Dell EMC Avamar Product Security Guide

Version 18.1

Product Security Guide

302-004-669
REV 06
March 2020

DELL EMC

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 guide 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
06	March 20, 2020	Added vSphere as a destination for port 443 with the Avamar Combined VMware Proxy.
05	November 15, 2019	This revision includes the following updates: • Utility node required inbound ports updates. • Importing commercially signed security certificates for Tomcat DTLT and Jetty updates. • Added steps for configuring LDAPS.
04	August 15, 2019	Updated the section "Required ports when using a Data Domain system."
03	December 11, 2018	Added ports required by Data Domain to "Avamar client required outbound ports."

Revision	Date	Description
		Updates to the section "Remote management interface ports"
02	October 10, 2018	Additional updates for Avamar 18.1
01	July 7, 2018	GA release of Avamar 18.1

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

Table 1 Typographical conventions (continued)

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://support.EMC.com/products.
2. Type a product name in the **Find a Product by Name** box.
3. Select the product from the list that appears.
4. Click the arrow next to the **Find a Product by Name** box.
5. (Optional) Add the product to the **My Products** list by clicking **Add to My Saved Products** in the upper right corner of the **Support by Product** page.

Documentation

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

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

Knowledgebase

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

To search the Knowledgebase:

1. Click **Search** at the top of the page.
2. Type either the solution number or keywords in the search box.
3. (Optional) Limit the search to specific products by typing a product name in the **Scope by product** box and then selecting the product from the list that appears.
4. Select **Knowledgebase** from the **Scope by resource** list.
5. (Optional) Specify advanced options by clicking **Advanced options** and specifying values in the available fields.
6. Click **Search**.

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

About this task

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 60 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.

About this task

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 **`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

User Authentication and Authorization

This chapter includes the following topics:

Overview of Avamar user accounts

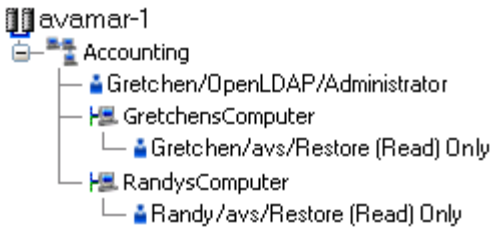
A user account in Avamar can administer a domain or client. The user account defines the authentication system that is used to grant users access to the Avamar server. It also defines the role for the user, which controls the operations that a user can perform.

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 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.

Authentication systems

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.

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.

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 3 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

Table 3 Supported directory service types (continued)

Type	Supported implementations
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.

Add a secure LDAP directory service

Avamar supports encrypted LDAP directory service authentication over SSL (LDAPS). To configure an Avamar system to use an LDAPS directory service for authentication, complete the following steps.

Before you begin

The following information is required:

- Domain name of the LDAP server (for example, *mydomain.com*)
- FQDN or IP address of the LDAP server (for example, *dc-server.mydomain.com*)
- The certificate that is used on the Domain Controller in base64 format (for example, *dc-server.cer*).

Export the Domain Controller's certificate and upload it to the Avamar Server `/tmp` directory.

Configure LDAP directory authentication (non-LDAPS). The *Avamar Administration Guide* provides more information.

About this task

This procedure uses the following examples:

- *mydomain.com*
  where *mydomain.com* is the domain name of the LDAP server.
- *dc-server.mydomain.com*
  where *dc-server.mydomain.com* is the FQDN or IP address of the LDAP server.
- *dc-server.cer*
  where *dc-server.cer* is the LDAP server certificate.

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 `su -`.

3. Back up the existing LDAP files by typing the following commands:

   cp /usr/local/avamar/etc/ldap.properties /usr/local/avamar/etc/ldap.properties.`date -I`

   cp /usr/local/avamar/etc/krb5.conf /usr/local/avamar/etc/krb5.conf.`date -I`

4. Log in to the root domain in Avamar Administrator.
5. In Avamar Administrator, click the **Administration** launcher link.

