIV feature and import the security certificates into the keystore by typing the following command:

   cac.pl --enable --cacert *<cacert>* --cert *<servercert>* --force

   where:

   - *<cacert>* is the filename of the CA issuer security certificate.
   - *<servercert>* is the filename of the optional server-specific CAC/PIV security certificate.

   Note

   If you do not have a server-specific CAC/PIV security certificate, omit the `--cert <servercert>` argument.

3. Verify that Avamar has enabled CAC/PIV authentication by typing the following command:

   cac.pl --status

When CAC/PIV authentication is enabled, the following output appears:

```
cac: enabled
```

4. Check the status of the CAC/PIV components by typing the following command:

   cac.pl --report

   Output similar to the following appears:

```
cac.enabled=true
client.auth=true
server-cert-exists=false
issuer-cert-exists=true
vas-installed=true
vas-running=true
vas-autostart-enabled=true
mc-running=true
apache-installed=true
apache-running=true
apache-secure=true
```

   The value of `server-cert-exists` may be true or false, depending on whether you imported a server-specific CAC/PIV security certificate.

Logging in using CAC/PIV authentication

Before trying to log into Avamar Installation Manager or Avamar Administrator by using CAC/PIV authentication, take the following actions:

- Enable CAC/PIV authentication on the Avamar server.
- Install Avamar Administrator on the local computer. This installs the necessary smart card libraries.

  Ensure that the local computer meets all other prerequisites that are listed in the *Avamar Administration Guide*.
- Connect a supported smart card reader to the local computer.
- Insert a smart card into the smart card reader.

Note

CAC/PIV authentication is not supported when launching Avamar Administrator from the web interface.

Smart card reader libraries

Review the following information before logging in using CAC/PIV authentication.

Avamar Administrator provides an option to install the required OpenSC smart card driver during installation of the management console software. The Avamar Desktop/Laptop interface also provides a stand-alone OpenSC driver.

If the site uses Gemalto smart card readers, you must obtain and install a Gemalto smart card driver. Ensure that the driver is compatible with the release of the JRE that is included with the Avamar software.

The OpenSC or Gemalto DLL file must reside in one of the following locations:

- A user-defined path that is specified in the `pkcs11_library` key in `mcclient.xml`
- For 64-bit Windows installations:
  - `C:\Program Files\OpenSC Project\PKCS11-Spy\pkcs11-spy.dll`

- C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS1164.dll

- For 32-bit Windows installations:
  - C:\Program Files (x86)\OpenSC Project\PKCS11-Spy\pkcs11-spy.dll
  - C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS11.dll

If the Avamar client software cannot locate the DLL file, the client prompts the user for the file's location, and then stores this information for the next session.

Logging in to the Avamar Installation Manager with CAC/PIV authentication

When CAC/PIV authentication is enabled, use the following steps to log in to the Avamar Installation Manager.

Procedure

1. In a supported web browser, type:

   https://*<AvamarServer>*/avi

   where *<AvamarServer>* is the hostname (as defined in DNS) or the IP address of the Avamar server. Ensure that you type the **s** in **https**.

   You may be required to acknowledge a browser warning regarding self-signed certificates before continuing.

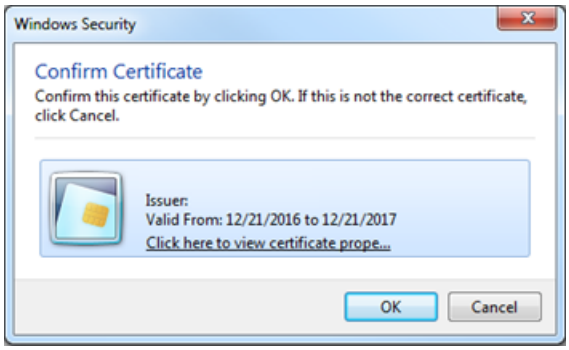
   A **Windows Security** dialog box appears, prompting the user to type the authentication PIN for the smart card.

   Figure 2 PIN Authentication dialog box

2. Type the PIN that is assigned to the smart card and click **OK**.
3. Confirm the details of the security certificate from the smart card and click **OK**. The security certificate must correspond to an account with administrator permissions.

Figure 3 Certificate Confirmation dialog box



The Avamar server validates the security certificate with the VA server and interfaces with the LDAP server to complete the login process.

The **Avamar Installation Manager** window appears.

After you finish

If you remove the smart card from the smart card reader, or a smart card is not inserted, the web browser displays a notification.

Figure 4 Insert Smart Card dialog box

Use of the Avamar Installation Manager is not possible until you insert a smart card.

Logging in to Avamar Administrator with CAC/PIV authentication

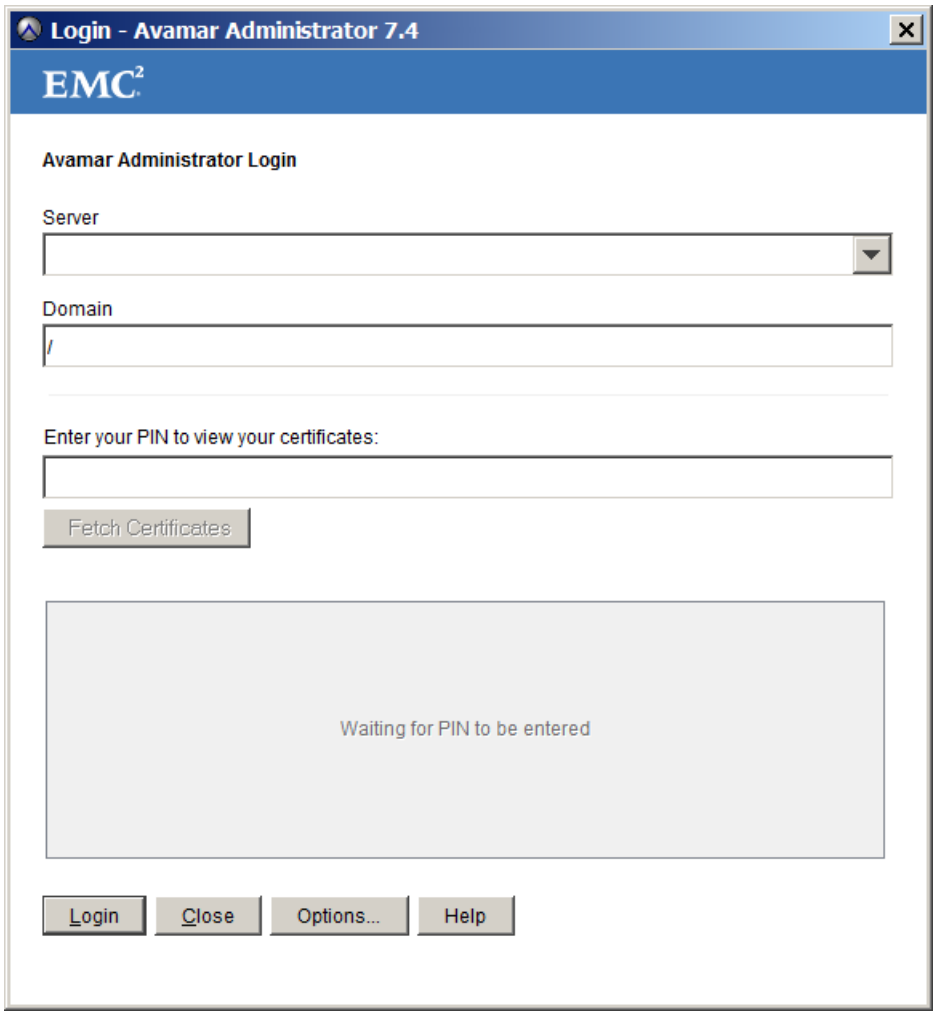
When CAC/PIV authentication is enabled, use the following steps to log in to Avamar Administrator.

Procedure

1. Launch Avamar Administrator by double-clicking the **Avamar Administrator** icon on the Windows desktop or from the **Avamar** folder on the **Start** menu.

   The **Login** window appears.

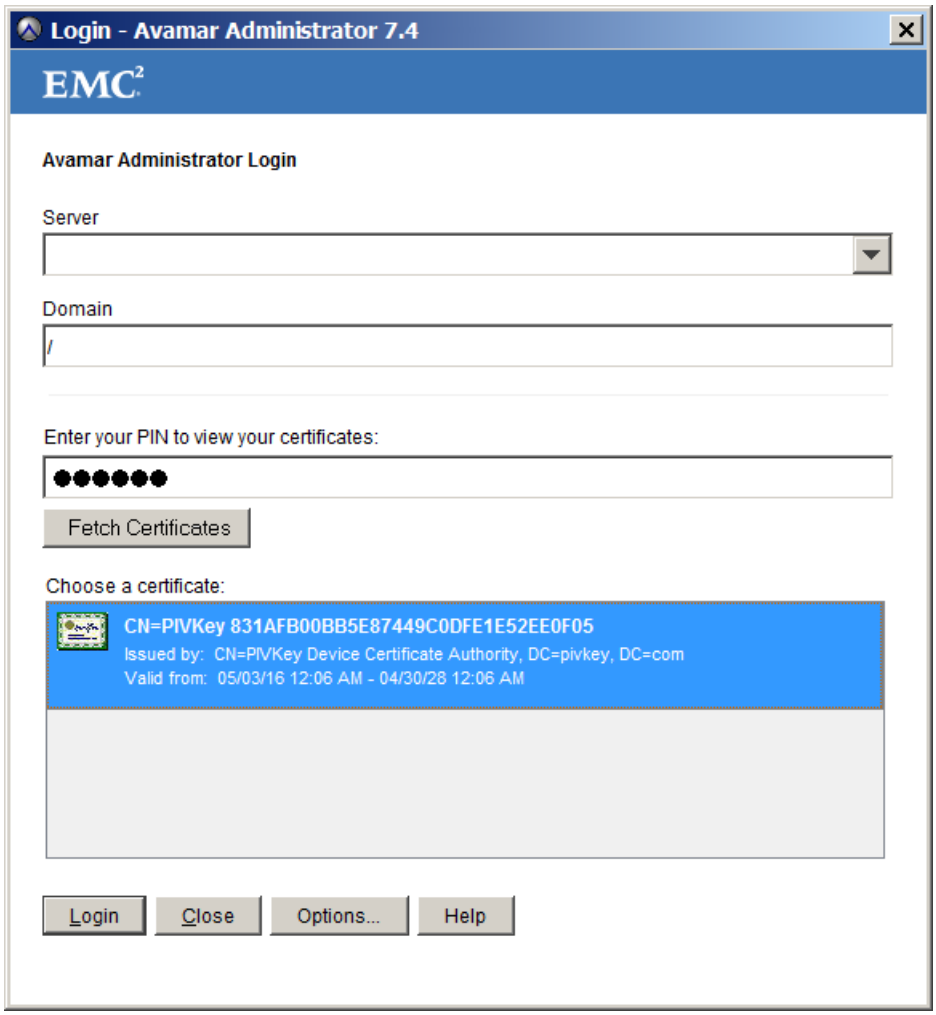
Figure 5 Avamar Administrator Login window



2. In the **Server** field, type the IP address or DNS name of the Avamar server to log in to.
3. In the **Domain** field, select or type the Avamar domain to log in to:
   - To log in to the root domain, use the default entry of a single slash (/) character.
   - To log in to a specific domain or subdomain, type the domain path by using the syntax `/domain/subdomain1/subdomain2`.
4. In the **Enter your PIN to view your certificates** field, type the PIN that is assigned to the smart card.
5. Click **Fetch Certificates**.

   Avamar Administrator retrieves the list of security certificates that are stored on the smart card.

Figure 6 Avamar Administrator Login window



6. In the **Choose a certificate** field, select a certificate from the list of security certificates on the smart card.

   To access all Avamar Administrator functionality, the account that is associated with this security certificate must be assigned the role of Administrator. Other roles provide reduced functionality.

7. Click **Login**.

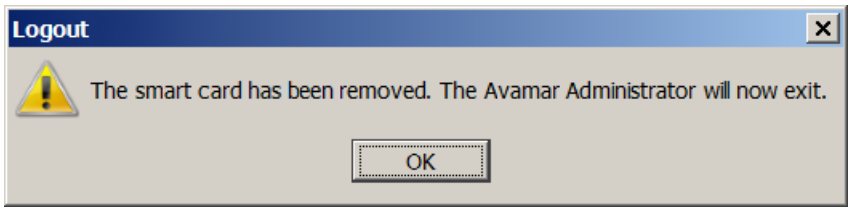
   The Avamar server validates the selected security certificate with the VA server and interfaces with the LDAP server to complete the login process.

   The Avamar Administrator dashboard appears.

After you finish

If you remove the smart card from the smart card reader, the Avamar Administrator window displays a notification and closes.

Figure 7 Logout dialog box



Disabling CAC/PIV authentication

Disabling CAC/PIV authentication on an Avamar server is a multi-step process that consists of the following tasks:

- Disabling the CAC/PIV feature, which includes:
  - Disabling two-way client authentication.
  - Configuring the Apache web server.
  - Restarting the AvInstaller, management console, VA, and Apache services.
  - Removing the security certificates from the keystore.
- Closing the VA service ports in the Avamar firewall.

Modifying the server configuration files is not required.

Disabling the CAC/PIV feature

This task disables CAC/PIV authentication prompts and removes the security certificate from the Avamar server keystore.

Procedure

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. Switch user to root by typing the following command:

   ```
   su -
   ```

3. Verify that CAC/PIV authentication is enabled by typing the following command:

   ```
   cac.pl --status
   ```

   When CAC/PIV authentication is enabled, the following output appears:

   ```
   cac: enabled
   ```

4. Check the status of the CAC/PIV components by typing the following command:

   ```
   cac.pl --report
   ```

   Output similar to the following appears:

   ```
   cac.enabled=true
   client.auth=true
   server-cert-exists=false
   issuer-cert-exists=true
   vas-installed=true
   vas-running=true
   vas-autostart-enabled=true
   mc-running=true
   ```

```
apache-installed=true
apache-running=true
apache-secure=true
```

The value of `server-cert-exists` may be true or false, depending on whether you imported a server-specific CAC/PIV security certificate.

Depending on the state of the Avamar subsystems, the values of `mc-running` or `apache-running` may be true or false.

5. Disable the CAC/PIV feature, and remove the security certificates from the keystore, by typing the following command:

   `cac.pl --disable --clean --force`

   Note

   If you do not need to remove the CA issuer and server-specific CAC/PIV security certificates, omit the `--clean` option.

6. Verify that CAC/PIV authentication is disabled by typing the following command:

   `cac.pl --status`

   When CAC/PIV authentication is disabled, the following output appears:

   ```
   cac: disabled
   ```

7. Check the status of the CAC/PIV components by typing the following command:

   `cac.pl --report`

   Output similar to the following appears:

   ```
   cac.enabled=false
   client.auth=false
   server-cert-exists=false
   issuer-cert-exists=false
   vas-installed=true
   vas-running=false
   vas-autostart-enabled=false
   mc-running=true
   apache-installed=true
   apache-running=true
   apache-secure=false
   ```

   Depending on the state of the Avamar subsystems, the values of `mc-running` or `apache-running` may be true or false.

   If you did not remove the security certificates, the values of `issuer-cert-exists` and `server-cert-exists` may be true.

Configuring the Avamar firewall

This task closes the two ports in the Avamar firewall that are used by the VA service to communicate with the VA server.

Procedure

1. Change directory by typing the following command:

   `cd /usr/local/avamar/lib/admin/security`

2. Run the firewall rules script by typing the following command:

   `./edit-firewall-rules.sh`

The following output appears:

```
Choose an Action
----------------
1) Add a custom rule
2) Remove a custom rule
3) List Current Custom Rules
4) Exit
5) Save & Exit
Enter desired action:
```

3. Type `2` to remove custom rules and press **Enter**.

   Output similar to the following appears:

   ```
   Rules in configuration file:
        1  |7080|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY
        2  |7043|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY

   Select line to remove (ENTER to go back):
   ```

4. Type the number of the rule corresponding to the VA server HTTP port, which is 7080 by default, and then press **Enter**.

   Output similar to the following appears:

   ```
   Line |7080|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY has been
   removed from configuration file
   Return to main menu? (Y/N):
   ```

5. Type `Y` to return to the main menu and press **Enter**.

   The following output appears:

   ```
   Choose an Action
   ----------------
   1) Add a custom rule
   2) Remove a custom rule
   3) List Current Custom Rules
   4) Exit
   5) Save & Exit
   Enter desired action:
   ```

6. Type `2` to remove additional custom rules and press **Enter**.

   Output similar to the following appears:

   ```
   Rules in configuration file:
        1  |7043|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY

   Select line to remove (ENTER to go back):
   ```

7. Type the number of the rule corresponding to the VA server HTTPS port, which is 7043 by default, and then press **Enter**.

   Output similar to the following appears:

   ```
   Line |7043|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY has been
   removed from configuration file
   Return to main menu? (Y/N):
   ```

8. Type `N` and press **Enter**.

   The following output appears:

   ```
   Save and execute rules now? (Y/N):
   ```

9. Type `Y` and press **Enter**.

   The script removes the CAC/PIV authentication rules from the system firewall tables, automatically restarts the Avamar firewall, and then exits.

   The following output appears:

```
Rules have been saved to /usr/local/avamar/lib/admin/security/
avfwb_custom_config.txt
```

Unauthenticated interfaces

The **Avamar Web Restore** (Desktop/Laptop) page requires no authentication to access the top-level navigation items. However, most top-level navigation items require subsequent authentication to use interfaces that may provide access to customer data.

Table 6 Avamar Web Restore interfaces that do not require authentication

Interface	Effects
Downloads	Allows a user to download platform-specific Avamar client plug-ins and related items.
Administrator	Allows a user to download the Avamar Administrator application for use on the local computer. The Avamar Administrator software requires authentication and authorization to access any system functions.
Help	Provides description of the functions available through Avamar Web Restore.

Selecting the authentication source

Select the authentication source during the process of creating a user account.

- If you have configured enterprise authentication, the AUI enables the **Authentication System** list when you create a user account.
- If you have not configured enterprise authentication, the **Authentication System** list is unavailable and the `Axion Authentication System` (Avamar internal authentication) becomes the default.

Directory service authentication requires no additional selection beyond the normal process of configuring LDAP maps.

The *Avamar Administration Guide* provides more information about creating user accounts.

How Avamar authenticates users and assigns roles

To provide backward compatibility with enterprise authentication and to account for the possibility of users in more than one LDAP mapped group, Avamar uses the following authentication and role assignment sequence for each login try:

1. When the username is in the format *user*, where *user* is a username without *@server* appended, then Avamar checks the internal Avamar authentication database.
   If the username, password, and domain match, then the login is successful and Avamar assigns the user a role in the Avamar database. If they do not match, then the login fails.
2. When the username is in the format *user@server*, where *user* is a username and *server* is the fully qualified domain name of the authentication server, then Avamar checks the login information by using enterprise authentication.

If the username, password, and domain match, then the login is successful and Avamar assigns the user a role in the Avamar database. If there is no match, then the evaluation continues.

3. When the username is in the format *user@server* and authentication by using enterprise authentication fails, then Avamar checks the LDAP mapping system. The login try is checked against all mapped groups for a match of each of the following identifiers:
   - Username, the portion of the **User Name** field entry before the @ symbol.
   - Password, as typed in the **Password** field.
   - Avamar domain, as typed in the **Domain Name** field.
   - Directory service domain, the portion of the **User Name** field entry after the @ symbol.

   When all identifiers match, the login is successful and Avamar assigns the user a role from the mapped group.

   A user can be the member of mapped groups in different directory service domains. The role of the mapped group that matches the directory service domain that is provided during login is assigned to the user for that session.

   When the user is a member of more than one mapped group in the same directory service domain, the role with the greatest authority is assigned.
4. When the login information does not meet the requirements of any of the previous steps, then the login fails and a failure message appears.

User and credential management

The following topics describe the local user accounts, default practices and credentials, and how to secure user account login and the associated credentials.

Pre-loaded user accounts

The Avamar server uses the following default user accounts and default passwords. Changing the default password is an installation requirement.

Table 7 Avamar server Linux OS default user accounts

User account	Default password	Description
root	changeme	Linux OS root account on all Avamar nodes. **Note** The use of ssh to the root user is allowed: • Internally on all nodes (via localhost) • From the utility node to itself and to all storage nodes.

Table 7 Avamar server Linux OS default user accounts (continued)

User account	Default password	Description
admin	changeme	Linux OS account for Avamar administrative user.

Table 8 Avamar server software default user account

User account	Default password	Description
root	8RttoTriz	Avamar server software root user account.

Table 9 MCS default user accounts

User account	Default password	Description
MCUser	MCUser1	Default Avamar Administrator administrative user account.
backuponly	backuponly1	Account for internal use by the MCS.
restoreonly	restoreonly1	Account for internal use by the MCS.
backuprestore	backuprestore1	Account for internal use by the MCS.
repluser	9RttoTriz	Account for internal use by the MCS for replication.

Table 10 MCS PostgreSQL database default user accounts

User account	Default password	Description
admin		No password, logged in on local node only.
viewuser	viewuser1	Administrator server database view account.

Table 11 Proxy virtual machine Linux OS default user account

User account	Default password	Description
root	avam@r	Linux OS root account on all proxies deployed using the Avamar proxy appliance. This account is for internal use only.
admin	avam@r	Linux OS admin account on all proxies deployed by using the Avamar proxy appliance.
AvamarCIM	avam@r	Linux OS AvamarCIM account for accessing CIM the

Table 11 Proxy virtual machine Linux OS default user account (continued)

User account	Default password	Description
		interface by using the Avamar proxy appliance.

Changing server passwords and OpenSSH keys

Use the `change-passwords` utility to change the passwords for operating system user accounts and Avamar server user accounts. Also use `change-passwords` to create and modify SSH keys for those accounts.

The `change-passwords` utility guides you through the following operations:

- Changing passwords for the operating system accounts: admin and root
- Changing passwords for the internal Avamar server accounts: root, MCUser, repluser, and viewuser
- Creating and changing SSH keys

Procedure

1. Suspend all scheduled operations:
   a. In Avamar Administrator, select **Tools** > **Manage Schedules**.
   b. On the **Manage All Schedules** window, click **Suspend All**.
2. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

3. Start the utility by typing `change-passwords`.

   On a multi-node server, the output prompts you to specify whether to change passwords on all nodes or selected nodes.
4. Type `y` to change passwords on all nodes or `n` to change passwords on selected nodes, and then press **Enter**.

   The output prompts you to indicate whether you plan to specify SSH private keys that are authorized for root operations.
5. Type `n` and press **Enter**.

   The output prompts you to specify whether to change admin or root operating system user account passwords.
6. Type `y` to change the passwords or `n` to skip the process of changing the passwords, and then press **Enter**.
7. If you typed `y` in the previous step, then follow the system prompts to change the passwords for one or more of the admin or root operating system user accounts.

The output prompts you to specify whether to change SSH keys.

8. Type `y` to change or create an SSH key, or type `n`, and then press **Enter**.
9. If you typed `y` in the previous step, then follow the system prompts to change or create the keys.

   The output prompts you to specify whether to change Avamar server passwords.
10. When prompted, type `y` to change the MCUser, Avamar root, repluser, and viewuser passwords, or if you do not want to change the passwords, type `n`, and then press **Enter**.
11. If you typed `y` in the previous step, then follow the system prompts to change the passwords.

    The output prompts you to accept or reject the changes that are made to passwords or SSH keys during this utility session.
12. Type `y` to accept the changes or type `n` to exit this utility session without changes, and then press **Enter**.

    The output provides the status of the operation.
13. When the operation completes, resume scheduled operations:

    a. In Avamar Administrator, select **Tools** > **Manage Schedules**.

    b. On the **Manage All Schedules** window, click **Resume All**.

Customer Support password

The Customer Support password in the Avamar Installation Manager is an additional control that restricts customers from installing certain packages which might lead to system instability or corruption when installed without assistance from Customer Support. This control is not intended to provide any confidentiality protection.

The Customer Support password is a predefined, hard-coded string that customers cannot change. However, the Customer Support password changes for each Avamar release.

Removing local account

This section describes how to disable and remove local accounts for Avamar.

To remove a user account from the Avamar MCGUI, do the following:

Procedure

1. Login to the Avamar administrator with the administrator credentials.
2. Navigate to **Switch to Administrator**.
3. Select the user that you want to remove.
4. Click **Delete User**.

   An MCGUI user account cannot be disabled from the Avamar administrator.

Disabling Avamar server account

To disable user access to Avamar server, do the following:

Procedure

1. Open a command shell and login with administrator credentials.

2. Update `/ect/passwd` user information to `sbin/nologin`.

For example, to disable avi user access, type the following command:

```
avi:x:510:510:Daemon user for Avamar Installation Manager:/home/avi:/
sbin/nologin
```

Password complexity

The following topics describe customer options for configuring password complexity rules:

Password complexity, length, and reuse

As part of the level-2 security features, Avamar requires that all local server operating system accounts have passwords with the following characteristics:

- Password complexity requires that you use at least three of the following four character sets:
  - Two or more lowercase characters
  - Two or more uppercase characters
  - Two or more numeric characters
  - Two or more special (non-alphanumeric) characters
- Password complexity determines the minimum length:
  - If you use any three character sets, the password must be at least 14 characters.
  - If you use all four character sets, the password must be at least 11 characters.
- Passwords must contain at least three characters that are different from the last password.
- The previous 10 passwords cannot be reused.
- The length of the password limits the number of pairs of neighboring alphabetical characters. For example, the string *23abcdfed* contains six pairs: *23*, *ab*, *bc*, *cd*, *fe*, *ed*.
  - For a minimum length password, four pairs are permitted.
  - For every 12 characters beyond the minimum length, another pair is permitted.

Configure password complexity, length, and reuse

The documentation for pam_cracklib provides more information about parameters and values.

Procedure

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, and then switch user to root by typing `su -`.
   - For a multi-node server, log in to the utility node as admin, and then switch user to root by typing `su -`.
2. Back up the login configuration file by typing the following command:

   ```
   cp /etc/pam.d/common-password /etc/pam.d/common-password.`date +
   %s`
   ```

3. Using a Linux text editor, such as `vi`, open the file `/etc/pam.d/common-password`.
4. Locate the line that begins with `password requisite`.

   For example: `password requisite pam_cracklib.so retry=3 minlen=14 lcredit=-2 ucredit=-2 dcredit=-2 ocredit=-2 difok=4`
5. Update the parameters that control the password complexity and length.

Parameter	Description
retry	The number of opportunities for a user to type a new password that meets the specified criteria, before the password change command fails.
minlen	The minimum password length, subject to adjustment in the form of "credit" toward shorter lengths, depending on the number of character sets in use and the credit parameters.
lcredit	The maximum credit toward password length for lowercase characters.
ucredit	The maximum credit toward password length for uppercase characters.
dcredit	The maximum credit toward password length for digit characters (0-9).
ocredit	The maximum credit toward password length for special (non-alphanumeric) characters.
difok	The minimum number of characters which must change from the previous password.

   Negative values for the credit parameters force users to select passwords that contain at least the specified number of characters from that character set.

   For example, with a setting of `ucredit=-2`, a user must include at least two uppercase characters in the password.
6. Locate the line that begins with `password sufficient`.

   For example: `password sufficient pam_unix.so use_authtok shadow remember=5 sha512`
7. Update the `remember` parameter that controls password history and reuse.

   The value for this parameter indicates the number of previous passwords that the new password cannot match.
8. Save and close the file.

For example, to configure a policy that requires passwords with a minimum of eight characters, one letter, and one digit, and that prevents the last three passwords from being reused:

```
password    requisite     pam_cracklib.so retry=6 minlen=8 ucredit=-1
dcredit=-1
password    sufficient    pam_unix.so use_authtok shadow remember=3
sha512
```

After you finish

For a multi-node server, repeat this task on all storage nodes.

Configure password aging

Password aging is a level-2 security feature. By default, all local Avamar server operating system accounts must have their passwords changed every 60 days. Once a password is changed, it cannot be changed again for at least 24 hours.

To change the password expiry interval, complete the following steps:

Procedure

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, and then switch user to root by typing **su -**.
   - For a multi-node server, log in to the utility node as admin, and then switch user to root by typing **su -**.
2. Back up the login configuration file by typing the following command:

   cp /etc/login.defs /etc/login.defs.`date +%s`
3. Using a Linux text editor, such as `vi`, open the file `/etc/login.defs`.
4. In the **Password aging controls** section, locate the `PASS_MAX_DAYS` parameter.
5. Change the `PASS_MAX_DAYS` parameter to a different value, in days.

   For example, **PASS_MAX_DAYS 90**.

   This value controls the maximum password age before expiry.
6. Verify that the value for the `PASS_WARN_AGE` parameter is appropriate for the new password expiry interval.
7. If required, change the value for the `PASS_WARN_AGE` parameter to a different value, in days.

   This value controls the warning period for a user to prepare for password expiry.
8. If required, change the value for the `PASS_MIN_DAYS` parameter to a different value, in days.

   This value controls the minimum password age before a password can be changed again.
9. Save and close the file.
10. List the operating system user accounts by typing the following command:

    cat /etc/passwd | cut -f 1 -d :
11. Set the password expiry interval for an operating system user account by typing the following command:

    chage -M *interval account-name*

    where:
    - *interval* is the new password expiry interval, in days.
    - *account-name* is one of the operating system user accounts from the previous step.

    Repeat this step for all Avamar operating system user accounts.

After you finish

For a multi-node server, repeat this task on all storage nodes.

Secure credential requirements

This section provides information on Secure credential requirements for Avamar.

Avamar requires an advance encryption level of AES128 for credential hashing algorithm. The salt size settings for hashed credentials is not applicable for Avamar.

Authentication to external systems

Configure authentication of components outside of Avamar, including components providing services to the Avamar server and remote clients.

Avamar supports the following external systems:

- Data Domain
- VMware vCenter
- EMC Secure Remote Services (ESRS)
- Dell EMC repository server
- External LDAP server
- KMIP server

For each external system, there are two common operations: identifying the system and establishing trust.

In most cases, identifying an external system is easy: a user or administrator specifies an IP address or a hostname for a known device that is under the users control, to which Avamar connects. Some external systems, such as ESRS are preconfigured in the Avamar software. Where applicable, follow the procedures in this section to authenticate external systems that are not under the user's control.

After you verify the identity of the external system, you can configure Avamar to trust many known external systems. In general, this process involves exchanging a certificate or other shared secret that distinguishes a known system from an imposter.

Configuring remote connections

The following topics provide information about the external systems to which Avamar connects, and the means of establishing trust with those systems.

Authentication with Data Domain

The following sections provide information about identifying the Data Domain system, and establishing trust between the Avamar server and Data Domain system.

Identifying a Data Domain system

Avamar and Data Domain do not verify the identity information that is supplied with the certificates. Rather, Avamar verifies that the certificate matches the one that was used during the import process. The user is required to provide accurate credentials when integrating a Data Domain system with an Avamar server. Additionally, a user must verify the information in the certificates before instructing the Avamar server or the Data Domain system to trust those certificates. No further identification occurs.

Establishing trust with the Data Domain system

When you integrate Data Domain with an Avamar server, mutual trust needs to be established between both systems. To establish a trusted connection, Avamar and Data Domain introduce security certificates to each end point that become known to the other end point. Each time a connection occurs, Avamar verifies the security certificate presented by the Data Domain, and vice versa. Successful verification establishes trust.

Avamar control data that is exchanged with the Data Domain travels via an SSH connection that is secured by means of public key authentication. These public keys are exchanged during the initial integration process. The Data Domain System Integration Guide provides more information.

After this pathway is established, Avamar controls the encryption of backup data.

Authentication with ESRS

The following sections provide information about identifying the EMC Secure Remote Services (ESRS) server, and establishing trust between the Avamar server and the ESRS server.

Identifying an ESRS server

To identify an EMC Secure Remote Services (ESRS) server, Avamar relies on a user to provide a hostname and IP address that the user has already identified. Log in to the ESRS Web UI to verify the configuration details and identify the ESRS server.

Establishing trust with the ESRS server

Integration of ESRS with an Avamar server requires the establishment of mutual trust between both systems. To establish a trusted connection, complete the following steps:

Procedure

1. Export the ESRS gateway certificate from the ESRS Web UI.

   The *ESRS Operations Guide* provides more information.

2. 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, and then switch user to root by typing **su -**.
   - For a multi-node server, log in to the utility node as admin, and then switch user to root by typing **su -**.
3. Load the rootid OpenSSH key by typing:

   ```
   ssh-agent bash
   ssh-add /root/.ssh/rootid
   ```

4. Copy the ESRS gateway certificate to the `/tmp` folder on the Avamar server.
5. Import the ESRS gateway certificate into the key store by typing the following command on one line:

   ```
   keytool -importcert -alias esrs -keystore /usr/local/avamar/lib/
   rmi_ssl_keystore -storepass changeme –file /tmp/esrs.cer
   ```

6. To proceed without establishing trust, update the `mcserver.xml` file:

a. Open `/usr/local/Avamar/var/mc/server_data/prefs/mcserver.xml` in a text editor.

b. Find the *ignore_cert* key.

c. Change the value to true.

```
<entry key="ignore_cert" value="true"/>
```

d. Close `mcserver.xml` and save the changes.

e. Restart the MCS by typing the following commands:

```
dpnctl stop mcs

dpnctl start mcs
```

Authentication with VMware vCenter

The following sections provide information about identifying the vCenter server, and establishing trust between the Avamar server and vCenter server.

Identifying a VMware vCenter server

To identify a vCenter server, Avamar relies on a user to provide a hostname and IP address that the user has already identified. Launch the vSphere Client or Web Client, and log in to the vCenter server to verify the configuration details and identify the vCenter server.

Establishing trust with the VMware vCenter server

Integration of vCenter with an Avamar server requires the establishment of mutual trust between both systems To establish a trusted connection, complete the following tasks:

1. Export the vCenter authentication certificate from vCenter.
   The VMware vSphere documentation provides more information.
2. Use the Avamar Web User Interface (AUI) to import the vCenter authentication certificate to the MCS keystore.
   The *VMware User Guide* describes how to import vCenter authentication certificates.

Authentication with the Dell EMC repository server

The following sections provide information about identifying the repository server, and establishing trust between the Avamar server and repository server.

Identifying the Dell EMC repository server

When a user connects to the Dell EMC repository server, the Local Downloader Service (LDLS) presents the certificate to the user through the Avamar Installation Manager UI. The Avamar sever requires the user to verify the information in the certificate and accept the certificate. No further identification occurs.

Establishing trust with the Dell EMC repository server

The legacy Avamar Downloader Service cannot establish trust. It does not verify the certificate provided by the repository.

- To establish trust for the source of packages:
  The Local Downloader Service (LDLS) presents the identification portion of the certificate to the user and prompts for acceptance. The user accepts the

certificate and the LDLS stores the certificate to verify future connections to the repository. This establishes one-way trust between the LDLS (and Avamar Installation Manager) and the repository.

- To establish trust for the authenticity of workflow packages:
  All workflow packages obtained from the repository are signed by a master GPG key that is controlled by Dell EMC. The corresponding public key is built into the Avamar Installation Manager. On receipt of the package, the Avamar Installation Manager verifies the signature on the workflow package against the public key to detect and reject invalid signatures that might indicate possible tampering or corruption.

Authentication with the LDAP server

The following sections provide information about identifying the LDAP server, and establishing trust between the Avamar server and LDAP server.

Identifying an LDAP server

To identify an LDAP server, Avamar requires the user to provide the correct hostname and IP address at the time that you configure Avamar to use the LDAP directory service. Log in to Avamar Administrator to verify the configuration details and identify the LDAP server.

By default, Avamar is configured to verify the identity of the LDAP server by using Kerberos. However, other methods are available. For more information, see the *Avamar Administration Guide*.

Establishing trust with the LDAP server

The establishment of mutual trust between the LDAP server and Avamar server is not required. Each LDAP session is unique and relies on the certificates that are used to establish each connection and the credentials that are provided during initial configuration.

Authentication with the KMIP server

Identifying a KMIP server

To identify a KMIP server, Avamar requires the user to provide the correct hostname and IP address at the time that you configure Avamar to work with the KMIP server. Connect to the KMIP server to verify configuration details and identify the KMIP server.

Establishing trust with the KMIP server

Integration of a KMIP server with an Avamar server requires the establishment of mutual trust between both systems. For the KMIP server, trust is established by means of public key authentication. These public keys are exchanged during the initial integration process. To establish a trusted connection, connect to the KMIP server at configuration time, and exchange keys for the Avamar and KMIP server.

For more information, contact Customer Support.

Remote component authentication

Some Avamar components can be customized to accept trustworthy certificates that the user provides, or that a user's remote environment is able to authenticate. Remote components can include an Avamar client operating system, Avamar client software, and a human user or web browser.

- Avamar client operating systems can use code signing to ensure the authenticity and integrity of Avamar software downloads. Code signing on page 76 provides more information.
- Avamar clients can use session security to secure all communications between the Avamar server and the Avamar client software. The Avamar server provides authentication to the Avamar client and the Avamar client provides authentication to the Avamar server. Session security features on page 54 provides more information.
- Web browsers and the human users who rely on them need security certificates to verify the authenticity of the content that is available on Avamar web portals. Certificates help these users identify the Avamar server to which they connect and provide credentials. You can replace the default self-signed certificates with certificates that are provided by your organization. Server authentication using Apache on page 65 and Commercially signed SSL certificates on page 72 provides more information.

Session security features

Avamar session security features are provided by the Avamar installation, Avamar Virtual Edition (AVE) configuration, and upgrade workflow packages as well as a standalone session security configuration workflow.

Session security features include security improvements for communications between Avamar system processes.

The Avamar system secures all communications between Avamar system processes by using session tickets. A valid session ticket is required before an Avamar system process accepts a transmission from another Avamar system process.

The session tickets have the following general characteristics:

- The session ticket is encrypted and signed to protect against modification
- The session ticket is valid for a very short time
- Each session ticket contains a unique signature and is assigned to only one Avamar system process
- The integrity of a session ticket is protected by encryption
- Each Avamar system node separately verifies the session ticket signature
- When required, a session can be extended beyond the life of the session ticket

Avamar server authentication

After installing the session security features, the Avamar system acts as a private certification authority and generates a unique server certificate for the Avamar system.

The Avamar system installs the public key for the server certificate on every Avamar client that is registered with the Avamar server. Avamar clients use the public key to authenticate transmissions from the Avamar system.

For clients that are currently registered, the public key for the server certificate and other required certificate files are propagated to the client within an hour of the installation.

The Avamar system also automatically shares the Avamar server certificate with the Avamar storage nodes. Sharing the certificate allows the utility node and the storage nodes to provide the same certificate for authentication.

Avamar client authentication

Enable client authentication when installing the session security features to have the Avamar system act as a private certification authority and generate a unique client certificate for each Avamar client.

A client certificate is generated when the Avamar server registers an Avamar client.

After generating a client certificate, the Avamar system uses an encrypted connection with the Avamar client to install the certificate on the client. The Avamar system also stores the public key for the client certificate. The public key is used to authenticate the client in all subsequent communications.

