# NetApp

# Security and data encryption

ONTAP 9

NetApp
March 09, 2023

# Table of Contents

# Security and data encryption

## Manage security with System Manager

### Security management overview with System Manager

Beginning with ONTAP 9.7, you can manage cluster security with System Manager.

With System Manager, you use ONTAP standard methods to secure client and administrator access to storage and to protect against viruses. Advanced technologies are available for encryption of data at rest and for WORM storage.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), refer to System Manager Classic (ONTAP 9.0 to 9.7)

#### Client authentication and authorization

ONTAP authenticates a client machine and user by verifying their identities with a trusted source. ONTAP authorizes a user to access a file or directory by comparing the user's credentials with the permissions configured on the file or directory.

#### Administrator authentication and RBAC

Administrators use local or remote login accounts to authenticate themselves to the cluster and storage VM. Role-Based Access Control (RBAC) determines the commands to which an administrator has access.

#### Virus scanning

You can use integrated antivirus functionality on the storage system to protect data from being compromised by viruses or other malicious code. ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

#### Encryption

ONTAP offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

#### WORM storage

*SnapLock* is a high-performance compliance solution for organizations that use *write once, read many (WORM)* storage to retain critical files in unmodified form for regulatory and governance purposes.

### Set up multifactor authentication

Security Assertion Markup Language (SAML) authentication allows users to log in to an application by using a secure identity provider (IdP).

In System Manager, in addition to standard ONTAP authentication, SAML-based authentication is provided as an option for multifactor authentication.

Security Assertion Markup Language (SAML) is an XML-based framework for authentication and authorization

between two entities: a service provider and an identity provider.

**Enable SAML authentication**



To enable SAML authentication, perform the following steps:

**Steps**

1. Click **Cluster > Settings**.

2. Next to **SAML Authentication**, click ⚙.

3. Ensure there is a check in the **Enable SAML Authentication** checkbox.

4. Enter the URL of the IdP URI (including "https://").

5. Modify the host system address, if needed.

6. Ensure the correct certificate is being used:

    ◦ If your system was mapped with only one certificate with type "server", then that certificate is considered the default and it isn't displayed.

    ◦ If your system was mapped with multiple certificates as type "server", then one of the certificates is displayed. To select a different certificate, click **Change**.

7. Click **Save**. A confirmation window displays the metadata information, which has been automatically copied to your clipboard.

8. Go to the IdP system you specified and copy the metadata from your clipboard to update the system metadata.

9. Return to the confirmation window (in System Manager) and check the checkbox **I have configured the IdP with the host URI or metadata**.

10. Click **Logout** to enable SAML-based authentication. The IdP system will display an authentication screen.

11. In the IdP system, enter your SAML-based credentials. After your credentials are verified, you will be directed to the System Manager home page.

**Disable SAML authentication**

To disable SAML authentication, perform the following steps:

**Steps**

1. Click **Cluster > Settings**.

2. Under **SAML Authentication**, click the **Enabled** toggle button.

3. *Optional*: You can also click ⚙ next to **SAML Authentication**, and then uncheck the **Enable SAML Authentication** checkbox.

## Control administrator access

The role assigned to an administrator determines which functions the administrator can perform with System Manager. Predefined roles for cluster administrators and storage VM administrators are provided by System Manager. You assign the role when you create the administrator's account, or you can assign a different role later.

Depending on how you have enabled account access, you might need to perform any of the following:

- Associate a public key with a local account.
- Install a CA-signed server digital certificate.
- Configure AD, LDAP, or NIS access.

You can perform these tasks before or after enabling account access.

**Assigning a role to an administrator**

Assign a role to an administrator, as follows:

**Steps**

1. Select **Cluster > Settings**.

2. Select → next to **Users and Roles**.

3. Select ＋ Add under **Users**.

4. Specify a user name, and select a role in the drop-down menu for **Role**.

5. Specify a login method and password for the user.

**Changing an administrator's role**

Change the role for an administrator, as follows:

**Steps**

1. Click **Cluster > Settings**.

2. Select the name of user whose role you want to change, then click the ⋮ that appears next to the user name.

3. Click **Edit**.

4. Select a role in the drop-down menu for **Role**.

## Diagnose and correct file access issues

**Steps**

1. In System Manager, select **Storage > Storage VMs**.

2. Select the storage VM on which you want to perform a trace.

3. Click ⋮ **More**.

4. Click **Trace File Access**.

5. Provide the user name and client IP address, then click **Start Tracing**.

   The trace results are displayed in a table. The **Reasons** column provides the reason why a file could not be accessed.