   The **Administration** window appears.
6. Click the **LDAP Management** tab.
7. Add the LDAPS server by completing the procedure for a regular LDAP server.

   To add a supported LDAP directory service, follow the steps in the *Avamar Administration Guide*.

   The subsequent steps modify the `ldap.properties` file to convert the configuration to LDAPS.
8. Click **Close** to close the **Directory Service Management** window.
9. Click **Edit LDAP file**:
10. Locate the following section:

    ```
    ldap.qualified-name-default=MyDomain.com
    ldap.url.MyDomain.com=ldap\://dc-server.MyDomain.com\:389
    ```

11. Change the **ldap.url.*MyDomain.com*** parameter from `ldap` to `ldaps`.
12. Change the port number to 636.
13. Add the following line:

    ldap.sasl.authentication=false

14. Save and close the `ldap.properties` file.

    The LDAP file resembles the following:

    ```
    ldap.qualified-name-default=MyDomain.com
    ldap.url.MyDomain.com=ldaps\://dc-server.MyDomain.com\:636
    ldap.sasl.authentication=false
    ```

15. Click **Edit KRB5 file**.
16. Locate the following lines in the `[libdefaults]` section.

    ```
    default_tkt_enctypes = rc4-hmac des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
    default_tgs_enctypes = rc4-hmac des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
    ```

17. Add the `aes256-cts` parameter to each line.
18. Save and close the `ldap.properties` file.

    The KRB5 file resembles the following:

    ```
    default_tkt_enctypes = aes256-cts rc4-hmac des3-cbc-sha1-kd des-cbc-crc
    des-cbc-md5
    default_tgs_enctypes = aes256-cts rc4-hmac des3-cbc-sha1-kd des-cbc-crc
    des-cbc-md5
    ```

19. Copy the LDAP server certificate to the `/tmp` directory on the Avamar utility node or single-node server.
20. Ensure that you are still logged in as the root user.

21. Back up `rmi_ssl_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-backup`

22. Import the LDAP server certificate to the keystore by typing the following command:

    `keytool -importcert -file /tmp/`*`dc-server.cer`*` -keystore /usr/local/avamar/lib/rmi_ssl_keystore -storepass `*`password`*

    The default keystore password is `changeme`.

23. Restart the MCS and the backup scheduler by typing the following commands:

    `su - admin`

    `mcserver.sh --stop`

    `mcserver.sh --start`

    `dpnctl start sched`

24. Verify that you can login to Avamar Administrator as an LDAPS user.

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.

Roles

Roles define the allowable operations for each user account.

There are three types of roles:

- Administrator roles
- Operator roles
- User roles

Administrator roles

Administrators are responsible for maintaining the system.

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.

Table 4 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.

Operator roles

Operator roles are generally implemented to allow certain users limited access to certain areas of the system 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 features in Avamar Administrator. Instead, after login, they are presented with a single window that provides access to the features that they are allowed to use.

The following table describes the four operator roles.

Table 5 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 system. 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.
Back up only operator	Back up 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. Back up only operators at the top-level (root) domain can perform backups for any client or group in the system. Back up only operators at domains other than root can only perform backups for clients or groups in that domain. Back up only operators can perform on-demand backups of a client or a group, as well as monitor activities in the assigned domain. • By default, back up 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, back up only operators cannot perform backups from the command line. To enable command line backups for a back up 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.
Back up/restore operator	Back up/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, back up/restore operators at the top-level (root) domain can perform backups and restores for any client or group in the system. Back up/restore operators at domains other than root can only perform backups and restores for clients or groups in that domain. Back up/restore operators can perform the following tasks in the assigned domain: • Perform on-demand backups for a client or group. • Perform restores. • Monitor activities. By default, back up/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

Table 5 Operator roles (continued)

Operator type	Description
	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 Avamar Administrator, Avamar Client Manager, or the Avamar client web UI.