Improved security for communications between Avamar system processes

Session security features are provided by several workflow packages, including installation, upgrade, and standalone session security configuration workflows.

The security features include:

- Generation and propagation of certificates
- Authentication that is based on X.509 v3 certificates
- Certificate expiration

Note

When upgrading from Avamar 7.3 and 7.4 to a subsequent release of Avamar when using secure session tickets, you must re-register your clients in order to generate new certificates for these clients.

Installing the session security features

Session security can be implemented and configured during the installation of the Avamar software, the configuration of AVE, and the upgrade from a previous version of the Avamar software. Session security also can be implemented post-installation or post-upgrade.

Install the session security features by running one of four workflows, whichever is appropriate to the Avamar server, including:

- Avamar software installation workflow
- AVE configuration workflow
- Avamar upgrade workflow
- **Session Security Configuration** workflow

Use the workflow's **Security Settings** tab to configure the session security features. The workflow guide that is associated with each workflow in the Avamar Installation Manager provides more information about each option. On the **Security Settings** tab, you can:

- Select the type of communication that is desired between the Management Server and Avamar client agents.
- Select the type of communication that is desired between the Avamar clients and Avamar server.
- Select the authentication type to use between the server and client when communication is initiated:

  - Single - the client authenticates the server
  - Dual - both client and server authenticate each other
- Create and propagate server certificates on the Avamar server and storage nodes, which are used for server or client authentication (or both). The certificates are created using the CA certificate that is installed in the keystore.
- Set a timeframe for the generated server certificates to expire.
- Run the `mcrootca` all command, which generates all new certificates for root, TLS, and EC root. This command forces the creation of new server certificates

Note

If you want to generate all new certificates for root, TLS, and EC root on an Avamar system, run the **Session Security Configuration** workflow and use the last option (**Generate All New Certificates**) on the **Security Settings** tab. The workflow guide provides complete instructions on the use of the workflow.

Requirements

Do not use the Avamar session security features in an environment that includes unsupported operating systems, clients, plug-ins, or devices. Installing the session security features stops communication with the Avamar processes on the unsupported operating systems, clients, plug-ins, and devices.

Table 12 Software version requirements

Software	Minimum version
Avamar server	Avamar 7.1 Service Pack 1 on SUSE Linux Enterprise Server (SLES) only
Avamar client	Avamar 7.1 Service Pack 1

Prepare multiple Avamar clients for the session security features by pushing out Avamar client upgrades with the Avamar Client Manager. Prepare individual Avamar clients by downloading and running a supported Avamar client software installer.

Table 13 Port requirements

Port/Protocol	Source	Destination	Description
29000/TCP	Utility node	Storage node	Avamar subsystem using SSL.
29000/TCP	Storage node	Utility node	Avamar subsystem using SSL.
30001/TCP	Utility node	Storage node	MCS using SSL.
30001/TCP	Storage node	Utility node	MCS using SSL.
30002/TCP	Avamar server	Avamar client	Avamar client using SSL.
30002/TCP	Avamar client	Avamar server	Avamar client using SSL.
30003/TCP	Utility node	Storage node	MCS using SSL.
30003/TCP	Storage node	Utility node	MCS using SSL.

The Avamar session security features are subject to some limitations:

- Server operating system
  Session security features cannot be used with an Avamar server running on the Red Hat Enterprise Linux (RHEL) operating system.
- Clients
  Session security features cannot be used with any of the following Avamar clients:
  - Avamar cluster client for Solaris on Veritas Cluster Server
  - Avamar client for Solaris in Solaris clusters
- Other products
  The use of NTP time synchronization of the Avamar server, Avamar clients, and the Data Domain system (if applicable) is strongly encouraged. If the time is not synchronized, it could result in registration and backup/restore failure due to certificate validity and expiration times. Changing the time zone on a host may have a similar impact and may require certificate regeneration.

Generation and propagation of certificates

Session security-enabling workflow packages enable automatic generation and propagation of certificates.

The Avamar system acts as a private certification authority and generates the certificates that permit the authentication and encryption of communications between Avamar system processes, including processes running on:

- The Avamar utility node
- The Avamar storage nodes
- Avamar clients

The Avamar system also securely propagates the certificates and the public keys to the required locations on each involved computer.

Generating new certificates with Data Domain systems
After generating new certificates on the Avamar server, 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.

Procedure

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
```

Results

If multiple Avamar servers are attached to a single Data Domain system and one of those Avamar servers is detached from the system, disable and then re-enable DD Boost to ensure that backups from the other Avamar servers succeed.

Authentication based on X.509 v3 certificates

The Avamar session security features use X.509 v3 certificates with the following default characteristics:

- Key type: RSA
- Key length: 3072 bits
- Cryptographic hash function and digest: SHA512

Certificate expiration

To enhance security, the Avamar session security features include the regular expiration of certificates.

Table 14 Default expiration periods and regeneration methods

Certificate type	Default expiration period	Regeneration method
Root authentication keys	Five years	Use the session security features workflow package to generate new certificates.
Session ticket signing key	One month	Avamar generates a new key automatically on a monthly cycle.
Client certificates	Five years	Generate a new certificate by manually reregistering the client.

Network configuration changes

Enabling the session security features requires changes to some network configuration tasks that are normally performed after installation.

- Changing the IP address or hostname of the Avamar server.
- Replacing the utility node.
- Replacing a storage node.
- Adding a storage node.

The following resources provide more information about changes to the network configuration tasks:

- *Avamar Server Software Post-Installation Network Configuration Technical Note*.

- Avamar SolVe Desktop procedure documentation.

Certificate acceptance workflow

Avamar uses a specific workflow when a client validates a server certificate, and when a server validates a client certificate:

1. Obtain the fully qualified domain name (FQDN) of the computer.

   When connected to a computer through an IP address, use reverse-DNS to determine the FQDN of the computer.
2. Compare the FQDN to the value specified in the Common Name (CN) field of the certificate.
   - When the FQDN matches the value that is specified in the CN field, accept that the certificate validates the computer.
   - When the FQDN does not match, continue the workflow.
3. If the certificate has a wildcard character (`*`) in the hostname portion of the value that is specified in the CN field, perform a simple wildcard match of the FQDN to the CN.
   - When the wildcard match is successful, accept that the certificate validates the computer.
   - When the match is unsuccessful, continue the workflow.

   For example, the value `r*.example.com` in the CN field of the certificate would match an FQDN such as `real.example.com`, `right.example.com`, or `reality.example.com`, but would not match `alright.example.com`.
4. Compare the IP address of the computer to each IP address listed in the Subject Alternative Name (SAN) field of the certificate.
   - When the IP address of the computer matches an IP address in the SAN field, accept that the certificate validates the computer.
   - When the match is unsuccessful, reject the certificate and terminate the connection.

Client/server authentication

Avamar clients and Avamar servers use Transport Layer Security (TLS) certificates and Public Key Infrastructure (PKI) for authentication and optional data-in-flight encryption.

Avamar supports the X.509 v3 standard for formatting digital certificates. Installing the Avamar server automatically generates a public/private key pair and a self-signed certificate in the `/data01/home/admin` directory on each Avamar server storage node and in the `/usr/local/avamar/etc` directory on the utility node.

Use the **Session Security Configuration** workflow to create the root certification authority (CA) certificates for the Avamar server, and the server and client certificates. Clients automatically sent a certificate signing request (CSR) the first time that they register with the Avamar server, and receive a client certificate signed by the Avamar server's root CA certificate.

Configure the Avamar environment for one-way or two-way authentication between Avamar clients and the Avamar server by using the **Session Security Configuration** workflow. This workflow is a maintenance task and can be invoked multiple times, as needed.

- Use one-way authentication to have the Avamar client request authentication from the Avamar server, and the server send a certificate to the client. The client

then validates the certificate. One-way authentication is also called server-to-client authentication in this guide.

- Use two-way authentication to have the client request authentication from the Avamar server, and have the Avamar server request authentication from the client. This client-to-server authentication combined with server-to-client authentication provides a stronger level of security.

In most cases, one-way authentication provides sufficient security. However, to provide more security, set up two-way authentication. Both configurations provide the capability of data-in-flight encryption.

One-way authentication
With one-way authentication, the Avamar client requests authentication from the Avamar server, and the server sends the appropriate certificate to the client. The client then validates the certificate, using the certificate acceptance workflow.

Create the certificates required for one-way authentication and install the certificates by running the **Session Security Configuration** workflow.

Two-way authentication
When two-way authentication is enabled, the Avamar server provides authentication to the Avamar client and the Avamar client provides authentication to the Avamar server.

With two-way authentication, both of the following occur:

- The Avamar client requests authentication from the Avamar server, and the server sends the appropriate certificate to the client. The client then validates the certificate, using the certificate acceptance workflow.
- The Avamar server requests authentication from the Avamar client, and the client sends the appropriate certificate to the server. The server then validates the certificate, using the certificate acceptance workflow.

Enforcing encrypted client/server communications

Configure the MCS to refuse plain-text communication from Avamar clients.

Completing this task forces Avamar clients to use the Avamar server's trusted public key to encrypt all communication sent to the Avamar server.

Procedure

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. Open `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` in a plain text editor.
3. Locate the `enforce_client_msg_encryption` preference and change it to the following:

   ```
   enforce_client_msg_encryption=true
   ```

4. Save and close the file.
5. Restart the MCS by typing the following commands:

   ```
   dpnctl stop mcs
   dpnctl start mcs
   ```

Verify client/server authentication
Verify an implementation of client/server authentication by running a test backup with server authentication enabled.

The test backup can be run by using either `avtar` from the command line or by using Avamar Administrator.

Verify authentication with the `avtar` command
Use the `avtar` command to verify client/server authentication by running a backup and including the server authentication option `--encrypt=tls-sa`.

The server authentication option requires authentication of the Avamar server by using the trusted certificates that are installed on the Avamar client.

Verify authentication with Avamar Administrator
To verify client/server authentication with Avamar Administrator, run a backup and select **High** from the **Encryption** method list. The **Encryption** method list appears on both the **On Demand Backup Options** dialog box and the **Restore Options** dialog box.

The *Avamar Administration Guide* provides more information on how to run a backup with the Avamar Administrator.

Note

In Avamar 7.5 and later and Avamar 18.1 and later:

- The **Medium** encryption method is not available.
- The **None** encryption method is not available when the session security features are enabled.

Mapping session security settings to data-in-flight encryption settings

The session security settings directly affect the selection of the communication protocol and work order flags for backup and replication jobs.

To map the communication protocol and work order flags for a replication job, repeat the following procedure on both the source and destination servers to determine the session security settings. The source and destination encryption methods are both obtained from the source server.

Note

The **Medium** encryption method is not available in Avamar 7.5 and later and Avamar 18.1 and later. If **Medium** encryption was in place before an upgrade from a previous version of Avamar, the upgrade does not change the existing behavior. However, Avamar Administrator displays this setting as **High**. The communication protocol and work order flag mapping is the same as for **High**, but with a different cipher level. If you change the encryption method to another value, you cannot select Medium again.

The **None** encryption method is not available in Avamar 7.5 and later and Avamar 18.1 and later when the session security features are enabled. If **None** was in place before an upgrade from a previous version of Avamar, the upgrade changes this setting to **High**. The session security features are enabled if the communication security setting is anything other than **Disabled/Off**.

Determining the communication security setting

To determine the communication security setting, examine the **Client-Server Communication and Authentication Type** setting in the **Session Security Configuration** workflow, or perform the following procedure.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Display the session security settings by typing the following command:

   ```
   /usr/local/avamar/bin/enable_secure_config.sh --showconfig
   ```

   Output similar to the following appears:

   ```
   Current Session Security Settings
   ---------------------------------
   "encrypt_server_authenticate"     ="true"
   "secure_agent_feature_on"         ="true"
   "session_ticket_feature_on"       ="true"
   "secure_agents_mode"              ="secure_only"
   "secure_st_mode"                  ="secure_only"
   "secure_dd_feature_on"            ="true"
   "verifypeer"                      ="yes"

   Client and Server Communication set to Authenticated mode with
   Two-Way/Dual Authentication.
   Client Agent and Management Server Communication set to
   secure_only mode.
   Secure Data Domain Feature is Enabled.
   ```

   Note the session security settings and use the following table to map session security settings to a communication security setting value.

Table 15 Communication security setting

Communication security setting	Session security setting	Value
Authenticated/Dual	encrypt_server_authenticate	true
	secure_agent_feature_on	true
	session_ticket_feature_on	true
	secure_agents_mode	secure_only
	secure_st_mode	secure_only
	secure_dd_feature_on	true
	verifypeer	yes
Authenticated/Single	encrypt_server_authenticate	true

Table 15 Communication security setting (continued)

Communication security setting	Session security setting	Value
	secure_agent_feature_on	true
	session_ticket_feature_on	true
	secure_agents_mode	secure_only
	secure_st_mode	secure_only
	secure_dd_feature_on	true
	verifypeer	no
Mixed/Single	encrypt_server_authenticate	true
	secure_agent_feature_on	true
	session_ticket_feature_on	true
	secure_agents_mode	mixed
	secure_st_mode	mixed
	secure_dd_feature_on	true
	verifypeer	no
Disabled/Off	encrypt_server_authenticate	false
	secure_agent_feature_on	false
	session_ticket_feature_on	false
	secure_agents_mode	unsecure_only
	secure_st_mode	unsecure_only
	secure_dd_feature_on	false
	verifypeer	no

Determining the source server encryption method

The source server encryption method controls communication between the source server and clients.

Procedure

1. In the AUI, navigate to **Administration** > **System** .
2. Click the **Replication Destination** tab, and then select the replication destination you want to edit.
3. Click **Edit**.

   The **Edit Replication Destination** wizard appears.
4. Note the selection in the **Encryption** field. This is the source encryption method. The options can be **High** or **None**.
5. Click **Cancel** to exit the **Edit Replication Destination** wizard.

Determining the destination server encryption method
The source server encryption method controls communication between the destination server and clients.

Procedure

1. In the AUI, navigate to **Administration** > **System** .
2. Click the **Replication Destination** tab, and then select the replication destination you want to edit.
3. Click **Edit**.

   The **Edit Replication Destination** wizard appears.
4. Note the selection in the **Encryption** field. This is the source encryption method. The options can be **High** or **None**.
5. Click **Cancel** to exit the **Edit Replication Destination** wizard.

Determining the communication protocol in use
Use the following table to map the communication security setting and encryption method to a communication protocol. The same rules apply to the selection of a communication protocol whether a client communicates with the source or the destination server.

Table 16 Mapping security and encryption settings to a communication protocol

Encryption method	Communication security setting			
	Disabled/Off	**Mixed/Single**	**Authenticated /Single**	**Authenticated /Dual**
None	Plain TCP with cleartext	TLS with server authentication and high encryption	TLS with server authentication and high encryption	TLS with mutual authentication of server and client, and high encryption
High	TLS with high encryption	TLS with server authentication and high encryption	TLS with server authentication and high encryption	TLS with mutual authentication of server and client, and high encryption

Determining the work order flags in use
Use the following tables to map the communication security settings and encryption methods to the flags that are applied to each work order.

The `dstencrypt` and `dstencrypt-strength` flags depend on:

- The destination server encryption method.
- The lowest setting of either the source or destination server communication security settings.

Table 17 Mapping security and encryption settings to source work order flags

Source server communication security setting	Source server encryption method	`encrypt` flag	`encrypt-strength` flag
Disabled/Off	**None**	proprietary	cleartext
	High	tls	high
Mixed/Single **Authenticated/Single** **Authenticated/Dual**	**None**	tls-sa	high
	High	tls-sa	high

Table 18 Mapping security and encryption settings to destination work order flags

Destination server communication security setting	Source server communication security setting	Destination server encryption method	`dstencrypt` flag	`dstencrypt-strength` flag
Disabled/Off	**Disabled/Off** **Mixed/Single** **Authenticated/Single** **Authenticated/Dual**	**None**	proprietary	cleartext
		High	tls	high
Mixed/Single **Authenticated/Single** **Authenticated/Dual**	**Disabled/Off**	**None**	proprietary	cleartext
		High	tls	high
Mixed/Single **Authenticated/Single** **Authenticated/Dual**	**Mixed/Single** **Authenticated/Single** **Authenticated/Dual**	**None**	tls-sa	high
		High	tls-sa	high

Server authentication using Apache

Several Avamar web-based services use the Apache HTTP server (Apache) to supply a secure web browser-based user interface. Web browser connections with these applications use secure socket layer/transport layer security (SSL/TLS) to provide authentication and data security.

Apache handles the SSL/TLS sockets for Avamar web-based services when a connection is made on the default HTTP port. Apache redirects the connection request to an SSL/TLS socket and handles the encryption and authentication for that socket.

Web browser authentication warning

When a web browser accesses a secure web page from an unauthenticated web server, the SSL/TLS protocol causes it to display an authentication warning. An unauthenticated web server is one that does not authenticate itself using a trusted public key certificate.

The Apache HTTP server that is provided with Avamar is installed with a self-signed certificate, not a trusted public key certificate. The self-signed certificate is sufficient to establish an encrypted channel between web browsers and the server, but it cannot be used for authentication.

To enable Apache to provide authentication, and prevent web browser authentication warnings, complete the following tasks:

- Create a private key for Apache
- Generate a certificate signing request for Apache
- Obtain a public key certificate for Apache
- Configure Apache to provide public key authentication

The tools that are used to perform these tasks are part of the OpenSSL toolkit. OpenSSL is provided with Avamar.

Note

Avamar web interfaces are unavailable to web browsers that do not support TLS 1.2. Ensure that the web browser supports TLS 1.2.

Support for Subject Alternative Names

On an Avamar system, the Apache HTTP server (Apache), and each Apache Tomcat (Tomcat) web server, supports the X509 Version 3 (RFC 2459, section 4.2.1.7) extension. This extension provides support for certificates that include the Subject Alternative Name (SAN) field.

Apache and Tomcat can use a certificate with several IP addresses in the SAN field to provide authentication for:

- A multi-homed server, by using any one of its IP addresses.
- Several servers that share the certificate, by parsing the list of IP addresses.

Not all combinations of browser and OS support Subject Alternative Names. Test a SAN certificate with the browser and OS combinations used by your company before installing the certificate on a production system.

Create a private key for Apache

The public key infrastructure (PKI) private key for an Avamar system's Apache HTTP server (Apache) can be generated using various levels of security.

Use the private key generation method that is appropriate for the level of security required by your organization.

The methods for generating a private key are:

- Create a private key without randomness and without a passphrase
- Create a private key with randomness and without passphrase
- Create a private key with passphrase and without randomness
- Create a private key with randomness and with a passphrase

When a passphrase-protected private key is used, Apache prompts for the passphrase every time the Apache process starts. The Apache configuration setting

`SSLPassPhraseDialog` can be used to obtain the passphrase from a script. For more information, refer to Apache documentation available through the Apache web site at www.apache.org.

Creating a private key for Apache

Create a public key infrastructure (PKI) private key for the Avamar system's Apache HTTP server (Apache).

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Type one of the following alternative commands.

Key type	Command
Private key without randomness and without a passphrase	`openssl genrsa -out` *server.key* `3072`
Private key with randomness and without a passphrase	`openssl genrsa -rand` *binary-files* `-out` *server.key* `3072`
Private key without randomness and with a passphrase	`openssl genrsa -aes128 -out` *server.key* `3072`
Private key with randomness and with a passphrase	`openssl genrsa -rand` *binary-files* `-aes128 -out` *server.key* `3072`

   where:

   - *server.key* is a pathname you provide for the private key.
   - *binary-files* is a colon-separated list of paths to two or more binary files that OpenSSL uses to generate randomness.

3. (Key with passphrase) At the prompt, type a passphrase.
4. (Key with passphrase) At the prompt, retype the passphrase.

Generating a certificate signing request for Apache

Create a certificate signing request (CSR) for the Apache HTTP server (Apache) on an Avamar system.

Before you begin

Generate a private key for Apache.

A commercial certification authority (CA) uses the CSR when issuing a trusted private key certificate.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Generate the CSR by typing:

   `openssl req -new -key` *server.key* **`-out`** *server.csr*

   where:

   - *server.key* is a name you provide for the private key.
   - *server.csr* is a name you provide for the CSR.

3. (Key with passphrase) Type the passphrase for the private key and press **Enter**.
4. At each prompt, type the information described in the following table. Press **`Enter`** after each entry.

   For optional fields, you can provide an empty value by typing a period (.) and pressing **`Enter`**.

Field	Description
Country Name	The two-letter ISO abbreviation for the country. The list of abbreviations is available on the ISO web site at www.iso.org.
State or Province Name	In countries where it is applicable, the state or province where the organization is located. This entry cannot be abbreviated.
Locality Name	City where the organization is located.
Organization Name	The exact legal name of the company. This entry cannot be abbreviated.

Field	Description
Organizational Unit Name	Optional entry for more information about the organization, such as a department name.
Common Name (CN)	FQDN of the computer, or a wildcard FQDN for several computers. The wildcard character (*) must only appear once, and only in the hostname portion of the FQDN value. Example for single computer: `corp-1.example.com`. Example wildcard FQDN for several computers: `corp-*.example.com`.
Email Address	Email address of the primary administrator of the computer or computers.
Challenge password	A password that must be provided before revoking the certificate. The password is only required if your certificate is compromised. Optional field.
Company name	Name for your company. The exact legal name is not required. Optional field.

OpenSSL creates the CSR and key in the current working directory.

After you finish

Use the CSR to obtain a trusted public key certificate from a commercial CA.

Obtain a public key certificate for Apache

Obtain a public key certificate for the Avamar system's Apache HTTP server (Apache) from a commercial CA.

Provide a commercial CA with the CSR that was generated for Apache and complete any other requirements specific to that CA. After its requirements are met, the CA provides a public key certificate for Apache in the form of an electronic file, usually with the `.crt` filename extension.

The CA may also provide a certificate chain. A certificate chain is a series of certificates that link the public key certificate you receive to a trusted root CA certificate. Combine the certificate chain into a single file.

Combining a multiple file certificate chain

Commercial certification authorities sometime provide a multiple file certificate chain that links the private key certificate to a trusted root CA certificate. Use this procedure to combine those files into a single file.

Before you begin

From a commercial CA, obtain a multiple file trusted root CA certificate chain.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Use `cat` with the redirect and append operators to combine the certificates by typing:

   ```
   cat chain-cert-1 > cachain.crt
   cat chain-cert-2 >> cachain.crt
   cat chain-cert-3 >> cachain.crt
   cat chain-cert-4 >> cachain.crt
   cat chain-cert-5 >> cachain.crt
   ```

   where *chain-cert-1* through *chain-cert-5* represent the path to each certificate in the certificate chain and *cachain.crt* is a name that you provide for the combined file.

Results

The `cat` command with the redirect and append operators combines all of the files into a single file.

Configuring Apache to use a key and a root CA certificate

Configure the Avamar system's Apache HTTP server (Apache) to use a private key, a public key certificate, and a trusted root CA certificate.

Before you begin

Place in a temporary directory on the Avamar system's utility node the following:

- Private key for Apache
- Public key certificate for Apache
- Trusted root CA certificate for the public key certificate used by Apache

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Change the working directory to the temporary location of the certificate, key, and certificate chain file.
3. Use the correct command sequence to move the certificate, key, and certificate chain file to the OS-specific default locations.
   - On Red Hat Enterprise Linux:

     ```
     mv server.crt /etc/httpd/conf/ssl.crt/server.crt
     mv server.key /etc/httpd/conf/ssl.key/server.key
     mv cachain.crt /etc/httpd/conf/ssl.crt/ca.crt
     ```

- On SUSE Linux Enterprise Server:

```
mv server.crt /etc/apache2/ssl.crt/server.crt
mv server.key /etc/apache2/ssl.key/server.key
mv cachain.crt /etc/apache2/ssl.crt/ca.crt
```

NOTICE

Custom locations can be specified for these files by changing the Apache SSL configuration file. However, the Apache SSL configuration file is overwritten during Avamar system upgrades. Restore that file after a system upgrade.

4. Restart Apache by typing:

```
website restart
```

Restoring the Apache SSL configuration file

The Apache SSL configuration file is overwritten during Avamar system upgrades. This also overwrites custom paths for the certificate, key, and certificate chain file. To use custom paths restore the Apache SSL configuration file from the backup copy made during the upgrade.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

```
su -
```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Back up the latest version of the Apache SSL configuration file.
   - On Red Hat Enterprise Linux:

```
cd /etc/httpd/conf.d/
cp ssl.conf ssl.conf.orig
```

   - On SUSE Linux Enterprise Server:

```
cd /etc/apache2/vhosts.d/
cp vhost-ssl.conf vhost-ssl.conf.orig
```

3. Change the current working directory.

```
cd /usr/local/avamar/var/avi/server_data/package_data/
UPGRADE_FROM_VERSION/ConfigureApacheSsl/
```

   where *UPGRADE_FROM_VERSION* is the name of the directory created during the latest upgrade.

4. Extract the previous version backup copy of the Apache SSL configuration file, by typing:

```
tar -xzf node_0.s_*.*.*.tgz -C /
```

5. Restart Apache, by typing:

   ```
   website restart
   ```

Commercially signed SSL certificates

An alternative to the self-signed Avamar security certificates for Tomcat DTLT, Jetty, and Apache is to use security certificates that are signed by a third party.

When you install Avamar, the installation process creates self-signed security certificates that rely on the authority of the Avamar server for trust. Some web browsers issue security exceptions for untrusted certificates. You may want to use security certificates that you submitted for signature by a commercial certificate authority (CA) or that are otherwise specific to the environment.

The installation of particular hotfixes may affect the tasks that follow. Before importing any security certificates, identify the installed hotfixes. Note whether hotfix 263998 or 275068 is installed and then leave the command shell open.

Identifying the installed hotfixes

Most hotfixes can be identified by inspecting the list of workflows that are installed on the Avamar server.

Procedure

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. Display the list of installed workflows by typing the following command:

   ```
   ls -1 /usr/local/avamar/var/avi/server_data/package_data
   ```

   Information similar to the following is displayed in the command shell:

   ```
   AvamarInstallSles-7.3.1-125.avp
   AvPlatformOsRollup_2016-Q4-v2.avp
   Hotfix275068-7.3.1-125.avp
   UpgradeClientDownloads-7.3.1-125.avp
   UpgradeClientPluginCatalog-7.3.1-125.avp
   ```

Importing commercially signed security certificates for Tomcat DTLT and Jetty

Tomcat DTLT answers requests on ports 8543 and 8444, and Jetty answers requests on port 7543. The Tomcat DTLT security certificate is stored in `/home/admin/.keystore -alias tomcat` and the Jetty security certificate is stored in `/root/.keystore -alias tomcat`.

Procedure

1. Switch user to root by typing the following command:

   ```
   su -
   ```

2. Back up the root and admin keystores by typing the following commands:

   ```
   cp /root/.keystore /root/.keystore_bak
   ```

   ```
   cp /home/admin/.keystore /home/admin/.keystore_bak
   ```

3. Delete the current security certificates from the root and admin keystores by typing the following commands, each on one line:

```
keytool -delete -alias tomcat -keystore /root/.keystore -
storepass changeit
```