6. Click ⌄ in the left column of the results table to view the file access permissions.

## Manage certificates with System Manager

Beginning with ONTAP 9.10.1, you can use System Manager to manage trusted certificate authorities, client/server certificates, and local (onboard) certificate authorities.

With System Manager, you can manage the certificates received from other applications so you can authenticate communications from those applications. You can also manage your own certificates that identify your system to other applications.

### View certificate information

With System Manager, you can view trusted certificate authorities, client/server certificates, and local certificate authorities that are stored on the cluster.

**Steps**

1. In System Manager, click **Cluster > Settings**.

2. Scroll to the **Security** area.
   In the **Certificates** section, the following details are displayed:

   - The number of stored trusted certificate authorities.

   - The number of stored client/server certificates.

   - The number of stored local certificate authorities.

3. Click any number to view details about a category of certificates, or click → to view the **Certificates** page, which contains information about all categories.
   The list displays the information for the entire cluster. If you want to display information for only a specific storage VM, perform the following steps:

   a. Click **Storage > Storage VMs**.

   b. Select the storage VM.

   c. View the **Settings** tab.

   d. Click a number shown in the **Certificate** section.

**What to do next**

- From the **Certificates** page, you can Generate a certificate signing request.

- The certificate information is separated into three tabs, one for each category. You can perform the following tasks from each tab:

| On this tab… | You can perform these procedures… |
|---|---|
| **Trusted certificate authorities** | • Install (add) a trusted certificate authority<br><br>• Delete a trusted certificate authority<br><br>• Renew a trusted certificate authority |
| **Client/server certificates** | • Install (add) a client/server certificate<br><br>• Generate (add) a self-signed client/server certificate<br><br>• Delete a client/server certificate<br><br>• Renew a client/server certificate |
| **Local certificate authorities** | • Create a new local certificate authority<br><br>• Sign a certificate using a local certificate authority<br><br>• Delete a local certificate authority<br><br>• Renew a local certificate authority |

### Generate a certificate signing request

You can generate a certificate signing request (CSR) with System Manager from any tab of the **Certificates** page. A private key and a corresponding CSR are generated, which can be signed using a certificate authority to generate a public certificate.

**Steps**

1. View the **Certificates** page. See View certificate information.
2. Click **+Generate CSR**.
3. Complete the information for the subject name:
    a. Enter a **common name**.
    b. Select a **country**.
    c. Enter an **organization**.
    d. Enter an **organization unit**.
4. If you want to override defaults, select **More Options** and provide additional information.

### Install (add) a trusted certificate authority

You can install additional trusted certificate authorities in System Manager.

**Steps**

1. View the **Trusted Certificate Authorities** tab. See View certificate information.
2. Click **+ Add**.
3. On the **Add Trusted Certificate Authority** panel, perform the following:

- Enter a **name**.

- For the **scope**, select a storage VM.

- Enter a **common name**.

- Select a **type**.

- Enter or import **certificate details**.

## Delete a trusted certificate authority

With System Manager, you can delete a trusted certificate authority.

ⓘ You cannot delete trusted certificate authorities that were preinstalled with ONTAP.

**Steps**

1. View the **Trusted Certificate Authorities** tab. See View certificate information.

2. Click the name of the trusted certificate authority.

3. Click ⋮ next to the name, then click **Delete**.

## Renew a trusted certificate authority

With System Manager, you can renew a trusted certificate authority that has expired or is about to expire.

**Steps**

1. View the **Trusted Certificate Authorities** tab. See View certificate information.

2. Click the name of the trusted certificate authority.

3. Click ⋮ next to the name, then click **Renew**.

## Install (add) a client/server certificate

With System Manager, you can install additional client/server certificates.

**Steps**

1. View the **Client/Server Certificates** tab. See View certificate information.

2. Click **+ Add**.

3. On the **Add Client/Server Certificate** panel, perform the following:

- Enter a **certificate name**.

- For the **scope**, select a storage VM.

- Enter a **common name**.

- Select a **type**.

- Enter or import **certificate details**.
  You can either write in or copy and paste in the certificate details from a text file or you can import the text from a certificate file by clicking **Import**.

- Enter a the **private key**.
  You can either write in or copy and paste in the private key from a text file or you can import the text from a private key file by clicking **Import**.

**Generate (add) a self-signed client/server certificate**

With System Manager, you can generate additional self-signed client/server certificates.