The following table describes the four user roles.

Table 6 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. 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.

Default user accounts

The Avamar system 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.
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.

Table 10 MCS PostgreSQL database default user accounts (continued)

User account	Default password	Description
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 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.

About this task

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 **`su -`**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

```
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.

CHAPTER 3

Client/Server Access and Authentication

This chapter includes the following topics:

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).

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.

About this task

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

```
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
	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

Table 15 Communication security setting (continued)

Communication security setting	Session security setting	Value
	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 Avamar Administrator, click the **Data Movement Policy** launcher link.

   The **Data Movement Policy** window appears.
2. Select the **Groups** tab.
3. Select the desired replication group.
4. Select **Actions** > **Edit Group**.

   The **Edit Replication Group** dialog box appears.
5. Record the value for **Avamar encryption method**. This is the source encryption method.
6. In the **Edit Replication Group** dialog box, click **Cancel**.

Determining the destination server encryption method

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

Procedure

1. In Avamar Administrator, click the **Data Movement Policy** launcher link.

   The **Data Movement Policy** window appears.
2. Select the **Destinations** tab.
3. Select the desired replication destination.
4. Select **Actions** > **Edit Destination**.

   The **Replication Destination** dialog box appears.
5. Record the value for **Encryption**. This is the destination encryption method.
6. In the **Replication Destination** dialog box, click **Cancel**.

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

   ```
   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.

About this task

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

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

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

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

      ```
      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 -l /usr/local/avamar/var/avi/server_data/package_data

   Information similar to the following appears 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 `/usr/local/avamar/lib/avi/avi_keystore -alias tomcat`.

Procedure

1. Switch user to root by typing **su -**.

2. Back up the keystores by typing the following commands, each on one line:

   cp -p /home/admin/.keystore /home/admin/.keystore_bak

   cp -p /usr/local/avamar/lib/rmi_ssl_keystore /usr/local/avamar/lib/rmi_ssl_keystore_bak

   cp -p /usr/local/avamar/lib/avi/avi_keystore /usr/local/avamar/lib/avi/avi_keystore_bak

3. Delete the current security certificate from the admin keystore by typing the following command on one line:

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

4. Regenerate the security certificate and keys from the admin keystore by typing the following command on one line:

   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 a certificate signing request (CSR) by typing the following command on one line:

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

6. Obtain the CSR from the server in the following location and submit it to a CA for signing.

   - `/home/admin/tomcat.csr`

7. 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 `/var/tmp/CA.crt` and that the signed certificate exists in `/var/tmp/tomcat_signed.crt`.

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

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

9. 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

10. Copy the admin keystore to the avi keystore by typing the following commands:

    cp -f /home/admin/.keystore /usr/local/avamar/lib/avi/avi_keystore

    chown avi:avi /usr/local/avamar/lib/avi/avi_keystore

    chmod 644 /usr/local/avamar/lib/avi/avi_keystore

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. Restart EM Tomcat by typing the following command:

    dpnctl stop emt && dpnctl start emt

14. 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.

CHAPTER 4

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 19 Cipher levels and associated OpenSSL suites

Avamar cipher level	OpenSSL suites
cleartext [a]	NULL-SHA

Table 19 Cipher levels and associated OpenSSL suites (continued)

Avamar cipher level	OpenSSL suites
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

While encrypted traffic using the TLS 1.0 and 1.1 is disabled for clients and components, TCP port 30002 is an internal-only exception that supports TLS 1.0 and 1.1. 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 **`su -`**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

```
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.