```
keytool -delete -alias tomcat -keystore /home/admin/.keystore -
storepass changeit
```

4. Regenerate the security certificates and keys by typing the following commands, each on one line:

   ```
   keytool -genkeypair -keysize 3072 -alias tomcat -keyalg RSA -
   sigalg SHA512withRSA -keystore /root/.keystore -storepass
   changeit -noprompt -dname "CN=CommonName, OU=OrganizationalUnit,
   O=Organization, L=LocalityName, S=StateName, C=Country"
   ```

   ```
   keytool -genkeypair -keysize 3072 -alias tomcat -keyalg RSA -
   sigalg SHA512withRSA -keystore /home/admin/.keystore -storepass
   changeit -noprompt -dname "CN=CommonName, OU=OrganizationalUnit,
   O=Organization, L=LocalityName, S=StateName, C=Country"
   ```

   where:

Field	Description
Country	The two-letter ISO abbreviation for the country. The list of abbreviations is available on the ISO web site at www.iso.org.
StateName	In countries where it is applicable, the state or province where the organization is located. This entry cannot be abbreviated.
LocalityName	City where the organization is located.
Organization	The exact legal name of the company. This entry cannot be abbreviated.
OrganizationalUnit	Optional entry for more information about the organization, such as a department name.
CommonName	FQDN of the server, or a wildcard FQDN for several servers. The wildcard character (`*`) must only appear once, and only in the hostname portion of the FQDN value. Example for single server: `corp-1.example.com`. Example wildcard FQDN for several servers: `corp-*.example.com`.

   Press **Enter** to retain the same keypass.

5. Create the certificate signing requests (CSRs) by typing the following commands, each on one line:

   ```
   keytool -certreq -alias tomcat -file /root/tomcat.csr -
   keystore /root/.keystore -storepass changeit
   ```

   ```
   keytool -certreq -alias tomcat -file /home/admin/tomcat.csr -
   keystore /home/admin/.keystore -storepass changeit
   ```

6. Obtain the CSRs from the server in the following locations and submit them to a CA for signing.

   - `/root/tomcat.csr`

- /home/admin/tomcat.csr

7. Obtain text files from the CA that contain each signed security certificate and place them on the server.

   The CA may supply additional security certificates, such as an intermediate or root CA certificate, or a certificate chain. Import these certificates before importing the signed certificate.

   The following steps assume that a CA root certificate exists in /var/tmp/CA.crt and that the signed certificate exists in /var/tmp/tomcat_signed.crt.

8. Import the CA root certificate into the root keystore by typing the following command on one line:

   keytool -importcert -file /var/tmp/CA.crt -keystore / root/.keystore -storepass changeit

9. Import the signed certificate into the root keystore by typing the following command on one line:

   keytool -importcert -file /var/tmp/tomcat_signed.crt -keystore / root/.keystore -storepass changeit -alias tomcat

10. Back up the Avamar keystore by typing the following command on one line:

    cp -p /usr/local/avamar/lib/rmi_ssl_keystore /usr/local/ avamar/lib/rmi_ssl_keystore.bak

11. Import the CA root certificate into the Avamar keystore by typing the following command on one line:

    keytool -importcert -file /var/tmp/CA.crt -keystore /usr/local/ avamar/lib/rmi_ssl_keystore -storepass changeme

12. Restart the Avamar Installation Manager by typing the following command:

    dpnctl stop avinstaller && dpnctl start avinstaller

13. Import the CA root certificate into the admin keystore by typing the following command on one line:

    keytool -importcert -file /var/tmp/CA.crt -keystore /home/ admin/.keystore -storepass changeit

14. Import the signed certificate into the admin keystore by typing the following command on one line:

    keytool -importcert -file /var/tmp/tomcat_signed.crt -keystore / home/admin/.keystore -storepass changeit -alias tomcat

15. Restart EM Tomcat by typing the following command:

    dpnctl stop emt && dpnctl start emt

16. If the REST API is installed, restart the REST server by typing the following commands:

    /usr/local/avamar/bin/restserver.sh --stop

    /usr/local/avamar/bin/restserver.sh --start

Importing commercially signed security certificates for Apache

Apache answers requests on port 443. The Apache security certificate is stored in `/etc/apache2/ssl.crt/server.crt`.

Procedure

1. Ensure that you are still logged in as the root user.
2. Back up the Apache security certificate by typing the following command on one line:

   `cp /etc/apache2/ssl.crt/server.crt /etc/apache2/ssl.crt/server.crt.bak`

3. Regenerate the security certificate and keys by typing the following command on one line:

   `openssl req -x509 -new -newkey rsa:3072 -nodes -keyout /etc/apache2/ssl.key/server.key -sha512 -out /etc/apache2/ssl.crt/server.crt -days 1825 -subj "/C=`*`Country`*`/ST=`*`StateName`*`/L=`*`LocalityName`*`/O=`*`Organization`*`/OU=`*`OrganizationalUnit`*`/CN=`*`CommonName`*`/emailAddress=`*`EmailContact`*`"`

   where:

Field	Description
Country	The two-letter ISO abbreviation for the country. The list of abbreviations is available on the ISO web site at www.iso.org.
StateName	In countries where it is applicable, the state or province where the organization is located. This entry cannot be abbreviated.
LocalityName	City where the organization is located.
Organization	The exact legal name of the company. This entry cannot be abbreviated.
OrganizationalUnit	Optional entry for more information about the organization, such as a department name.
CommonName	FQDN of the server, or a wildcard FQDN for several servers. The wildcard character (`*`) must only appear once, and only in the hostname portion of the FQDN value. Example for single server: **`corp-1.example.com`**. Example wildcard FQDN for several servers: **`corp-*.example.com`**.
EmailContact	Email address of the primary administrator of the server or servers.

   Ensure that there are no spaces in the `subj` parameter.

4. Create the CSR by typing the following command on one line:

   `openssl x509 -x509toreq -in /etc/apache2/ssl.crt/server.crt -signkey /etc/apache2/ssl.key/server.key -out /etc/apache2/apache.csr`

5. Obtain the CSR from the server at `/etc/apache2/apache.csr` and submit it to a CA for signing.
6. Obtain a text file from the CA that contains the signed security certificate and place it on the server.

   The CA may supply additional security certificates, such as an intermediate or root CA certificate, or a certificate chain. Import these certificates before importing the signed certificate.

   The following steps assume that a CA root certificate exists in `/etc/apache2/ssl.crt/CA.crt` and that you have overwritten the existing certificate at `/etc/apache2/ssl.crt/server.crt` with the signed certificate.

7. Set the ownership and group of the security certificates by typing the following command on one line:

   chown root:root /etc/apache2/ssl.crt/server.crt /etc/apache2/ssl.crt/CA.crt

8. Set the file permissions for the security certificates by typing the following command on one line:

   chmod 600 /etc/apache2/ssl.crt/server.crt /etc/apache2/ssl.crt/CA.crt

9. Delete the existing security certificate and key from the Network Security Services (NSS) database by typing the following command:

   certutil -F -n Server-Cert -d /etc/apache2/mod_nss.d

   When prompted, type the password **changeme123!**.

10. Create a `.p12` file containing the signed security certificate and key by typing the following command on one line:

    openssl pkcs12 -export -in /etc/apache2/ssl.crt/server.crt -inkey /etc/apache2/ssl.key/server.key -out /etc/apache2/server-cert.p12 -name "Server-Cert" -passin pass:foo -passout pass:foo

    If the CA provided additional security certificates, add a `-certfile` argument for each additional certificate. For example:

    openssl pkcs12 -export -in /etc/apache2/ssl.crt/server.crt -*certfile /etc/apache2/ssl.crt/CA.crt* -inkey /etc/apache2/ssl.key/server.key -out /etc/apache2/server-cert.p12 -name "Server-Cert" -passin pass:foo -passout pass:foo

11. Import the `.p12` file into the NSS database by typing the following command on one line:

    pk12util -i /etc/apache2/server-cert.p12 -d /etc/apache2/mod_nss.d -W foo

    When prompted, type the password **changeme123!**.

12. Restart Apache by typing the following command:

    service apache2 restart

Code signing

Avamar provides signed client (RPM/DEB) and server (RPM) packages to ensure the authenticity and integrity of software components. This digital signature ensures that

the packages have not been modified or corrupted in transit and come from a trusted source.

Newer AVE images contain GPG public keys that enable the Avamar server to verify the authenticity of signed packages. Upgrades to Avamar 7.5.1 and later and Avamar 18.1 and later also supply these public keys. Avamar clients obtain the public keys from the Avamar server via Web Restore.

Avamar Installation Manager installs some internal components of the Avamar server from signed RPM files. The public keys allow the Avamar to verify the authenticity of the packages and the package payloads.

The public keys also allow the Avamar clients and the Avamar Installation Manager to install signed and unsigned packages and RPMs. Both the public keys and the signed packages can be deployed via the Avamar Client Manager (ACM).

Avamar Installation Manager and ACM retain the ability to accept unsigned packages.

Limitations

The applicability of code signing is subject to the following limitations:

- The Avamar Windows client is not signed with the GPG key because the client is already signed by a certificate.
- The Avamar Solaris client is not signed with the GPG key. Signing support for this platform is expected in a future release.

Clients and the GPG public keys

The **Downloads** section of the **Avamar Web Restore** page (DTLT) contains an entry for **Public GPG keys for Avamar Client RPM/Debian packages**.

Linux and UNIX clients should download this key and the installer script:

- `avpkgkey.pub`
- `import_avpkgkey.sh`

Run the script to import the Avamar GPG public keys.

Credential security

The following sections provide information about how to secure the credentials that are used to connect Avamar to remote components.

Data Domain

Avamar uses DD Boost software, SSH, and REST-based communication to interact with the Data Domain system:

- DD Boost and SSH—Avamar connects to the Data Domain system with credentials that are secured by means of Transport Layer Security (TLS) with a presigned certificate that belongs to Avamar. Avamar securely stores the certificate in a keystore and provides the certificate to Data Domain for authentication.
- Rest API—Avamar connects to the Data Domain system with credentials that are secured based on HTTPS transport-level security with a presigned certificate that belongs to Avamar.

Data Domain credentials are stored in a local file with the name `dr_info` in the `/usr/local/Avamar/var/` directory. The local keystore file is encrypted with a 128-bit AES key.

ESRS
Avamar uses an RSA token, which is a one-time password authentication method, to connect to the EMC Secure Remote Services (ESRS) Gateway. Avamar does not store the username and password (token). The token is valid for only 1 minute.

VMware vCenter
Avamar stores the vCenter username and password as a value in the MCS database. The password is encrypted with AES encryption and relies on the database's native protection.

The vCenter public key is stored in the `/user/local/Avamar/lib/rmi_ssl_keystore` keystore.

Dell EMC repository server
The Support Zone account credentials are encrypted with Java Cryptography Extension and saved in a local configuration file.

LDAP server
Avamar relies on the LDAP mapping system to store LDAP credentials. For more information, see the *Avamar Administration Guide*.

FLR UI
The FLR UI does not store credentials on the Avamar server.

KMIP server
The certificates that belong to the KMIP server are stored in the `/usr/local/avamar/etc/akm` folder.

Avamar stores the username and password for the KMIP server in the `akm.xml` configuration file. The password is encrypted with a 256-bit AES key.

CHAPTER 3

Authorization

This chapter includes the following topics:

About authorization

After a user authenticates to Avamar, the concept of user authorization places limits on the actions that an authenticated user may take.

Roles define the allowable operations for each user account. In general, Avamar authorization proceeds by assigning users to one of the default roles.

Default roles

There are three types of default roles:

- Administrator roles
- Operator roles
- User roles

Administrator roles

Administrators are responsible for maintaining the server.

You can only assign the role of administrator to user accounts at a domain level. Domain level includes the top-level (root) domain and any other domain or subdomain. You cannot assign the administrator role to user accounts at a client level.

You can assign the administrator role to users at the top-level (root) domain or to a specific domain or subdomain.

Avamar 18.2 introduces the concept of the vCenter administrator. This role is specific to the AUI and has no counterpart in Avamar Administrator.

Table 19 Administrator roles

Administrator type	Description
Root administrators	Administrators at the top-level (root) domain have full control of the system. They are sometimes referred to as “root administrators.”
Domain administrators	Administrators at domains other than root generally have access to most of the features that are described in this guide. Administrators typically can only view or operate on objects in the domain. Any activity that would allow a domain administrator to view data outside the domain is disallowed. Access to server features of a global nature (for example, suspending or resuming scheduled operations or changing runtimes for maintenance activities) is disallowed. Domain administrators: • Cannot add or edit other subdomain administrators. • Cannot change their assigned role. • Can change their password. Domain administrators do not have access to the AUI dashboard.
vCenter administrator	vCenter administrators have access to the same features as domain administrators, but additionally have access to the AUI dashboard and to event management area within the vCenter domain.

Operator roles

Operator roles are generally implemented to allow certain users limited access to certain areas of the server to perform backups and restores, or obtain status and run

reports. These roles allow greater freedom in assigning backup, restore, and reporting tasks to persons other than administrators.

You can only assign operator roles to user accounts at the domain level. You cannot assign these roles to user accounts at the client level. To add the user account to subdomains, you must have administrator privileges on the parent domain or above.

Users with an operator role do not have access to all administrative features. Instead, after login, they are presented with an interface that provides access to the features that they are allowed to use.

The following table describes the four operator roles.

Table 20 Operator roles

Operator type	Description
Restore only operator	Restore only operators are generally only allowed to perform restores and to monitor those activities to determine when they complete and if they completed without errors. Restore only operators at the top-level (root) domain can perform restores for any client in the server. Restore only operators at a domain other than root can only perform restores for clients in that domain. Restore only operators can restore backup data and monitor activities in the assigned domain. • By default, restore only operators cannot perform restores to a different location or restores to multiple locations. To enable this option, you must set the `restore_admin_can_direct_restores` attribute to true in the `mcserver.xml` file. • By default, restore only operators cannot browse backups from the command line or the Avamar Web Restore interface. To enable these activities for a restore only operator, add the `noticketrequired` privilege by using the `avmgr chgv` command:**`avmgr chgv --acnt=`*`location`*** **`--u=`*`name`*** **`--ud=`*`auth`*** **`\ --pv="enabled,read,mclogin,noticketrequired"`** where *location* is the subdomain of the operator, *name* is the Avamar username of the user, and *auth* is the external authentication system that is used to authenticate the user.
Backup only operator	Backup only operators are generally only allowed to perform backups and to monitor those activities to determine when they complete and if they completed without errors. Backup only operators at the top-level (root) domain can perform backups for any client or group in the server. Backup only operators at domains other than root can only perform backups for clients or groups in that domain. Backup only operators can perform on-demand backups of a client or a group, as well as monitor activities in the assigned domain. • By default, backup only operators cannot perform restores to a different location or restores to multiple locations. To enable this option, you must set the `restore_admin_can_direct_restores` attribute to true in the `mcserver.xml` file. • By default, backup only operators cannot perform backups from the command line. To enable command line backups for a backup only operator, add the `noticketrequired` privilege by using the `avmgr chgv` **`avmgr chgv --acnt=`*`location`*** **`--u=`*`name`*** **`--ud=`*`auth`*** **`\ --pv="enabled,read,mclogin,backup,noticketrequired"`**command: where *location* is the subdomain of the operator, *name* is the Avamar username of the user, and *auth* is the external authentication system that is used to authenticate the user.
Backup/restore operator	Backup/restore operators are generally only allowed to perform backups or restores and to monitor those activities to determine when they complete and if they completed without errors. As with roles that are assigned to other domain user accounts, backup/restore operators at the top-level (root) domain can perform backups and restores for any client or group in the server. Backup/restore operators at domains other than root can only perform backups and restores for clients or groups in that domain. Backup/restore operators can perform the following tasks in the assigned domain:

Table 20 Operator roles (continued)

Operator type	Description
	• Perform on-demand backups for a client or group. • Perform restores. • Monitor activities. By default, backup/restore operators cannot browse backups from the command line or by using the Avamar Web Restore interface, and cannot perform backups from the command line. To enable these activities, add the `noticketrequired` privilege by using the `avmgr chgv` command: **`avmgr chgv --acnt=`*`location`*` --u=`*`name`*` --ud=`*`auth`*` \ --pv="enabled,read,mclogin,backup,noticketrequired"`** where *location* is the subdomain of the operator, *name* is the Avamar username of the user, and *auth* is the external authentication system that is used to authenticate the user.
Activity operator	Activity operators are generally only allowed to monitor backup and restore activities and to create certain reports. Activity operators at the top-level (root) domain can view or create reports for backup and restore activities in all domains and subdomains. Activity operators at domains other than root can only view or create reports for backup and restore activities in that domain. Activity operators can perform the following tasks in the assigned domain: • Monitor activities. • View the group status summary. • View the Activity Report. • View the Replication Report.

User roles

User roles limit the operations that are allowed for a user account to a specific client.

Users who are assigned to one of the user roles cannot log in to the Avamar Administrator, the AUI, Avamar Client Manager, or the Avamar client web UI.

Note

Avamar Administrator provides the ability to add a user account to a client. However, you cannot add a user account to a client from the Avamar Web User Interface (AUI).

The following table describes the four user roles.

Table 21 User roles

User type	Description
Back Up Only User	Users assigned this role can start backups directly from the client by using the `avtar` command line.
Restore (Read) Only User	Users assigned this role can start restores directly from the client by using the `avtar` command line or Management Console Server (MCS) web services.
Back Up/Restore User	Users assigned this role can start backups and restores directly from the client by using the `avtar` command line or MCS web services.
Restore (Read) Only/ Ignore File Permissions	Similar to the Restore (Read) Only User role except that operating system file permissions are ignored during restores. This user is allowed to restore any file that is stored for an Avamar client.

Table 21 User roles (continued)

User type	Description
	This role is only available when users are authenticated by using Avamar internal authentication. To ensure trouble-free restores, Windows client user accounts should be assigned this role only when both of the following are true: • Users are authenticated using Avamar internal authentication. • Users do not require access to the Avamar client web UI.

Role-based access control and the AUI

The AUI provides role-based security for users who access the web-based interface.

Each time that a user logs in to the AUI, the security subsystem maps the user to any assigned roles and domains. Avamar uses that information to construct a table of the administrative areas and URLs that correspond to a user's access level.

After logging in, the AUI directs the user to a default page for their role, and hides any controls and areas that do not correspond to the user's access level. For example, a backup only operator sees the **Asset Management** and **Activity** areas in the navigation pane, but not the server management areas.

Each time that a user goes to an area within the AUI, regardless of the method, the security subsystem checks the incoming request against the access table and grants or denies the request accordingly. The AUI reroutes any attempts to access unauthorized areas.

The following tables indicate the user roles that can access each of the specified feature panes within the AUI.

Table 22 AUI feature pane access by administrator user role

AUI feature pane	Root administrator	Domain administrator	vCenter administrator
Dashboard	Yes	No	Yes
Asset Management	Yes	Yes[a]	Yes[a]
Asset Management Domain	Yes	Yes[a]	Yes[a]
Asset Management Backup	Yes	Yes[a]	Yes[a]
Asset Management Restore	Yes	Yes[a]	Yes[a]
Backup Policy	Yes	Yes[a]	Yes[a]
Advanced Policy	Yes	Yes[a]	Yes[a]

Table 22 AUI feature pane access by administrator user role (continued)

AUI feature pane	Root administrator	Domain administrator	vCenter administrator
Replication Policy	Yes	No	No
Cloud Tier Policy	Yes	No	No
Setting	Yes	Yes[a]	Yes[a]
Proxy Management	Yes	Yes[a]	Yes[a]
System	Yes	Yes[a]	Yes[a]
Activity	Yes	Yes[a]	Yes[a]
Event	Yes	No	Yes[a]

a. Within the specified domain

Table 23 AUI feature pane access by operator user role

AUI feature pane	Backup/ restore operator	Backup only operator	Restore only operator	Activity operator
Dashboard	No	No	No	No
Asset Management	Yes	Yes	Yes	No
Asset Management Domain	No	No	No	No
Asset Management Backup	Yes	Yes	No	No
Asset Management Restore	Yes	No	Yes	No
Backup Policy	No	No	No	No
Advanced Policy	No	No	No	No
Replication Policy	No	No	No	No
Cloud Tier Policy	No	No	No	No
Setting	No	No	No	No
Proxy Management	No	No	No	No

Table 23 AUI feature pane access by operator user role (continued)

AUI feature pane	Backup/ restore operator	Backup only operator	Restore only operator	Activity operator
System	No	No	No	No
Activity	Yes	Yes	Yes	Yes
Event	No	No	No	No

Role mapping

Administrators can assign roles at the time of account creation, or change the assigned roles at any point afterward. The *Avamar Administration Guide* contains specific tasks to configure a user's roles.

External role associations

Authorization follows the same process, whether you choose to configure users via internal authentication or network authentication (for example, LDAP and NIS). Network authentication provides no additional predetermined authorization. Instead, assign LDAP users to an existing Avamar role through an LDAP map.

The *Avamar Administration Guide* provides more information about network authentication.

Default authorizations

A new Avamar user account comes without any authorization, until the administrator assigns a role to the account from the list of available roles during the process of account creation.

However, after installation, the Avamar server contains several default user accounts with preconfigured authorizations. The Avamar server requires many of these accounts for proper operation. Pre-loaded user accounts on page 43 provides additional information.

The Avamar Customer Support password for the Avamar Installation Manager provides limited authorization to perform more complex operations.

Running commands with elevated privileges

The SLES OS for Avamar servers reserves many commands for the root user. However, the administrative OS user can run a limited number of reserved commands with elevated privileges by using the `sudo` command.

Many of the listed commands are intended to be run from scripts and utilities, and not directly from the command line. The file `/etc/sudoers` contains a full list of these commands.

Table 24 Commands authorized for `sudo`

`/opt/dell/srvadmin/bin/omconfig`

Table 24 Commands authorized for `sudo` (continued)

/opt/MegaRAID/CmdTool2/CmdTool2
/sbin/arping
/sbin/chkconfig --add akm
/sbin/chkconfig --add connectemc
/sbin/chkconfig --del akm
/sbin/chkconfig snmpd off
/sbin/chkconfig snmpd on
/sbin/dumpe2fs
/sbin/ethtool bond[0-9]
/sbin/ethtool bond[0-9]*.*[0-9]
/sbin/ethtool bond[0-9][0-9]
/sbin/ethtool eth[0-9]
/sbin/service akm restart
/sbin/service akm start
/sbin/service akm status
/sbin/service akm stop
/sbin/service apache2 status
/sbin/service apache2 stop
/sbin/service axionfs restart
/sbin/service axionfs status
/sbin/service axionfs stop
/sbin/service connectemc restart
/sbin/service connectemc start
/sbin/service connectemc stop
/sbin/service rabbitmq-server restart
/sbin/service rabbitmq-server start
/sbin/service rabbitmq-server status
/sbin/service snmpd restart
/sbin/service snmpd start
/sbin/service snmpd status
/sbin/service sshd restart
/sbin/service sshd status
/sbin/service syslog restart
/sbin/service syslog start

Table 24 Commands authorized for `sudo` (continued)

/usr/Arcconf/arcconf
/usr/bin/atq
/usr/bin/chage -l root
/usr/bin/crontab -u admin -l
/usr/bin/crontab -u dpn -l
/usr/bin/crontab -u root -l (root)
/usr/bin/flashupdt/flashupdt -i
/usr/bin/omreport
/usr/local/avamar/bin/avsetup_snmp --testconfigured (root)
/usr/local/avamar/bin/emwebapp.sh
/usr/local/avamar/bin/mccipher encrypt --all
/usr/local/avamar/bin/mccipher --encrypt_mcs
/usr/local/avamar/bin/mccipher --encrypt_mcs
/usr/local/avamar/bin/mccipher --encrypt_mcs
/usr/local/avamar/bin/mccipher --encrypt_mcs /usr/local/avamar/lib (rootAP)
/usr/local/avamar/bin/mccipher --encrypt_mcs /usr/local/avamar/lib/ mcserver.xml
/usr/local/avamar/bin/mccipher --encrypt_mcs /usr/local/ avamar/var/mc/server_data/prefs (MCUSERAP|rootAP)
/usr/local/avamar/bin/mccipher --update
/usr/local/avamar/bin/mcsnmp
/usr/local/avamar/bin/secure.dpn
/usr/local/avamar/bin/tomcatctl
/usr/sbin/dmidecode
/opt/dell/linux/supportscripts/srvadmin-services.sh
/opt/dell/srvadmin/bin/omreport
/opt/dell/srvadmin/omil/srvadmin-services.sh
/opt/dell/srvadmin/sbin/racadm getconfig -g cfgracvirtual -o cfgvirmediaattached
/opt/dell/srvadmin/sbin/srvadmin-services.sh
/opt/MegaRAID/CmdTool2/CmdTool264
/sbin/chkconfig --del connectemc
/sbin/ethtool eth[0-9][0-9]
/sbin/service apache2 restart

Table 24 Commands authorized for `sudo` (continued)

/sbin/service apache2 start
/sbin/service axionfs start
/sbin/service connectemc status
/sbin/service rabbitmq-server stop
/sbin/service snmpd stop
/sbin/service sshd start
/sbin/service syslog status
/usr/bin/chage -l admin
/usr/bin/ipmitool
/usr/bin/omconfig
/usr/local/avamar/bin/avagent.bin
/usr/local/avamar/bin/avsetup_connectemc.pl
/usr/local/avamar/bin/backup_upgrade_files \"\"
/usr/local/avamar/bin/clean_db.pl
/usr/local/avamar/bin/createFSLink.pl
/usr/local/avamar/bin/dpnfsctl
/usr/local/avamar/bin/getlogs
/usr/local/avamar/bin/killProcess.pl
/usr/local/avamar/bin/mccipher encrypt --all
/usr/local/avamar/bin/mccipher encrypt --all
/usr/local/avamar/bin/mccipher encrypt --all /usr/local/avamar/lib
/usr/local/avamar/bin/mccipher --encrypt_mcs
/usr/local/avamar/bin/mccipher --encrypt_mcs
/usr/local/avamar/bin/mccipher --encrypt_mcs
/usr/local/avamar/bin/mccipher --encrypt_mcs /usr/local/avamar/lib (MCUSERAP)
/usr/local/avamar/bin/mccipher --encrypt_mcs /usr/local/avamar/lib (MCUSERAP|rootAP)
/usr/local/avamar/bin/mccipher --init
/usr/local/avamar/bin/mccipher --init_mcs
/usr/local/avamar/bin/mccipher --upgrade
/usr/local/avamar/bin/mccipherHelper.pl (root)
/usr/local/avamar/bin/mcddrsnmp
/usr/local/avamar/bin/msgbrokerctl.pl --start
/usr/local/avamar/bin/msgbrokerctl.pl --stop

Table 24 Commands authorized for `sudo` (continued)

/usr/local/avamar/bin/rabbitCertificateGen.pl
/usr/local/avamar/lib (rootAP|MCUSERAP)
/usr/local/avamar/lib (viewuserAP)
/usr/local/avamar/lib/dpnutils/avictl
/usr/local/avamar/lib/dpnutils/connectemcctl (root)
/usr/local/avamar/lib/dpnutils/dtltctl
/usr/local/avamar/lib/dpnutils/unattended-restart-ctl
/usr/local/avamar/var/mc/server_data/prefs
/usr/local/avamar/var/mc/server_data/prefs (MCUSERAP)
/usr/local/avamar/var/mc/server_data/prefs (rootAP)
/usr/local/avamar/var/mc/server_data/prefs (rootAP|MCUSERAP)
/usr/local/avamar/var/mc/server_data/prefs (viewuserAP)
/usr/sbin/flashupdt -i

Entitlement export

An administrator can export a list of authorized users, along with their respective roles and domains, from the command prompt.

After logging in to the Avamar server, type the following command:

```
mccli user show
```

Avamar returns output similar to the following:

```
0,23000,CLI command completed successfully.
Name          Role                      Domain Authenticator
------------- ------------------------- ------
---------------------------
MCUser        Administrator             /      Axion Authentication
System
backuponly    Back up Only User         /      Axion Authentication
System
backuprestore Back up/Restore User      /      Axion Authentication
System
repluser      Replication User          /      Axion Authentication
System
restoreonly   Restore (Read) Only User  /      Axion Authentication
System
root          Administrator             /      Axion Authentication
System
```

Actions that do not require authorization

Most actions that a user can perform on an Avamar server require some degree of authentication and authorization, including any actions that provide access to

customer data. However, for convenience, a limited number of actions do not require authorization.

Table 25 Actions that do not require authorization

Location	Action	Effects	Notes
Avamar Web Restore (Desktop/Laptop)	Downloads	Allows a user to download platform-specific Avamar client plug-ins and related items.	An administrator must activate a client and assign it to a policy before the Avamar server performs a backup of that client. Installing the Avamar client software does not automatically start backups of that client.
Avamar Web Restore (Desktop/Laptop)	Administrator	Allows a user to download the Avamar Administrator application for use on the local computer.	The Avamar Administrator software requires authentication and authorization to access any system functions. The server permits only the software download without authorization.
Avamar Web Restore (Desktop/Laptop)	Help	Provides description of the functions available through Avamar Web Restore.	

CHAPTER 4

Network Security

This chapter includes the following topics:

Network exposure

The following topics describe the exposed or required ports and protocols for communication between the Avamar server and external components.

Terminology

This chapter uses specific terms to refer to network concepts that concern Avamar servers:

Source

Computer that originates a network transmission. The source computer transmits network packets through a network interface, over a network connection, and to a specific port on a target computer.

Target

Computer that receives a network transmission. The target computer receives transmitted network packets on the port that the source computer specified. A service on the target computer that is listening on the specified port processes the packets. Processing may include a response sent to the source computer or the establishment of two-way communication with the source computer.

Inbound

Direction of travel of network packets that are sent from another computer to a referenced Avamar computer. The referenced Avamar computer is the target and the other computer is the source. The referenced Avamar computer receives inbound network packets on an inbound port. The inbound port is a port on the referenced Avamar computer with a specific service for receiving and handling those network packets. The inbound port is also known as a listening port.

Outbound

Direction of travel of network packets that an Avamar computer sends to a destination computer. The referenced Avamar computer is the source and the other computer is the target. The outbound port is the port on which the other computer listens for the transmissions from the referenced Avamar computer.

Required ports

Inbound and outbound ports that must be open to allow the Avamar server to perform its core functions. Relevant routers, switches, and firewalls must allow the network packets to reach these required ports. Core functionality is reduced when a process listening on a required target port cannot receive packets from a source computer.

Note

When an Avamar server undergoes security hardening some of the required ports are intentionally closed. Security hardening provides an increase in security in exchange for a loss of some functionality.

Optional ports

Inbound and outbound ports that are used by the Avamar server to provide additional functionality. Closing these ports reduces or eliminates the additional

functionality but does not prevent the Avamar server from performing its core functions.

Utility node ports

The Avamar utility node has specific port requirements both for inbound and outbound ports.

The tables in this section list the following port requirements for the utility node:

- Required inbound ports

  Ports on the utility node that must be open to network transmissions from specified source computers.
- Optional inbound ports

  Ports on the utility node that can be optionally opened to network transmissions from specified source computers to enable a specific feature.
- Required outbound ports

  Ports on another computer that the utility node must be allowed to access.

Utility node required inbound ports

The following table describes the inbound ports that must be open on an Avamar utility node. For every port listed in this table, the Avamar utility node is the destination and the source is listed in the Source computer column.

Note

Avamar 7.5.1 removes support for HTTP access to TCP ports 80 and 7580. Use the HTTPS ports 443 and 7543 to access these services instead.

Table 26 Required inbound ports on the utility node

Port	Protocol	Service name	Source computer	Additional information
N/A	ICMP Types 3, 8, and 11	ICMP	• Avamar clients • Other Avamar servers • Data Domain system	Avamar clients periodically ping the Avamar server to determine the best interface for communicating with the MCS. The Avamar server sends an ICMP response. Avamar servers also ping associated systems, such as replication destinations and Data Domain.
22	TCP	SSH	• Administrator computers • Other Avamar server nodes	Secure shell access.

Table 26 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
69	TCP	TFTP	Internal switch	
123	TCP/UDP	NTP	NTP time servers	Provides clock synchronization from network time protocol servers.
161	UDP	SNMP	Data Domain system	Getter/setter port for SNMP objects from a Data Domain system. Required when storing Avamar client backups on a Data Domain system.
443	TCP	HTTPS protocol over TLS/SSL	• Web browser clients • Reverse proxy web server • AvInstaller • Avamar Downloader Service host • Avamar Key Manager	Provides web browsers with HTTPS access to Avamar services. A reverse proxy web server can be used to limit access to this port.
700	TCP/UDP	Login Manager	• Web browser clients • Reverse proxy web server	
703	TCP	AKM service	Avamar server nodes	Used for key management.
1234	TCP	Avamar installation utility HTTPS	Web browser clients	Only open this port for installation of the Avamar software. Only permit access from trusted administrator computers that are used during software installation.

Table 26 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
				NOTICE Close this port when installation of the Avamar software is complete. Avamar services do not listen on port 1234.
2888	TCP	AVDTO	Avamar Extended Retention Media Access Node	The firewall rules open this port when you install support for Avamar Extended Retention.
5555	TCP	PostgreSQL administrator server	• Clients running Avamar Client Manager and Data Protection Advisor • PostgreSQL administrator client computers	This port is open by default. Securing the Postgres firewall port on page 214 provides more instructions to enable selective access. Limit access to trusted administrator computers.
5568	TCP	PostgreSQL	Avamar Extended Retention Media Access Node	The firewall rules open this port when you install support for Avamar Extended Retention.
5671	TCP	RabbitMQ	• localhost • Other Avamar utility nodes • Avamar Extended Retention computers • Backup and Recovery Manager computers	RabbitMQ is a message broker who is used to enhance asynchronous interprocess communication.
6667	TCP	Archive Service Event	Avamar Extended Retention Media Access Node	The firewall rules open this port when you install support for Avamar Extended Retention.
7000	TCP	Apache Tomcat	Avamar Extended Retention Media Access Node	The firewall rules open this port when you install support for

Table 26 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
				Avamar Extended Retention.
7443	TCP	Apache Tomcat	Avamar Extended Retention Media Access Node	The firewall rules open this port when you install support for Avamar Extended Retention.
7543	HTTPS/SSL	Update Manager	Web browser clients	Web browser clients use this port to create HTTPS connections to Avamar Installation Manager. Limit access to trusted administrator computers.
7544	TCP	Update Manager	Jetty socket clients	Jetty socket clients use this port to send a shutdown signal to its Jetty web server. Limit access to trusted administrator computers.
7781	TCP	RMI	Avamar Administrator management console	Limit access to trusted administrator computers.
8105	TCP	Apache Tomcat	Avamar client computers	Used by Avamar Desktop/Laptop.
8109	TCP	Apache Tomcat	Avamar client computers	Used by Avamar Desktop/Laptop.
8181	TCP	Apache Tomcat	Avamar client computers	Connections from Avamar client computers and from AvInstaller hosts are redirected to this port.
8444	TCP	Apache Tomcat	Web browser clients	Web browser connections from Avamar Desktop/ Laptop client computers are redirected to this port.
8505	TCP	Apache Tomcat	Utility node or single-node server	Avamar Desktop/ Laptop uses this port to send a shutdown command to its Apache Tomcat server. Limit access to the utility

Table 26 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
				node or single-node server.
8580	TCP	AvInstaller	Web browser clients	Used for connections from Avamar Downloader Service computer, and for access to AvInstaller from other web browser clients.
9443	TCP	RMI - Avamar Management Console web services	Web browser clients	
19000	TCP/UDP	Avamar subsystem (also known as GSAN)	Avamar server nodes	Avamar subsystem communication.
19500	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
20000	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
20500	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
25000	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
25500	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
26000	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
26500	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
27000	TCP	Avamar server	• Avamar client computers • Avamar server nodes • Avamar nodes acting as a replicator source	Avamar subsystem communication. This port is blocked by default for new Avamar installations. Open this port to allow unencrypted backups.
27500	TCP	Avamar server	• Avamar server nodes • Avamar nodes acting as a replicator source	Avamar subsystem communication.

Table 26 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
28001	TCP	• Avamar server CLI • MCS • Avagent	• Avamar client computers • VMware proxy • Replication source • Replication target	• CLI commands from client computers. • Avagent to MCS communication. • Bi-directional communication between avagent and MCS on the replication source Avamar server and the replication destination Avamar server to permit authentication key exchange.
28002–28011	TCP		Avamar Extended Retention Media Access Node	The firewall rules open this port when you install support for Avamar Extended Retention.
28009	TCP	avagent	VMware proxy	Unsecure communication with VMware proxy.
28810-28819	TCP	ddrmaint	localhost	Internal use only for token-based authentication when connecting to Data Domain; only localhost can use it.
29000	TCP	Avamar server SSL	• Avamar client computers • Avamar server nodes	Avamar subsystem communication.
30001	TCP	MCS	• Avamar client computers • VMware proxy • Avamar server nodes	• 2-way secure socket communication. • Avagent to MCS communication. • MCS communication over SSL.
30002	TCP	avagent	Avamar client computers	Client communication over SSL.

Table 26 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
30003	TCP	MCS	• Avamar client computers • Avamar server nodes	MCS communication over SSL.
30102–30109	TCP	avagent	VMware proxy	Secure communication with VMware proxy.
61617	TCP	Apache ActiveMQ SSL	Avamar Extended Retention Media Access Node	The firewall rules open this port when you install support for Avamar Extended Retention.

Utility node optional inbound ports

The following table describes the recommended, but optional, inbound ports for an Avamar utility node. For every port listed in this table, the Avamar utility node is the destination and the source is listed in the Source computer column.

Table 27 Optional inbound ports on the utility node

Port	Protocol	Service name	Source computer	Additional information
514	UDP	syslog	Utility node or single-node server	Avamar server connects to this port to communicate events to syslog.
8509	TCP	Apache Tomcat	Utility node or single-node server	The Apache JServ Protocol (AJP) uses port 8509 to balance the work load for multiple instances of Tomcat.

Utility node required outbound ports

The following table describes the outbound ports that must be accessible to network packets that are sent from an Avamar utility node. For each row, the utility node is the source computer that must have outgoing access to the listed port on the listed destination computer.

Table 28 Required outbound ports for the utility node

Port	Protocol	Destination computer	Additional information
N/A	ICMP Types 3, 8, and 11	• Avamar clients • Other Avamar servers	Avamar clients periodically ping the Avamar server to determine the best interface

Table 28 Required outbound ports for the utility node (continued)

Port	Protocol	Destination computer	Additional information
		• Data Domain system	for communicating with the MCS. The Avamar server sends an ICMP response. Avamar servers also ping associated systems, such as replication destinations and Data Domain.
7	TCP	Data Domain system	Required to register a Data Domain system for storing Avamar client backups.
23	TCP	Internal	Required for communication with internal switches and for firmware upgrades.
25	TCP	Avamar Customer Support	Required to allow ConnectEMC to make an SMTP connection with Customer Support.
53	TCP/UDP	DNS	Required for name resolution and DNS zone transfers. VMware proxy nodes require the TCP connection to DNS.
88		Key Distribution Center (KDC)	Required for access to Kerberos authentication system.
111	TCP/UDP	RPC port mapper service on Data Domain system	Only required when backups are stored on a Data Domain system. Access to RPC and NFS port mapper functionality on a Data Domain system.
123	TCP/UDP	NTP time servers	Provides synchronization of system time from network time protocol servers.
163	UDP	SNMP service on Data Domain system	Only required when backups are stored on a Data Domain system.
389	TCP/UDP	LDAP	Provides access to directory services.
443	• vSphere API • TCP	• VMware vCenter • Avamar Key Manager	
464	TCP	Key Distribution Center (KDC)	Required for access to the Kerberos Change/Set password.

Table 28 Required outbound ports for the utility node (continued)

Port	Protocol	Destination computer	Additional information
902	TCP	VMware ESX server proxy service	
2049	TCP/UDP	NFS daemon on Data Domain system	Only required when backups are stored on a Data Domain system.
2052	TCP/UDP	NFS mountd process on Data Domain system	Only required when backups are stored on a Data Domain system. Outbound communication must be open for both TCP and UDP protocols.
5671	TCP	• localhost • Other Avamar utility nodes • Avamar Extended Retention computers • Backup and Recovery Manager computers	RabbitMQ messaging. RabbitMQ is a message broker used to enhance asynchronous interprocess communication.
5696	TCP	KMIP-compliant key management server	Recommended port for AKM external key management operation.
7443	TCP	Media Access node that hosts Avamar Extended Retention	Only required when using the Avamar Extended Retention feature.
7444	TCP	VMware vCenter	For utility node configurations that also run the VMware Backup Appliance this port is opened by an if/then clause in the firewall rules. Otherwise, this port is not required. Used to test vCenter credentials.
7543	HTTPS/SSL	Update Manager	Web browser clients use this port to create HTTPS connections to Avamar Installation Manager. Limit access to trusted administrator computers.
7544	TCP	Update Manager	Jetty socket clients use this port to send a shutdown signal to its Jetty web server. Limit access to trusted administrator computers.
7543	HTTPS	Update Manager	Used for connections from the Avamar Downloader Service computer, and for

Table 28 Required outbound ports for the utility node (continued)

Port	Protocol	Destination computer	Additional information
			access Update Manager from other web browser clients.
8080	TCP	NetWorker server	For utility node configurations that also run the VMware Backup Appliance this port is opened by an if/then clause in the firewall rules. Otherwise, this port is not required. Used to register with a NetWorker server.
8580	TCP	Computer running Avamar Downloader Service	Used to make requests for package downloads from the Avamar Downloader Service computer.
9443	TCP	Managed Avamar servers	Avamar Management Console web services use this outbound port for RMI communication via a dynamically assigned port on managed Avamar servers.
19000	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
19500	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
20000	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
20500	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
25000	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
25500	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
26000	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
26500	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
27000	TCP	Avamar server nodes	Avamar subsystem communication.
28001	TCP	Replication source system and replication target system	Replication requires bi-directional access between the replication source Avamar server and the replication destination Avamar server to

Table 28 Required outbound ports for the utility node (continued)

Port	Protocol	Destination computer	Additional information
			permit authentication key exchange.
28009	TCP	VMware proxy	MCS access to proxy logs.
28011	TCP	Avamar Extended Retention Media Access Node	The firewall rules open this port when you install support for Avamar Extended Retention.
29000	TCP	Avamar server nodes	Avamar subsystem communication over SSL.
30001	TCP	Avamar server nodes	MCS communication over SSL.
30002	TCP	Avamar client computers	Communication with avagent.
30003	TCP	Avamar server nodes	MCS communication over SSL.
30002 - 30009	TCP	VMware proxy	Avagent paging port. Secured communication with VMware proxy.
30102	TCP	VMware proxy	Avagent paging port. Secure communication with VMware proxy.
61617	TCP	Media Access node that hosts Avamar Extended Retention	Only required when using the Avamar Extended Retention feature.
61619	TCP	Computer running Backup and Recovery Manager.	Required to permit communication with Backup and Recovery Manager.

Storage node ports

Avamar storage nodes have specific port requirements both for inbound and outbound ports.

The tables in this section list the following port requirements for storage nodes:

- Required inbound ports

  Ports on each storage node that must be open to network transmissions from specified source computers.
- Required outbound ports

  Ports on another computer that each storage node must be allowed to access.

Storage node required inbound ports

The following table describes the inbound ports that must be open on each Avamar storage node. For every port listed in this table, the Avamar storage node is the destination and the source is listed in the Source computer column.

Table 29 Required inbound ports on each storage node

Port	Protocol	Service name	Source	Additional information
22	TCP	SSH	• Administrator computers • Other Avamar server nodes	Secure shell access.
123	TCP/UDP	NTP	• NTP time servers • Avamar utility node	Permits clock synchronization from network time protocol servers (exochronous) and from the utility node (isochronous).
19000	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
19500	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
20000	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
20500	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
25000	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
25500	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
26000	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
26500	TCP/UDP	Avamar subsystem	Avamar server nodes	Avamar subsystem communication.
27000	TCP	Avamar server	• Avamar client computers • Avamar nodes acting as a replicator source	Avamar subsystem communication. This port is blocked by default for new installations. Open this port to allow unencrypted backups.
29000	TCP	Avamar server SSL	• Avamar client computers • Avamar server nodes	Avamar subsystem communication.
30001	TCP	MCS SSL	Avamar server nodes	MCS communication.
30003	TCP	MCS SSL	Avamar server nodes	MCS communication.

Storage node required outbound ports

The following table describes the outbound ports that must be accessible to network packets that are sent from each Avamar storage node. For each row, the storage node is the source computer that must have outgoing access to the listed port on the listed destination computer.

Table 30 Required outbound ports for each storage node

Port	Protocol	Destination	Additional information
53	TCP/UDP	DNS	Required for name resolution and DNS zone transfers. TCP connection to DNS is required by VMware proxy nodes.
123	TCP/UDP	NTP time servers and the Avamar utility node	Permits clock synchronization from network time protocol servers (exochronous) and from the utility node (isochronous).
703	TCP	Utility node	Permits access to the AKM service on the utility node.
19000	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
19500	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
20000	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
20500	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
25000	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
25500	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
26000	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
26500	TCP/UDP	Avamar server nodes	Avamar subsystem communication.
27000	TCP	Avamar server nodes	Avamar subsystem communication.
29000	TCP	Avamar server nodes	Avamar subsystem communication over SSL.
30001	TCP	Avamar server nodes	MCS communication over SSL.
30003	TCP	Avamar server nodes	MCS communication over SSL.

Avamar client ports

Avamar clients have specific port requirements both for inbound and outbound ports.

The tables in this section list the following port requirements for Avamar clients:

- Required inbound ports

  Ports on an Avamar client that must be open to network transmissions from specified source computers.
- Required outbound ports

  Ports on another computer that an Avamar client must be allowed to access.

Avamar client required inbound ports

The following table describes the inbound ports that must be open on an Avamar client. For every port listed in this table, an Avamar client is the destination and the source is listed in the Source computer column.

Table 31 Required inbound ports on an Avamar client

Port	Protocol	Service name	Source	Additional information
28002	TCP	avagent	Avamar server	Provides management functionality from Avamar Administrator.
30001	TCP	MCS	Avamar utility node	2-way secure socket
30002	TCP	avagent	Avamar utility node	

Avamar client required outbound ports

The following table describes the outbound ports that must be accessible to network packets that are sent from an Avamar client. For each row, the Avamar client is the source computer that must have outgoing access to the listed port on the listed destination computer.

Note

Avamar 7.5.1 removes support for HTTP access to TCP port 80. Use the HTTPS port 443 to access these services instead.

Table 32 Required outbound ports for an Avamar client

Port	Protocol	Destination	Additional information
53	TCP/UDP	DNS	Required for name resolution and DNS zone transfers.
111	TCP/UDP	Data Domain system	Required for backing up clients to Data Domain.
123	UDP	NTP time servers	Provides clock synchronization from network time protocol servers.

Table 32 Required outbound ports for an Avamar client (continued)

Port	Protocol	Destination	Additional information
443	TCP	Avamar server HTTPS service	Required to use the web browser UI of Avamar Desktop/Laptop and the web browser UI of Avamar Web Restore.
2049	TCP/UDP	Data Domain system	Required for backing up clients to Data Domain.
2052	TCP/UDP	Data Domain system	Required for backing up clients to Data Domain.
3008	TCP	Archive tier service on Data Domain system	Only required when backups are stored on a Data Domain system and archive tier is used.
8105	TCP	Avamar server	Used by Avamar Desktop/ Laptop.
8109	TCP	Avamar server	Used by Avamar Desktop/ Laptop.
8181	TCP	Avamar server HTTP redirect port	Required to use the web browser UI of Avamar Desktop/Laptop and the web browser UI of Avamar Web Restore.
8444	TCP	Avamar server HTTPS redirect port	Required to use the web browser UI of Avamar Desktop/Laptop and the web browser UI of Avamar Web Restore.
27000	TCP	Avamar server	Avamar subsystem communication.
28001	TCP	Avamar server	CLI commands from client computers.
29000	TCP	Avamar server	Avamar subsystem communication.
30001	TCP	Avamar utility node	MCS
30003	TCP	Avamar utility node	MCS

Avamar Downloader Service host ports

An Avamar Downloader service host has specific port requirements both for inbound and outbound ports.

The tables in this section list the following port requirements for an Avamar Downloader service host:

- Required inbound port

Port on an Avamar Downloader service host that must be open to network transmissions from specified source computers.

- Required outbound ports

  Ports on another computer that an Avamar Downloader service host must be allowed to access.

Avamar Downloader Service host required inbound port

The following table describes the inbound port that must be open on an Avamar Downloader Service host. For the port listed in this table, an Avamar Downloader Service host is the destination and the source is listed in the Source computer column.

Table 33 Required inbound port on an Avamar Downloader Service host

Port	Protocol	Service name	Source	Additional information
8580	TCP	Avamar Downloader Service	Avamar server	Avamar server connects to this port to access the Avamar Downloader Service.

Avamar Downloader Service host required outbound ports

The following table describes the outbound ports that must be accessible to network packets that are sent from an Avamar Downloader Service host. For each row, an Avamar Downloader Service host is the source computer that must have outgoing access to the listed port on the listed destination computer.

Note

Avamar 7.5.1 removes support for HTTP access to TCP port 80. Use the HTTPS port 443 to access these services instead.

Table 34 Required outbound ports for an Avamar Downloader Service host

Port	Protocol	Destination	Additional information
21	TCP	Avamar FTP server	Provides the Avamar Downloader Service with FTP access to updates, security rollup packages, hotfixes, and patches.
53	TCP/UDP	DNS	Required for name resolution and DNS zone transfers.
123	UDP	NTP time servers	Provides clock synchronization from network time protocol servers.
443	TCP	Avamar server HTTPS service	Provides HTTPS access to the AvInstaller service.

Ports when using a Data Domain system

An Avamar system that is deployed with a Data Domain system as a storage target has specific port requirements.

Also to the port requirements described in this section, implement the additional Data Domain system port requirements that are described in the Knowledgebase article: "Port Requirements for Allowing Access to Data Domain System Through a Firewall." This article is available from: https://support.EMC.com.

Required ports when using a Data Domain system

The following table describes the general port requirements when an Avamar system is deployed with a Data Domain system as a storage target

Table 35 Required ports when using a Data Domain system

Port	Protocol	Source	Destination	Service	Additional information
7	TCP	Utility node	Data Domain system	ECHO	Required to register a Data Domain system for storing Avamar client backups.
22	TCP	Utility node	Data Domain system	SSH	Secure shell communication with the Data Domain system.
111	TCP/UDP	Utility node	Data Domain system	RPC port mapper service	Access to RPC and NFS port mapper functionality on a Data Domain system.
161	UDP	Data Domain system	Utility node	SNMP	This is the getter/setter port for SNMP objects from a Data Domain system.
163	UDP	Utility node	Data Domain system	SNMP	none
2049	TCP/UDP	Utility node	Data Domain system	NFS daemon	none
2052	TCP/UDP	Utility node	Data Domain system	NFS mountd process	Outbound communication must be open for both protocols: TCP and UDP.
3008	TCP	Avamar client	Data Domain system	Archive tier service	Only required when archive tier is used.

NDMP accelerator node ports

Avamar NDMP accelerator nodes have specific port requirements for outbound ports.

The table in this section lists the following port requirements for NDMP accelerator nodes:

- Required inbound ports

  Ports on an accelerator node that must be open to network transmissions from specified source computers.
- Required outbound ports

Ports on another computer that each accelerator node must be allowed to access.

NDMP accelerator node required inbound ports

The following table describes the inbound ports that must be accessible to network packets that are sent to each Avamar accelerator node. For each row, the accelerator node is the destination and the source is listed in the Source computer column.

Table 36 Required inbound ports for each accelerator node

Port	Protocol	Source	Additional information
7543	HTTP/SSL	Web browser clients	Web browser clients use this port to create HTTPS connections to Avamar Installation Manager. Limit access to trusted administrator computers.
28002-28202	TCP	Avamar client/agent	
30002-30202	TCP	Avamar client/agent	

NDMP accelerator node required outbound ports

The following table describes the outbound ports that must be accessible to network packets that are sent from each Avamar accelerator node. For each row, the accelerator node is the source computer that must have outgoing access to the listed port on the listed destination computer.

Table 37 Required outbound ports for each accelerator node

Port	Protocol	Destination	Additional information
7	TCP	Data Domain system	
25	TCP	Customer Support	Required for SMTP connections between ConnectEMC and Customer Support.
111	TCP/UDP	Data Domain system	
443	TCP	Customer Support	LDLS communication with Customer Support.
2049	TCP/UDP	Data Domain system	
2052	TCP/UDP	Data Domain system	
3008	TCP	Data Domain system	
8080	TCP	Isilon	Required for Isilon platform API access.
8580	TCP	Computer running Avamar Downloader Service	Used to make requests for package downloads from the Avamar Downloader Service computer.

Table 37 Required outbound ports for each accelerator node (continued)

Port	Protocol	Destination	Additional information
9443	TCP	RMI - Avamar Management Console web services	
10000	TCP	NAS filer	Required for NDMP control messages.
28001	TCP	Avamar Administrator management console	
30001	TCP	Avamar Administrator management console	
30003	TCP	Avamar server nodes	MCS communication over SSL.

Mounting a NAS share

Avamar 18.1 and later releases include additional operating system and firewall hardening packages for NDMP accelerator nodes. To mount a NAS share on an NDMP accelerator node, add the NAS IP address to the firewall table. Remove the NAS from the firewall table when you no longer need to mount the NAS share.

Procedure

1. Open a command shell:
   a. Log in to the NDMP accelerator node as admin.
   b. Switch user to root by typing `su -`.
2. Add the NAS to the firewall table by typing the following commands:
   ```
   iptables -I OUTPUT -p tcp -d IPv4-addr -j ACCEPT
   iptables -I OUTPUT -p udp -d IPv4-addr -j ACCEPT
   ```
   where *IPv4-addr* is a specific IPv4 address for the NAS.
3. Remove the NAS from the firewall table by typing the following commands:
   ```
   iptables -D OUTPUT -p tcp -d IPv4-addr -j ACCEPT
   iptables -D OUTPUT -p udp -d IPv4-addr -j ACCEPT
   ```
   where *IPv4-addr* is a specific IPv4 address for the NAS.

Remote management interface ports

The remote management interface on Avamar utility, storage, and accelerator nodes has specific port requirements both for inbound and outbound ports.

The remote management interface depends on the type of ADS platform:

- The Gen4T platform uses the Baseboard Management Controller (BMC) Web Console
- The Gen4S platform uses the Remote Management Module 4 (RMM4)

Gen4-based Avamar nodes have reached end-of-life. Past releases of this guide provide further information about Gen4-based Avamar nodes.

The tables in this section list the inbound port requirements for the remote management interface on all the nodes. The ports that must be opened to network

transmissions from specified source computers are based on your network environment.

NOTICE

It is recommended to isolate the management network.

Connection to the remote management interfaces depends on the type of ADS platform and is made through the relevant BMC Web Console or RMM4 IP address. Do not use the backup interface for this purpose.

Note that the remote management console interface is only compatible with Java versions 1.7.x and 1.8 versions earlier than 1.8u161. If Java version 1.8u161 and later is installed on the machine used to connect to the remote management console, the KVM console fails to launch using either ping or a web browser.

NOTICE

The dedicated port and shared port cannot be the same IP address. If the IP address is the same, set the IP address of the shared port to 0.0.0.0. Also, connection of the dedicated port through a switch may require gratuitous ARP to be turned on.

Remote management interface inbound ports

The following table describes the inbound ports that should be open on the remote management interface of all Gen4T-based Avamar nodes. The actual ports that should be open depend on your network environment. For every port listed in this table, the remote management interface on the node is the destination and the source is listed in the Source computer column.

Table 38 Inbound ports for the remote management interface on all Gen4T-based nodes

Port	Protocol	Service name	Source computer	Additional information
80	TCP	HTTP	Administrator computers	HTTP access
443	TCP	HTTP protocol over TLS/SSL	Administrator computers	HTTPS access
2068	TCP	Virtual console and media redirection	Administrator computers	Virtual console keyboard/mouse, virtual media server, virtual media secure service, and virtual console video

The following table describes the inbound ports that should be open on the remote management interface of all Gen4S-based Avamar nodes. The actual ports that should be open depend on your network environment. For every port listed in this table, the remote management interface on the node is the destination and the source is listed in the Source computer column.

Table 39 Inbound ports for the remote management interface on all Gen4S-based nodes

Port	Protocol	Service name	Source computer	Additional information
80	TCP	HTTP	Administrator computers	HTTP access
443	TCP	HTTPS	Administrator computers	HTTPS access
5120	TCP	CDROM media redirection	Administrator computers	
5123	TCP	Floppy/USB media redirection	Administrator computers	
7578	TCP	Keyboard, video, mouse	Administrator computers	

Gen4-based Avamar nodes have reached end-of-life. Past releases of this guide provide further information about Gen4-based Avamar nodes.

Note

Ensure that the local network environment allows for the creation of these connections.

If using a private intranet, configure the setup of firewall and Network Address Translation (NAT) accordingly.

Ensure that you open the ports bi-directionally at the firewall level.

Remote management interface outbound ports

The following table describes the outbound ports that should be accessible to network packets that are sent from the remote management interface on all Avamar nodes. The actual ports that should be open depend on your network environment. By default, none of these outbound ports are configured to be in use. You must modify the configuration to use those protocols. For each row, the node is the source computer that must have outgoing access to the listed port on the listed destination computer.

Table 40 Outbound ports for the remote management interface on all Avamar nodes

Port	Protocol	Destination computer	Additional information
25	TCP	Administrator computers	Required to make an SMTP connection with Administrator computers.
53	TCP/UDP	DNS server	Required for DNS queries.
68	UDP	Administrator computers	Required for DHCP-assigned IP address.
69	UDP	Administrator computers	Required for trivial file transfers (TFTP).
162	UDP	Administrator computers	Required to send SNMP traps.

Table 40 Outbound ports for the remote management interface on all Avamar nodes (continued)

Port	Protocol	Destination computer	Additional information
636	TCP/UDP	LDAPS server	Required to make Secure LDAP queries.
3269	TCP /UDP	LDAPS server	Required for LDAPS global catalog (CG).

Note

Ensure that the local network environment allows for the creation of these connections.

If using a private intranet, configure the setup of firewall and Network Address Translation (NAT) accordingly.

Ensure that you open the ports bi-directionally at the firewall level.

Avamar VMware Combined Proxy ports

This section outlines the requirements for the Avamar VMware Combined Proxy.

Avamar VMware Combined Proxy inbound ports

The following table describes the inbound ports requirements for the Avamar VMware Combined Proxy.

Table 41 Required inbound ports for the Avamar VMware Combined Proxy

Port	Protocol	Source	Additional information
22	TCP / SSH TCP / SSH	Avamar Administrator	Diagnostic support is optional, but recommended.
902	TCP / VMware ESX server proxy service	Avamar Server	
5489	TCP / CIM service	Avamar Avamar Deployment	Used to register the proxy.
28009	TCP / Access proxy logs	Avamar MCS	
28102 - 28109	TCP / avagent paging port	Avamar MCS	Avamar 7.0 and Avamar 7.1
30102 - 30109	TCP / avagent paging port	Avamar MCS	Avamar 7.2
30002 - 30009	TCP / avagent paging port	Avamar Server	Secured communication with the Avamar Server Utility Node.

Avamar VMware Combined Proxy outbound ports

The following table describes the outbound ports requirements for the Avamar VMware Combined Proxy.

Table 42 Required outbound ports for the Avamar VMware Combined Proxy

Port	Protocol	Destination	Additional information
53	UDP + TCP / DNS	DNS server	UDP + TCP
111	TCP / UDP	Data Domain system	Access to RPC and NFS port mapper functionality on a Data Domain system.
443	TCP / vSphere API	ESXi hosts	
902	TCP / VDDK	ESX hosts	
2049	TCP/UDP	Data Domain system	
2052	TCP/UDP	Data Domain system	Outbound communication must be open for both protocols: TCP and UDP.
27000	TCP / GSAN communication	Avamar server	Non-secured communication
28001	TCP / Avamar MCS/avagent	Avamar server	
28002 - 28010	TCP / Avamar MCS/avagent	Avamar server	
29000	TCP / GSAN communication	Avamar server	Secured communication
30001	TCP / avagent to MCS communication	Avamar MCS	Avamar 7.2
30002 - 30010	TCP / Avamar MCS/avagent	Avamar server	
30102 - 30109	TCP / Avagent paging port	Avamar server	Secured communication with Avamar Server Utility Node

Avamar vSphere Combined Proxy ports

The following table describes the ports that are required for the Avamar vSphere Combined Proxy.

Table 43 Required ports for the Avamar vSphere Combined Proxy

Port	Protocol	Source	Destination
443	TCP / vSphere API	Avamar Deployment Manager	ESXi hosts
443	TCP / vSphere API	Avamar MCS	vCenter
7444	TCP / Test vCenter credentials	Avamar MCS	vCenter

Ports when using Avamar Virtual Edition

Avamar Virtual Edition (AVE) has specific Azure network security group port requirements both for inbound and outbound ports.

Inbound ports for the Azure network security group

The following tables describe the rules that should be added to an Azure network security group.

Note

If you want to restrict the source of traffic, set the source with IPv4 or IPv6 CIDR block, or a single IPv4 or IPv6 address.

Note

Avamar no longer supports HTTP access to TCP port 80. Use the HTTPS ports 443 to access these services instead.

For all table entries:

- The **Source** and **Destination** fields are `Any`.
- The **Source port range** field is `*`
- The **Action** is `Allow`.
- Assign a unique priority value to each rule, starting at 100.
- Type a unique description for each rule. The value must be unique for both inbound and outbound rules.

Table 44 Inbound ports for the Azure network security group

Type	Protocol	Destination port range
SSH	TCP	22
Custom TCP Rule	TCP	161
Custom UDP Rule	UDP	161
Custom TCP Rule	TCP	163
Custom UDP Rule	UDP	163
HTTPS	TCP	443
Custom TCP Rule	TCP	700
Custom TCP Rule	TCP	7543
Custom TCP Rule	TCP	7778 - 7781
Custom TCP Rule	TCP	8543
Custom TCP Rule	TCP	9090
Custom TCP Rule	TCP	9443
Custom TCP Rule	TCP	27000
Custom TCP Rule	TCP	28001 - 28002

Table 44 Inbound ports for the Azure network security group (continued)

Type	Protocol	Destination port range
Custom TCP Rule	TCP	28810 - 28819
Custom TCP Rule	TCP	29000
Custom TCP Rule	TCP	30001 - 30010

Outbound ports for the Azure network security group

Note

If you want to restrict the source of traffic, set the source with IPv4 or IPv6 CIDR block, or a single IPv4 or IPv6 address.

By default, Azure has a rule AllowInternetOutBound with priority `65001` to allow all outbound internet traffic. Override this rule by adding a rule with a priority (that is, an integer number) that is greater than all customized rules' priority, and less than 65000: **`source: *, destination: *, protocol: *, action: Deny`**. Azure documentation contains information about creating a firewall rule.

For all table entries:

- The **Source** and **Destination** fields are `Any`.
- The **Source port range** field is `*`
- The **Action** is `Allow`.
- Assign a unique priority value to each rule, starting at 100.
- Type a unique description for each rule. The value must be unique for both inbound and outbound rules.

Table 45 Outbound ports for the Azure network security group

Type	Protocol	Destination port range
Custom TCP Rule	TCP	7
SSH	TCP	22
SMTP	TCP	25
DNS (UDP)	UDP	53
Custom TCP Rule	TCP	111
Custom UDP Rule	UDP	111
Custom TCP Rule	TCP	161
Custom UDP Rule	UDP	161
Custom TCP Rule	TCP	163
Custom UDP Rule	UDP	163
HTTPS	TCP	443
Custom TCP Rule	TCP	700

Table 45 Outbound ports for the Azure network security group (continued)

Type	Protocol	Destination port range
Custom TCP Rule	TCP	2049
Custom UDP Rule	UDP	2049
Custom TCP Rule	TCP	2052
Custom UDP Rule	UDP	2052
Custom TCP Rule	TCP	3008
Custom TCP Rule	TCP	8443
Custom TCP Rule	TCP	8888
Custom TCP Rule	TCP	9090
Custom TCP Rule	TCP	9443
Custom TCP Rule	TCP	27000
Custom TCP Rule	TCP	28001-28010
Custom TCP Rule	TCP	29000
Custom TCP Rule	TCP	30001-30010

Communication security

The following topics provide information about securing communication between Avamar and remote systems:

External Web interfaces

Interfaces for all components (for example, Avamar Installation Manager, Avamar Administrator, MCS) are secure.

All Avamar external web interfaces are only HTTPS accessible. Automatic redirection from HTTP to HTTPS is disabled.

Consider the following limitation:

- Recent releases of Avamar enable only TLS 1.2, might impact compatibility with older Avamar clients that do not support TLS 1.2.
- Avamar web interfaces are unavailable to web browsers that do not support TLS 1.2.
- Installations of the Avamar Downloader Service on older operating systems, such as Windows 7, that do not support TLS 1.2 might experience issues with connecting to recent releases of Avamar.

To enable TLS1.2 for Windows 7, Windows 2008 and Windows 2012, refer to the documentation on the Microsoft Support.

Network access control

Control of networking in the Avamar environment starts with awareness of several parts of the network.

Subnet and gateway assignments
Avamar client machines must be able to connect to every node in the Avamar environment directly, and each node in the environment must be able to connect to the client machines.

Assign a default gateway to the router in the Avamar environment.

DNS requirements
The Avamar environment requires a Domain Name System (DNS) server. Within the DNS domain, assign forward mapping to the Avamar utility node, or to the single-node Avamar server. Optionally, also assign reverse mapping to the utility node or single-node server.

For example, use the following forward mapping entry in a BIND environment:

```
avamar-1        A        10.0.5.5
```

Continuing the example, use the following optional reverse mapping for a zone serving the 5.0.10.in-addr.arpa subnet:

```
5        PTR        avamar-1.example.com.
```

Remote access control
Protect all nodes and the switch in the Avamar server against unauthorized access. Use a Virtual Private Network (VPN) system when accessing the Avamar system from a remote location.

SNMP
Avamar provides support for system monitoring and event notification through the Simple Network Management Protocol (SNMP).

Firewall settings

The Avamar firewall daemon runs on every Avamar node. The Avamar firewall daemon controls access to all inbound ports on each node and controls transmissions sent from each node.

The Avamar firewall daemon is called `avfirewall`. When a change is made to a firewall rule, restart `avfirewall` to load the new configuration.

The Avamar firewall daemon uses the rules in `/etc/firewall.base`. Use the symlink: `/ect/firewall.default` to access the rules file.

The following topics describe how to configure and verify the operation of the Avamar firewall:

Controlling the firewall daemon

Stop, start, restart, and check the status of the Avamar firewall daemon.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Stop the firewall daemon by typing:

   ```
   service avfirewall stop
   ```

3. Start the firewall daemon by typing:

   ```
   service avfirewall start
   ```

4. Restart the firewall daemon by typing:

   ```
   service avfirewall restart
   ```

5. Check the status of the firewall daemon by typing:

   ```
   service avfirewall status
   ```

Editing the Firewall in Avamar

Edit the status of the Avamar firewall.

Firewall edit functionality allows the user to open and close nondependent ports for customized data transfer and to modify associated rules. Rules and ports can be initiated, edited, and terminated through manual configuration of a designated text file, executing those changes, and then restarting the firewall on the Avamar server. Editing the firewall is essentially understanding the content of the config file, editing that content, and then executing those changes.

Procedure

1. Log in to the utility node (or single node server) as root.

   Provide the appropriate password.

2. Change the working directory to the following: `/usr/local/avamar/lib/admin/security`.
3. Open `avfwb_custom_config.txt` in a plain text editor.

   See section below for config file example and how to edit the file.

4. Save and close the file.
5. Run the following command:`manage-custom-rules.sh –execute-rules`.

   This command copies the new firewall rules to all nodes in the system and restarts the firewall.

6. Exit the command session.

The firewall customization lines that you add to the **avfwb_custom_config.txt** file must be structured in a pipe-delimited fashion such as the following:

Source IP | Source Port | Destination IP | Destination Port | Protocol | ICMP-type | Target | Chain | Node type

where:

Table 46 Firewall customization

Section	Description
Source IP	Source specification - address can be a network IP address (with /mask) or a plain IP address.
Source Port	Port of origin for traffic.
Destination IP	IP address of destination machine.
Destination Port	Destination port or port range specification.
Protocol	TCP, UDP, or ICMP.
ICMP-type	If ICMP is entered for Protocol, enter the type.
Target	ACCEPT, REJECT, DROP, or LOGDROP.
Chain	INPUT, OUTPUT, or LOGDROP
Node type	ALL (all nodes), DATA (data nodes only), or UTILITY (only applies to the utility node).

If a field does not apply, leave the field blank.

Miscellaneous information

To delete all firewall rules, delete the rules in **avfwb_custom_config.txt** and run **manage-custom-rules.sh --execute-rules** again.

For diagnostic purposes, the log file is located in /var/log/custom-firewall.

To view the current state of the firewall iptable on the utility node or a single-node server, run the following command: **iptables -L** (for ipv4) or **ip6tables -L** (for ipv6).

To view the current state of the firewall iptable on all of the nodes of a multi-node server, run the following command: **mapall --all+ --user=root iptables -L**.

Configuring the Avamar firewall

Use the following instructions whenever you need to open or close particular ports in the Avamar firewall, or restrict access to a particular IP address.

Users should be familiar with the operation of `iptables`, including order of precedence, before creating custom firewall rules.

Opening a firewall port

If the Avamar server is a dual-stack configuration, repeat this task to create rules for both addressing systems.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Change directory by typing the following command:

   ```
   cd /usr/local/avamar/lib/admin/security
   ```

3. Run the firewall rules script by typing the following command:

   ```
   ./edit-firewall-rules.sh
   ```

   The following output appears:

   ```
   Choose an Action
   ----------------
   1) Add a custom rule
   2) Remove a custom rule
   3) List Current Custom Rules
   4) Exit
   5) Save Changes
   Enter desired action:
   ```

4. Type `1` to add a custom rule and press **Enter**.

   The following output appears:

   ```
   Firewall Rule Types
   -------------------
   1) IPv4 Rule
   2) IPv6 Rule
   Enter Firewall Rule Type:
   ```

5. Type the number that corresponds to the addressing system in use and press **Enter**.

   The following output appears:

   ```
   Firewall Chains
   ---------------
   1) OUTPUT
   2) INPUT
   3) LOGDROP
   4) FORWARD
   Select Chain:
   ```

6. Type `1` to add an output rule or `2` to add an input rule and press **Enter**.

   The following output appears:

   ```
   Protocol
   --------
   1) TCP
   2) UDP
   ```

```
3) ICMP
Enter Protocol:
```

7. Type the number that corresponds to the required protocol and press **Enter**.

   The following output appears:

   ```
   Enter source IP (leave blank for none):
   ```

8. For outbound connections, perform the following substeps:

   a. Type the IP address of this Avamar server and press **Enter**.

      The following output appears:

      ```
      Enter source port (leave blank for none):
      ```

   b. Type the number of the port to open and press **Enter**.

      The following output appears:

      ```
      Enter Destination IP Address (leave blank for none):
      ```

   c. Leave this field blank and press **Enter**.

      If you want to restrict connections to a particular IP address, type the IP address instead and press **Enter**.

      The following output appears:

      ```
      Enter Destination Port (leave blank for none):
      ```

   d. Leave this field blank and press **Enter**.

      The following output appears:

      ```
      Targets
      -------
      1) ACCEPT
      2) REJECT
      3) DROP
      4) LOGDROP
      Select Target:
      ```

9. For inbound connections, perform the following substeps:

   a. Leave this field blank and press **Enter**.

      If you want to restrict connections to a particular IP address, type the IP address instead and press **Enter**.

      The following output appears:

      ```
      Enter source port (leave blank for none):
      ```

   b. Leave this field blank and press **Enter**.

      The following output appears:

      ```
      Enter Destination IP Address (leave blank for none):
      ```

   c. Type the IP address of this Avamar server and press **Enter**.

      The following output appears:

      ```
      Enter Destination Port (leave blank for none):
      ```

   d. Type the number of the port to open and press **Enter**.

      The following output appears:

      ```
      Targets
      -------
      1) ACCEPT
      2) REJECT
      3) DROP
      ```

```
4) LOGDROP
Select Target:
```

10. Type `1` to allow packets for the specified port and press **Enter**.

    The following output appears:

    ```
    Node Types
    ----------
    1) ALL
    2) DATA
    3) UTILITY
    4) ACCELERATOR
    Select node type to apply rule to:
    ```

11. Type the number that corresponds to the node type and press **Enter**.

    Unless otherwise indicated by the tables in this appendix, most ports only require the utility node.

    Output similar to the following appears:

    ```
    Add rule |7080|||tcp||ACCEPT|OUTPUT|UTILITY to custom rules
    file? (Y/N):
    ```

12. Type `Y` to save the new rule and press **Enter**.

    The script writes the new rule to `avfwb_custom_config.txt`.

    Output similar to the following appears:

    ```
    Adding |7080|||tcp||ACCEPT|OUTPUT|UTILITY to pending actions...
    Add another firewall rule? (Y/N):
    ```

13. If you require more rules, type `Y` and press **Enter**. Otherwise, type `N` and press **Enter**.

    The following output appears:

    ```
    Return to main menu? (Y/N):
    ```

14. Type `N` and press **Enter**.

    The following output appears:

    ```
    Save and execute rules now? (Y/N):
    ```

15. Type `Y` to save the new firewall rules and press **Enter**.

    The script saves the new rules to the system firewall tables and automatically restarts the Avamar firewall, then exits.

    Output similar to the following appears:

    ```
    Rules have been saved to /usr/local/avamar/lib/admin/security/
    avfwb_custom_config.txt
    |7080|||tcp||ACCEPT|OUTPUT|UTILITY will be applied
    Applying /usr/sbin/iptables -A OUTPUT -p tcp --sport 7080 -j
    ACCEPT...
    ```

Closing a firewall port

If the Avamar server is a dual-stack configuration, repeat this task to create rules for both addressing systems.

Procedure

1. Open a command shell:

   a. Log in to the server as admin.

   b. Switch user to root by typing the following command:

      ```
      su -
      ```

c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Change directory by typing the following command:

```
cd /usr/local/avamar/lib/admin/security
```

3. Run the firewall rules script by typing the following command:

```
./edit-firewall-rules.sh
```

The following output appears:

```
Choose an Action
----------------
1) Add a custom rule
2) Remove a custom rule
3) List Current Custom Rules
4) Exit
5) Save Changes
Enter desired action:
```

4. Type `1` to add a custom rule and press **Enter**.

The following output appears:

```
Firewall Rule Types
-------------------
1) IPv4 Rule
2) IPv6 Rule
Enter Firewall Rule Type:
```

5. Type the number that corresponds to the addressing system in use and press **Enter**.

The following output appears:

```
Firewall Chains
---------------
1) OUTPUT
2) INPUT
3) LOGDROP
4) FORWARD
Select Chain:
```

6. Type `1` to add an output rule or `2` to add an input rule and press **Enter**.

The following output appears:

```
Protocol
--------
1) TCP
2) UDP
3) ICMP
Enter Protocol:
```

7. Type the number that corresponds to the required protocol and press **Enter**.

The following output appears:

```
Enter source IP (leave blank for none):
```

8. For outbound connections, perform the following substeps:

a. Leave this field blank and press **Enter**.

The following output appears:

```
Enter source port (leave blank for none):
```

b. Type the number of the port to close and press **Enter**.

The following output appears:

```
Enter Destination IP Address (leave blank for none):
```

c. Leave this field blank and press **Enter**.

If you want to block connections to a particular IP address, type the IP address instead and press **Enter**.

The following output appears:

```
Enter Destination Port (leave blank for none):
```

d. Leave this field blank and press **Enter**.

The following output appears:

```
Targets
-------
1) ACCEPT
2) REJECT
3) DROP
4) LOGDROP
Select Target:
```

9. For inbound connections, perform the following substeps:

a. Leave this field blank and press **Enter**.

If you want to block connections from a particular IP address, type the IP address instead and press **Enter**.

The following output appears:

```
Enter source port (leave blank for none):
```

b. Leave this field blank and press **Enter**.

The following output appears:

```
Enter Destination IP Address (leave blank for none):
```

c. Type the IP address of this Avamar server and press **Enter**.

The following output appears:

```
Enter Destination Port (leave blank for none):
```

d. Type the number of the port to close and press **Enter**.

The following output appears:

```
Targets
-------
1) ACCEPT
2) REJECT
3) DROP
4) LOGDROP
Select Target:
```

10. Type `2` to reject packets for the specified port, or `3` to drop packets for the specified port, and press **Enter**.

The following output appears:

```
Node Types
----------
1) ALL
2) DATA
3) UTILITY
4) ACCELERATOR
Select node type to apply rule to:
```

11. Type the number that corresponds to the node type and press **Enter**.

    Unless otherwise indicated by the tables in this appendix, most ports only require the utility node.

    Output similar to the following appears:

    ```
    Add rule ||10.7.100.1|7080|tcp||REJECT|INPUT|UTILITY to custom
    rules file? (Y/N):
    ```

12. Type **Y** to save the new rule and press **Enter**.

    The script writes the new rule to `avfwb_custom_config.txt`.

    Output similar to the following appears:

    ```
    Adding ||10.7.100.1|7080|tcp||REJECT|INPUT|UTILITY to pending
    actions...
    Add another firewall rule? (Y/N):
    ```

13. If you require more rules, type **Y** and press **Enter**. Otherwise, type **N** and press **Enter**.

    The following output appears:

    ```
    Return to main menu? (Y/N):
    ```

14. Type **N** and press **Enter**.

    The following output appears:

    ```
    Save and execute rules now? (Y/N):
    ```

15. Type **Y** to save the new firewall rules and press **Enter**.

    The script saves the new rules to the system firewall tables and automatically restarts the Avamar firewall, then exits.

    Output similar to the following appears:

    ```
    Rules have been saved to /usr/local/avamar/lib/admin/security/
    avfwb_custom_config.txt
    ||10.7.100.1|7080|tcp||REJECT|INPUT|UTILITY will be applied
    Applying rule /usr/sbin/iptables -A INPUT -p tcp -d 10.7.100.1
    --dport 7080 -j REJECT
    ```

Removing a custom firewall rule

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Change directory by typing the following command:

   ```
   cd /usr/local/avamar/lib/admin/security
   ```

3. Run the firewall rules script by typing the following command:

   ```
   ./edit-firewall-rules.sh
   ```

The following output appears:

```
Choose an Action
----------------
1) Add a custom rule
2) Remove a custom rule
3) List Current Custom Rules
4) Exit
5) Save Changes
Enter desired action:
```

4. Type `2` to remove custom rules and press **Enter**.

   Output similar to the following appears:

   ```
   Rules in configuration file:
        1  |7080|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY

   Select line to remove (ENTER to go back):
   ```

5. Type the number of the line that corresponds to the custom rule and then press **Enter**.

   Output similar to the following appears:

   ```
   Line |7080|10.7.100.105||tcp||ACCEPT|OUTPUT|UTILITY will be
   flagged for removal from custom configuration file.
   ```

   The script returns to the main menu.

   ```
   Choose an Action
   ----------------
   1) Add a custom rule
   2) Remove a custom rule
   3) List Current Custom Rules
   4) Exit
   5) Save Changes
   Enter desired action:
   ```

6. If you need to remove additional custom rules, repeat the previous steps. Otherwise, type `5` to save changes and press **Enter**.

   The following output appears:

   ```
   Rules have been saved to /usr/local/avamar/lib/admin/security/
   avfwb_custom_config.txt
   Return to main menu? (Y/N):
   ```

7. Type `N` and press **Enter**.

   The following output appears:

   ```
   Save and execute rules now? (Y/N):
   ```

8. Type `Y` and press **Enter**.

   The script removes the custom firewall rules from the system firewall tables, automatically restarts the Avamar firewall, and then exits.

   The following output appears:

   ```
   Rules have been saved to /usr/local/avamar/lib/admin/security/
   avfwb_custom_config.txt
   ```

CHAPTER 5

Data Security and Integrity

This chapter includes the following topics:

About Data-in-flight encryption

Avamar can encrypt all data sent between Avamar clients and the Avamar server during transmission (data-in-flight encryption). Encryption methodology and levels are different depending on the Avamar system version.

You specify the default encryption method to use for client/server data transfers when you create and edit groups. You also can override the group encryption method for a specific client on the **Client Properties** tab of the **Edit Client** dialog box, for a specific backup on the **On Demand Backup Options** dialog box, or for a specific restore on the **Restore Options** dialog box. The *Avamar Administration Guide* provides details.

To enable encryption of data in transit, the Avamar server data nodes each require a unique public/private key pair and a signed X.509 certificate that is associated with the public key.

When the Avamar server is installed, a public/private key pair and a self-signed certificate are generated automatically in the `/data01/home/admin` directory on each Avamar server storage node and in the `/usr/local/avamar/etc` directory on the utility node. However, because self-signing is not recommended in production environments, you should generate and install a key and signed certificate from either a commercial or private CA.

You can also configure Avamar for two-way authentication, where the client requests authentication from the Avamar server, and then the Avamar server also requests authentication from the client. One-way, or server-to-client, authentication typically provides sufficient security. However, in some cases, two-way authentication is required or preferred.

The following steps detail the encryption and authentication process for client/server data transfers in a server-to-client authentication environment:

1. The Avamar client requests authentication from the Avamar server.
2. The server sends the appropriate certificate to the client. The certificate contains the public key.
3. The client verifies the server certificate and generates a random key, which is encrypted using the public key, and sends the encrypted message to the server.
4. The server decrypts the message by using its private key and reads the key generated by the client.
5. This random key is then used by both sides to negotiate on a set of temporary symmetric keys to perform the encryption. The set of temporary encryption keys is refreshed at a regular interval during the backup session.

Note

Higher cipher levels result in slower Avamar system performance.

Data-in-flight encryption

To provide enhanced security during client/server data transfers, Avamar supports two levels of data-in-flight encryption: `cleartext` and `high`. The exact encryption technology and bit strength that is used for a client/server connection depends on a number of factors, including the client platform and Avamar server version.

Each cipher level maps to a specific set of OpenSSL suites as shown in the following table.

Table 47 Cipher levels and associated OpenSSL suites

Avamar cipher level	OpenSSL suites
cleartext [a]	NULL-SHA
medium [b]	ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA:AECDH-AES128-SHA
high	ECDHE-ECDSA-AES256-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA

a. The `cleartext` cipher level is not available in Avamar 7.5 and later and Avamar 18.1 and later when the session security features are enabled. If `cleartext` was in place before an upgrade from a previous version of Avamar, the upgrade changes this setting to `high`. The session security features are enabled if the communication security setting is anything other than `Disabled/Off`.

b. The `medium` cipher level is not available in Avamar 7.5 and later and Avamar 18.1 and later. If `medium` encryption was in place before an upgrade from a previous version of Avamar, the upgrade does not change the existing behavior. However, Avamar Administrator displays this setting as `high`. If you change the cipher level to another value, you cannot select medium again.

The default Avamar cipher level is the `high` setting. When you use the `avtar` command with the `--encrypt-strength=high` option or you include `–encrypt-strength=high` in `/usr/local/avamar/var/avtar.cmd`, the shared cipher is AES256-SHA.

Avamar 7.5 and later and Avamar 18.1 and later clients support TLS encryption of the data-in-flight for backups that are stored on a Data Domain system. However, Avamar clients cannot provide encryption of the data-in-flight for backups that are stored on a Data Domain version 5.4 or earlier system.

Encrypted traffic using the TLS 1.0 and 1.1 protocols is no longer supported. Browsers, clients, and other components that require these protocols are not allowed to connect to the server. Only TLS 1.2 encryption is supported.

Closing TCP port 30002

TCP port 30002 was an internal-only exception that supported TLS 1.0 and 1.1. In Avamar 18.2, encrypted traffic using TLS 1.0 and 1.1 is disabled for clients and components. Only TLS 1.2 encryption is supported now. To disable external access to this port, add the port to the Avamar firewall.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Add TCP port 30002 to the Avamar firewall by typing the following command on one line:

   ```
   iptables -I INPUT ! -s <SERVER> -p tcp -m tcp --dport 30002 -j REJECT
   ```

   where *<SERVER>* is the IP address of the utility node or single-node server.

Data-in-flight encryption in Avamar versions 7.1 through 7.4

To provide enhanced security during client/server data transfers, Avamar server versions 7.1 through 7.4 supported six levels of data-in-flight encryption: `cleartext`, `insecure`, `low`, `legacy`, `medium`, and `high`. The exact encryption technology and bit strength that was used for a client/server connection depended on a number of factors, including the client platform and Avamar server version.

The *Avamar Product Security Guide* for these versions provides more information.

Unencrypted data-in-flight

For new installations, the Avamar firewall blocks all transfers of unencrypted data-in-flight.

To prevent disruption of existing backup tasks, upgrading an older version of the Avamar software does not automatically block unencrypted data-in-flight, nor existing backup policies that include transfer of unencrypted data-in-flight. This policy applies if unencrypted data-in-flight was not blocked before the upgrade.

However, new installations include firewall settings that block unencrypted data-in-flight. This firewall policy increases data security. Enabling unencrypted data-in-flight on new installations requires manual changes to the firewall settings.

Permitting unencrypted data-in-flight

Change the Avamar firewall settings to permit unencrypted data-in-flight on new installations.

NOTICE

This task reduces the security of data-in-flight. Only perform this task to meet a specific business requirement.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Open in a plain text editor a new file named `/usr/local/avamar/lib/admin/security/gsan-port`.
3. Add the following line to the new file:

   `GSAN_PLAIN_TEXT='27000,'`

4. Save and close the file.
5. (Multi-node systems only) Use `mapall` to copy the file to the storage nodes, by typing:

   `mapall --user=root copy /usr/local/avamar/lib/admin/security/gsan-port`

6. (Multi-node systems only) Use `mapall` to move the file, by typing:

   `mapall --user=root mv usr/local/avamar/lib/admin/security/gsan-port /usr/local/avamar/lib/admin/security/`

7. Restart the Avamar firewall service.
   - For a single-node server, type: **`service avfirewall restart`**
   - For a multi-node server, type: **`mapall --noerror --all+ --user=root 'service avfirewall restart'`**

Client/server encryption behavior

Client/server encryption functional behavior in any given circumstance is dependent on a number of factors, including the `mcserver.xml` `encrypt_server_authenticate` value, and the `avtar` encryption settings used during that activity.

The `encrypt_server_authenticate` value is set to true when you configure server-to-client authentication.

During backup and restore activities, you control client/server encryption by specifying an option flag pair: `--encrypt` and `--encrypt-strength`. The `--encrypt-strength` option takes one of two values: `None` or `High`.

Note

In Avamar 7.5 and later and Avamar 18.1 and later:

- The **Medium** encryption method is not available.
- The **None** encryption method is not available when the session security features are enabled.

Increasing Avamar server cipher strength

By default, the Management Console server supports cipher strengths up to 128-bit. You can increase the cipher strength that is used by this server to 256-bit for communications on the following ports:

- Ports 7778 and 7779 for the Management Console Server (MCS)
- Port 9443 for the Management Console Web Services

Increasing cipher strength for the MCS

Procedure

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. Open `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` in a plain text editor.
3. Locate the `rmi_cipher_strength` setting and change it to **`high`**.

   `rmi_cipher_strength=`**`high`**
4. Close `mcserver.xml` and save the changes.
5. Download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6:
   a. In a web browser, go to http://java.sun.com.
   b. Search for "Java Cryptography Extension."
   c. Download the file associated with Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 (`jce_policy-6.zip`).
   d. Unzip the jce_policy-6.zip file in a temporary folder and follow the instructions in the `README.txt` file to install.
6. Restart the MCS and the scheduler by typing the following command:

   ```
   dpnctl stop mcs
   dpnctl start mcs
   dpnctl start sched
   ```

SHA-2 SSL security certificates

SSL security certificates in the Remote Method Invocation (RMI) keystore (`/usr/local/avamar/lib/rmi_ssl_keystore`) control remote access to the Management Console Server (MCS) and the Management Console (MC) RMI interface.

This remote access is essential for operations such as replication, server migration, and management via the Avamar Client Manager (ACM).

Avamar 7.4.*x* and earlier use SHA-1 security certificates that expire in 2018. Avamar 7.5 and later use SHA-2 security certificates. These types of security certificates are incompatible and some older versions of Avamar do not support SHA-2 security certificates.

As a result, in an environment that contains mixed software versions, RMI calls from Avamar software with SHA-1 security certificates to the MCS on an Avamar server with a SHA-2 security certificate may fail.

To avoid connection failure, select one of two alternatives:

- Upgrade all servers and related software to Avamar 7.5 or later. This alternative is the preferred method.
- If upgrading is not possible, contact Customer Support for hotfixes to enable support for and deploy SHA-2 security certificates for Avamar 7.2.1, 7.3.1, and

7.4.*x*. As part of this process, Customer Support may also install a cumulative hotfix for the MCS.

If you have imported any custom security certificates into the RMI keystore, you may need to import them again after installing the hotfix. Commercially signed SSL certificates on page 72 provides additional details.

Data-at-rest encryption

An Avamar server can be configured to encrypt the data that is stored on it. This configuration is called data-at-rest encryption.

Avamar provides two choices for managing data-at-rest encryption keys:

- Internal key management using the `avmaint` command
- External key management using the Avamar Key Manager program

Note

In general, data-at-rest encryption can only be enabled during installation of the Avamar software. To configure external key management or enable data-at-rest encryption after installing the Avamar software, request a Dell EMC Professional Services engagement. For more information about configuring data-at-rest encryption, see KB article 333575. SupportZone account required for KB article access.

Internal data-at-rest encryption key management

When you enable data-at-rest encryption with Avamar's internal key management, the server accepts a user-defined salt that is then used to generate an encryption key. The salt is stored on the Avamar server for subsequent encryption/decryption activities.

The internal key management is completely automatic:

- Old encryption keys are automatically stored in a secure manner so that data stripes encrypted with previous keys can always be decrypted and read.
- During server maintenance, crunched stripes are, over time, converted to use the current key.

The Avamar software performs encryption using the AES-256 CFB block cipher mode. Note that since any reads/writes from disk require encryption processing with this feature enabled, there is a performance impact to the Avamar server of approximately 33 percent.

Avamar Key Manager

An alternative to internal key management for data-at-rest encryption is to use external key management by enabling Avamar Key Manager. Avamar Key Manager acts as a client of an external key management system (a supported KMIP-compliant key management server).

Note

Avamar supports the SafeNet KeySecure 8.6 KMIP key management server. The RSA Data Protection Manager is no longer supported. KMIP-compliant key management servers are only supported on the Avamar Data Store Gen4T platform.

When you install Avamar Key Manager, it configures data-at-rest encryption on all Avamar nodes and registers with the external key management system. Avamar Key Manager then permits the external key management system to handle all key management tasks for data-at-rest encryption. Residing on the utility node or single-node server, Avamar Key Manager retrieves keys from the external key management system and then shares the keys with the storage nodes. Key communication is protected by SSL.

Avamar Key Manager uses public-key cryptography to secure all communications with the external key management system. As preparation for using external key management, you install a private key for Avamar Key Manager and a public key certificate for the external key management system on the Avamar server. Also, the external key management system administrator installs the public key for Avamar Key Manager on the external key management system.

It is not possible to convert an Avamar server from one type of external key management system to another. Only one type of external key management system can be active at a time, and changing the external key management system type is not supported after the initial configuration.

If the existing data was encrypted by using the RSA Data Protection Manager with a previous version of the Avamar software and you need to move to a KMIP-compliant key management server, perform a full server migration to move the data to another Avamar server that you have configured as a client of the KMIP-compliant key management server.

Note

Data-at-rest encryption through Avamar Key Manager cannot be reversed. Data encrypted by this process can only be read using Avamar Key Manager's decryption algorithms and through keys that are stored in the external key management system database. The required Avamar files for this process are stored in `/usr/local/avamar/etc/akm`. Do not delete these files. The external key management system database must be backed up as described in that product's documentation.

Data integrity

Checkpoints are server backups taken for the express purpose of assisting with disaster recovery. Checkpoints are typically scheduled twice daily and validated once daily (during the maintenance window). You also can create and validate additional server checkpoints on an on-demand basis. The *Avamar Administration Guide* provides details on creating, validating, and deleting server checkpoints.*Avamar Administration Guide*

Checkpoint validation, which is also called an Avamar Hash Filesystem check (HFS check), is an internal operation that validates the integrity of a specific checkpoint. Once a checkpoint has passed an HFS check, it can be considered reliable enough to be used for a system rollback.

The actual process that performs HFS checks is `hfscheck`; it is similar to the UNIX `fsck` command.

You can schedule HFS checks by using Avamar Administrator. You also can manually initiate an HFS check by running `avmaint hfscheck` directly from a command shell.

An HFS check might take several hours depending on the amount of data on the Avamar server. For this reason, each validation operation can be individually configured to perform all checks (full validation) or perform a partial rolling check

which fully validates all new and modified stripes, then partially checks a subset of unmodified stripes.

Initiating an HFS check requires significant amounts of system resources. To reduce contention with normal server operation, an HFS check can be throttled.

Additionally, during this time, the server is placed in read-only mode. Once the check has been initiated, normal server access is resumed. You can also optionally suspend command dispatches during this time, although this is not typically done.

If HFS check detects errors in one or more stripes, it automatically attempts to repair them.

Data erasure

When you manually delete a backup using Avamar Administrator or you automatically delete a backup when its retention policy expires and garbage collection runs, data is marked as deleted but is left on disk.

You can permanently and securely delete backups from an Avamar server in a manner that satisfies stringent security requirements by overwriting the data that is unique to a backup with random data.

Requirements for securely deleting backups

Avamar requirements

- All nodes must be in the ONLINE state, and no stripes should be in the OFFLINE state. This can be checked using the status.`dpn` command.
- The most recent checkpoint must have been successfully validated.
- Pending garbage collection operations can increase the time needed to complete the secure deletion process, or can cause extra data to be overwritten. Therefore, you should run garbage collection until all pending non-secure deletions have successfully completed. No errors should be reported by the garbage collection process.
- The server should be idle:
  - There should be no backups in progress, nor should the server be running garbage collection or HFS checks.
  - The backup scheduler and maintenance windows scheduler should be stopped for the duration of the secure deletion process, so that no new backups or maintenance activities are initiated.
- Avamar storage node ext3 file systems should not be configured to operate in `data=journal` mode. If this is the case, data might persist on the disk after the secure deletion process has completed.

Other requirements

- You must be familiar with basic- to intermediate-level Avamar server terminology and command-line administration.
- Some steps to securely delete backups might require the use of third party tools such as the open-source `srm` or GNU `shred` utilities. The documentation for those utilities provides additional information regarding proper use, capabilities, and limitations of those utilities.
- Use of any non-certified storage hardware, including RAID controllers and disk storage arrays, might impact the effectiveness of the secure backup deletion.

Consult the manufacturers of those devices for information about disabling or clearing write caches, or about any other features that impact data transfer to the storage media.

Securely deleting a backup

The `securedelete` program enables you to securely erase a backup on the Avamar server.

This procedure can be used in conjunction with the existing procedures at a company to securely delete data from other parts of the operating system or hardware. Contact Avamar Customer Support for any questions regarding the effect of company procedures on the Avamar server software.

Procedure

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 the following command:

     ```
     ssh-agent bash
     ssh-add ~admin/.ssh/admin_key
     ```
2. Locate the backups to securely delete by typing the following command:

   securedelete getb --id=*user*@*auth* --password=*password* --account=*domain*/*client*

   where:
   - *user* is the Avamar username.
   - *auth* is is the authentication system used by that user (the default internal authentication domain is `avamar`).
   - *password* is the password for the *user*@*auth* account.
   - *domain*/*client* is the full location of the client machine.
3. Locate the backup to delete in the list, and then note the date in the **created** field.
4. Securely delete the backup by typing the following command:

   securedelete delb --account=*location* --date=*date* --id=*user*@*auth* --password=*password*

   where:
   - *location* is is the location of the backup, expressed as a file path relative to the current working directory. However, if the first character is a slash (/), the value is treated as an absolute file path.
   - *date* is the backup date noted in the previous step.
   - *user* is the Avamar username.
   - *auth* is is the authentication system used by that user (the default internal authentication domain is `avamar`).
   - *password* is the password for the *user*@*auth* account.

This operation typically takes several minutes to complete while the server securely overwrites data.

Note

Do not interrupt `securedelete delb` command. If interrupted, all data will not be securely deleted.

If successful, the `securedelete delb` command returns the following response:

```
1 Request succeeded
```

If unsuccessful, the `securedelete delb` command returns the following response:

```
0 ERROR! Exit code 0: Request failed.
```

5. If an error is encountered:
   - Search the knowledge base in Online Support, for the specific error code.
   - If the required information is not found, engage Avamar Customer Support using Live Chat, or create a Service Request.
6. Check the server logs for any `ERROR` or `WARN` messages that might indicate a failure of the secure deletion operation by typing:

   ```
   mapall --noerror 'grep "ERROR\|WARN" /data01/cur/gsan.log*'
   ```
7. If any such messages are present:
   - Search the knowledge base in Online Support, for the specific error code.
   - If the required information is not found, engage Avamar Customer Support using Live Chat, or create a Service Request.
8. If any stripes on the system have been repaired or rebuilt due to data corruption, then the bad versions remain on disk. Overwrite or securely delete these files by using an appropriate third-party tool.

   Locate these stripes by typing:

   ```
   mapall --noerror 'ls /data??/cur/*.bad*'
   ```

   Information similar to the following appears in the command shell:

   ```
   /data06/cur/
   0000000300000016.0000000300000016.bad1240015157
   /data06/cur/0000000300000016.cdt.bad1240015157
   /data06/cur/0000000300000016.chd.bad1240015157
   /data06/cur/0000000300000016.wlg.bad1240015157
   ```
9. If backups were performed before the most recent checkpoint was taken, roll the server back to the most recent checkpoint, and then attempt to securely delete the backup again.
10. Repeat the previous step for all applicable checkpoints.
11. Repeat this entire procedure on all other Avamar servers to which this Avamar server replicates backups.

CHAPTER 6

System Monitoring, Auditing, and Logging

This chapter includes the following topics:

Auditing and logging

This section describes how Avamar logs events and protects against tampering.

Auditing and logging helps you to monitor the Avamar environment including the server status, system events, interpret logs, and event information.

Monitoring server status

Avamar systems provide monitoring of several items on the Avamar server.

You can monitor the status of the following items on the Avamar server:

- Overall Avamar server status
- Capacity usage
- Modules
- Nodes
- Partitions
- Checkpoints
- Garbage collection
- Maintenance activities

If you use a Data Domain system as storage for Avamar client backups, you also can monitor CPU, disk activity, and network activity for each node on the Data Domain system.

This status information is provided on the tabs in the Avamar Server window in Avamar Administrator. The *Avamar Administration Guide* provides details on how to access the Avamar Server window and the information available on each tab.

Monitoring system events

All Avamar system activity and operational status is reported as various events to the MCS. Examples of various Avamar events include client registration and activation, successful and failed backups, hard disk status, and others.

Events are listed in the Event Management tab in the Administration window of Avamar Administrator. The *Avamar Administration Guide* provides details on how to access the Event Management tab and filter the events that appear in the tab.

You can also configure Avamar to notify you when events occur. There are several features and functions available.

Pop-up alerts
Events can be configured on an event-by-event basis to generate a graphical pop-up alert each time one of these events occurs. One significant limitation of this feature is that Avamar Administrator software must be running in order for the pop-up alerts to be displayed.

Acknowledgment required list
Events can be configured on an event-by-event basis such that when events of this type occur, an entry is added to a list of events that requires interactive acknowledgment by the Avamar system administrator.

Email messages
Events can be configured on an event-by-event basis to send an email message to a designated list of recipients. Email notifications can be sent immediately or in batches at regularly scheduled times.

Syslog support
Events can be configured on an event-by-event basis to log information to local or remote syslog files that are based on filtering rules that are configured for the syslog daemon receiving the events.

Third-party monitoring tools and utilities capable of examining log entries can access the syslog files and process them to integrate Avamar event information into larger site activity and status reports.

NOTICE

For maximum security, we recommend implementing remote syslog monitoring as described in the *Avamar Administration Guide*.

SNMP support
Simple Network Management Protocol (SNMP) is a protocol for communicating monitoring and event notification information between an application, hardware device or software application, and any number of monitoring applications or devices.

The Avamar SNMP implementation provides two distinct ways to access Avamar server events and activity completion status:

- SNMP requests provide a mechanism for SNMP management applications to "pull" information from a remote SNMP-enabled client (in this case, the Avamar server).
- SNMP traps provide a mechanism for the Avamar server to "push" information to SNMP management applications whenever designated Avamar events occur. Events can be configured on an event-by-event basis to output SNMP traps.

Avamar also can collect and display data for health monitoring, system alerts, and capacity reporting on a configured Data Domain system by using SNMP. The *Avamar and Data Domain System Integration Guide* provides details on how to configure SNMP for Avamar with Data Domain.

ConnectEMC support
Events can be configured on an event-by-event basis to send a notification message directly to Customer Support using ConnectEMC.

The *Avamar Administration Guide* provides details on how to configure each of these notification mechanisms.

Event notification profiles

Profiles are a notification management feature that are used to logically group certain event codes together and specify which notifications should be generated when these events occur.

You can create custom profiles to organize system events and generate the selected notifications when any of those events occur. The *Avamar Administration Guide* provides details on how to create and manage profiles.

Email home notification

Avamar systems provide an email home feature.

When fully configured and enabled, the email home feature automatically emails the following information to Avamar Customer Support twice daily:

- Status of the daily data integrity check
- Selected Avamar server warnings and information messages
- Any Avamar server errors
- Any RAID errors (single-node servers only)

By default, these email messages are sent at 6 a.m. and 3 p.m. each day (based on the local time on the Avamar server). The timing of these messages is controlled by the Notification Schedule.

The*Avamar Administration Guide* provides details on how to enable and schedule the email home feature.

Auditing

The Avamar Audit Log provides details on the operations that users start in the Avamar system.

The data in this log allows enterprises that deploy Avamar to enforce security policies, detect security breaches or deviation from policies, and hold appropriate users accountable for those actions. The audit log includes the following information for each operation:

- The date and time the action occurred
- The event code number that is associated with the action
- The ID and role of the user that started the action
- The product and component from which the action was started
- The severity of the action
- The domain in which the action occurred

The Audit Log is available in Avamar Administrator as a subtab of the Event Management tab in the Administration window. The Avamar Administration Guide provides details on how to access the Audit Log and filter the events that appear in the log.

Gen4 and later Avamar Data Stores running the SUSE Linux Enterprise Server (SLES) operating system implement improved auditing features, such as Advanced Intrusion Detection Environment (AIDE) and the `auditd` service.

Audit logging

The audit log keeps a permanent log of system actions that users begin with. The data in this log enables enterprises that deploy Avamar to enforce security policies, detect security breaches or deviation from policies, and hold users accountable for those actions.

Only actions that users begin with are logged. Actions that the system begins with without a user account, such as scheduled backups, maintenance activities, are not logged.

System events with a category of SECURITY and type of AUDIT are used to implement the Avamar audit logging feature. Because the underlying data for audit log entries are system events, this information is available in two places:

- Event Monitor, which also contains all other system events
- Audit Log, which only contains events that are also audit log entries

By default, audit log information is retained for 1 year.

You can increase or reduce the audit log retention period by editing the value of `clean_db_audits_days` in `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml`, and restarting the MCS.

Viewing the Audit Log

Procedure

1. In Avamar Administrator, click the **Administration** launcher link.

   The **Administration** window is displayed.
2. Click the **Event Management** tab.
3. Click the **Audit Log** tab near the bottom of the window.

   The Avamar Administrator online help provides details on each of the columns in the Audit Log.
4. Select the display mode for the Audit Log:
   - To display the most recent 5,000 audit log entries for a defined range of dates, select **Query**.
   - To display the most recent 5,000 audit log entries during the past 24 hours, select **Monitor**.
5. (Optional) Filter the entries that appear in the Audit Log:
   a. Open the **Actions** menu and select **Event Management** > **Filter**.

      The **Filter** dialog box appears.
   b. If you selected the **Query** display mode for the Audit Log, select the range of dates for the entries to display by using the **From Date** and **To Date** fields.
   c. From the **Severity** list, select the severity of the log entries to display.
   d. To view log entries for all domains, select **All Domains**. Or, to view entries for a specific domain, select **Domain** and then browse to or type the domain name.
   e. To display only log entries that contain certain case-sensitive keywords in the audit log entry data XML element, type the keyword in the **Data** box.

      This criterion promotes easy filtering on important keywords across log entry attributes. For example, filtering the log in `error` returns all log entries that contain the word `error` in any XML attribute (for example, category, type, or severity).
   f. To view additional filtering criteria, click **More**.
   g. To limit the Audit Log to events with a certain event code, select **Only include codes** and then add and remove codes from the list. Or, to exclude events with a certain event code from the Audit Log, select **Exclude codes** and then add and remove codes from the list.

h. Click **OK**.

Logs

Avamar software includes log files for server and client components, maintenance tasks, various utilities, and backup clients. These log files enable you to examine various aspects of the Avamar system.

Log information is organized into tables for each Avamar component. For more information about log files, refer to the Avamar guide for the specific component.

Single-node system log files

The following table lists the pathnames for the log files that are created by components of a single-node Avamar system.

Table 48 Component log files on a single-node Avamar system

Component	Pathname
Avamar Administrator	/usr/local/avamar/var/mc/server_log/flush.log /usr/local/avamar/var/mc/server_log/restore.log /usr/local/avamar/var/mc/server_log/mcserver.log.# /usr/local/avamar/var/mc/server_log/mcserver.out /usr/local/avamar/var/mc/server_log/pgsql.log /usr/local/avamar/var/mc/server_data/postgres/data/pg_log/postgresql-DATE_TIME.log /usr/local/avamar/var/mc/server_data/mcs_data_dump.sql
Avamar EM (Server)	/usr/local/avamar/var/em/server_log/flush.log /usr/local/avamar/var/em/server_log/restore.log /usr/local/avamar/var/em/server_log/emserver.log.# /usr/local/avamar/var/em/server_log/emserver.out /usr/local/avamar/var/em/server_log/pgsql.log /usr/local/avamar/var/em/server_data/postgres/data/pg_log/postgresql-DATE_TIME.log /usr/local/avamar/var/em/server_data/emt_data_dump.sql
Maintenance	/usr/local/avamar/var/cron/clean_emdb.log /usr/local/avamar/var/cron/dpn_crontab.log /usr/local/avamar/var/cron/cp.log /usr/local/avamar/var/cron/gc.log /usr/local/avamar/var/cron/hfscheck.log /usr/local/avamar/var/cron/ntpd_keepalive_cron.log /usr/local/avamar/var/cron/ntpd_keepalive_cron.log.# /usr/local/avamar/var/cron/suspend.log
avw_install utility	/usr/local/avamar/var/avw_cleanup.log /usr/local/avamar/var/avw_install.log /usr/local/avamar/var/avw-time.log /usr/local/avamar/var/log/dpnavwinstall-VERSION.log
axion_install utility	/usr/local/avamar/var/axion_install_DATE_TIME.log

Table 48 Component log files on a single-node Avamar system (continued)

Component	Pathname
Avamar File System (AvFS)	/usr/local/avamar/var/axionfs.log
change-passwords utility	/usr/local/avamar/var/change-passwords.log
ddrmaint utility	/usr/local/avamar/var/log/ddrmaint.log
dpnctl utility	/usr/local/avamar/var/log/dpnctl.log
dpnnetutil utility	/usr/local/avamar/var/log/dpnnetutil-version.log /usr/local/avamar/var/log/dpnnetutil.log* /usr/local/avamar/var/log/dpnnetutilbgaux.log /usr/local/avamar/var/log/dpnnetutilbgaux-stdout-stderr.log
permctl utility	/usr/local/avamar/var/log/permctl.log
resite utility	/usr/local/avamar/var/dpnresite-version.log /usr/local/avamar/var/mcspref.log /usr/local/avamar/var/nataddr.log /usr/local/avamar/var/smtphost.log
timedist utility	/usr/local/avamar/var/timedist.log
timesyncmon program	/usr/local/avamar/var/timesysncmon.log
Avamar license server	/usr/local/avamar/var/ascd-PORT.log
Storage server	/data01/cur/err.log /data01/cur/gsan.log

Utility node log files

The following table lists the pathnames for the log files that are created by components of the utility node.

Table 49 Component log files on a utility node

Component	Pathname
Avamar Administrator	/usr/local/avamar/var/mc/server_log/flush.log /usr/local/avamar/var/mc/server_log/restore.log /usr/local/avamar/var/mc/server_log/mcddrssh.log /usr/local/avamar/var/mc/server_log/mcddrsnmp.out /usr/local/avamar/var/mc/server_log/mcddrsnmp.log /usr/local/avamar/var/mc/server_log/mcserver.log.# /usr/local/avamar/var/mc/server_log/mcserver.out /usr/local/avamar/var/mc/server_log/pgsql.log

Table 49 Component log files on a utility node (continued)

Component	Pathname
	/usr/local/avamar/var/mc/server_data/postgres/data/pg_log/postgresql-DATE_TIME.log /usr/local/avamar/var/mc/server_data/mcs_data_dump.sql
Avamar EM (Server)	/usr/local/avamar/var/em/server_log/flush.log /usr/local/avamar/var/em/server_log/restore.log /usr/local/avamar/var/em/server_log/emserver.log.# /usr/local/avamar/var/em/server_log/emserver.out /usr/local/avamar/var/em/server_log/pgsql.log /usr/local/avamar/var/em/server_data/postgres/data/pg_log/postgresql-DATE_TIME.log /usr/local/avamar/var/em/server_data/emt_data_dump.sql
Maintenance	/usr/local/avamar/var/cron/clean_emdb.log /usr/local/avamar/var/cron/dpn_crontab.log /usr/local/avamar/var/cron/cp.log /usr/local/avamar/var/cron/gc.log /usr/local/avamar/var/cron/hfscheck.log /usr/local/avamar/var/cron/ntpd_keepalive_cron.log /usr/local/avamar/var/cron/ntpd_keepalive_cron.log.# /usr/local/avamar/var/cron/suspend.log
avw_install utility	/usr/local/avamar/var/avw_cleanup.log /usr/local/avamar/var/avw_install.log /usr/local/avamar/var/avw-time.log /usr/local/avamar/var/log/dpnavwinstall-VERSION.log
axion_install utility	/usr/local/avamar/var/axion_install_DATE_TIME.log
Avamar File System (AvFS)	/usr/local/avamar/var/axionfs.log
change-passwords utility	/usr/local/avamar/var/change-passwords.log
ddrmaint utility	/usr/local/avamar/var/log/ddrmaint.log
dpnctl utility	/usr/local/avamar/var/log/dpnctl.log
dpnnetutil utility	/usr/local/avamar/var/log/dpnnetutil-version.log /usr/local/avamar/var/log/dpnnetutil.log* /usr/local/avamar/var/log/dpnnetutilbgaux.log /usr/local/avamar/var/log/dpnnetutilbgaux-stdout-stderr.log
permctl utility	/usr/local/avamar/var/log/permctl.log
timedist utility	/usr/local/avamar/var/timedist.log
timesyncmon program	/usr/local/avamar/var/timesyncmon.log

Table 49 Component log files on a utility node (continued)

Component	Pathname
Avamar license server	/usr/local/avamar/var/ascd-PORT.log
switch_monitoring utility	/usr/local/avamar/var/log/switch_monitoring.log

Storage node log files

The following table lists the pathnames for the log files that an Avamar storage node creates.

Table 50 Component log files on a storage node

Component	Pathname
Storage server log	/data01/cur/err.log /data01/cur/gsan.log
dpnnetutil utility	/usr/local/avamar/var/log/dpnnetutilbgaux-stdout-stderr.log /usr/local/avamar/var/log/dpnnetutilbgaux.log
Maintenance task	/usr/local/avamar/var/ntpd_keepalive_cron.log*
timesyncmon program	/usr/local/avamar/var/timesyncmon.log*

Spare node log file

The following table lists the pathname for the spare node log file.

Table 51 Component log file on a spare node

Component	Pathname
dpnnetutil utility	/usr/local/avamar/var/log/dpnnetutilbgaux-stdout-stderr.log /usr/local/avamar/var/log/dpnnetutibgaux.log

Avamar NDMP Accelerator log files

The following tables list the pathnames for the log files created by the Avamar NDMP Accelerator.

Table 52 Component log files for the NDMP Accelerator

Component	Pathname
avndmp log	/usr/local/avamar/var/{FILER-NAME}/*.avdnmp.log
dpnnetutil utility	/usr/local/avamar/var/log/dpnnetutilbgaux-stdout-stderr.log /usr/local/avamar/var/log/dpnnetutilbgaux.log

Access node log files

The following table lists the pathname for the log files created by an access node.

Table 53 Component log files on an access node

Component	Pathname
dpnnetutil utility	/usr/local/avamar/var/log/dpnnetutilbgaux-stdout-stderr.log /usr/local/avamar/var/log/dpnnetutilbgaux.log

Avamar Administrator client log files

The following tables list the pathnames for the log files created by the Avamar Administrator client.

Table 54 Component log files on an Avamar Administrator client

Component	Operating system	Pathname
Avamar Administrator management console	Windows 7 Windows Vista Windows XP Linux	C:\Users\USERNAME\.avamardata\var\mc\gui_log C:\Documents and Settings\USERNAME\.avamardata\var\mc\gui_log $HOME/.avamardata/var/mc/gui_log/mcclient.log.0
Avamar Administrator management console command line interface	UNIX	$HOME/.avamardata/var/mc/gui_log/mccli.log.0

Backup client log files

The following table lists the pathnames for the log files created by Avamar components on an Avamar backup client.

Table 55 Component log files for an Avamar backup client

Component	Pathname
Client avagent process (all clients)	C:\Program Files\avs\var\avagent.log
Client avtar process (all clients)	C:\Program Files\avs\var\clientlogs\{WORKORDER-ID}.alg C:\Program Files\avs\var\clientlogs\{WORKORDER-ID}.log
Avamar Client for Windows tray applet	C:\Program Files\avs\var\avscc.log
Avamar Plug-in for DB2	/usr/local/Avamar /var/client/{WORKORDER-ID}.log
Avamar Exchange Client	/usr/local/Avamar /var/client/{WORKORDER-ID}.log

Table 55 Component log files for an Avamar backup client (continued)

Component	Pathname
Avamar NDMP Accelerator	/usr/local/Avamar /var/client/{WORKORDER-ID}.log
Avamar Client for NetWare	/usr/local/Avamar /var/client/{WORKORDER-ID}.log
Avamar Plug-in for Oracle	/usr/local/Avamar /var/client/{WORKORDER-ID}.log
Avamar Plug-in for SQL Server	/usr/local/Avamar /var/client/{WORKORDER-ID}.log

Monitoring server status and statistics

The **Server** window in Avamar Administrator enables you to monitor status and statistics for the Avamar server as a whole, for individual nodes on the Avamar server, and for any configured Data Domain systems.

The following tabs appear on the **Server** window:

- The **Server Monitor** tab presents a summarized view of CPU, network, and hard drive performance statistics for the Avamar server. A separate subtab provides the same information for any configured Data Domain systems.
- The **Server Management** tab shows a detailed view of the server hardware resources for the Avamar server and any configured Data Domain systems.
- The **Session Monitor** tab shows a list of active client backup and restore sessions.
- The **Checkpoint Management** tab shows detailed information for all system checkpoints that are performed for this Avamar server.
- The **Data Domain NFS Datastores** tab lists the temporary NFS share for VMware instant access on any configured Data Domain systems. The *Avamar for VMware User Guide* provides more information on instant access.

Server Monitor tab

The **Server Monitor** tab on the **Server** window in Avamar Administrator includes separate tabs for the Avamar server and any configured Data Domain systems.

Avamar tab

The **Avamar** tab in the Server Monitor presents a summarized view of CPU, network, and hard drive performance statistics for the Avamar server.

The following tables describe the information available on the **Avamar** tab.

Table 56 Node details on the Avamar tab of the Server Monitor

Property	Description
Status indicators	Status of the node. One of the following values: • Online (green)—The node is functioning correctly.

Table 56 Node details on the Avamar tab of the Server Monitor (continued)

Property	Description
	• Read-Only (blue)—This status occurs normally as background operations are performed and when backups have been suspended. • Time-Out (gray)—MCS could not communicate with this node. • Unknown (yellow)—Node status cannot be determined. • Offline (red)—The node has experienced a problem. If ConnectEMC has been enabled, a Service Request (SR) is logged. Go to Avamar Support to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.
ID	Each node in the Avamar server has a unique logical identifier. This node ID is expressed in the format *module.node*. **Note** Module and node numbering begins with zero. Therefore, the ID for the third node in the first module is 0.2.

Table 57 CPU details on the Avamar tab of the Server Monitor

Property	Description
Load	Average number of CPU threads over the past minute.
User	Percentage of CPU capacity that is consumed by running server instructions (anything other than operating system overhead).
Sys	Percentage of CPU capacity that is consumed by operating system overhead.

Table 58 Network details on the Avamar tab of the Server Monitor

Property	Description
Ping	Time in seconds that this node took to respond to a ping request.
In	Received packet throughput reported in KB per second.
Out	Sent packet throughput reported in KB per second.

Table 59 Disk details on the Avamar tab of the Server Monitor

Property	Description
Reads	Average number of hard drive reads per second as reported by the operating system.
Writes	Average number of hard drive writes per second as reported by the operating system.
Utilization	Percentage of total available server storage capacity currently used.

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

Table 61 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 62 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 63 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.

Server Management tab

The **Server Management** tab on the **Server** window in Avamar Administrator shows a detailed view of the server hardware resources, including both the Avamar server and any configured Data Domain systems.

Avamar server information is listed under the **Avamar** folder in the tree, and configured Data Domain systems are listed under the **Data Domain** folder in the tree.

The information in the right pane of the window changes when you select different items in the tree.

Table 64 Data display based on selections on the Server Management tab

Selected item	Information in the right pane of the Server Management tab
Servers node	Summary of bytes protected
Avamar or Data Domain nodes	Blank
Avamar server name	Detailed information for the Avamar server
Module	Detailed information for that module
Node	Detailed information for that node
Partition	Detailed information for that logical hard drive partition
Data Domain system	Detailed information for that Data Domain system

NOTICE

Avamar is licensed in decimal units. Therefore, **Total capacity** and **Capacity used** are displayed in decimal units on the **Server Management** tab. All other parts of the product that output capacity is displayed in binary units.

Bytes Protected Summary

The following table provides details on the **Bytes Protected Summary** properties on the **Server Management** tab.

The amount is the pre-compress size on the client side.

Table 65 Bytes Protected Summary properties on the Server Management tab

Property	Description
Properties	Name of the Avamar server and configured Data Domain systems.
Values	Number of bytes of protected data on the server or Data Domain system. The amount is the pre-compress size on the client side.

Server information

The following tables describe the **Server Information** that is provided when an Avamar server is selected on the **Server Management** tab.

Table 66 Server Details on the Server Management tab

Property	Description
Active sessions	Current number of active client sessions. Click the **Session Monitor** tab for more information.
Total bytes free in partitions	Disk free size from the OS level.

Table 66 Server Details on the Server Management tab (continued)

Property	Description
Server bytes reserved	The maximum size that the current stripe files occupy.
Total capacity	Total amount of server storage capacity.
Server utilization	Percentage of total available server storage capacity currently used. This value is derived from the largest **Disk Utilization** value on the **Avamar** tab in the Server Monitor, and therefore represents the absolute maximum Avamar server storage utilization. Actual utilization across all modules, nodes, and drives might be slightly lower.
Bytes protected (client pre-comp size)	Total amount of client data in bytes that has been backed up (protected) on this server. The amount is the pre-compress size on the client side.
Bytes protected quota (client pre-comp size)	Maximum amount of client data in bytes that is licensed for protection on this server. The amount is the pre-compress size on the client side.
License expiration	Calendar date on which this server's licensing expires. When the licensing is perpetual, the value is `never`.
Time since Server initialization	Number of hours, days, and minutes that have elapsed since this Avamar server was initialized.
Last checkpoint	Date and time that the last server checkpoint was performed. Checkpoints are typically performed twice daily.
Last validated checkpoint	Date and time that the server checkpoint was last validated. Checkpoint validation normally occurs once per day. Therefore, the **Last validated checkpoint** time and **Last checkpoint time** might be different depending on the time of day that you view this information. **Note** If the **Last validated checkpoint** and **Last checkpoint times** are more than 36 hours apart, checkpoint validation is not occurring, which is a problem.
System Name	User-assigned name of this Avamar server.
System ID	Unique identifier for this Avamar server.

Table 66 Server Details on the Server Management tab (continued)

Property	Description
HFSAddr	Hash File System (HFS) address (Addr). The hostname or IP address that backup clients use to connect to this Avamar server.
HFSPort	HFS data port. The data port that backup clients use to connect to this Avamar server. The default is port 27000.
IP Address	IP address of this Avamar server. If the HFSAddr is an IP address, this value is the same as the HFSAddr.

Table 67 Maintenance Activities Details on the Server Management tab

Property	Description
Suspended	One of the following values: • No — Server maintenance activities are not currently suspended (that is, server maintenance activities will run normally during the next maintenance window). • Yes — Server maintenance activities are currently suspended.

Table 68 Garbage Collection Details on the Server Management tab

Property	Description
Status	One of the following values: • Idle — Garbage collection is not currently taking place. • Processing — Garbage collection is taking place.
Result	One of the following values: • OK — Last garbage collection activity successfully completed. • Error code — Last garbage collection activity did not successfully complete.
Start time	Date and time that the last garbage collection activity began.
End time	Date and time that the last garbage collection activity ended.
Passes	Total number of passes during the last garbage collection activity.

Table 68 Garbage Collection Details on the Server Management tab (continued)

Property	Description
Bytes recovered	Total amount of storage space in bytes that was recovered during the last garbage collection activity.
Chunks deleted	Total number of data chunks that were deleted during the last garbage collection activity.
Index stripes	Total number of index stripes.
Index stripes processed	Total number of index stripes that were processed during the last garbage collection activity.

Module information

The following table provides details on the **Module** properties on the **Server Management** tab.

Table 69 Module properties on the Server Management tab

Property	Description
Total bytes free in partitions	Disk free size from the OS level.
Server bytes reserved	The maximum size that the current stripe files occupy.
Total capacity	Total amount of server storage capacity.
Server utilization	Percentage of total available server storage capacity currently used. This value is derived from the largest **Disk Utilization** value that is shown on the Avamar tab in the Server Monitor, and therefore represents the absolute maximum Avamar server storage utilization. Actual utilization across all modules, nodes, and drives might be slightly lower.
Number of nodes	Total number of nodes in this module.
IP address	Base IP address of this module.

Node information

The following tables provide details on the **Node** properties on the **Server Management** tab.

Table 70 Status indicators on the Node Information part of Server Management

Property	Description
Status indicators	One of the following values:

Table 70 Status indicators on the Node Information part of Server Management

Property	Description
	• Online (green) — Node is functioning correctly. • Read-Only (blue) — This option occurs normally as background operations and when backups have been suspended. • Time-Out (gray) — MCS could not communicate with this node. • Unknown (yellow) — Node status cannot be determined. • Offline (red) — Node has experienced a problem. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to Avamar Support to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.

Table 71 Server details on the Node Information part of Server Management

Property	Description
State	Current operational state of the server. One of the following values: • ONLINE — Node is functioning correctly. • DEGRADED — One or more disk errors have been detected. • OFFLINE — Node has experienced a problem. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to Avamar Support to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792. • READONLY — Occurs normally as background operations are performed and when backups have been suspended.
Runlevel	Current operational state of the server. One of the following values: • fullaccess — This Avamar server is fully operational. • admin — Avamar server is fully operational but only the administrator root account can access the server. • adminonly — Avamar server is fully operational but only the administrator root account can access the server.

Table 71 Server details on the Node Information part of Server Management (continued)

Property	Description
	• adminreadonly — Avamar server is in a read-only condition and only the administrator root account can access the server. • readonly — Avamar server is in a read-only condition. Restores are allowed but no new backups can be taken. • suspended — Scheduled backups are disabled until you reenable the scheduler. • synchronizing — Avamar server is priming or synchronizing stripes. A temporary condition. Some operations might be delayed.
Accessmode	Current access level of the server. The full server access mode is typically represented as 3 4-bit fields. For example: `mhpu+mhpu +0000` The most significant bits show server privileges, the middle bits show root user privileges, and the least significant bits show privileges for all other users. Individual bits in these fields convey the following information: • m — Migrate allowed. • h — Hash File System (HFS) is writable. • p — Persistent store is writable. • u — User accounting is writable.
Port	Data port that is used for intra-node communication.
Dispatcher	Data port that is used by various utilities to communicate with this node.
Server uptime	Number of hours, days, and minutes that have elapsed since this Avamar server was initialized.
Server bytes reserved	The maximum size that the current stripe files occupy.
Amount of reserved used	The size for backup data in the stripe files and cache.
Total capacity	Total amount of server storage capacity.
Capacity used	Total amount of server storage capacity that has been used for any reason.
Server utilization	Percentage of total available node storage capacity currently used.
Number of stripes	Total number of stripes on this node.

Table 71 Server details on the Node Information part of Server Management (continued)

Property	Description
Server version	Version of Avamar software running on this node.

Table 72 OS details on the Node Information part of Server Management

Property	Description
Version	Current operating system version running on this node.
Node uptime	Number of hours, days, and minutes that have elapsed since this node was last started.
Total bytes free in partitions	Disk free size from the OS level.
Total bytes used in partitions	Disk used size from the OS level.
Load average	The average number of CPU threads over the past minute.
CPU %	Percentage of this node's CPU currently being used.
Ping time (sec)	Time in seconds this node took to respond to a ping request.
Disk reads	Number of hard drives read operations per second.
Disk writes	Number of write operations per second for the hard drive.
Network reads	Number of kilobytes per second read by way of this node's network connection.
Network writes	Number of kilobytes per second written by way of this node's network connection.

Table 73 Hardware details on the Node Information part of Server Management

Property	Description
IP address	IP address of this node.
MAC address	Media Access Control (MAC) address. A low-level hardware address that uniquely identifies this node in the Avamar server.
Number of partitions	Total number of logical hard drive partitions in this node.
Generation	The hardware platform type.
Generation Description	The hardware platform type description.

Partition information

The following tables provide details on the **Partition Information** that is available when a partition is selected on the **Server Management** tab.

Table 74 Status indicators on the Partition Information part of Server Management

Property	Description
Status indicators	One of the following values: • Online (green) — The partition is functioning correctly. • Offline (yellow) — The partition has one or more offline stripes. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the Avamar Support website to view existing SRs. • Read-Only (blue) — The partition is read-only. • Nonfunctional (red) — The partition is not functioning. Search the knowledgebase on the Avamar Support website for solution esg108474.
Server bytes reserved	The maximum size that the current stripe files occupy.
Amount of reserved used	The size for backup data in the stripe files and cache.

Table 75 Server Details on the Node Information part of Server Management

Property	Description
Total capacity	Total amount of server storage capacity.
Capacity used	Total amount of server storage capacity that has been used.
Server utilization	Percentage of total available partition storage capacity that is used.
State	Current operational state of this partition. One of the following values: • ONLINE — The partition is functioning correctly. • MIGRATING — Transitional state that might or might not be due to normal operation. • OFFLINE — Transitional state that might or might not be due to normal operation. • READY — Transitional state that might or might not be due to normal operation.

Table 75 Server Details on the Node Information part of Server Management (continued)

Property	Description
	• RESTARTING — Transitional state that might or might not be due to normal operation.
Number of offline stripes	Total number of stripes on this partition that are offline due to media errors.
Number of transitioning stripes	Total number of stripes on this partition that are in a transitional state that might or might not be due to normal operation.
Properties	Various operating system properties (if known).
Values	Settings for operating system properties (if known).
Total bytes free in partitions	Disk free size from the OS level.
Total bytes used in partitions	Disk used size from the OS level.

Data Domain system information

The following table provides details on the Data Domain system properties on the Server Management tab.

Table 76 Data Domain system properties on the Server Management tab

Property	Description
Status indicators	One of the following values: • Online (green)—The Data Domain system is functioning correctly. • Offline (yellow)—The Data Domain system is offline. The *Data Domain Offline Diagnostics Suite User Guide*, which is available on Avamar Support, provides more information. • Read-Only (blue)—The Data Domain system is read-only. • Nonfunctional (red)—The Data Domain system is not functioning. The *Data Domain Offline Diagnostics Suite User Guide* provides more information.
IPv4 Hostname	IPv4 hostname of the Data Domain system as defined in corporate DNS.
IPv6 Hostname	IPv6 hostname of the Data Domain system as defined in corporate DNS.
Total Capacity (post-comp size)	The total capacity for compressed data on the Data Domain system.

Table 76 Data Domain system properties on the Server Management tab (continued)

Property	Description
Server Utilization (post-comp use%)	The percentage of capacity that is used on the Data Domain system for any reason after compression of the data.
Bytes Protected (client pre-comp size)	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 DDFS.
File System Used (post-comp used)	The total amount of disk space that is used in the DDFS for compressed data.
Username	The username of the Data Domain OpenStorage (OST) account that Avamar should use to access the Data Domain system for backups, restores, and replication, if applicable. This username is specified when you add the Data Domain system to the Avamar configuration.
Default Replication Storage System	Whether the Data Domain system is configured as default replication storage. This option is selected or cleared when you add the Data Domain system to the Avamar configuration.
Target For Avamar Checkpoint Backups	Indicate whether to store Avamar Checkpoint Backups on the Data Domain system or not.
Maximum Streams For Avamar Checkpoint Backups	The maximum number of reserved streams for Avamar CheckPoint Backup on Data Domain system.
Maximum Streams	The maximum number of Data Domain system streams that Avamar can use at any one time to perform backups and restores. This number is configured for the Data Domain system when you add the system to the Avamar configuration.
Maximum Streams Limit	The maximum number of Data Domain systems backup write streams.
Instant Access Limit	The amount limit of VMs that generated from Instant Access Restore.
DDOS Version	Version number of the Data Domain Operating System (DD OS) on the Data Domain system.
Serial Number	The manufacturer's serial number for the disk in the Data Domain system.
Model number	Model number of the Data Domain system.

Table 76 Data Domain system properties on the Server Management tab (continued)

Property	Description
Encryption Strength	The default global encryption strength of DDBoost clients on Data Domain system. The values are none, medium, and high.
Authentication Mode	The default global authentication mode of DDBoost clients on Data Domain system. The values are none, one-way, two-way, and anonymous.
Monitoring Status	Monitoring status of the Data Domain system. The *Avamar and Data Domain System Integration Guide* provides details on the available values.
Monitoring status details	When the monitoring status is a value other than OK, then additional information appears in a list below the **Monitoring Status** row. The following entries describe the available values. **Note** The *Avamar and Data Domain System Integration Guide* provides details on how to troubleshoot error conditions that result from each of these values. DD Boost licensing status, either: • DDBoost Licensed • DDBoost not Licensed DD Boost status, either: • DDBoost Enabled • DDBoost Disabled Whether the DD Boost user is enabled or disabled, either: • DDBoost User Enabled • DDBoost User Disabled DD Boost user status, either: • DDBoost User Valid • DDBoost User Changed DD Boost option status, either: • DDBoost Option Enabled • DDBoost Option Disabled • DDBoost Option not Available Status of the non-OST user, if configured, either:

Table 76 Data Domain system properties on the Server Management tab (continued)

Property	Description
	• Non-ost user state is Unknown • Non-ost user Invalid • Non-ost user disabled • Non-ost user is not an admin user **Note** The non-OST user row does not appear when a non-OST user has not been configured. SNMP status, either: • SNMP Enabled • SNMP Disabled Status of the Data Domain file system, either: • File System Running • File System Enabled • File System Disabled • File System Unknown • File system status unknown since SNMP is disabled Whether synchronization of maintenance operations, such as checkpoints, HFS checks, and Garbage Collection, between the Avamar server and the Data Domain system can occur, either: • Synchronization of maintenance operations is off. • Synchronization of maintenance operations is on.
Cloud Tier	The status of Cloud Tier. If enabled, display the Cloud Unit name, or display as disabled.

Event monitoring

All Avamar system activity and operational status is reported as events to the MCS. Examples of Avamar events include client registration and activation, successful and failed backups, and hard disk status.

Each event contains the information in the following table.

Table 77 Event information

Information	Description
Event code	Unique identifier

Table 77 Event information (continued)

Information	Description
Date and time	Date and time the event was reported
Category	Category of event: • SYSTEM • APPLICATION • USER • SECURITY
Type	Type of event: • INTERNAL • ERROR • WARNING • INFORMATION • DEBUG
Summary	A one-line summary description of the event
Hardware source	System node that reported the event
Software source	System or application module that reported the event

Event notifications

The following features generate notifications when specific events occur.

Pop-up alerts
You can configure individual events to generate a graphical pop-up alert each time the event occurs. Avamar Administrator must be running for the pop-up alerts to appear.

Acknowledgment required list
You can specify that when a certain event type occurs, the Avamar system administrator must acknowledge the event.

Email messages
You can specify that when a certain event type occurs, an email message is sent to a designated list of recipients. Email notifications can be sent immediately or in batches at scheduled times.

A typical batch email notification message looks like the following example.

Table 78 Example of a batch email notification message