**Steps**

1. View the **Client/Server Certificates** tab. See View certificate information.
2. Click **+Generate Self-signed Certificate**.
3. On the **Generate Self-Signed Certificate** panel, perform the following:

   - Enter a **certificate name**.
   - For the **scope**, select a storage VM.
   - Enter a **common name**.
   - Select a **type**.
   - Select a **hash function**.
   - Select a **key size**.
   - Select a **storage VM**.

**Delete a client/server certificate**

With System Manager, you can delete client/server certificates.

**Steps**

1. View the **Client/Server Certificates** tab. See View certificate information.
2. Click the name of the client/server certificate.
3. Click ⋮ next to the name, then click **Delete**.

**Renew a client/server certificate**

With System Manager, you can renew a client/server certificate that has expired or is about to expire.

**Steps**

1. View the **Client/Server Certificates** tab. See View certificate information.
2. Click the name of the client/server certificate.
3. Click ⋮ next to the name, then click **Renew**.

**Create a new local certificate authority**

With System Manager, you can create a new local certificate authority.

**Steps**

1. View the **Local Certificate Authorities** tab. See View certificate information.
2. Click **+ Add**.
3. On the **Add Local Certificate Authority** panel, perform the following:

   - Enter a **name**.
   - For the **scope**, select a storage VM.
   - Enter a **common name**.

4. If you want to override defaults, select **More Options** and provide additional information.

**Sign a certificate using a local certificate authority**

In System Manager, you can use a local certificate authority to sign a certificate.

**Steps**

1. View the **Local Certificate Authorities** tab. See View certificate information.
2. Click the name of the local certificate authority.
3. Click ⋮ next to the name, then click **Sign a certificate**.
4. Complete the **Sign a Certificate Signing Request** form.
   - You can either paste in the certificate signing content or import a certificate signing request file by clicking **Import**.
   - Specify the number of days for which the certificate will be valid.

**Delete a local certificate authority**

With System Manager, you can delete a local certificate authority.

**Steps**

1. View the **Local Certificate Authority** tab. See View certificate information.
2. Click the name of the local certificate authority.
3. Click ⋮ next to the name, then click **Delete**.

**Renew a local certificate authority**

With System Manager, you can renew a local certificate authority that has expired or is about to expire.

**Steps**

1. View the **Local Certificate Authority** tab. See View certificate information.
2. Click the name of the local certificate authority.
3. Click ⋮ next to the name, then click **Renew**.

# Manage administrator authentication and RBAC with the CLI

## Administrator authentication and RBAC overview with the CLI

You can enable login accounts for ONTAP cluster administrators and storage virtual machine (SVM) administrators. You can also use role-based access control (RBAC) to define the capabilities of administrators.

You enable login accounts and RBAC in the following ways:

- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.
- You want to use best practices, not explore every available option.

- You are not using SNMP to collect information about the cluster.

## Administrator authentication and RBAC workflow

You can enable authentication for local administrator accounts or remote administrator accounts. The account information for a local account resides on the storage system and the account information for a remote account resides elsewhere. Each account can have a predefined role or a custom role.



You can enable local administrator accounts to access an admin storage virtual machine (SVM) or a data SVM with the following types of authentication:

- Password
- SSH public key
- SSL certificate
- SSH multifactor authentication (MFA)

  Beginning with ONTAP 9.3, authentication with password and public key is supported.

You can enable remote administrator accounts to access an admin SVM or a data SVM with the following types of authentication:

- Active Directory
- SAML authentication (only for admin SVM)

  Beginning with ONTAP 9.3, Security Assertion Markup Language (SAML) authentication can be used for

accessing the admin SVM by using any of the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

- Beginning with ONTAP 9.4, SSH MFA can be used for remote users on LDAP or NIS servers. Authentication with nsswitch and public key is supported.

## Worksheets for administrator authentication and RBAC configuration

Before creating login accounts and setting up role-based access control (RBAC), you should gather information for each item in the configuration worksheets.