About this task

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 **`su -`**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

      ```
      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

About this task

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:

```
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 50 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 7.5.1 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 not supported on the Avamar Data Store Gen4 or Gen4S platforms.

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.

About this task

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:

     ```
     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 5

System Monitoring, Auditing, and Logging

This chapter includes the following topics:

Client activity monitoring

You can monitor client backup, restore, and validation activity to verify that backups are successfully completing and that no abnormal activity is occurring.

The Activity Monitor tab on the Activity window in Avamar Administrator provides details on client activity, including the type, status, start, and end time, error code (if applicable), and other details for each client activity.

The *Avamar Administration Guide* provides details on how to access the Activity Monitor tab and filter the activities that appear in the tab.

Server monitoring

There are several features available to assist you in monitoring the Avamar environment, including server status and system events.

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.

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 20 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 20 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 21 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 21 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 21 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 22 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 23 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 24 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 25 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 26 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 27 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

Table 27 Component log files for an Avamar backup client (continued)

Component	Pathname
Avamar Exchange Client	/usr/local/avamar/var/client/{WORKORDER-ID}.log
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

CHAPTER 6

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 28 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 29 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 30 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 **`su -`**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

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

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

```
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 **su -**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

   ```
   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 **su -**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

```
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,qla2xxx,scsi_tr
   ansport_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 60 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 31 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
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

Table 31 STIG requirements satisfied by the additional OS hardening package (continued)

Requirement ID	Requirement title
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.

Additional password hardening satisfies the STIG requirements in the following table.

Table 32 STIG requirements satisfied by additional password hardening

Requirement ID	Requirement title
GEN000540	Password Change 24 Hours
GEN000560	Password Protect Enabled Accounts

Table 32 STIG requirements satisfied by additional password hardening (continued)

Requirement ID	Requirement title
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
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 111 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

About this task

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

About this task

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

      ```
      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.

About this task

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.

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 **`su -`**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

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

```
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.

About this task

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

About this task

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 `su -`.
3. Type the following command:

   `avmaint config sslciphers=`*`level`*` --ava`

   where *level* is the Avamar cipher level in the following table.

Table 33 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.

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 `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.

About this task

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

      ```
      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 `su -`.

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

```
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 `su -`.

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

   ```
   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 `su -`.

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

```
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 `su -`.

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

   ```
   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 `dpnctl start emt`.

CHAPTER 7

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 34 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.
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.

Table 34 Descriptions of security tasks for the IPMI subsystem (continued)

Task	Description
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

Port Requirements

This appendix includes the following topics:

Terminology

This appendix uses specific terms to refer to network concepts that concern Avamar systems.

The following terms are used in this appendix.

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 system 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 system to provide additional functionality. Closing these ports reduces or eliminates the additional functionality but does not prevent the Avamar system from performing its core functions.

Avamar firewall

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.

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 **`su -`**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

   ```
   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.

About this task

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 35 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 **`su -`**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

   ```
   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 `su -`.

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

```
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 **su -**.
   c. For a multi-node server, load the rootid OpenSSH key by typing:

```
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
   ```

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 36 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.
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	Provides web browsers with HTTPS access to Avamar services. A reverse proxy web server can be used to

Table 36 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
			• Avamar Downloader Service host • Avamar Key Manager	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. **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 89 provides more instructions to enable selective access. Limit access to trusted administrator computers.

Table 36 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
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 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

Table 36 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
				trusted administrator computers.
7778–7781	TCP	RMI	Avamar Administrator management console	Used for connections from the Avamar 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 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	

Table 36 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
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.
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

Table 36 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
				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.
30003	TCP	MCS	• Avamar client computers • Avamar server nodes	MCS communication over SSL.
30102–30109	TCP	avagent	VMware proxy	Secure communication with VMware proxy.

Table 36 Required inbound ports on the utility node (continued)

Port	Protocol	Service name	Source computer	Additional information
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 37 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 38 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 • 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.

Table 38 Required outbound ports for the utility node (continued)

Port	Protocol	Destination computer	Additional information
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.
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.

Table 38 Required outbound ports for the utility node (continued)

Port	Protocol	Destination computer	Additional information
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 access Update Manager from other web browser clients.