```
MCS: avamar-1.example.com

   MCS Version: 7.1.0-nnn
   Avamar Server: avamar-1.example.com
   Avamar Server Version: 7.1.0-nnn

   Event profile: My Custom Profile
```

Table 78 Example of a batch email notification message (continued)

```
Count of events: 3

Summary of events:
Type
-----------
INFORMATION
INFORMATION
INFORMATION

Type           Code           Count          Summary
-----------    ------         ------         -------
INFORMATION    22207          1              New group
INFORMATION    22208          1              created
INFORMATION    22209          1              Group modified
                                             Group deleted

Event Code = 22207
Event Date/Time = 5/10/14 09:58:20 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = New group created
Software Source = MCS:CR

Event Code = 22209
Event Date/Time = 5/10/14 09:58:25 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = Group deleted
Software Source = MCS:CR

Event Code = 22208
Event Date/Time = 5/10/14 10:55:28 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = Group modified
Software Source = MCS:CR
```

Syslog support

You can specify that when an event type occurs, Avamar logs information to local or remote syslog files that are based on filtering rules that are configured for the syslog daemon that receives the events. Third-party monitoring tools and utilities capable of examining log entries can access the syslog files and process them to integrate Avamar event information into larger site activity and status reports.

SNMP support

The Avamar SNMP implementation provides two ways to access Avamar server events and activity completion status:

- SNMP requests provide a mechanism for SNMP management applications to "pull" information from a remote SNMP-enabled client (in this case, the Avamar server).
- SNMP traps provide a mechanism for the Avamar server to "push" information to SNMP management applications whenever designated Avamar events occur. You can configure an event type to output SNMP traps.

Usage intelligence
Enables the Avamar server to automatically collect and transfer reporting information to Avamar Support via the ESRS gateway.

Event profiles

Profiles are a notification management feature that is used to logically group certain event codes together and specify which notifications to generate when the events occur.

There are two basic types of event profiles:

- **System profile** — There is only one system event profile. It contains all possible system event codes.
- **Custom profiles** — Custom profiles are used to send various notifications when certain system events occur. You can create as many custom profiles as you should. This step is done to organize system events and generate notifications when any of those events occur.

Profile catalog

The Avamar system includes a set of preconfigured event profiles by default.

System profile
There is only one system event profile. It contains all possible system event codes.

Evaluation profile
The evaluation profile is primarily intended to be used to support system evaluations. If enabled, this profile generates an email notification and attaches 2 weeks' worth of Activities - DPN Summary report information to the email message. The *Avamar Reports Guide* provides more information about the Activities - DPN Summary report.

High Priority Events profile
The High Priority Events profile is enabled by default. This special event profile automatically email messages the following information to Avamar Support (`emailhome@avamar.com`) twice daily:

- Status of the daily data integrity check
- Selected Avamar server warnings and information messages
- Any Avamar server errors

The only change that you can make to the High Priority Events profile is to add email addresses to the Recipient Email List. If you require custom High Priority Events profile settings, copy the profile and then edit the copy.

Local SNMP Trap profile
The Local SNMP Trap profile is read-only and is intended to be used for test purposes only. The profile enables you to verify successfully generated traps and that the local `snmptrapd` process receives the traps, which then writes the trap information to a syslog file.

Local Syslog profile
If enabled, the Local Syslog profile reports status by way of the local `syslogd` process on the Avamar server.

Usage Intelligence profile
Enables the Avamar server to automatically collect and transfer reporting information to Avamar Support via the ESRS gateway.

Editing the system event profile

The system event profile contains all possible system event codes. You can edit the system event profile to control whether an event generates a pop-up alert in Avamar Administrator, an entry in the common unacknowledged events list, or neither.

Procedure

1. In Avamar Administrator, select **Tools** > **Manage Profiles**.

   The **Manage All Profiles** window is displayed.
2. Select **System Profile** in the left pane and click **Edit**.

   The **Edit Profile** dialog box appears with a list of event codes.
3. To show a graphical pop-up alert in Avamar Administrator each time an event occurs, select the **GUI Alert** checkbox next to the event.
4. To add an entry to the common unacknowledged events list each time that an event occurs, select the **Acknowledgement Required** checkbox.
5. Click **OK**.

Creating a custom event profile

Custom event profiles enable you to send notifications when specific system events occur.

You cannot view system events and profiles outside the domain that you are logged in to. This step affects the profiles that you can edit and the events that you can add to a profile.

Procedure

1. In Avamar Administrator, select **Tools** > **Manage Profiles**.

   The **Manage All Profiles** window is displayed.
2. In the left pane, select the domain for the custom event profile, and click **New**.

   The **New Profile** wizard appears.
3. In the **Profile Name** box, type a name for the event profile.
4. For **Profile Type**, leave the default setting of **Email, Syslog, and SNMP Trap Notification**.

   Note

   Because the Usage Intelligence feature uses the preconfigured Usage Intelligence profile, do not create a profile that is based on the Usage Intelligence profile type. This step results in redundant data being sent to Avamar Support.
5. Choose whether to enable or disable the profile by selecting or clearing the **Profile Enabled** checkbox.

6. Choose whether to enable email notifications for the profile by selecting or clearing the **Email Enabled** checkbox.
7. If you enabled email notifications, then specify whether to send email notifications as soon as events occur or on a scheduled basis:
   - To send email notifications as soon as events occur, select **Send data as events occur**.
   - To send email notifications on a scheduled basis, select **Send data on a schedule**, and then select the schedule from the list.
8. Choose whether to enable or disable syslog notification for the profile by selecting or clearing the **Syslog Notification – Enabled** checkbox.
9. Choose whether to enable or disable SNMP notification for the profile by selecting or clearing the **SNMP Trap Notification – Enabled** checkbox.
10. Click **Next**.

    The **Event Codes** page appears.
11. Click the **All Codes** tab, and then select the **Notify** checkbox next to the errors that should trigger notifications.

    NOTICE

    An asterisk (*) next to an event indicates an event of such severity that a notification is sent when that event occurs, even if other event notifications are sent on a schedule.

12. Click the **Audit Codes** tab, and then select the **Notify** checkbox next to the audit events that should trigger notifications.

    NOTICE

    An asterisk (*) next to an event code indicates an event of such severity that a notification is sent when that event occurs, even if other event notifications are sent on a schedule.

13. If you are adding this custom event profile at the top-level (that is, not to a domain or subdomain), specify the parameters to control capacity forecast alerts:
    a. Click the **Parameters** tab.
    b. Select the checkbox next to the parameter, and then type a new value for the parameter.
    c. Repeat the previous step as necessary for each parameter.
14. Click **Next**.

    The **Attachments** page appears.
15. (Optional) If the profile includes email notification messages, select the **Attach Server status in email (XML)** checkbox to include a report of overall Avamar server status in XML format in the messages.
16. (Optional) To include Avamar server logs in email notification messages, select the **Attach Server logs in email** checkbox and then type the full path to the location of Avamar server logs in the **Directory** box. The default location is `/usr/local/avamar/var/cron/`.

17. Specify the reports to include in email notification messages:
    a. Select the **Attach** checkbox next to the report to include.
    b. Select the checkbox next to the report for the file formats in which to send the report. You can select **XML**, **CSV**, or **TXT**.
    c. Specify the number of historical reports of this type to send with each notification message using the **Since Count** and **Since Unit** fields. For example, send the past 2 months of these reports.

       The following values are available from the **Since Count** list:

       - **day(s) ago**
       - **week(s) ago**
       - **month(s) ago**
       - **since last modified**

18. Click **Next**.

    The **Email Notification** page appears.

19. If the profile includes email notification messages, then specify the recipients and options for the email notification messages:
    a. In the **Email Subject Header** box, type an email subject line for the notification message.
    b. Add an email recipient to the list by typing a valid email address in the **Enter Recipient** box and then clicking **+**.
    c. (Optional) To remove a recipient from the **Recipient Email List**, select the recipient and click **-**.
    d. To insert all attachments into the body of the email notification message, select the **Inline attachments** checkbox.

       NOTICE

       When you insert the attachments, the email message may be very long.

    e. To immediately send a test email message, click **Send Email**.

       If the test email message is sent successfully, an `Email accepted by transport layer` confirmation message appears.

20. Click **Next**.

    The **Syslog Notification** page appears.

21. If the profile includes syslog notification messages, then specify the syslog notification parameters:
    a. In the **Address (IP or hostname)** box, type the IP address or hostname of the Avamar server node running the `syslogd` process.
    b. In the **Port Number** box, type the port number that is used for syslog communication.
    c. Choose whether to include extended event code information in the syslog message by selecting or clearing the **Include extended event data** checkbox.

       The extended information is delimited by using the following tags:

```
<Code>
<Type>
<Severity>
<Category>
<HwSource>
<Summary>
<active>
<lastEmailSendDate>
<domain>
<scheduleID>
<num_prefs>
<name>
<isSystem>
```

d. From the **Facility** list, select one of the following: **user**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, or **local7**.

e. To test the syslog notification parameters, click **Send Test Syslog Entry**.

22. Click **Next**.

    The **SNMP Trap Notification** page appears.

23. If the profile includes SNMP notification messages, then specify SNMP notification parameters:

    a. In the **SNMP Trap address (IP or hostname)** box, type the IP address or hostname of the computer running an application that can receive and process an SNMP trap.

    b. In the **Port Number** box, type the port number on the host server that is listening for SNMP traps. The default data port is 162.

    c. In the **SNMP Community** box, type the name of the SNMP community that the SNMP trap listener is configured to use.

    The SNMP community is a text string that the local Net-SNMP agent uses to authenticate itself with the SNMP management application.

    d. To test the SNMP notification parameters, click **Send Test SNMP Trap**.

24. Click **Finish**.

Editing a custom event profile

After you create a custom event profile for notifications of specific system events, you can edit any of the properties of the profile.

You cannot view system events and profiles outside the domain that you are logged in to. This step affects the profiles that you can edit and the events that you can add to a profile.

Procedure

1. In Avamar Administrator, select **Tools** > **Manage Profiles**.

   The **Manage All Profiles** window is displayed.

2. In the left pane, select the custom event profile and click **Edit**.

   The **Edit Profile** dialog box appears.

3. Edit the custom event profile. The properties are the same as when you create the profile.

4. Click **OK**.

Copying a custom event profile

You can create a custom event profile with the same properties as a profile that you already created by copying the profile. You can copy the profile to the same domain or to a different domain.

Procedure

1. In Avamar Administrator, select **Tools** > **Manage Profiles**.

   The **Manage All Profiles** window is displayed.
2. In the left pane, select the profile and click **Copy**.

   The **Save As** dialog box appears.
3. Type a name for the new custom event profile in the **Save As** box.
4. (Optional) To copy the new custom event profile to a different domain, click the **...** button, browse to the new domain, and then click **OK**.
5. Click **OK**.

Testing custom event profile notifications

You can test custom event profile notification mechanisms by sending a short email message or writing a short message to the syslog file.

Procedure

1. In Avamar Administrator, select **Tools** > **Manage Profiles**.

   The **Manage All Profiles** window is displayed.
2. In the left pane, select the custom event profile and click **Edit**.

   The **Edit Profile** dialog box appears.
3. Test the custom event profile:
   - To send a test email message, select the **Email Notification** tab and click **Send Email**.
   - To write a test message to the syslog file, select the **Syslog Notification** tab and click Send **Test Syslog Entry**.
   - To send a test SNMP trap message, select the **SNMP Trap Notification** tab and click **Send Test SNMP Trap**.

   If the test message is successfully sent, a confirmation message appears.
4. Click **OK**.
5. To close the **Edit Profile** dialog box, click **OK**.

Enabling and disabling a custom event profile

When you disable an event profile, no email notifications are sent until you reenable the profile. You can disable any profile except the system events profile.

Procedure

1. In Avamar Administrator, select **Tools** > **Manage Profiles**.

   The **Manage All Profiles** window is displayed.
2. In the left pane, select the event profile.

3. To disable the event profile, click **Disable**, or to enable the event profile, click**Enable**.

Deleting a custom event profile

You can permanently delete any custom event profile except the system events profile.

Procedure

1. In Avamar Administrator, select **Tools** > **Manage Profiles**.

   The **Manage All Profiles** window is displayed.
2. Select the event profile and click **Delete**.

   A confirmation message appears.
3. Click **Yes**.

Viewing events in the Event Monitor

Procedure

1. In Avamar Administrator, click the **Administration** launcher link.

   The **Administration** window is displayed.
2. Click the **Event Management** tab.
3. Click the **Event Monitor** tab near the bottom of the window.

   The Avamar Administrator online help provides details on each of the columns in the Event Monitor.
4. Select the display mode for the Event Monitor:
   - To display the most recent 5,000 system events for a defined range of dates, select **Query**.
   - To display the most recent 5,000 system events during the past 24 hours, select **Monitor**.
5. (Optional) Filter the events that appear in the Event Monitor:
   a. Open the **Actions** menu and select **Event Management** > **Filter**.

      The **Filter** dialog box appears.
   b. If you selected the **Query** display mode for the Event Monitor, select the range of dates for the events to display by using the **From Date** and **To Date** fields.
   c. From the **Category** list, select the category of events to display.
   d. From the **Type** list, select the type of events to display.
   e. From the **Severity** list, select the severity of the events to display.
   f. To view events for all domains, select **All Domains**. Or, to view events for a specific domain, select **Domain** and then browse to or type the domain name.
   g. To display only events that contain certain case-sensitive keywords in the event code data XML element, type the keyword in the **Data** box.

      This criterion promotes easy filtering on important keywords across event attributes. For example, filtering the Event Monitor on `error` returns all events that contain the word `error` in any XML attribute (for example, category, type, or severity).

h. Choose whether to display events from all sources, from only the Avamar server, from all Data Domain systems, or from a single Data Domain system:

- To view events from all sources, leave the default selection of **All Sources** in the **Source** list.
- To view events from only the Avamar server, select **Avamar** from the **Source** list.
- To view events from all Data Domain systems, select **Data Domain Systems** from the **Source** list and leave the default selection of **All Systems**.
- To view events from a single Data Domain system, select **Data Domain Systems** from the **Source** list, select the **System** option, and then either type or browse to the Data Domain system.

i. Click **More** to view additional filtering criteria.

j. To limit the Event Monitor to events with a certain event code, select **Only include codes** and then add and remove codes from the list. Or, to exclude events with a certain event code from the Event Monitor, select **Exclude codes** and then add and remove codes from the list.

k. Click **OK**.

Viewing the event catalog

A sequential listing of all event codes and summary information is available in `/usr/local/avamar/doc/event_catalog.txt` on the Avamar server. You can also view `event_catalog.txt` by using a web browser.

Procedure

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

   `https://`*`Avamar_server`*

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

   The **Avamar Web Restore** page appears.
2. Click **Documentation**.

   The **Avamar Documentation** page appears.
3. Click the plus icon next to **Avamar Event Codes**.
4. Click **event_catalog.txt**.

   The file opens in the web browser.

Acknowledging system events

System events that are configured to require acknowledgment each time they occur, remain in the unacknowledged events list until they are explicitly cleared, or acknowledged, by an Avamar server administrator.

Procedure

1. In Avamar Administrator, click the **Administration** launcher link.

   The **Administration** window is displayed.
2. Click the **Event Management** tab.
3. Click the **Unacknowledged Events** tab near the bottom of the window.

4. Acknowledge the events:
   - To acknowledge one or more events, select the event entries and select **Actions** > **Event Management** > **Acknowledge Unacknowledged Events**.
   - To acknowledge all events in the list, select **Actions** > **Event Management** > **Clear All Alerts**.

Customizing error events

By default, Avamar software continually monitors `/var/log/messages` for any occurrence of the case-insensitive search string `error`. Any occurrences of `error` create an event code of the type ERROR. You can customize this default behavior.

Procedure

1. Define additional case-insensitive search strings that also create Avamar ERROR events.
2. Add the search strings to `/usr/local/avamar/var/mc/server_data/adminlogpattern.xml`.

Log management

This section describes how to manage logs for Avamar.

Server monitoring with syslog

The syslog system logging feature on UNIX and Linux systems collects system log messages and writes them to a designated log file. You can configure the Avamar server to send event information in syslog format.

The Avamar server supports both syslog and syslog-ng implementations.

Note

Persons configuring syslog monitoring of an Avamar server should be familiar with basic syslog concepts. A complete discussion of basic syslog concepts and implementation is beyond the scope of this guide. The http://www.syslog.org website provides additional information.

At the operating system level, system monitoring and logging rely on the `syslogd` process to collect system log messages and write them to a designated log file. The `syslogd` process runs locally on every Avamar server node.

However, without additional configuration, each node's `syslogd` only collects system information for that node, and writes it to a local log file on that node. From a syslog perspective, each Avamar server node is unaware that any other server nodes exist. Also, the utility node syslog process is not aware that the Avamar Management Console Server (MCS) is collecting and logging Avamar event information.

You can configure an Avamar event profile to format Avamar server event messages in syslog format and send this data to the `syslogd` process running on the Avamar server utility node.

The following table describes how an event profile maps Avamar server event data to syslog fields.

Table 79 Mappings of syslog fields to Avamar event data

Field in syslog	Avamar event data
Facility	Either `User` or `Local#`, where # is a number from 0 to 7.
Priority	One of the following values, which are based on the Avamar event type: • `debug`, if the Avamar event type is DEBUG • `err`, if the Avamar event type is ERROR • `info`, if the Avamar event type is INFO • `none`, if the Avamar event type is INTERNAL • `warning`, if the Avamar event type is WARNING
Date	Avamar event date.
Time	Avamar event time.
Hardware source	Avamar event hardware source.
Software source	Avamar event software source.
Message	The following fields from the Avamar event code: • event code • category • summary • event data

Configuring local syslog

The most basic way to implement Avamar server syslog monitoring is to configure the MCS to output Avamar event information to the local `syslogd` process running on the utility node. The local `syslogd` service merges the Avamar event information with the operating system messages in a single local log file.

Procedure

1. Enable the Local Syslog event profile on the Avamar server:
   a. In Avamar Administrator, select **Tools** > **Manage Profiles**.
   b. Select the **Local Syslog** event profile in the left pane and click **Enable**.
2. On single-node servers and utility nodes with SLES 11 or later, configure the local utility node syslogd process to listen for MCS event messages on UDP data port 514:
   a. Open a command shell and log in as admin on the single-node server or the utility node of a multi-node server.
   b. Switch user to root by typing `su -`.

c. Open `/etc/syslog-ng/syslog-ng.conf` in a text editor.

d. Locate the following entry:

```
#
# uncomment to process log messages from network:
#
# udp(ip("0.0.0.0") port(514));
```

e. Add the following entry, including the comment:

```
#
# uncomment to process log messages from MCS:
#
udp(ip("0.0.0.0") port(514));
```

f. Save and close the file.

g. Restart the syslog process by typing the following command:

```
service syslog restart
```

h. Verify that syslog is listening on port 514 by typing the following command:

```
netstat -nap | grep 514
```

The following output appears in the command shell:

```
udp 0 0 127.0.0.1:514 127.0.0.1:* 8043/syslog-ng
```

Configuring remote syslog

Remote syslog monitoring includes the following:

- Configuring each server node to send syslog data to a remote logging host.
- Creating a custom syslog event profile that sends Avamar server event messages in syslog format to the remote logging host.

Sites that implement remote syslog monitoring of an Avamar server in most cases already have a remote logging host that is configured and deployed.

Many different syslog monitoring tools are available. Any syslog monitoring tool generally works with Avamar as long as it is configured to listen for remote syslog messages over a LAN connection on UDP data port 514.

NOTICE

For maximum security, implement remote syslog monitoring.

Procedure

1. Create a custom syslog event profile that sends Avamar server event messages in syslog format to the remote logging host.
2. Configure all server nodes to send syslog messages to the remote logging host.
3. Configure the remote logging host to listen for syslog messages over a LAN connection on UDP data port 514.
4. If a firewall is enabled on the remote logging host, configure the firewall to allow UDP traffic on port 514 for a defined IP range.

Creating a custom syslog event profile

Procedure

1. In Avamar Administrator, select **Tools** > **Manage Profiles**.

   The **Manage All Profiles** window is displayed.
2. Select the **Local Syslog** event profile in the left pane and click **Copy**.

   The **Save As** dialog box appears.
3. Type a name for the new custom event profile in the **Save As** field.
4. Leave the domain set to root (/). Custom syslog profiles must reside in the root domain.
5. Click **OK**.
6. In the **Manage All Profiles** dialog box, select the custom syslog event profile that you created and click **Edit**.

   The **Edit Profile** dialog box appears.
7. Select the **Syslog Notification** tab and specify syslog notification parameters:
   a. In the **Address (IP or hostname)** field, type the IP address or hostname of the remote logging host.
   b. In the **Port Number** field, leave the port number set to **514**.
   c. Select the **Include extended event data** option to include extended event code information in the syslog message.

      The extended information is delimited by using the following tags:

      ```
      <Code>
      <Type>
      <Severity>
      <Category>
      <HwSource>
      <Summary>
      <active>
      <lastEmailSendDate>
      <domain>
      <scheduleID>
      <num_prefs>
      <name>
      <isSystem>
      ```

   d. From the **Facility** list, select one of the following values: **user**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, or **local7**.
8. (Optional) To test the syslog notification parameters, click **Send Test Syslog Entry**.
9. Click **OK**.

Configuring server nodes to send syslog messages to the remote logging server

As part of the process to configure remote syslog, you must configure all Avamar server nodes to send syslog messages to a remote logging server over a LAN connection on UDP data port 514.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Open `/etc/syslog-ng/syslog-ng.conf` in a text editor.
3. Add the following entry:

   ```
   destination logserver {udp("ip_address" port(514)); };
   log { source(src); destination(logserver); };
   ```

   where *ip_address* is the IP address of the remote logging host.

4. Save and close the file.
5. Restart the syslog process by typing the following command:

   ```
   service syslog restart
   ```

6. On multi-node servers, repeat the previous steps for each node.

Configuring RHEL remote logging hosts running syslog

Procedure

1. Open a command shell and log in to the remote logging host as root.
2. Open `/etc/sysconfig/syslog` in a text editor.
3. Locate the following entry:

   ```
   SYSLOGD_OPTIONS="-m 0"
   ```

4. Add the `-r` parameter to the entry:

   ```
   SYSLOGD_OPTIONS="-r -m 0"
   ```

5. Save and close the file.
6. Restart the `syslogd` process by typing the following command:

   ```
   service syslog restart
   ```

Configuring SLES remote logging hosts running syslog-ng

Procedure

1. Open a command shell and log in to the remote logging host as root.

2. Open `/etc/syslog-ng/syslog-ng.conf` in a text editor.
3. Locate the following entry:

```
#
# uncomment to process log messages from network:
#
# udp(ip("0.0.0.0") port(514));
```

4. Uncomment the entry:

```
#
# uncomment to process log messages from network:
#
udp(ip("0.0.0.0") port(514));
```

5. Save and close the file.
6. Restart the syslog process by typing the following command:

```
service syslog restart
```

7. Verify that syslog is listening on port 514 by typing the following command:

```
netstat -nap | grep 514
```

The following output appears in the command shell:

```
udp 0 0 0.0.0.0:514 0.0.0.0:* 8043/syslog-ng
```

Configuring the firewall on the remote logging host

If a firewall is enabled on the remote logging host, configure the firewall to allow UDP traffic on port 514 for a defined IP range.

Procedure

1. Restrict the source IP addresses of the remote log messages in iptables or another firewall to avoid Denial Of Service (DOS) attacks on the remote logging host.

   The following example rule for iptables would allow client system logs for an IP address range of Avamar server nodes:

   ```
   # Rules to allow remote logging for syslog(-ng) on the log
   HOST system
   iptables -A INPUT -p udp -s 192.168.1.0/24 --dport 514 -j
   ACCEPT
   ```

   where *192.168.1.0/24* is in the IP address range of the Avamar server nodes.

   The following example rule for iptables specifies the IP address for each Avamar server node on a single line and includes the Mac address of the Network Interface Card (NIC) for the node:

   ```
   iptables -A INPUT -p udp -s 192.168.1.12 -m mac --mac-
   source 00:50:8D:FD:E6:32 --dport 514 -j ACCEPT
   iptables -A INPUT -p udp -s 192.168.1.13 -m mac --mac-
   source 00:50:8D:FD:E6:33 --dport 514 -j ACCEPT
   iptables -A INPUT -p udp -s 192.168.1.14 -m mac --mac-
   source 00:50:8D:FD:E6:34 --dport 514 -j ACCEPT
   iptables -A INPUT -p udp -s 192.168.1.15 -m mac --mac-
   source 00:50:8D:FD:E6:35 --dport 514 -j ACCEPT
   ```

```
...
```

No rules are necessary for the outgoing syslog traffic on the client side.

2. Restart the firewall service on the remote logging host for the changes to take effect.
3. Restart the `syslog-ng` service on all server nodes and the remote logging host for the changes to take effect:

   ```
   service syslog restart
   ```

Server monitoring with SNMP

Simple Network Management Protocol (SNMP) is a protocol for communicating and monitoring event notification information between an application, hardware device, or software application and any number of monitoring applications or devices.

Note

Persons configuring an Avamar server to send event information over SNMP should be familiar with basic SNMP concepts. A complete discussion of basic SNMP concepts and implementation is beyond the scope of this guide. The http://www.net-snmp.org website provides additional information.

The Avamar www.net-snmp.orgSNMP implementation provides SNMP requests and SNMP traps to access Avamar server events and activity status. The Avamar server supports SNMP versions v1 and v2c.

SNMP requests

SNMP requests provide a mechanism for SNMP management applications to "pull" information from a remote SNMP-enabled application or device (in this case, the Avamar server). The SNMP management application sends a request to an SNMP master agent running on the Avamar server. The SNMP master agent then communicates with the Avamar SNMP sub-agent, which passes the request to the MCS. The MCS retrieves the data and sends it back to the Avamar SNMP sub-agent, which passes it back to the management application by way of the SNMP master agent. Data port 161 is the default data port for SNMP requests.

Avamar servers that are purchased directly from Avamar use the Net-SNMP master agent. Avamar servers that are built with other industry standard hardware likely use an SNMP master agent that is provided by the hardware manufacturer.

SNMP traps

SNMP traps provide a mechanism for the Avamar server to "push" information to SNMP management applications when designated Avamar events occur. Data port 162 is the default data port for SNMP traps. Typically, the SNMP management application listens for the SNMP traps that designated remote hosts generate.

Configuring server monitoring with SNMP

Procedure

1. To enable an SNMP management application to monitor an Avamar server, load the Avamar Management Information Base (MIB) definition file (`AVAMAR-MCS-MIB.txt`) into the master MIB used by the SNMP management application.

   The MIB contains definitions of the information that can be monitored or which traps are sent for each SNMP application or device.

   The following table provides the locations for the Avamar MIB definition file.

Table 80 Locations for the Avamar MIB definition file

Computer type	MIB location
Single-node server	`/usr/local/avamar/doc`
Multi-node server	`/usr/local/avamar/doc` on the utility node
Computer with Avamar Administrator	*`install_dir`*`/doc`, where *install_dir* is typically: • `C:\Program Files\avs\administrator` on Microsoft Windows computers • `/usr/local/avamar` on Linux computers • `/opt/AVMRconsl` on Solaris computers

A copy of the Avamar MIB definition file also resides in the `/usr/share/snmp/mibs` directory on single-node servers and utility nodes. This copy is used by the Avamar SNMP sub-agent and should not be moved or distributed.

2. Configure the Net-SNMP agent. Configuring the Net-SNMP agent on page 184 provides instructions.
3. Configure a custom event profile to output designated Avamar server events to an SNMP trap. Creating a custom event profile for an SNMP trap on page 186 provides instructions.

Configuring the Net-SNMP agent

The `avsetup_snmp` command line utility configures the Net-SNMP agent to communicate with the Avamar server by using the Avamar SNMP sub-agent.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Type the following commands to launch the utility:

   ```
   cd /root
   avsetup_snmp
   ```

   The output prompts you to specify the port on which to listen for SNMP requests.
3. Specify the SNMP request data port:

- To use port 161, the default SNMP request data port, press **Enter**.
- To use a different SNMP request data port, type the data port number and press **Enter**.

If `avsetup_snmp` was not able to detect any SNMP communities, the output prompts you to specify whether to allow SNMPv3 read-write user based access.

4. Type **n** and press **Enter**.

   The output prompts you to specify whether to allow SNMPv3 read-only user based access.

5. Type **n** and press **Enter**.

   The output prompts you to specify whether to allow SNMPv1/v2c read-write community access.

6. Type **n** and press **Enter**.

   The output prompts you to specify whether to allow SNMPv1/v2c read-only community access.

7. To accept the default value of **y**, press **Enter**.

   The output prompts you to specify the community name to which to add read-only access. The SNMP community is a text string that the local Net-SNMP agent uses to authenticate itself with the SNMP management application.

8. Type the SNMP community name and press **Enter**.

   The output prompts you to specify the hostname or network address from which to accept this community name.

9. To accept the community name from all hostnames or network addresses, press **Enter**.

   The output prompts you to specify the OID to which this community should be restricted.

10. To specify no restriction, press **Enter**.

    The output prompts you to specify whether to configure another community.

11. Type **n** and press **Enter**.

    The output indicates that `/etc/snmp/snmpd.conf` was created and run to configure the system_setup group. Then the output prompts you to specify the location of the system.

12. Type the physical location of the Avamar server and press **Enter**.

    The output prompts you to specify contact information.

13. Type contact information (for example, email address, telephone extension) and press **Enter**.

    The output prompts you to specify whether to correctly set the value of the sysServices.0 OID.

14. Type **n** and press **Enter**.

    The output indicates that `/etc/snmp/snmpd.conf` was installed and that `snmpd` was enabled.

Creating a custom event profile for an SNMP trap

As part of the process of configuring server monitoring with SNMP, create a custom event profile to output designated Avamar server events to an SNMP trap.

The default Avamar configuration includes a **Local SNMP Trap** profile that outputs Avamar server event messages to the local Net-SNMP trap listener (`snmptrapd` process). However, you cannot edit the Local SNMP Trap profile. The profile is intended to be used for test purposes only, to verify that the local `snmptrapd` process can successfully generate and receive the traps. The process then writes the trap information to a syslog file. Usually, the next step is to configure another custom profile to send Avamar SNMP traps to a remote Net-SNMP trap listener.

Procedure

1. Create a custom event profile by using the steps in Creating a custom event profile on page 170.

   On the first page of the **New Profile** wizard, select the option to enable SNMP trap notification.
2. Continue through the wizard until the **SNMP Trap Notification** page appears.
3. In the **SNMP Trap Address (IP or hostname)** box, type the IP address or hostname of a computer with an application capable of receiving and processing an SNMP trap.
4. In the **Port Number** box, type the port number on the host computer that listens for SNMP traps.
5. In the **SNMP Community** box, type the name of the SNMP community that the SNMP trap listener is configured to use.
6. (Optional) To test the SNMP notification parameters, click **Send Test SNMP Trap**.
7. Click **Finish**.

Logging format

This section describes Avamar logging formats.

Monitoring server status

Avamar systems provide monitoring of several items on the Avamar server.

You can monitor the status of the following items on the Avamar server:

- Overall Avamar server status
- Capacity usage
- Modules
- Nodes
- Partitions
- Checkpoints
- Garbage collection
- Maintenance activities

If you use a Data Domain system as storage for Avamar client backups, you also can monitor CPU, disk activity, and network activity for each node on the Data Domain system.

This status information is provided on the tabs in the Avamar Server window in Avamar Administrator. The *Avamar Administration Guide* provides details on how to access the Avamar Server window and the information available on each tab.

Monitoring system events

All Avamar system activity and operational status is reported as various events to the MCS. Examples of various Avamar events include client registration and activation, successful and failed backups, hard disk status, and others.

Events are listed in the Event Management tab in the Administration window of Avamar Administrator. The *Avamar Administration Guide* provides details on how to access the Event Management tab and filter the events that appear in the tab.

You can also configure Avamar to notify you when events occur. There are several features and functions available.

Pop-up alerts
Events can be configured on an event-by-event basis to generate a graphical pop-up alert each time one of these events occurs. One significant limitation of this feature is that Avamar Administrator software must be running in order for the pop-up alerts to be displayed.

Acknowledgment required list
Events can be configured on an event-by-event basis such that when events of this type occur, an entry is added to a list of events that requires interactive acknowledgment by the Avamar system administrator.

Email messages
Events can be configured on an event-by-event basis to send an email message to a designated list of recipients. Email notifications can be sent immediately or in batches at regularly scheduled times.

Syslog support
Events can be configured on an event-by-event basis to log information to local or remote syslog files that are based on filtering rules that are configured for the syslog daemon receiving the events.

Third-party monitoring tools and utilities capable of examining log entries can access the syslog files and process them to integrate Avamar event information into larger site activity and status reports.

NOTICE

For maximum security, we recommend implementing remote syslog monitoring as described in the *Avamar Administration Guide*.

SNMP support
Simple Network Management Protocol (SNMP) is a protocol for communicating monitoring and event notification information between an application, hardware device or software application, and any number of monitoring applications or devices.

The Avamar SNMP implementation provides two distinct ways to access Avamar server events and activity completion status:

- SNMP requests provide a mechanism for SNMP management applications to "pull" information from a remote SNMP-enabled client (in this case, the Avamar server).
- SNMP traps provide a mechanism for the Avamar server to "push" information to SNMP management applications whenever designated Avamar events occur. Events can be configured on an event-by-event basis to output SNMP traps.

Avamar also can collect and display data for health monitoring, system alerts, and capacity reporting on a configured Data Domain system by using SNMP. The *Avamar and Data Domain System Integration Guide* provides details on how to configure SNMP for Avamar with Data Domain.

ConnectEMC support
Events can be configured on an event-by-event basis to send a notification message directly to Customer Support using ConnectEMC.

The *Avamar Administration Guide* provides details on how to configure each of these notification mechanisms.

Email home notification

Avamar systems provide an email home feature.

When fully configured and enabled, the email home feature automatically emails the following information to Avamar Customer Support twice daily:

- Status of the daily data integrity check
- Selected Avamar server warnings and information messages
- Any Avamar server errors
- Any RAID errors (single-node servers only)

By default, these email messages are sent at 6 a.m. and 3 p.m. each day (based on the local time on the Avamar server). The timing of these messages is controlled by the Notification Schedule.

The*Avamar Administration Guide* provides details on how to enable and schedule the email home feature.

Auditing

The Avamar Audit Log provides details on the operations that users start in the Avamar system.

The data in this log allows enterprises that deploy Avamar to enforce security policies, detect security breaches or deviation from policies, and hold appropriate users accountable for those actions. The audit log includes the following information for each operation:

- The date and time the action occurred
- The event code number that is associated with the action
- The ID and role of the user that started the action
- The product and component from which the action was started
- The severity of the action
- The domain in which the action occurred

The Audit Log is available in Avamar Administrator as a subtab of the Event Management tab in the Administration window. The Avamar Administration Guide

provides details on how to access the Audit Log and filter the events that appear in the log.

Gen4 and later Avamar Data Stores running the SUSE Linux Enterprise Server (SLES) operating system implement improved auditing features, such as Advanced Intrusion Detection Environment (AIDE) and the `auditd` service.

Server monitoring with syslog

The syslog system logging feature on UNIX and Linux systems collects system log messages and writes them to a designated log file. You can configure the Avamar server to send event information in syslog format.

The Avamar server supports both syslog and syslog-ng implementations.

Note

Persons configuring syslog monitoring of an Avamar server should be familiar with basic syslog concepts. A complete discussion of basic syslog concepts and implementation is beyond the scope of this guide. The http://www.syslog.org website provides additional information.

At the operating system level, system monitoring and logging rely on the `syslogd` process to collect system log messages and write them to a designated log file. The `syslogd` process runs locally on every Avamar server node.

However, without additional configuration, each node's `syslogd` only collects system information for that node, and writes it to a local log file on that node. From a syslog perspective, each Avamar server node is unaware that any other server nodes exist. Also, the utility node syslog process is not aware that the Avamar Management Console Server (MCS) is collecting and logging Avamar event information.

You can configure an Avamar event profile to format Avamar server event messages in syslog format and send this data to the `syslogd` process running on the Avamar server utility node.

The following table describes how an event profile maps Avamar server event data to syslog fields.

Table 81 Mappings of syslog fields to Avamar event data

Field in syslog	Avamar event data
Facility	Either `User` or `Local#`, where # is a number from 0 to 7.
Priority	One of the following values, which are based on the Avamar event type: • `debug`, if the Avamar event type is DEBUG • `err`, if the Avamar event type is ERROR • `info`, if the Avamar event type is INFO • `none`, if the Avamar event type is INTERNAL • `warning`, if the Avamar event type is WARNING

Table 81 Mappings of syslog fields to Avamar event data (continued)

Field in syslog	Avamar event data
Date	Avamar event date.
Time	Avamar event time.
Hardware source	Avamar event hardware source.
Software source	Avamar event software source.
Message	The following fields from the Avamar event code: • event code • category • summary • event data

Alerting

This section describes Avamar features and options for generating alerts.

Additionally, Avamar components send alerts to Dell EMC via Secure Remote Services (ESRS).

Server monitoring with SNMP

Simple Network Management Protocol (SNMP) is a protocol for communicating and monitoring event notification information between an application, hardware device, or software application and any number of monitoring applications or devices.

Note

Persons configuring an Avamar server to send event information over SNMP should be familiar with basic SNMP concepts. A complete discussion of basic SNMP concepts and implementation is beyond the scope of this guide. The http://www.net-snmp.org website provides additional information.

The Avamar www.net-snmp.orgSNMP implementation provides SNMP requests and SNMP traps to access Avamar server events and activity status. The Avamar server supports SNMP versions v1 and v2c.

SNMP requests

SNMP requests provide a mechanism for SNMP management applications to “pull” information from a remote SNMP-enabled application or device (in this case, the Avamar server). The SNMP management application sends a request to an SNMP master agent running on the Avamar server. The SNMP master agent then communicates with the Avamar SNMP sub-agent, which passes the request to the MCS. The MCS retrieves the data and sends it back to the Avamar SNMP sub-agent, which passes it back to the management application by way of the SNMP master agent. Data port 161 is the default data port for SNMP requests.

Avamar servers that are purchased directly from Avamar use the Net-SNMP master agent. Avamar servers that are built with other industry standard hardware likely use an SNMP master agent that is provided by the hardware manufacturer.

SNMP traps

SNMP traps provide a mechanism for the Avamar server to "push" information to SNMP management applications when designated Avamar events occur. Data port 162 is the default data port for SNMP traps. Typically, the SNMP management application listens for the SNMP traps that designated remote hosts generate.

Configuring server monitoring with SNMP

Procedure

1. To enable an SNMP management application to monitor an Avamar server, load the Avamar Management Information Base (MIB) definition file (`AVAMAR-MCS-MIB.txt`) into the master MIB used by the SNMP management application.

   The MIB contains definitions of the information that can be monitored or which traps are sent for each SNMP application or device.

   The following table provides the locations for the Avamar MIB definition file.

   Table 82 Locations for the Avamar MIB definition file

Computer type	MIB location
Single-node server	`/usr/local/avamar/doc`
Multi-node server	`/usr/local/avamar/doc` on the utility node
Computer with Avamar Administrator	*`install_dir`*`/doc`, where *install_dir* is typically: • `C:\Program Files\avs\administrator` on Microsoft Windows computers • `/usr/local/avamar` on Linux computers • `/opt/AVMRconsl` on Solaris computers

   A copy of the Avamar MIB definition file also resides in the `/usr/share/snmp/mibs` directory on single-node servers and utility nodes. This copy is used by the Avamar SNMP sub-agent and should not be moved or distributed.

2. Configure the Net-SNMP agent. Configuring the Net-SNMP agent on page 184 provides instructions.
3. Configure a custom event profile to output designated Avamar server events to an SNMP trap. Creating a custom event profile for an SNMP trap on page 186 provides instructions.

Configuring the Net-SNMP agent

The `avsetup_snmp` command line utility configures the Net-SNMP agent to communicate with the Avamar server by using the Avamar SNMP sub-agent.

Procedure

1. Open a command shell:

a. Log in to the server as admin.

b. Switch user to root by typing the following command:

```
su -
```

c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Type the following commands to launch the utility:

```
cd /root
avsetup_snmp
```

The output prompts you to specify the port on which to listen for SNMP requests.

3. Specify the SNMP request data port:
   - To use port 161, the default SNMP request data port, press **Enter**.
   - To use a different SNMP request data port, type the data port number and press **Enter**.

   If `avsetup_snmp` was not able to detect any SNMP communities, the output prompts you to specify whether to allow SNMPv3 read-write user based access.

4. Type **n** and press **Enter**.

   The output prompts you to specify whether to allow SNMPv3 read-only user based access.

5. Type **n** and press **Enter**.

   The output prompts you to specify whether to allow SNMPv1/v2c read-write community access.

6. Type **n** and press **Enter**.

   The output prompts you to specify whether to allow SNMPv1/v2c read-only community access.

7. To accept the default value of **y**, press **Enter**.

   The output prompts you to specify the community name to which to add read-only access. The SNMP community is a text string that the local Net-SNMP agent uses to authenticate itself with the SNMP management application.

8. Type the SNMP community name and press **Enter**.

   The output prompts you to specify the hostname or network address from which to accept this community name.

9. To accept the community name from all hostnames or network addresses, press **Enter**.

   The output prompts you to specify the OID to which this community should be restricted.

10. To specify no restriction, press **Enter**.

    The output prompts you to specify whether to configure another community.

11. Type **n** and press **Enter**.

    The output indicates that `/etc/snmp/snmpd.conf` was created and run to configure the system_setup group. Then the output prompts you to specify the location of the system.

12. Type the physical location of the Avamar server and press **Enter**.

    The output prompts you to specify contact information.

13. Type contact information (for example, email address, telephone extension) and press **Enter**.

    The output prompts you to specify whether to correctly set the value of the sysServices.0 OID.

14. Type **n** and press **Enter**.

    The output indicates that `/etc/snmp/snmpd.conf` was installed and that `snmpd` was enabled.

Creating a custom event profile for an SNMP trap

As part of the process of configuring server monitoring with SNMP, create a custom event profile to output designated Avamar server events to an SNMP trap.

The default Avamar configuration includes a **Local SNMP Trap** profile that outputs Avamar server event messages to the local Net-SNMP trap listener (`snmptrapd` process). However, you cannot edit the Local SNMP Trap profile. The profile is intended to be used for test purposes only, to verify that the local `snmptrapd` process can successfully generate and receive the traps. The process then writes the trap information to a syslog file. Usually, the next step is to configure another custom profile to send Avamar SNMP traps to a remote Net-SNMP trap listener.

Procedure

1. Create a custom event profile by using the steps in Creating a custom event profile on page 170.

   On the first page of the **New Profile** wizard, select the option to enable SNMP trap notification.

2. Continue through the wizard until the **SNMP Trap Notification** page appears.
3. In the **SNMP Trap Address (IP or hostname)** box, type the IP address or hostname of a computer with an application capable of receiving and processing an SNMP trap.
4. In the **Port Number** box, type the port number on the host computer that listens for SNMP traps.
5. In the **SNMP Community** box, type the name of the SNMP community that the SNMP trap listener is configured to use.
6. (Optional) To test the SNMP notification parameters, click **Send Test SNMP Trap**.
7. Click **Finish**.

Automatic notifications to Avamar Support

The Email Home and ConnectEMC feature automatically send notifications to Avamar Support. These notifications include alerts for high priority events and daily reports to facilitate monitoring the Avamar server.

Usage Intelligence

Usage Intelligence is a feature that enables the Avamar server to automatically collect and transfer reporting information to Avamar Support. The types of reports that are sent to Avamar Support vary depending on how the Avamar server is licensed.

The use of this feature requires that:

- ESRS gateway is installed and deployed in the local environment.
- You have the credentials to authorize registration with ESRS.

Installing and activating the ESRS license

To use Avamar with ESRS, you must have an Avamar license key file that includes ESRS licensing.

contains information about how to install and activate an Avamar license key file.

Importing the ESRS Gateway certificate to the Avamar server's keystore

Before registering the Avamar server with the ESRS Gateway, you must import the ESRS Gateway certificate to the Avamar server's keystore.

Procedure

1. Export the ESRS Gateway certificate:
   a. Point a browser at https://*esrs_gateway*:9443

      where *esrs_gateway* is the hostname or IP address of the local ESRS gateway.

   b. Use the browser's functionality to export the certificate.

      For example, in Internet Explorer 11:

      a. Click the lock icon in the URL field and select **View Certificates**.
      b. Click the **Details** tab.
      c. Click **Copy to File** and complete the steps in the **Certificate Export Wizard**.

2. Copy the exported certificate to a temporary location on the Avamar server.
3. 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.
4. Switch user to root by typing the following command:

   ```
   su -
   ```

5. Back up the keystore by typing the following command on one line:

   ```
   cp -p /usr/local/avamar/lib/rmi_ssl_keystore /usr/local/
   avamar/lib/rmi_ssl_keystore.bak
   ```

6. Import the ESRS server certificate into the keystore by typing the following command on one line:

   ```
   keytool -importcert -keystore /usr/local/avamar/lib/
   rmi_ssl_keystore -storepass changeme -file <certfile>.crt
   ```

   where *<certfile>* is the name of the ESRS server certificate, including path.

7. Restart the MCS by typing the following command:

   ```
   mcserver.sh --restart
   ```

Registering Avamar with ESRS

To enable the Usage Intelligence feature, you must register the Avamar server with ESRS.

Procedure

1. In Avamar Administrator, select **Tools** > **Manage ESRS**.

   The **Edit ESRS Gateaway Information** window appears.
2. Type the IP address of the ESRS gateway in the **ESRS Gateway** field.
3. Type the port number of the ESRS gateway in the **Port** field.
4. Type the username and password of the ESRS gateway user with permissions to register to the gateway.
5. Click **Register**.
6. A message window indicates that the registration was successful. Click **OK** to clear.

Results

Once the Avamar server has been registered with the ESRS gateway, no further configuration of the Usage Intelligence feature is required.

Email Home

The Avamar Email Home feature automatically sends configuration, capacity, and general system information to Avamar Support once daily, and provides critical alerts in near-real time as needed.

By default, notification schedule email messages are sent at 6 a.m. and 3 p.m. each day. The Notification Schedule controls the timing of these messages.

Editing Email Home mail settings

Email Home is configured and enabled during Avamar server installation. You can edit the mail settings for Email Home after the installation.

Procedure

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 the following command:

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

2. Change directories by typing the following command:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

3. Open `mcserver.xml` in a UNIX text editor.
4. Find the `com.avamar.asn.module.mail` node.

   The `com.avamar.asn.module.mail` node contains the `smtpHost` and `admin_mail_sender_address` entries.

5. Verify that the value for the `smtpHost` entry is the DNS name of the outgoing SMTP mail server that is used to send Email Home messages, such as `smtp.example.com`.

   If the value for the entry is incorrect, edit the value.

   NOTICE

   The Avamar server installation or upgrade automatically completes the value for the `smtpHost` entry. In most cases, some arrangement must be made to enable email messages originating from the Avamar server to be forwarded through the outgoing SMTP mail server to Avamar Support over the Internet.

6. Specify a valid email address with access to a corporate outgoing SMTP mail server as the value for the `admin_mail_sender_address` entry.

   NOTICE

   If you do not configure the Email Home feature to send messages from a valid email address, the incoming email server rejects messages that are generated by the Email Home feature. Avamar Support is completely unaware that these programmatically generated messages were rejected. In addition, because a valid sending email account is not known, programmatically generated warnings to the sender that these messages could not be sent are never viewed by anyone who can correct the problem.

7. Save the changes and close the file.
8. Restart the MCS by typing the following commands:

   ```
   dpnctl stop mcs
   dpnctl start
   ```

9. Close the command shell.

ConnectEMC

ConnectEMC is a program that runs on the Avamar server and sends information to Avamar Support. ConnectEMC is typically configured to send alerts for high priority events as they occur, as well as reports once daily.

ConnectEMC is integrated with EMC Secure Remote Support (ESRS), provided that it is installed, operational, and network accessible by the Avamar server. Contact the Avamar Sales Representative for more information about implementing ESRS.

Although ConnectEMC is initially configured during Avamar server software installation, Avamar Administrator enables you to manage ConnectEMC settings, in the form of three user-configurable transports, after the server is operational:

- Primary transport
- Failover transport
- Notification transport

The primary and failover transports send alerts for high priority events as they occur. The primary transport is used unless it fails, at which time the failover transport is used.

The notification transport sends email notifications messages to one or more customer email addresses under certain conditions.

You also can control whether the MCS generates and sends ConnectEMC messages by enabling, disabling, stopping, and starting ConnectEMC.

Enabling and disabling ConnectEMC

Disabling ConnectEMC causes the MCS to stop generating ConnectEMC messages until ConnectEMC is reenabled. To allow the MCS to continue generating ConnectEMC messages but to queue the messages, stop ConnectEMC.

Procedure

1. In Avamar Administrator, select **Tools** > **Manage ConnectEMC**.

   The **Manage ConnectEMC** window is displayed.
2. Specify whether the MCS generates and sends ConnectEMC messages:
   - To stop the MCS from generating messages, click **Disable**.
   - To restart the generation of messages, click **Enable**.
   - To continue generating messages but queue the messages, click **Stop**.
   - To start sending the messages, click **Start**.

   If you disable ConnectEMC, you are prompted to type a password.
3. Type a valid password and click **OK**.

Editing the primary and failover transports

Procedure

1. In Avamar Administrator, select **Tools** > **Manage ConnectEMC**.

   The **Manage ConnectEMC** window is displayed.
2. Select either **Primary Transport** or **Failover Transport** in the left pane, and click **Edit**.

   The **Edit Primary/Secondary Transport** dialog box appears.
3. Select the transport type from the **Transport Type** list:
   - **Email**
   - **FTP**
   - **HTTPS**

   Note

   An operational Secure Remote Support gateway is required to use the FTP or HTTPS transport types.
4. (Email only) After selecting **Email**, complete the following steps.

a. In the **SMTP Host (Email Server)** field, specify the mail server hostname or IPv4 address.

b. In the **Email Address** field, specify one or more recipients of these email messages. Separate multiple email addresses with commas.

c. In the **Email Sender Address** field, specify the email address from which to send the message.

d. (Optional) To configure advanced settings, click **Advanced**, and then specify the following settings in the **Edit Advanced Email Settings** dialog box:

- **Retries** – The number of retries to perform before reporting a failure. The default setting is five retries.
- **Timeout** – The number of seconds to wait before reporting that the operation timed out. The default setting is 5 minutes (300 s).
- **Description** – A description of this transport that appears in the **Manage ConnectEMC** window. The default description is `Email Transport`.
- **Email Subject** – The subject line in the email. The default subject line is `Avamar ConnectEMC Notification Email`.

  Do not change the email subject unless instructed to do so by Avamar Support. Avamar spam filters can reject email messages with other subject lines.

e. Click **OK**.

5. (FTP only) After selecting **FTP**, complete the following steps.

a. In the **IP Address** field, specify an IPv4 address.

b. In the **Username** field, specify an FTP username. The setting depends on the FTP server software.

c. In the **Password** field, specify the password for the username.

d. (Optional) To configure advanced settings, click **Advanced**, and then specify the following settings in the **Edit Advanced FTP Settings** dialog box:

- **Retries** – The number of retries to perform before reporting a failure. The default setting is five retries.
- **Timeout** – The number of seconds to wait before reporting that the operation timed out. The default setting is 5 minutes (300 s).
- **Description** – A description of this transport that appears in the **Manage ConnectEMC** window. The default description is `FTP Transport`.
- **FEP Folder** – A unique customer UNIX path in the ConnectEMC Front End Processor (FEP). Use the folder location that is supplied by Avamar Support.
- **FTP Port** – An IP port. The default setting is port 21.
- **Mode** – Either Active or Passive. The default setting is Active.

  Do not change the email subject unless instructed to do so by Avamar Support. Avamar spam filters can reject email messages with other subject lines.

e. Click **OK**.

6. (HTTPS only) After selecting **HTTPS**, complete the following steps.
   a. Type a valid URL for the Secure Remote Support home page in the **URL** field.

      Valid URLs use the following format:

      `https://home_name[:port]/target_directory`

      where *home_name*, *port*, and *target_directory* are the home name, data port, and target directory, respectively.

      Use the URL provided by Avamar Support.

   b. (Optional) To configure advanced settings, click **Advanced**, and then specify the following settings in the **Edit Advanced HTTPS Settings** dialog box:
      - **Retries** – The number of retries to perform before reporting a failure. The default setting is five retries.
      - **Timeout** – The number of seconds to wait before reporting that the operation timed out. The default setting is 5 minutes (300 s).
      - **Private Key Pass Phrase** – The passphrase that is associated with the private key file.
      - **Private Key File** – The file name of the private key file.
      - **Client Certificate** – The client certificate to use. The default setting is "Default," which uses the certificate that the MCS uses. Otherwise, type the file name of the client certificate.
      - **Server CA Bundle** – File containing a list of root certificates.
      - **Verify Server Name** – Whether to verify the server name. Either Yes or No. The default setting is No.

   c. Click **OK**.

   Sample key files are provided in `/opt/connectemc/certs/` and `https-privatekey.pem`. Sample client certificates are provided in `/opt/connectemc/certs/` and `https-cert.pem`. Sample root certificate bundles are provided in `/opt/connectemc/certs/` and `https-ca-cert.pem`.
7. Click **OK** on the **Edit Primary/Secondary Transport** dialog box.

Editing the notification transport

Procedure

1. In Avamar Administrator, select **Tools** > **Manage ConnectEMC**.

   The **Manage ConnectEMC** window is displayed.
2. Select **Notification Transport** and click **Edit**.

   The **Edit Notification Transport** dialog box appears.
3. From the **Notification Type** list, select one of the following types:
   - **On Success** — Notify recipients when an event file is successfully transferred to EMC.
   - **On Failure** — Notify recipients when an event file is not successfully transferred to EMC.
   - **On Success or Failure** — Notify recipients when an attempt is made to transfer an event file to EMC, regardless of the outcome.

- **On All Failure** — Notify recipients when all attempts to transfer an event file to EMC have failed.

4. In the **SMTP Host (Email Server)** box, type the mail server hostname or IPv4 address.
5. In the **Email Address** box, type one or more recipients of these email messages. Separate multiple email addresses with commas.
6. In the **Email Sender Address** box, type the email address from which the notification is sent.
7. (Optional) To specify advanced settings, click **Advanced** and then specify the settings in the **Edit Advanced Email Settings** dialog box:
   a. In the **Retries** box, specify the number of retries to attempt before reporting a failure. The default setting is five retries.
   b. In the **Timeout** box, specify the number of seconds to wait before reporting that the operation timed out. The default setting is 300 s (5 minutes).
   c. In the **Description** box, specify the description of this transport that appears in the **Manage ConnectEMC** window. The default description is `Email Transport`.
   d. In the **Email Subject** box, specify the subject line for the email. The default subject line is `Avamar ConnectEMC Notification Email`.

      NOTICE

      Do not change the email subject unless instructed to do so by Avamar Support. EMC spam filters may reject email messages with other subject lines.

   e. From the **Email Format** list, select the format of the email, either ASCII or HTML. The default setting is ASCII.
   f. Choose whether to include attachments that are sent to ConnectEMC in the notification email message by selecting or clearing the **Include CallHome Data** checkbox.
   g. Click **OK**.
8. On the **Edit Notification Transport** dialog box, click **OK**.

Editing the site name

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing:

      ```
      su -
      ```

2. Type the following commands to launch the utility and change the site name:

   ```
   cd /root
   ```

   ```
   avsetup_ connectemc.pl --site_name=site_name
   ```

   Where *site_name* is the name of the customer site.

3. Disable and then enable ConnectEMC.
4. Restart MCS.

Testing transports

Procedure

1. In Avamar Administrator, select **Tools** > **Manage ConnectEMC**.

   The **Manage ConnectEMC** window is displayed.
2. Click **Test**.

CHAPTER 7

Server Security Hardening

This chapter includes the following topics:

Overview

Avamar servers running the SUSE Linux Enterprise Server (SLES) operating system can implement various server security hardening features.

STIG compliance

Avamar servers running the SLES operating system offer a number of improved security features, which are primarily targeted for customers needing to comply with *US Department of Defense (DoD) Security Technical Implementation Guide (STIG) for Unix* requirements.

Server security hardening levels

The server security hardening features are grouped in increasingly more secure levels. Select a level of security appropriate for your organization, and make the changes in that level and any level beneath it. For example, level-3 security requires all changes described in level-1 and level-2 in addition to those described in level-3.

Level-1 security hardening

Many Level-1 security hardening features are part of the base SLES operating system.

Advanced Intrusion Detection Environment (AIDE)

The Advanced Intrusion Detection Environment (AIDE) is a SLES feature that is used to take a snapshot of an Avamar server configuration for purposes of establishing a reliable system baseline reference.

AIDE is a level-1 hardening feature that is implemented as part of the base SLES operating system. AIDE satisfies the STIG requirements in the following table.

Table 83 STIG requirements satisfied by AIDE

Requirement ID	Requirement title
GEN000140	Create and maintain system baseline
GEN000220	System baseline for system libraries and binaries checking
GEN002260	System baseline for device files checking
GEN002380	SUID files baseline
GEN002400	System baseline for SUID files checking
GEN002440	SGID files baseline
GEN002460	System baseline for SGID files checking

The system baseline snapshot is stored in `/var/lib/aide/aide.db`.

AIDE reports are run weekly as part of the `/etc/cron/weekly/aide` cron job.

AIDE output is logged to `/var/log/secure`.

The auditd service

The `auditd` service is a SLES feature that implements a CAPP-compliant (Controlled Access Protection Profiles) auditing feature, which continually monitors the server for any changes that could affect the server's ability to perform as intended. The `auditd` service writes log output in `/var/log/audit/audit.log`.

The `auditd` service is a level-1 hardening feature that is implemented as part of the base SLES operating system.

The `auditd` service feature satisfies the STIG requirements in the following table.

Table 84 STIG requirements satisfied by the auditd service

Requirement ID	Requirement title
GEN002660	Configure and implement auditing
GEN002680	Audit logs accessibility
GEN002700	Audit Logs Permissions
GEN002720	Audit Failed File and Program Access Attempts
GEN002740	Audit File and Program Deletion
GEN002760	Audit Administrative, Privileged, and Security Actions
GEN002800	Audit Login, Logout, and Session Initiation
GEN002820	Audit Discretionary Access Control Permission Modifications
GEN002860	Audit Logs Rotation

sudo implementation

The `sudo` command is an alternative to direct root login. The admin user account is automatically added to the `sudoers` file. This enables admin users to run commands that would otherwise require operating system root permission.

Implementation of the `sudo` command for admin users is a level-1 hardening feature that is implemented as part of the base SLES operating system.

Implementation of the `sudo` command for admin users satisfies the STIG requirements in the following table.

Table 85 STIG requirements satisfied by the implementation of sudo

Requirement ID	Requirement title
GEN000260	Shared Account Documentation
GEN000280	Shared Account Direct Logon
GEN001100	Encrypting Root Access
GEN001120	Encrypting Root Access

Note

Only a limited subset of commands can be executed with the `sudo` command.

Prefixing commands with "sudo"

Instead of switching user to root with the `su` command, admin users can directly issue commands normally requiring root permissions by prefixing each command with `sudo`.

If prompted for a password, type the admin user password and press **Enter**.

You might be periodically prompted to retype the admin password when prefixing other commands with `sudo`.

Command logging

The base SLES operating system logs all Bash shell commands issued by any user.

Bash command logging is a level-1 hardening feature that is implemented as part of the base SLES operating system.

Bash command logging does not satisfy any particular STIG requirements. It is intended to be used as a generalized debugging and forensics tool.

Locking down single-user mode on RHEL servers

For RHEL servers, limit access in single-user mode to the root user. This task is not required on SLES servers.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Create a backup copy of `/etc/inittab`:
   - Single-node server:
     `cp -p /etc/inittab /etc/inittab.backup`
   - Multi-node server:
     `mapall --all --user=root "cp /etc/inittab /etc/inittab.backup"`
3. Open `/etc/inittab` in a plain text editor.
4. Add the following entry:

   Change:

   ```
   # System initialization
   si::sysinit:/etc/rc.d/rc.sysinit
   ```

   To:

   ```
   # System initialization
   si::sysinit:/etc/rc.d/rc.sysinit
   ss:S:respawn:/sbin/sulogin
   ```

5. Close `inittab` and save your changes.
6. (Multi-node system only) Copy the changes made to `/etc/inittab` to all nodes by typing:

```
cd /etc
mapall --all --user=root copy inittab
mapall --all --user=root "cp /root/inittab /etc/inittab"
mapall --all --user=root "rm -f /root/inittab"
```

Disabling Samba

For RHEL servers, and SLES servers with the optional Samba packages installed, disabling Samba prevents the use of Samba commands to obtain valid local and domain usernames and to obtain the Avamar server's browse list. The browse list is a list of the computers nearest to the Avamar server.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

```
su -
```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Disable Samba:
   - Single-node server:

```
service smb stop
chkconfig smb off
```

   - Multi-node server:

```
mapall --all --user=root "service smb stop"
mapall --all --user=root "chkconfig smb off"
```

Results

Samba is disabled and will not start when the Avamar system boots.

Removing suid bit from non-essential system binaries on RHEL

On RHEL systems, remove the suid bit from non-essential system binaries to prevent them from running with elevated permissions.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

```
su -
```

c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Type the following commands:

```
chmod u-s /sbin/pam_timestamp_check
chmod u-s /opt/dell/srvadmin/oma/bin/omcliproxy
chmod u-s /usr/lib64/squid/pam_auth
```

Preventing unauthorized access to GRUB configuration

Changes to the configuration file of GNU GRUB bootloader (GRUB) can change the startup configuration of the Avamar system. Install an encrypted password to prevent unauthorized changes to this file.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

```
su -
```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Start the encryption application.
   - On SLES, type **/usr/sbin/grub-md5-crypt**.
   - On RHEL, type **/sbin/grub-md5-crypt**.
3. When prompted, type the GRUB password.

   The MD5 hash of the password appears.
4. Copy and save the MD5 hash.
5. Open `/boot/grub/menu.lst` in a plain text editor.
6. Add the following entry below the `timeout` entry:

   `password --md5 hash`

   where *hash* is the MD5 hash.
7. Close `menu.lst` and save your changes.
8. (Multi-node system only) Push the change to the storage nodes by typing the following commands:

```
cd /boot/grub
mapall --all --user=root copy menu.lst
mapall --all --user=root "cp /root/menu.lst /boot/grub/menu.lst"
mapall --all --user=root "rm -f /root/menu.lst"
```

Preventing the OS from loading USB storage

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Open `/etc/modprobe.d/blacklist` in a plain text editor.
3. Add the following entry:

   ```
   blacklist usb_storage
   ```

4. Close the file and save your changes.
5. (Multi-node system only) Push the change to the storage nodes by typing the following commands:

   ```
   cd /etc/modprobe.d/
   mapall --all --user=root copy blacklist
   mapall --all --user=root "cp /root/blacklist /etc/modprobe.d/
   blacklist"
   mapall --all --user=root "rm -f /root/blacklist"
   ```

6. If the USB module is currently loaded, remove it:
   a. Check to see if the module is loaded:

      ```
      root@host:~/#: lsmod |grep usb_storage
      (multinode system)
      mapall --all --user=root "lsmod |grep usb_storage"

      usb_storage 51381 0
      usbcore 220541 4 usb_storage,ehci_hcd,usbhid
      scsi_mod 188384 11
      usb_storage,mpt2sas,scsi_transport_sas,raid_class,mptctl,qla2x
      xx,scsi_transport_fc,scsi_tgt,sg,sd_mod,megaraid_sas
      ```

   b. Remove the module:

      Single node: `root@host:~/#: modprobe -r usb_storage`

      Nodes which require the removal can be provided by the `--nodes` option:
      `mapall --all --user=root --nodes=0.0,0.2,0.s "modprobe -r usb_storage"`

Level-2 security hardening

Level-2 security hardening features can be installed on a feature-by-feature basis.

All level-2 security hardening features can be installed on supported versions of SLES.

Password hardening and firewall hardening features can be installed on supported versions of RHEL.

Note

Installing or upgrading the Avamar server software installs hardening and firewall packages that improve security capabilities on the Avamar server. Installation of the hardening package does not restrict supported server functionality. Installation of the firewall package prevents unencrypted backups from running. These packages cannot be uninstalled.

If you are upgrading from an older version and the scheduled backups are unencrypted, follow the instructions in Permitting unencrypted data-in-flight on page 132 to enable unencrypted backups. For some other tasks, Customer Support provides the steps and tools that are required to complete the task (for instance, FTP capabilities for downloading packages to the server).

Additional operating system hardening

The additional OS hardening package provides the following capabilities for servers running supported versions of SLES:

- Setting terminal timeout at 15 minutes
- Applying read-only permission to root `home` directory
- Removal of world read permissions on log files
- Removal of world read permissions on cron files
- Lockdown of some important `/etc` system configuration files
- Removal of world read permissions from admin and gsan `home` directories
- Removal of unnecessary default accounts and groups
- Disabling of SSH v1 protocol
- Removal of unnecessary tomcat directories
- Changing system and user umask settings to `077`
- Removing unowned files
- Enabling `cron` logging in `syslog`

The additional OS hardening package is a level-2 hardening feature that can be installed during Avamar server software installation, or manually after server software installation. This package satisfies the STIG requirements in the following table.

Table 86 STIG requirements satisfied by the additional OS hardening package

Requirement ID	Requirement title
GEN000460	Unsuccessful Login Attempts - Account Disabled
GEN000480	Unsuccessful Login Attempts - Fail Delay

Table 86 STIG requirements satisfied by the additional OS hardening package (continued)

Requirement ID	Requirement title
GEN000500	Terminal Lockout
GEN000980	Root Console Access
GEN001000	Remote Consoles Defined
GEN001020	Direct Root Login
GEN001120	Encrypting Root Access
GEN001160	Unowned Files
GEN001240	System Files, Programs, and Directories Group Ownership
GEN001260	Log File Permissions
GEN001480	User Home Directory Permissions
GEN001500	Home Directory Permissions
GEN001560	Home Directories Files Permissions
GEN002420	User Filesystems Not Mounted With NoSUID
GEN002580	Permissive umask Documentation
GEN002680	Audit Logs Accessiblity
GEN002700	Audit Logs Permissions
GEN002960	Cron Utility Accessibility
GEN002980	The cron.allow Permissions **Note** In addition to the root user, Avamar also requires that the admin user admin have access to cron.allow.
GEN003000	Cron Executes World Writable Programs
GEN003020	Cron Executes Programs in World Writable Directories
GEN003040	Crontabs Ownership
GEN003080	Crontab Files Permissions
GEN003100	Cron and Crontab Directories Permissions
GEN003160	Cron Logging
GEN003180	Cronlog Permissions
GEN003200	cron.deny Permissions
GEN003400	The at Directory Permissions
GEN003520	Core Dump Directory Ownership and Permissions

Additional password hardening

Avamar servers can be configured to provide additional password hardening features such as:

- Aging — how long a password can be used before it must be changed
- Complexity — required number and type of characters in passwords
- Reuse — number of previously used passwords that can be recycled

Note

Password hardening is not appropriate for all customers. Successful implementation of this feature requires structures and policies that enforce changes to all operating system user accounts every 60 days, and require users to log into those accounts at least once every 35 days. Failure to implement proper structures and policies before installing the password hardening feature might cause you to be locked out of your Avamar server.

Note

With Avamar 18.1, system user accounts admin passwords and root passwords expire every 60 days. A prompt to change the password is requested in the SSH console.

Additional password hardening is a level-2 hardening feature that can be installed during Avamar server software installation, or manually after server software installation. You can also change the current complexity configuration and aging rules, as specified in the section Complexity and aging configuration changes for password hardening. However, ensure that you use the same caution when changing any password configuration details to ensure successful implementation, and that you perform a backup of the `/etc/pam.d/common-password` file before making any configuration changes.

Additional password hardening satisfies the STIG requirements in the following table.

Table 87 STIG requirements satisfied by additional password hardening

Requirement ID	Requirement title
GEN000540	Password Change 24 Hours
GEN000560	Password Protect Enabled Accounts
GEN000580	Password Length
GEN000600	Password Character Mix
GEN000620	Password Character Mix
GEN000640	Password Character Mix
GEN000660	Password Contents
GEN000680	Password Contents
GEN000700	Password Change Every 60 Days
GEN000740	Password Change Every Year
GEN000760	Inactive Accounts are not locked

Table 87 STIG requirements satisfied by additional password hardening (continued)

Requirement ID	Requirement title
GEN000780	Easily Guessed Passwords
GEN000800	Password Reuse
GEN000820	Global Password Configuration Files
GEN000840	Root Account Access

Following successful installation and configuration, the following rules are enforced for all local Avamar server operating system user accounts and passwords:

- Password aging
- Password complexity, length, and reuse

Password aging
All local Avamar server operating system accounts must have their passwords changed every 60 days. Once a password is changed, it cannot be changed again for at least 24 hours.

Password complexity, length, and reuse
All local Avamar server operating accounts are required to have passwords with the following characteristics:

- Password complexity requires that you use at least three of the following four character sets:
  - Two or more lowercase characters
  - Two or more uppercase characters
  - Two or more numeric characters
  - Two or more special (non-alphanumeric) characters
- Minimum length is determined by complexity:
  - If you use any three character sets, the password must be at least 14 characters.
  - If you use all four character sets, the password must be at least 11 characters.
- Passwords must contain at least three characters that are different from the last password.
- The previous 10 passwords cannot be reused.
- The number of pairs of neighboring alphabetical characters is limited by the length of the password. For example, the string *23abcdfed* contains six pairs: *23*, *ab*, *bc*, *cd*, *fe*, *ed*.
  - For a minimum length password, four pairs are permitted.
  - For every 12 characters beyond the minimum length, another pair is permitted.

Additional firewall hardening (avfirewall)

Avamar servers running supported versions of SLES and RHEL operating systems can be configured to use Linux IPTABLES.

Additional firewall hardening is a level-2 hardening feature that can be installed during Avamar server software installation, or manually after server software installation.

Additional server firewall hardening satisfies the GEN006580 - Access Control Program STIG requirement.

This feature is implemented by way of the `avfirewall` service.

The output for `avfirewall` is logged to `/var/log/firewall` on SLES servers only. The `/var/log/firewall` file is not available on RHEL servers. However, firewall logging can be implemented using `syslog` on RHEL servers. The *Avamar Administration Guide* provides details about implementing `syslog`.

Note

If you are backing up a Hyper-V or Microsoft SQL plug-in to a server running the `avfirewall` service and the encryption method for the backup is set to **None**, the backup will fail with errors indicating a problem connecting to the server. Set the encryption method to **High**.

Securing the Postgres firewall port

The Avamar Client Manager and Data Protection Advisor access TCP port 5555 to connect to Postgres SQL.

To reduce exposure to potential Postgres security vulnerabilities, you can restrict access to this port to a limited subset of IP addresses. For all other IP addresses, close this port on the utility node.

After compiling a list of IP addresses, use the instructions in Configuring the Avamar firewall on page 121 to allow access for those IP addresses and deny access for all others. This port is only open on the utility node and not on the storage nodes.

Installing level-2 security hardening features

Level-2 security hardening features can be installed during Avamar server software installation. The *Avamar SLES Installation Workflow Guide* provides information about installing and enabling security hardening features. This guide is available during installation when you click the help icon in Avamar Installation Manager. If you did not install level-2 security hardening features during Avamar server software installation, you can manually install them after server software installation is complete.

Manually installing level-2 hardening packages on SLES

Note

Avamar 18.1 and later releases include additional operating system and firewall hardening packages for NDMP accelerator nodes. Installing or upgrading the accelerator software via the Avamar Installation Manager workflow packages automatically installs the hardening packages.

The *Avamar NDMP Accelerator for NAS Systems User Guide* provides more information about installing and upgrading the accelerator software via the Avamar Installation Manager.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Change directory to where the install packages reside by typing:

```
cd /usr/local/avamar/src/SLES11_64/
```

3. If installing on a multi-node server, copy one or more level-2 hardening packages to all other server nodes by typing the following commands:

```
mapall --all+ --user=root copy avhardening-version.x86_64.rpm
mapall --all+ --user=root copy avpasswd-version.x86_64.rpm
```

where *version* is the specific version you are installing.

If you are not installing a particular level-2 hardening feature, omit the command to copy that install package.

4. Install the hardening packages by doing one of the following:

- If installing on a single-node server, type:

```
rpm -Uvh avhardening-version.x86_64.rpm
rpm -Uvh avpasswd-version.x86_64.rpm
rpm -Uvh avfwb-version.x86_64.rpm
```

- If installing on a multi-node server, type:

```
mapall --all+ --user=root "rpm -Uvh avhardening-
version.x86_64.rpm"
mapall --all+ --user=root "rpm -Uvh avpasswd-
version.x86_64.rpm"
mapall --all+ --user=root "rpm -Uvh avfwb-version.x86_64.rpm"
```

where *version* is the specific version you are installing.

If you are not installing a particular level-2 hardening feature, omit the command to copy that install package.

5. If installing on a multi-node server, delete the install packages by typing:

```
mapall --user=root "rm -f avhardening*"
mapall --user=root "rm -f avpasswd*"
mapall --user=root "rm -f avfwb*"
```

If you did not copy a particular install package, omit the command to delete that package.

Configuring replication for level-2 firewall hardening

Implementing level-2 firewall hardening can cause replication to fail unless TLS encryption is enabled on the destination server.

Configuring policy-based replication for level-2 firewall hardening

Installing the level-2 firewall hardening package might cause policy-based replication to fail. If this occurs, enable TLS encryption on the destination server by including the **--dstencrypt=tls** option with each `avrepl` command.

The *Avamar Administration Guide* provides additional information about policy-based replication and the `avrepl` command.

Custom ssh banner not supported

STIG requirement GEN005550 requires that the `ssh` protocol support a customer banner. However, the Avamar system is not compliant with this requirement. Custom `ssh` banners are not supported.

Complexity and aging configuration changes for password hardening

An additional feature of password hardening allows you to change the complexity configuration and password aging rules by performing the following procedures.

Change the complexity configuration for password hardening

As part of password hardening, you can change the existing complexity configuration to meet your specific requirements.

Before you begin

Ensure that the password hardening package is installed on your system. For more information about how to install password hardening package manually, please refer to Installing level-2 security hardening features on page 214.

Procedure

1. Log in to the Avamar server as **administrator**, and then change to the **root** user by typing `su -` in a command prompt.
2. Perform a backup of the existing `/etc/pam.d/common-password` file in case the configuration changes fail and you need to revert to the original file. For example, `# cp /etc/pam.d/common-password-pc /etc/pam.d/common-password-pc.bak.`date +%s`.`
3. Open the `/etc/pam.d/common-password` file in a plain-text editor.
4. Change the complexity configuration settings under `minlen/lcredit/ucredit/dcredit/ocredit` to meet your specific requirements.

Note

Making these changes might require some knowledge about the **pam_cracklib** module.

Change the aging rules for password hardening

You can also change a specific user's password expiry settings and aging strategies by performing the following.

Before you begin

Ensure that the password hardening package is installed on your system. For more information on how to install password hardening package manually, please refer to Installing level-2 security hardening features on page 214.

Procedure

1. Log in to the Avamar server as **administrator**, and then change to the **root** user by typing `su -` in a command prompt.
2. Type the following command to set the number of days until the password expires for the specific user:

   ```
   # chage -M MAX_DAYS ACCOUNT_NAME
   ```

3. Perform a backup of the `/etc/login.defs` file by running the following:

   ```
   # cp /etc/login.defs /etc/login.defs.bak.`date +%s`
   ```

4. Open the `/etc/login.defs` file in a plain-text editor.
5. Change the following settings as required:
   - *PASS_MAX_DAYS* — The maximum number of days you can use the password. Once the password reaches the maximum number of days, a password change will be forced. If you do not specify a value, the default -1 is used, which disables the restriction.
   - *PASS_MIN_DAYS* — The minimum number of days a password must be retained before changes are permitted. Any password changes attempted earlier than this date will be rejected. If you do not specify a value, the default -1 is used, which disables the restriction.
   - *PASS_WARN_AGE* — The number of days before password expiry that a warning message will display. A value of 0 (zero) will display the warning only on the day of password expiration. If you do not specify a value, or you specify a negative value, no warning will display.

   Note

   PASS_MAX_DAYS, *PASS_MIN_DAYS* and *PASS_WARN_AGE* are only used at the time of account creation. Any changes to these settings will not affect existing accounts. More information is provided in the Linux **LOGIN.DEFS** man page.

Preventing host header injection vulnerabilities on Apache web server

Use the following procedure to prevent host header injection on the Apache web server. Performing this procedure ensures that the Avamar server web UI can only be accessed through FQDN if the full URI is not used.

Procedure

1. Open a command shell and edit the `vhost-nss.conf` file:
   a. Log in to the Avamar server as admin.

b. Use a plain text editor to open the following file:

```
/etc/apache2/vhosts.d/vhost-nss.conf
```

c. In the `vhost-nss.conf` file, add the following line after the line <VirtualHost _default_:443>:

```
UseCanonicalName On
```

The file should look similar to the following example:

```
<VirtualHost _default_:443>
UseCanonicalName On
DocumentRoot "/usr/local/avamar/httpds/html"
ServerName av-vm-237-63.ccoe.lab.emc.com
Include /etc/apache2/conf.d/avamar.conf
```

2. Restart the Apache service by using the following command:

```
Service apache2 restart
```

Results

The Apache web server prevents host header injection. If you do not use the full URI, the web UI of Avamar server can only be accessed by using the FQDN.

Level-3 security hardening

Level-3 security hardening disables all web-based services and reduces other services to the minimum required to manage and use the Avamar system.

Level-3 security hardening features can be applied to a running, fully functional Avamar server

Note

Level-1 and level-2 security hardening must be completely implemented prior to implementing level-3 security hardening.

Disabling Apache web server

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

```
su -
```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Turn off the Apache web server by typing `website stop`.

3. Disable the Apache web server by typing `chkconfig apache2 off`.

Results

The Apache web server is disabled and will not automatically run when the Avamar server is restarted.

Stopping the EMT

Procedure

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 EM Tomcat server by typing the following command:

   ```
   dpnctl stop emt
   ```

Results

Although the EMT is stopped, it restarts when the server is restarted. Repeat this task each time the Avamar server is restarted.

Disabling Dell OpenManage web server

Disabling the web server for Dell OpenManage prevents web browser access to that service. The Dell OpenManage services remain available at the console.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Stop the Dell OpenManage web server.
   - On multi-node servers, type:
     `mapall --all+ --user=root "service dsm_om_connsvc stop"`
   - On single-node servers, type:
     `service dsm_om_connsvc stop`
3. Disable the Dell OpenManage web server.
   - On multi-node servers, type:
     `mapall --all+ --user=root "chkconfig dsm_om_connsvc off"`
   - On single-node servers, type:
     `chkconfig dsm_om_connsvc off`
4. (Optional) Verify that the Dell OpenManage web server is not running.
   - On multi-node servers, type:
     `mapall --all+ --user=root "chkconfig dsm_om_connsvc --list"`

- On single-node servers, type:
  `chkconfig dsm_om_connsvc -list`

Disabling SSLv2 and weak ciphers

Configure the Avamar server to disallow the use of SSL v.2 and weak ciphers in communication between server nodes and backup clients.

Note

Enforcing the use of strong ciphers prevents clients that do not support strong ciphers from connecting with Avamar server.

Configuring Avamar servers to use strong ciphers

Complete this task to enforce the use of strong ciphers on Avamar systems with Avamar server version 7.5 or newer.

Procedure

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. Switch user to root by typing the following command:

   ```
   su -
   ```

3. Type the following command:

   ```
   avmaint config sslciphers=level --ava
   ```

   where *level* is the Avamar cipher level in the following table.

   Table 88 Cipher levels and associated OpenSSL suites

Avamar cipher level	OpenSSL suites
cleartext [a]	NULL-SHA
medium [b]	ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA:AECDH-AES128-SHA
high	ECDHE-ECDSA-AES256-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA

   a. The `cleartext` cipher level is not available in Avamar 7.5 and later and Avamar 18.1 and later when the session security features are enabled. If `cleartext` was in place before an upgrade from a previous version of Avamar, the upgrade changes this setting to `high`. The session security features are enabled if the communication security setting is anything other than `Disabled/Off`.
   b. The `medium` cipher level is not available in Avamar 7.5 and later and Avamar 18.1 and later. If `medium` encryption was in place before an upgrade from a previous version of Avamar, the upgrade does not change the existing behavior. However, Avamar Administrator displays

Table 88 Cipher levels and associated OpenSSL suites (continued)

this setting as `high`. If you change the cipher level to another value, you cannot select medium again.

Configuring the NDMP accelerator to use strong ciphers

Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing the following command:

   ```
   su -
   ```

3. Open `/usr/local/avamar/var/avtar.cmd` in a plain text editor.

Updating OpenSSH

Before you begin

Contact your Avamar Customer Support professional to obtain and install the latest Avamar platform security rollup package. The platform security rollup package installs the latest version of OpenSSH.

Updating to the latest version of OpenSSH and performing this task configures OpenSSH to:

- Deny empty passwords
- Log at INFO level
- Use protocol 2
- Harden for security audit vulnerabilities

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Open `/etc/ssh/sshd_config` in a plain text editor.
3. Add the following entries:

   ```
   PermitEmptyPasswords no
   LogLevel INFO
   Protocol 2
   Ciphers cipher_suite
   ```

   where *cipher_suite* is one of the following:

   - For SLES:

     ```
     aes128-ctr,aes192-ctr,aes256-ctr
     ```

- For RHEL:

  ```
  arcfour,aes128-ctr,aes192-ctr,aes256-ctr
  ```

4. Close `sshd_config` and save your changes.
5. Restart the `sshd` service by typing **`service sshd restart`**.

   Restarting the `sshd` service can cause current SSH sessions to terminate.

Disabling RPC

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Stop the RPC service.
   - On SLES, type **`service rpcbind stop`**.
   - On RHEL, type **`service portmap stop`**.
3. Disable the RPC service at startup.
   - On SLES, type:

     ```
     chkconfig nfs off
     chkconfig rpcbind off
     ```

   - On RHEL, type **`chkconfig portmap off`**.
4. Repeat these steps on each server node.

Configuring the firewall to block access to port 9443

Avamar Management Console Web Services normally use Port 9443 for Java Remote Method Invocation (RMI). Configure iptables to block port 9443.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Open `/etc/firewall.default` in a plain text editor.
3. Add the following entries:

```
$IPT -A INPUT -p tcp -m tcp --dport 9443 -j DROP
$IPT -A INPUT -p udp -m udp --dport 9443 -j DROP
```

4. Close `firewall.default` and save your changes.
5. Restart the `avfirewall` service by typing the following commands:

```
service avfirewall stop
service avfirewall start
```

Changing file permissions

Use the `chmod o-w` command to prevent users in the Others group from writing to specific folders and files.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

```
su -
```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

```
ssh-agent bash
ssh-add /root/.ssh/rootid
```

2. Type the following commands:

```
chmod o-w -R /etc/openldap
chmod o-w -R /root/
chmod o-w /data01/avamar/var
chmod o-w /data01/avamar/var/change-passwords.log
chmod o-w /data01/avamar/var/local
chmod o-w /data01/avamar/var/local/ziptemp
chmod o-w /data01/avamar/var/p_*dat
chmod o-w /opt/dell/srvadmin/iws/config/keystore.db.bak
chmod o-w /tmp/replicate
chmod o-w /usr/local/avamar/bin/benchmark
chmod o-w /.avamardata/var/mc/cli_data/prefs/mcclimcs.xml
chmod o-w /.avamardata/var/mc/cli_data/prefs/
mccli_logging.properties
chmod o-w /.avamardata/var/mc/cli_data/prefs/prefs.tmp
chmod o-w /.avamardata/var/mc/cli_data/prefs/mccli.xml
chmod o-w /data01/home/admin/.avamardata/var/mc/cli_data/prefs/
mccli.xml
chmod o-w /data01/home/admin/.avamardata/var/mc/cli_data/prefs/
mcclimcs.xml
chmod o-w /data01/home/admin/.avamardata/var/mc/cli_data/prefs/
mccli_logging.properties
chmod o-w /data01/home/admin/.avamardata/var/mc/cli_data/prefs/
```

```
prefs.tmp
chmod o-w /data01/avamar/var/mc/server_log/mcddrsnmp.out
```

Preparing for a system upgrade

To permit a successful system upgrade, some of the level-3 security hardening changes must be temporarily reversed. After the system upgrade is complete, reapply those changes.

Enabling the Apache web server

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Enable the Apache web server by typing the following command:

   ```
   chkconfig --add apache2
   ```

3. Start the Apache web server by typing the following command:

   ```
   website start
   ```

Starting the EMT

Procedure

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. Start the EM Tomcat server by typing the following command:

   ```
   dpnctl start emt
   ```

CHAPTER 8

Intelligent Platform Management Interface

This chapter includes the following topics:

IPMI subsystem security

Avamar system computer hardware can contain manufacturer-specific implementations of the Intelligent Platform Management Interface (IPMI). The IPMI subsystem provides out-of-band management of a computer system. A comprehensive plan to secure an Avamar system includes tasks that secure the IPMI subsystem.

IPMI software interacts with the hardware through the baseboard management controller (BMC). IPMI provides management and monitoring of the computer through a subsystem that is separate from the computer's operating system, CPU, and firmware.

On July 26, 2013 the United States Computer Emergency Response Team (US-CERT) released an alert that is entitled: "Risks of Using the Intelligent Platform Management Interface (IPMI)" (TA13-207A). In the alert US-CERT warns that:

> Attackers can use IPMI to essentially gain physical-level access to the server. An attacker can reboot the system, install a new operating system, or compromise data, bypassing any operating system controls.

To secure the IPMI subsystem of an Avamar system, complete the tasks that are described in the following table.

Table 89 Descriptions of security tasks for the IPMI subsystem

Task	Description
Find all channels with the "802.3 LAN" media type	Channels with the "802.3 LAN" media type provide access to the IPMI subsystem from the LAN. LAN access is a known attack vector.
Disable privileges for Cipher Suite 0	IPMI subsystems provide Cipher Suite 0 as an option that permits unauthenticated access for the designated privilege level. Prevent unauthenticated access for all privilege levels by setting the privilege level of this cipher suite to 0.
Secure anonymous logins	IPMI subsystems reserve the account with user ID 1 for anonymous log in. Secure anonymous logins by: • Disabling the anonymous account for Serial over LAN access • Placing the privileges for the account at the lowest level • Disabling IPMI support for the account
Create strong passwords for each baseboard management controller (BMC) account	Strong passwords reduce the possibility of unauthorized access to the IPMI subsystem.
Isolate the LAN port that is used for BMC management	Limit access to the BMC management LAN port.

Table 89 Descriptions of security tasks for the IPMI subsystem (continued)

Task	Description
Disable remote media redirection	Disable BMC access to remote media. Only allow access to remote media during the time it is required to perform a valid IPMI task.
Disable the keyboard/video/monitor (KVM) functionality of the BMC	Disable the KVM functionality of the BMC. Only allow KVM functionality during the time it is required to perform a valid IPMI task.
Prevent access to the BIOS and POST serial interfaces	Isolate the BIOS and POST serial interfaces within the corporate LAN.
Disable boot from USB and boot from CD/DVD	Prevent the possibility of the computer starting from unauthorized media by changing the computer BIOS settings to prevent boot from USB and boot from CD/DVD.
Redirect all incoming HTTP packets sent to Port 80 to the HTTPS port	Force encryption of all HTTP packets by redirecting HTTP sockets to the HTTPS port.

Finding all LAN channels

Channels with the "802.3 LAN" media type provide access to the IPMI subsystem from the LAN. LAN access is a known attack vector. Find all LAN channels to help manage LAN access to the IPMI subsystem.

Before you begin

Obtain console access to the Avamar system computers.

Procedure

1. At the Avamar system utility node console, log in as root.
2. Type the following command for each channel ID:

   `ipmitool channel info` ***`channel_id`***

   where *channel_id* is each of the following channel ID hexadecimal values: 0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A, 0x0B, 0x0C, and 0x0D.

   Each time the command is typed, the system displays information for the specified channel ID.
3. Record the value of the **Channel Medium Type** field for each channel ID.

   When the value of the **Channel Medium Type** field is `802.3 LAN` the channel is accessible from the LAN.
4. Repeat these steps for each storage node.

Results

This task creates a record of all IPMI subsystem channels that can be accessed from the LAN.

For example, to determine whether channel with the ID value of 0x01 is accessible from the LAN, type the following command:

ipmitool channel info 0x01

The system returns the following information:

```
Channel 0x1 info:
  Channel Medium Type   : 802.3 LAN
  Channel Protocol Type : IPMB-1.0
  Session Support       : multi-session
  Active Session Count  : 1
  Protocol Vendor ID    : 7154
  Volatile(active) Settings
    Alerting            : disabled
    Per-message Auth    : enabled
    User Level Auth     : enabled
    Access Mode         : always available
  Non-Volatile Settings
    Alerting            : disabled
    Per-message Auth    : enabled
    User Level Auth     : enabled
    Access Mode         : always available
```

Disabling privileges for Cipher Suite 0

IPMI subsystems provide Cipher Suite 0 as an option that permits access without authentication, without integrity checks, and without encryption to ensure confidential communication. Prevent unauthenticated access for all privilege levels by setting the privilege level of this cipher suite to 0.

Before you begin

Find all channels with the "802.3 LAN" media type.

Procedure

1. At the Avamar system utility node console, log in as root.
2. Type the following command:

   ipmitool raw 0x0C 0x02 *channel_id* 0x18 0x00 0x00

   where *channel_id* is a channel ID hexadecimal value for a channel that has the "802.3 LAN" media type.

   For example, for channel 0x01, type:

   ipmitool raw 0x0C 0x02 0x01 0x18 0x00 0x00
   The following response appears:

   ```
   11 00 44 44 44 44 44 44 44 44 44 44
   ```

   The system returns a string of 12 half-bytes. The value of the third half-byte indicates the privilege level that is assigned to Cipher Suite 0. In this example, the value of the third half-byte, 44, indicates that the administrator privilege level is assigned to Cipher Suite 0. Change this value to 40 to disable privileges for Cipher Suite 0.
3. Type the following command:

   ipmitool raw 0x0C 0x01 *channel_id* 0x18 0x00 0x40 0x44 0x44 0x44 0x44 0x44 0x44 0x44 0x44 0x44

where *channel_id* is the channel ID hexadecimal value that is used in the previous step. The value `0x40` in the command represents Cipher Suite 0 with privilege level 0.

4. Type the following command to verify the change:

   ipmitool raw 0x0C 0x02 *channel_id* 0x18 0x00 0x00

   For example, for channel 0x01, type:

   ipmitool raw 0x0C 0x02 0x01 0x18 0x00 0x00
   The following response appears:

   ```
   11 00 40 44 44 44 44 44 44 44 44 44
   ```

   The value of the third half-byte is 40 which means that the Cipher Suite 0 privilege level is set to 0 (no privileges) for the specified channel.
5. Repeat these steps for each channel that has the "802.3 LAN" media type.
6. Repeat these steps for each Avamar storage node.

Results

The IPMI subsystem prohibits unauthenticated LAN access.

Securing anonymous logins

IPMI subsystems reserve the account with user ID 1 for anonymous log in. Secure anonymous logins by disabling the anonymous account for Serial over LAN access, placing the privileges for the account at the lowest level, and disabling IPMI support for the account.

Before you begin

Find all channels with the "802.3 LAN" media type.

Procedure

1. At the Avamar system utility node console, log in as root.
2. Type the following command:

   ipmitool sol payload disable *channel_id* 1

   where *channel_id* is a channel ID hexadecimal value for a channel that has the "802.3 LAN" media type.

   The ipmitool disables anonymous user logins through Serial over LAN for the specified channel.
3. Repeat the previous step for each channel that has the "802.3 LAN" media type.
4. Type the following command:

   ipmitool channel setaccess *channel_id* 1 callin=off ipmi=off link=off privilege=1

   where *channel_id* is a channel ID hexadecimal value for a channel that has the "802.3 LAN" media type.

   The ipmitool puts the anonymous user at the lowest privilege level for the specified channel.
5. Repeat the previous step for each channel that has the "802.3 LAN" media type.

6. Type the following command:

   ipmitool user disable 1

   The ipmitool disables support for the BMC anonymous user account.
7. Repeat these steps for each Avamar storage node.

Results

The IPMI subsystem secures anonymous logins.

Creating strong passwords for BMC accounts

Identify the existing baseboard management controller (BMC) accounts and create a strong password for each account. Strong passwords reduce the possibility of unauthorized access to the IPMI subsystem.

Procedure

1. At the Avamar system utility node console, log in as root.
2. Type the following command:

   ipmitool user list

   The system displays a list that has columns of information about each BMC user account.
3. For each user account, type the following command:

   ipmitool user set password *user_ID new_password*

   where *user_ID* is the integer value that is listed in the ID column for the user account and *new_password* is the new strong password for the account.
4. Repeat these steps for each Avamar storage node.

Results

The BMC requires the strong passwords for BMC account access.

For example, type:

ipmitool user list

The following response appears:

```
ID  Name             Callin  Link Auth  IPMI Msg   Channel Priv Limit
2   root             false   false      true       ADMINISTRATOR
3   admin            true    true       true       ADMINISTRATOR
```

Change the password for the root account, by typing the following:

ipmitool user set password 2 *new_password*

Change the password for the admin account by typing the following:

ipmitool user set password 3 *new_password*

Additional BMC security tasks

Limit access to the baseboard management controller (BMC) by completing these additional tasks.

Refer to the hardware manufacturer's documentation for information about the additional security tasks that are described in the following sections.

Isolate the BMC management LAN port
The BMC provides a management interface through a dedicated NIC that opens a LAN port on channel 4. Restrict access to this port by the following:

- Never expose the port to internet access
- Never expose the port to access from outside of the corporate LAN
- Assign a static private address to the port
- Only allow access to the port from the subnet

Disable remote media redirection
By default, Avamar systems have remote media redirection disabled. Only enable this BMC feature when it is required.

Disable the KVM functionality
By default, Avamar systems have keyboard/video/monitor (KVM) functionality of the BMC disabled. Only enable this BMC feature when it is required, and only with authentication and strong passwords.

Prevent access to the BIOS and POST serial interfaces
The BMC management port provides BIOS and POST serial interfaces. Do not connect the management port to a device that permits BIOS and POST serial access from outside of the corporate LAN.

Disable boot from USB and boot from CD/DVD
Disable boot from USB and boot from CD/DVD in the BIOS settings of the Avamar system computers to prevent starting the computers from remote media. Do not put the USB interface in the boot path.

Redirect HTTP packets to the HTTPS port
Help secure the BMC management web UI by redirecting traffic sent to the web UI from port 80 (HTTP) to port 443 (HTTPS). Also, improve authentication by configuring the BMC management web UI to use a certification authority-issued trusted public key certificate.

APPENDIX A

IAO Information

US Department of Defense (DoD) Security Technical Implementation Guide (STIG) for UNIX mandates information that should be disclosed to an Information Assurance Officer (IAO).

This appendix includes the following topics:

System-level accounts

Pursuant to the disclosure requirements of STIG compliance rule GEN000360, the following lists contains the names of accounts that are system-level, and are not privileged-user-level:

at
avi
mysql
admin
dnsmasq
messagebus
polkituser
puppet
stunnel
suse-ncc
uuidd
wwwrun

Files with SUID bit and SGID bit

Pursuant to the disclosure requirements of STIG compliance rule GEN002440, the following list contains the pathnames for files that have the set user ID (SUID) bit and the set group ID (SGID) attributes enabled:

```
/data01/connectemc/archive
/data01/connectemc/failed
/data01/connectemc/history
/data01/connectemc/logs
/data01/connectemc/output
/data01/connectemc/poll
/data01/connectemc/queue
/data01/connectemc/recycle
/lib64/dbus-1/dbus-daemon-launch-helper
/opt/dell/srvadmin/oma/bin/omcliproxy
/usr/bin/lockfile
/usr/bin/slocate
/usr/bin/ssh-agent
/usr/bin/vlock
/usr/bin/wall
/usr/bin/write
/usr/lib/PolicyKit/polkit-explicit-grant-helper
/usr/lib/PolicyKit/polkit-grant-helper
/usr/lib/PolicyKit/polkit-grant-helper-pam
/usr/lib/PolicyKit/polkit-read-auth-helper
/usr/lib/PolicyKit/polkit-revoke-helper
/usr/lib/PolicyKit/polkit-set-default-helper
/usr/lib/vte/gnome-pty-helper
/usr/sbin/lockdev
/usr/sbin/postdrop
```

```
/usr/sbin/postqueue
/usr/sbin/sendmail.sendmail
/usr/sbin/utempter
/usr/sbin/zypp-refresh-wrapper
```

Permissions within /var folder

Many components of the Avamar system write to the /var folder.

Permissions on the /var folder of an Avamar node are world writeable because many components of the Avamar system write files such as logs there. On physical Avamar servers, the folder in question is /usr/local/avamar/var; on virtual Avamar servers, it is /space/avamar/var. This security exception is necessary for the operation of the product.

APPENDIX B

Enterprise Authentication

This appendix includes the following topics:

Enterprise authentication

Enterprise (or external) authentication enables users to use the same user ID and password to log in to multiple systems.

NOTICE

For backward compatibility, this appendix preserves information about the deprecated Enterprise authentication method. The functionality of this method is replaced, and improved on, by the directory service authentication method. Information about the directory service authentication method is available in the Avamar Administration Guide.

The Avamar Enterprise authentication feature is not a single user ID/password login, fully integrated into an external authentication system on which users are created and managed. Instead, the same user ID must be created on both Avamar and external systems while the password is set and managed externally.

Avamar Login Manager provides access to the external authentication databases through the standard Pluggable Authentication Module (PAM) library of the Linux operating system.

Login Manager runs on the utility node and is installed and started during Avamar server installation and upgrade. It uses the domains configuration file to identify the supported domains.

Supported components and systems

Enterprise authentication is only available for specific Avamar components. Enterprise authentication supports two external authentication systems.

Avamar components

Avamar Administrator and Avamar Web Access support the use of Enterprise authentication for user accounts.

Enterprise authentication is not available for Avamar server-level administration user accounts, including:

- Operating system user accounts: root and admin.
- Special Avamar system administrative user accounts, for example MCUser and root.

External systems

Avamar supports the external authentication systems that are described in the following table.

Table 90 Supported external authentication systems

Category	Description
Lightweight Directory Access Protocol (LDAP)	Hierarchical directory structure, X.500-standard, system such as: • Microsoft Active Directory Service (MS ADS) • Novell NDS and eDirectory

Table 90 Supported external authentication systems (continued)

Category	Description
Network Information Service (NIS) SUN Yellow Pages (YP)	Flat, workgroup-based, database structure of user IDs, passwords, and other system parameters comparable to Microsoft Windows NT such as: • Master NIS Server - Primary Domain Controller (PDC) • Slave NIS Servers - Backup Domain Controllers (BDC)

Configuring Enterprise authentication

Configuring Enterprise authentication involves the completion of a series of tasks, including configuring either an LDAP or an NIS interface.

Complete the sequence of tasks outlined below to complete Enterprise authentication configuration.

Procedure

1. Back up the current configuration files.
2. Configure an LDAP or an NIS interface.

   Complete the steps described in either Configuring an LDAP interface or Configuring an NIS interface.
3. Use Avamar Administrator to create the users who require login access to Avamar. The *Avamar Administration Guide* provides detailed instructions.

   The username must match exactly the user ID on the LDAP or NIS server. Create external users in the proper LDAP or NIS server domain location (for example, the root "/" or other directory like "/clients/"). When creating users, the external domain appears in the Authentication System list.
4. Confirm the ability of the external users to log in to Avamar Administrator.

   Log in according to the following rules:

   a. User ID followed by `@DOMAIN`.

      where DOMAIN is the LDAP or NIS server domain that you specified when you edited the `/etc/avamar/domain.cfg` file while configuring the LDAP or NIS interface.
      For example: **`SueV@example.com`**.

   b. User password as used in the external LDAP or NIS system.

   c. Domain path where external users reside (for example, "`/clients/`").
5. Back up the configuration files again.

   As a best practice, back up configuration files before installing software upgrades to prevent the possibility of configuration files being overwritten with default values.

Configuring an LDAP interface

Configure an LDAP interface on the Avamar system to use with Enterprise authentication.

Before you begin

Gather the following information:

- LDAP information: LDAP domain name, IP address or FQDN of LDAP authentication server, and distinguished name (DN) of the account to use for LDAP queries.
- Avamar system information: OS root password, OS admin password, and Avamar system admin password.

Procedure

1. Open a command shell:
   a. Log in to the server as admin.
   b. Switch user to root by typing the following command:

      ```
      su -
      ```

   c. For a multi-node server, load the rootid OpenSSH key by typing the following command:

      ```
      ssh-agent bash
      ssh-add /root/.ssh/rootid
      ```

2. Open `/etc/avamar/domain.cfg` in a plain text editor.
3. Add the following entry in the Customer Specific Domains section, and then save the file:

   ```
   DOMAIN=ID
   ```

   where:

   - *DOMAIN* (format: example.com) is a unique customer-specific LDAP domain that is used for addressing PAM.
   - ID is an integer larger than 1. IDs 0 and 1 are reserved for Avamar internal use.

   Note

   The next step creates a symbolic link for this entry. However, the Avamar system provides an existing symbolic link when you uncomment the line:

   ```
   ldap=3
   ```

   If you use `ldap=3`, skip the next step.
   The DOMAIN part of the entry (either ldap or a unique LDAP domain) appears in the Avamar Administrator Authentication System list. Typing a unique DOMAIN can help clarify which LDAP domain is used for external authentication.

4. Create a unique lm_ldap file and symbolically link to it by typing:

   ```
   ln -sf /etc/pam.d/lm_ldap /etc/pam.d/lm_NUMBER
   ```

   where *NUMBER* is the LDAP domain ID used in the previous step.

5. Log in to the server as admin.
6. Load the admin OpenSSH key by typing:

   ssh-agent bash

   ssh-add ~admin/.ssh/admin_key
7. When prompted, type the admin user account passphrase and press **Enter**.
8. Confirm that the system name and lmaddr are set up correctly by typing:

   avmaint config --avamaronly | grep systemname

   avmaint config --avamaronly | grep lmaddr

   These commands display the hostname and IP address of the utility node, respectively.
9. As root, create a symbolic link from ldap.conf to ldap.conf.winad by typing:

   ln -sf /etc/ldap.conf.winad /etc/ldap.conf
10. Set correct group ownership and file permissions for ldap.conf by typing:

    chown root:root /etc/ldap.conf

    chmod 0600 /etc/ldap.conf
11. Confirm the symbolic link by typing:

    ls -l /etc/ldap.conf

    The following information appears in the command shell:
    `/etc/ldap.conf -> /etc/ldap.conf.winad`
12. In a UNIX text editor, open `/etc/ldap.con`.
13. Modify the following entries, and then save the file:

    host *HN-IPADD*
    where *HN-IPADD* is the fully qualified hostname or IP address of the LDAP server.

    base dc=*DOMAIN*, dc=com

    where *DOMAIN* is the first part of the LDAP domain name. For example: example.com would be displayed as dc=example, dc=com.

    binddn cn=*PROXYUSER*, ou=*PROXYUNIT*, ou=*PROXYORG*, dc=*DOMAIN*, dc=com

    where *PROXYUSER*, *PROXYUNIT*, *PROXYORG*, and *DOMAIN* comprise parts of the distinguished name of the user account that is used to bind with the LDAP server. Components include:

    - cn - common name
    - ou - organizational or unit name
    - dc - domain

    For example: Distinguished name avamaruser.users.avamar.example.com

    Components: cn=avamaruser, ou=users, ou=avamar, dc=example, dc=com

    bindpw *PWD*

    where *PWD* is the password of the user account that is used to bind with the LDAP server.

14. Restart Login Manager by typing:

    ```
    service lm restart
    ```

15. Confirm acceptance of the configuration changes, by typing:

    ```
    avmgr lstd
    ```

    All of the Avamar authentication domains are listed.

16. Confirm that the LDAP server can be queried by typing the following command:

    ```
    ldapsearch -x -w -h
    HOSTNAME -b dc=DISTINGUISHED_NAME -D cn=VALID_USERNAME,
    cn=users, dc=DISTINGUISHED_NAME
    ```

    where:

    - *HOSTNAME* is the hostname or IP address of the LDAP server.
    - dc=*DISTINGUISHED_NAME* is the domain part of the distinguished name (the two "dc" components).
    - *VALID_USERNAME* is a valid user in the LDAP server domain.

    A success message or referral result appears.

    For example:

    ```
    ldapsearch -x -w -h 10.0.100.21 -b dc=aelab01, dc=com -D
    cn=administrator, cn=users, dc=aelab01, dc=com
    ```

After you finish

Confirm the ability to log in to Avamar Administrator as an external user.

Configuring an NIS interface

Configure an NIS interface on the Avamar system to use with Enterprise authentication.

Procedure

1. Open a command shell and log in:
   - If logging in to a single-node server, log in to the server as root.
   - If logging in to a multi-node server, log in to the utility node as root.
2. Open `/etc/avamar/domains.cfg` in a UNIX text editor.
3. Add the following entry in the **Customer Specific Domains** section, and then save the file:

   ```
   DOMAIN=ID
   ```

   where:

   - *DOMAIN* (format: example.com) is a unique customer-specific NIS domain that is used for addressing PAM.
   - *ID* is an integer larger than 1. IDs 0 and 1 are reserved for Avamar internal use.

Note

The next step creates a symbolic link for this entry. However, the Avamar system provides an existing symbolic link when you uncomment the line:

```
nis=2
```

If you use `nis=2`, skip the next step.
The DOMAIN part of the entry (either nis or a unique NIS domain) appears in the Avamar Administrator Authentication System list. Typing a unique DOMAIN can help clarify which NIS domain is used for external authentication.

4. Create a unique lm_nis file and symbolically link to it by typing:

   ```
   ls -sf /etc/pamd/lm_nis /etc/pam.d/lm_NUMBER
   ```

   where *NUMBER* is the NIS domain ID used in the previous step.

5. Set correct group ownership and file permissions for the `lm_nis` file by typing:

   ```
   chown root:root /etc/pam.d/lm_NUMBER
   chmod 0600 /etc/pam.d/lm_NUMBER
   ```

   where *NUMBER* is the NIS domain ID.

6. Confirm the symbolic link by typing:

   ```
   ls -l /etc/pam.d/lm_NUMBER
   ```

   where lm_NUMBER is the file that is created earlier.

   The following information appears in the command shell:
   `/etc/pam.d/lm_NUMBER -> lm_nis`

7. In a UNIX text editor, open lm_NUMBER.
8. Modify the following entries, and then save the file:

   ```
   auth required /lib/security/pam_nis.so domain=NISDOMAIN
   account required /lib/security/pam_nis.so domain=NISDOMAIN
   ```

9. Log in to the server as admin.
10. Load the admin OpenSSH key by typing:

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

11. When prompted, type the admin user account passphrase and press **Enter**.
12. Confirm that the system name and lmaddr are set up correctly by typing:

    ```
    avmaint confi --avamaronly | grep systemname
    avmaint config --avamaronly | grep lmaddr
    ```

    These commands display the hostname and IP address of the utility node, respectively.

13. As root, restart Login Manager by typing:

    ```
    service lm restart
    ```

14. With keys loaded, confirm acceptance of the configuration changes by typing:

    ```
    avmgr lstd
    ```

All Avamar authentication domains are listed.

15. Open `/etc/sysconfig/network` in a UNIX text editor.
16. Add the following entry, and then save the file:

    `NISDOMAIN=`*`DOMAINNAME`*

    where *DOMAINNAME* is the NIS domain.
17. Open `/etc/yp.conf` in a UNIX text editor.
18. Add the following entry:

    `domain` *`NISDOMAIN`* `server` *`NISSERVERNAME_IP`*

    where:

    - *NISDOMAIN* is the NIS domain.
    - *NISSERVERNAME_IP* is the NIS server hostname or IP address.

    Examples:
    `domain hq server 122.138.190.3`

    `domain hq server unit.example.com`
19. Set `ypbind` to start automatically by typing:

    `/sbin/chkconfig ypbind on`
20. Confirm the previous settings by typing:

    `/sbin/chkconfig --list ypbind`

    The following information appears in the command shell:

    ```
    ypbind 0:off   1:off  2:off  3:on  4:on  5:on  6:off
    ```

    Numbers 3, 4, and 5 should be "on." If not, type:

    `/sbin/chkconfig --level `*`NUMBERS`*` ypbind on`

    where *NUMBERS* is a comma-separated list of the numbers to set "on" (for example, `/sbin/chkconfig --level 3,4, ypbind on`).
21. Start the ypbind daemon by typing:

    `service ypbind restart`

    The following information appears in the command shell:

    ```
    Shutting down NIS services:  [ OK or FAIL ]
    Binding to the NIS domain:  [ OK ]
    Listening for NIS domain server:
    ```

Note

If NIS services has not started, shutting down NIS services can fail. In that case, listening for the NIS domain server should fail because the default NIS domain has not yet been set up.
A delay in the start() section is usually required between the ypbind and ypwhich (in the next step) commands.

22. Confirm NIS configuration by typing:

    ypwich

    This command displays the IP address or the fully qualified domain name of the NIS server.
    ypcat -d *NISDOMAIN* password | grep *USER-ID*

    where:

    - *NISDOMAIN* is the NIS domain.
    - *USER-ID* is the partial or whole name of a user who is registered in the external authentication system.

    These commands verify that data can be retrieved from the NIS domain server by returning user login data from the NIS server.

After you finish

Confirm the ability to log in to Avamar Administrator as an external user.

Enabling certificate authorization for PostgreSQL

This section describes how to enable certificate authorization mode for PostgreSQL.

Procedure

1. Open a command shell on the Avamar server and log in as admin.
2. Type the following command:

```
dbssl.sh enable --restart
```

Results

This command generates certificates, changes configurations, and restarts the Management Console Server.

Configuring DTLT to use PostgreSQL certificate authorization mode

To use DTLT to use PostgreSQL certificate authorization mode, perform the following task:

Procedure

1. Open the file `/usr/local/avamar-tomcat/webapps/dtlt/META-INF/context.xml` in a text editor.

2. Modify the `URL` value with the following:

   "jdbc:postgresql://*host*:5555/mcdb?ssl=true&sslfactory=org.postgresql.ssl.jdbc4.LibPQFactory&sslmode=verify-full"
   where *host* is the value of `local_hfsaddr` in `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml`.

   Save and close the file.

3. Copy the directory `/home/admin/.postgresql` to the `/root/` folder and change owner and group permissions to root.
4. Restart DTLT:

   emwebapp.sh --restart

APPENDIX C

Avamar internal certificate usage and note

This topic helps the user to manually customize the mcssl certificate.

Avamar internal mcssl certificate usage and note

The MCS RMI interface uses mcssl certificate and also for MCSDK security communication. Avamar does not support customization certificate solution currently, but if the user wants the customization, it can be done manually as mentioned below.

To achieve manual customization, do as follows:

Procedure

1. Generate the CA by customer owen, but use the CA alias as "mcssl".
2. Import CA into the existing `/usr/local/avamar/lib/rmi_ssl_keystore`.

   Ensure not to change the file password.
3. To make the MCGUI and MCCLI work in utility node, restart MCS.
4. For DTLT and AvInstaller, import the public key of this CA into the tomcat and AVI trust keystore.

   The path should under: `/home/admin/.keystore or /root/.keystore`. Then the DTLT and AvInstaller should not block to call mcsdk.
5. The user need to import the new public key to the 3rd part dependency processor.

   As the main impact are remote mcsdk service like replication, Concerto, BRM, EMA and IDPA.
6. If the user has multi grids replicates connection below each other, then all grid needs to use or upgrade to the same mcssl certificate.
7. For upgrade impact, the user needs to manually import and replace again as mentioned in the above steps.