### Create or modify login accounts

You provide these values with the `security login create` command when you enable login accounts to access a storage virtual machine (SVM). You provide the same values with the `security login modify` command when you modify how an account accesses an SVM.

| Field | Description | Your value |
|---|---|---|
| `-vserver` | The name of the SVM that the account accesses. The default value is the name of the admin SVM for the cluster. | |
| `-user-or-group-name` | The user name or group name of the account. Specifying a group name enables access to each user in the group. You can associate a user name or group name with multiple applications. | |
| `-application` | The application that is used to access the SVM:<br><br>• `http`<br><br>• `ontapi`<br><br>• `snmp`<br><br>• `ssh` | |

| | | |
|---|---|---|
| `-authmethod` | The method that is used to authenticate the account:<br><br>• `cert` for SSL certificate authentication<br><br>• `domain` for Active Directory authentication<br><br>• `nsswitch` for LDAP or NIS authentication<br><br>• `password` for user password authentication<br><br>• `publickey` for public key authentication<br><br>• `community` for SNMP community strings<br><br>• `usm` for SNMP user security model<br><br>• `saml` for Security Assertion Markup Language (SAML) authentication | |
| `-remote-switch-ipaddress` | The IP address of the remote switch. The remote switch can be a cluster switch monitored by the cluster switch health monitor (CSHM) or a Fibre Channel (FC) switch monitored by the MetroCluster health monitor (MCC-HM). This option is applicable only when the application is `snmp` and the authentication method is `usm`. | |
| `-role` | The access control role that is assigned to the account:<br><br>• For the cluster (the admin SVM), the default value is `admin`.<br><br>• For a data SVM, the default value is `vsadmin`. | |
| `-comment` | (Optional) Descriptive text for the account. You should enclose the text in double quotation marks ("). | |

| | | |
|---|---|---|
| `-is-ns-switch-group` | Whether the account is an LDAP group account or NIS group account (`yes` or `no`). | |
| `-second-authentication -method` | Second authentication method in case of multifactor authentication in **ONTAP 9.3**:<br><br>• `none` if not using multifactor authentication, default value<br><br>• `publickey` for public key authentication when the `authmethod` is password or nsswitch<br><br>• `password` for user password authentication when the `authmethod` is public key<br><br>• `nsswitch` for user password authentication when the authmethod is publickey<br><br>    (i)   Beginning with ONTAP 9.4, support for nsswitch is available.<br><br>The order of authentication is always the public key followed by the password. | |
| `-is-ldap-fastbind` | Beginning with ONTAP 9.11.1, when set to true, enables LDAP fast bind for nsswitch authentication; the default is false. To use LDAP fast bind, the `-authentication-method` value must be set to `nsswitch`. Learn about LDAP fastbind for nsswitch authentication. | |

**Define custom roles**

You provide these values with the `security login role create` command when you define a custom role.

| Field | Description | Your value |
|---|---|---|
| | | |

| | | |
|---|---|---|
| `-vserver` | (Optional) The name of the SVM that is associated with the role. | |
| `-role` | The name of the role. | |
| `-cmddirname` | The command or command directory to which the role gives access. You should enclose command subdirectory names in double quotation marks ("). For example, `"volume snapshot"`. You must enter `DEFAULT` to specify all command directories. | |
| `-access` | (Optional) The access level for the role. For command directories: <br><br> • `none` (the default value for custom roles) denies access to commands in the command directory <br><br> • `readonly` grants access to the `show` commands in the command directory and its subdirectories <br><br> • `all` grants access to all of the commands in the command directory and its subdirectories <br><br> For *nonintrinsic commands* (commands that do not end in `create`, `modify`, `delete`, or `show`): <br><br> • `none` (the default value for custom roles) denies access to the command <br><br> • `readonly` is not applicable <br><br> • `all` grants access to the command <br><br> To grant or deny access to intrinsic commands, you must specify the command directory. | |

| | |
|---|---|
| `-query` | (Optional) The query object that is used to filter the access level, which is specified in the form of a valid option for the command or for a command in the command directory. You should enclose the query object in double quotation marks ("). For example, if the command directory is `volume`, the query object `"-aggr aggr0"` would enable access for the `aggr0` aggregate only. |

**Associate a public key with a user account**

You provide these values with the `security login publickey create` command when you associate an SSH public key with a user account.

| Field | Description | Your value |
|---|---|---|
| `-vserver` | (Optional) The name of the SVM that the account accesses. | |
| `-username` | The user name of the account. The default value, `admin`, which is the default name of the cluster administrator. | |
| `-index` | The index number of the public key. The default value is 0 if the key is the first key that is created for the account; otherwise, the default value is one more than the highest existing index number for the account. | |
| `-publickey` | The OpenSSH public key. You should enclose the key in double quotation marks ("). | |
| `-role` | The access control role that is assigned to the account. | |
| `-comment` | (Optional) Descriptive text for the public key. You should enclose the text in double quotation marks ("). | |