Table 38 Required outbound ports for the utility node (continued)

Port	Protocol	Destination computer	Additional information
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 permit

Table 38 Required outbound ports for the utility node (continued)

Port	Protocol	Destination computer	Additional information
			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 39 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.

Table 39 Required inbound ports on each storage node (continued)

Port	Protocol	Service name	Source	Additional information
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 40 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.

Table 40 Required outbound ports for each storage node (continued)

Port	Protocol	Destination	Additional information
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 41 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 42 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.
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.

Table 42 Required outbound ports for an Avamar client (continued)

Port	Protocol	Destination	Additional information
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 43 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 44 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 45 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.
		Avamar client			

Table 45 Required ports when using a Data Domain system (continued)

Port	Protocol	Source	Destination	Service	Additional information
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
		Avamar client	Data Domain system	NFS daemon	Only required when backups are stored on a Data Domain system.
2052	TCP/UDP	Utility node	Data Domain system	NFS mountd process	Outbound communication must be open for both protocols: TCP and UDP.
		Avamar client	Data Domain system	NFS mountd process	Only required when backups are stored on a Data Domain system.
3008	TCP	Avamar client	Data Domain system	Archive tier service	Only required when the archive tier feature 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 46 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

Table 46 Required inbound ports for each accelerator node (continued)

Port	Protocol	Source	Additional information
			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 47 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.
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	

Table 47 Required outbound ports for each accelerator node (continued)

Port	Protocol	Destination	Additional information
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 48 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 49 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 50 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.
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 51 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 52 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	
443	TCP / vSphere API	vCenter	
902	TCP / VDDK	ESXi hosts	
2049	TCP/UDP	Data Domain system	
2052	TCP/UDP	Data Domain system	Outbound communication must be open for both protocols: TCP and UDP

Table 52 Required outbound ports for the Avamar VMware Combined Proxy (continued)

Port	Protocol	Destination	Additional information
8543	TCP	Avamar server	Used for VMware snapshot operations
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 53 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 7.5.1 removes support for HTTP access to TCP port 80. Use the HTTPS ports 443 to access these services instead.

Table 54 Inbound ports for the Azure network security group

Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
SSH	TCP	22	::/0
Custom TCP Rule	TCP	161	0.0.0.0/0
Custom TCP Rule	TCP	161	::/0
Custom UDP Rule	UDP	161	0.0.0.0/0
Custom UDP Rule	UDP	161	::/0
Custom TCP Rule	TCP	163	0.0.0.0/0
Custom TCP Rule	TCP	163	::/0
Custom UDP Rule	UDP	163	0.0.0.0/0
Custom UDP Rule	UDP	163	::/0
HTTPS	TCP	443	0.0.0.0/0
HTTPS	TCP	443	::/0
Custom TCP Rule	TCP	700	0.0.0.0/0
Custom TCP Rule	TCP	700	::/0
Custom TCP Rule	TCP	7543	0.0.0.0/0
Custom TCP Rule	TCP	7543	::/0
Custom TCP Rule	TCP	7778 - 7781	0.0.0.0/0
Custom TCP Rule	TCP	7778 - 7781	::/0
Custom TCP Rule	TCP	8543	0.0.0.0/0
Custom TCP Rule	TCP	8543	::/0
Custom TCP Rule	TCP	9090	0.0.0.0/0
Custom TCP Rule	TCP	9090	::/0
Custom TCP Rule	TCP	9443	0.0.0.0/0
Custom TCP Rule	TCP	9443	::/0
Custom TCP Rule	TCP	27000	0.0.0.0/0
Custom TCP Rule	TCP	27000	::/0
Custom TCP Rule	TCP	28001 - 28002	0.0.0.0/0
Custom TCP Rule	TCP	28001 - 28002	::/0
Custom TCP Rule	TCP	28810 - 28819	0.0.0.0/0
Custom TCP Rule	TCP	28810 - 28819	::/0
Custom TCP Rule	TCP	29000	0.0.0.0/0
Custom TCP Rule	TCP	29000	::/0
Custom TCP Rule	TCP	30001 - 30010	0.0.0.0/0

Table 54 Inbound ports for the Azure network security group (continued)

Type	Protocol	Port Range	Source
		Draft comment: Defect 293864	
Custom TCP Rule	TCP	30001 - 30010 **Draft comment:** Defect 293864	::/0

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.

Table 55 Outbound ports for the Azure network security group

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	7	0.0.0.0/0
Custom TCP Rule	TCP	7	::/0
SSH	TCP	22	0.0.0.0/0
SSH	TCP	22	::/0
SMTP	TCP	25	0.0.0.0/0
SMTP	TCP	25	::/0
DNS (UDP)	UDP	53	0.0.0.0/0
DNS (UDP)	UDP	53	::/0
Custom TCP Rule	TCP	111	0.0.0.0/0
Custom TCP Rule	TCP	111	::/0
Custom TCP Rule	UDP	111	0.0.0.0/0
Custom TCP Rule	UDP	111	::/0
Custom TCP Rule	TCP	161	0.0.0.0/0
Custom TCP Rule	TCP	161	::/0
Custom UDP Rule	UDP	161	0.0.0.0/0
Custom UDP Rule	UDP	161	::/0
Custom TCP Rule	TCP	163	0.0.0.0/0
Custom TCP Rule	TCP	163	::/0

Table 55 Outbound ports for the Azure network security group (continued)

Type	Protocol	Port Range	Source
Custom UDP Rule	UDP	163	0.0.0.0/0
Custom UDP Rule	UDP	163	::/0
HTTPS	TCP	443	0.0.0.0/0
HTTPS	TCP	443	::/0
Custom TCP Rule	TCP	700	0.0.0.0/0
Custom TCP Rule	TCP	700	::/0
Custom TCP Rule	TCP	2049	0.0.0.0/0
Custom TCP Rule	TCP	2049	::/0
Custom UDP Rule	UDP	2049	0.0.0.0/0
Custom UDP Rule	UDP	2049	::/0
Custom TCP Rule	TCP	2052	0.0.0.0/0
Custom TCP Rule	TCP	2052	::/0
Custom UDP Rule	UDP	2052	0.0.0.0/0
Custom UDP Rule	UDP	2052	::/0
Custom TCP Rule	TCP	3008	0.0.0.0/0
Custom TCP Rule	TCP	3008	::/0
Custom TCP Rule	TCP	8443	0.0.0.0/0
Custom TCP Rule	TCP	8443	::/0
Custom TCP Rule	TCP	8888	0.0.0.0/0
Custom TCP Rule	TCP	8888	::/0
Custom TCP Rule	TCP	9090	0.0.0.0/0 **Draft comment:** Defect 293864
Custom TCP Rule	TCP	9090	::/0 **Draft comment:** Defect 293864
Custom TCP Rule	TCP	9443	0.0.0.0/0
Custom TCP Rule	TCP	9443	::/0
Custom TCP Rule	TCP	27000	0.0.0.0/0
Custom TCP Rule	TCP	27000	::/0
Custom TCP Rule	TCP	28001-28010	0.0.0.0/0
Custom TCP Rule	TCP	28001-28010	::/0
Custom TCP Rule	TCP	29000	0.0.0.0/0

Table 55 Outbound ports for the Azure network security group (continued)

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	29000	::/0
Custom TCP Rule	TCP	30001-30010	0.0.0.0/0
Custom TCP Rule	TCP	30001-30010	::/0

APPENDIX B

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 C

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 56 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
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.

About this task

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 `su -`.

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

```
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 D

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 **`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.
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.

Property name	Value description
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.

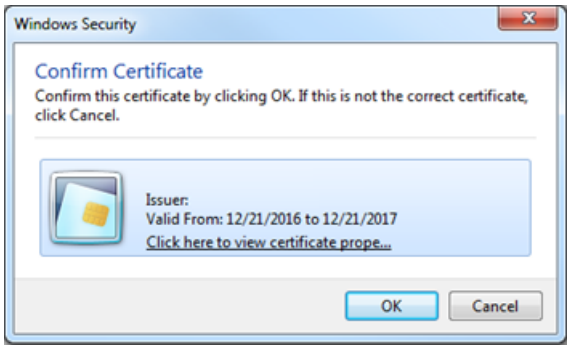
   A **Windows Security** dialog box appears, prompting the user to type the authentication PIN for the smart card.

   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

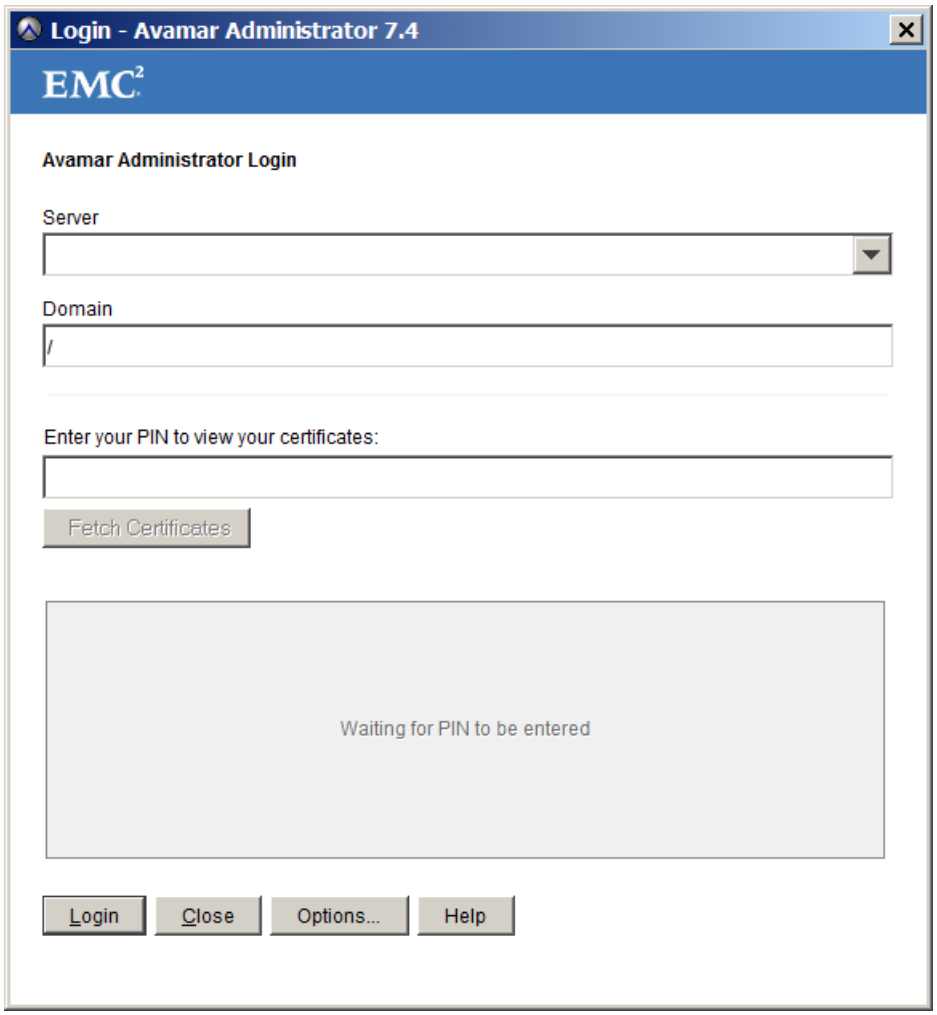
When CAC/PIV authentication is enabled, use the following steps to log in to Avamar Administrator.

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.

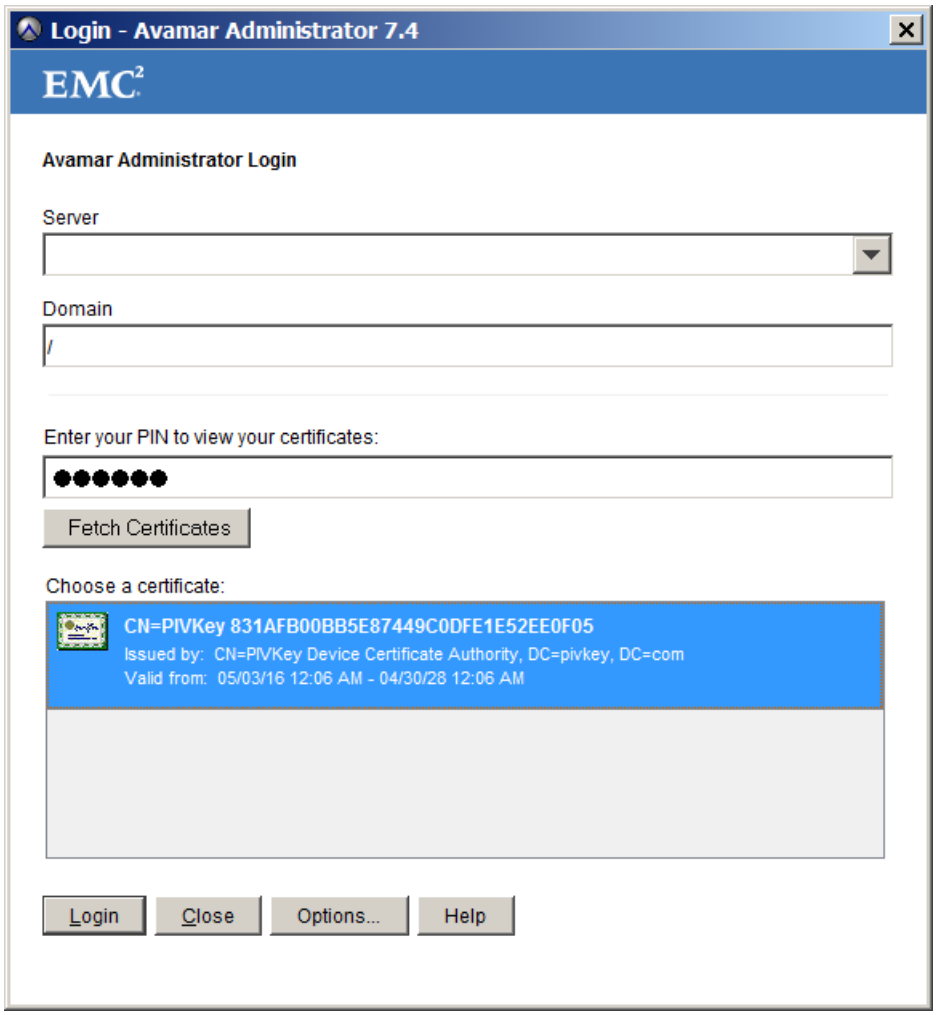
Figure 5 Avamar Administrator Login window



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**.

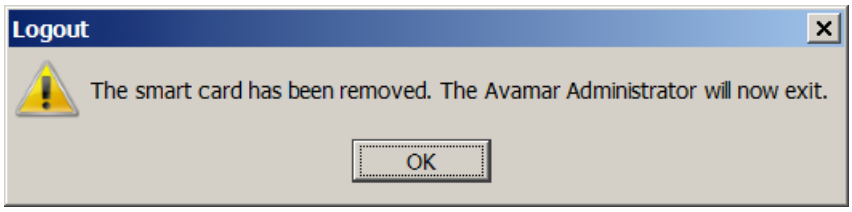
   The Avamar server validates the selected security certificate with the VA server and interfaces with the LDAP server to complete the login process.

   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 `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
```