**Install a CA-signed server digital certificate**

You provide these values with the `security certificate generate-csr` command when you generate a digital certificate signing request (CSR) for use in authenticating an SVM as an SSL server.

| Field | Description | Your value |
|---|---|---|
| `-common-name` | The name of the certificate, which is either a fully qualified domain name (FQDN) or a custom common name. | |
| `-size` | The number of bits in the private key. The higher the value, the more secure the key. The default value is `2048`. Possible values are `512`, `1024`, `1536`, and `2048`. | |
| `-country` | The country of the SVM, in a two-letter code. The default value is `US`. See the man pages for a list of codes. | |
| `-state` | The state or province of the SVM. | |
| `-locality` | The locality of the SVM. | |
| `-organization` | The organization of the SVM. | |
| `-unit` | The unit in the organization of the SVM. | |
| `-email-addr` | The email address of the contact administrator for the SVM. | |
| `-hash-function` | The cryptographic hashing function for signing the certificate. The default value is `SHA256`. Possible values are `SHA1`, `SHA256`, and `MD5`. | |

You provide these values with the `security certificate install` command when you install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server. Only the options that are relevant to account configuration are shown in the following table.

| Field | Description | Your value |
|---|---|---|
| `-vserver` | The name of the SVM on which the certificate is to be installed. | |

| | | |
|---|---|---|
| `-type` | The certificate type:<br><br>• `server` for server certificates and intermediate certificates<br><br>• `client-ca` for the public key certificate of the root CA of the SSL client<br><br>• `server-ca` for the public key certificate of the root CA of the SSL server of which ONTAP is a client<br><br>• `client` for a self-signed or CA-signed digital certificate and private key for ONTAP as an SSL client | |

**Configure Active Directory domain controller access**

You provide these values with the `security login domain-tunnel create` command when you have already configured a SMB server for a data SVM and you want to configure the SVM as a gateway or *tunnel* for Active Directory domain controller access to the cluster.

| Field | Description | Your value |
|---|---|---|
| `-vserver` | The name of the SVM for which the SMB server has been configured. | |

You provide these values with the `vserver active-directory create` command when you have not configured a SMB server and you want to create an SVM computer account on the Active Directory domain.

| Field | Description | Your value |
|---|---|---|
| `-vserver` | The name of the SVM for which you want to create an Active Directory computer account. | |
| `-account-name` | The NetBIOS name of the computer account. | |
| `-domain` | The fully qualified domain name (FQDN). | |
| `-ou` | The organizational unit in the domain. The default value is `CN=Computers`. ONTAP appends this value to the domain name to produce the Active Directory distinguished name. | |

**Configure LDAP or NIS server access**

You provide these values with the `vserver services name-service ldap client create` command when you create an LDAP client configuration for the SVM.

> ⓘ Beginning with ONTAP 9.2, the `-ldap-servers` field replaces the `-servers` field. This new field can take either a host name or an IP address as the value for the LDAP server.

Only the options that are relevant to account configuration are shown in the following table:

| Field | Description | Your value |
|---|---|---|
| `-vserver` | The name of the SVM for the client configuration. | |
| `-client-config` | The name of the client configuration. | |
| `-servers` | **ONTAP 9.0, 9.1**: A comma-separated list of IP addresses for the LDAP servers to which the client connects. | |
| `-ldap-servers` | **ONTAP 9.2**: A comma-separated list of IP addresses and host names for the LDAP servers to which the client connects. | |
| `-schema` | The schema that the client uses to make LDAP queries. | |
| `-use-start-tls` | Whether the client uses Start TLS to encrypt communication with the LDAP server (`true` or `false`). <br><br> ⓘ Start TLS is supported for access to data SVMs only. It is not supported for access to admin SVMs. | |

You provide these values with the `vserver services name-service ldap create` command when you associate an LDAP client configuration with the SVM.

| Field | Description | Your value |
|---|---|---|

| | | |
|---|---|---|
| `-vserver` | The name of the SVM with which the client configuration is to be associated. | |
| `-client-config` | The name of the client configuration. | |
| `-client-enabled` | Whether the SVM can use the LDAP client configuration (`true` or `false`). | |

You provide these values with the `vserver services name-service nis-domain create` command when you create an NIS domain configuration on an SVM.

ⓘ Beginning with ONTAP 9.2, the `-nis-servers` field replaces the `-servers` field. This new field can take either a host name or an IP address as the value for the NIS server.

| Field | Description | Your value |
|---|---|---|
| `-vserver` | The name of the SVM on which the domain configuration is to be created. | |
| `-domain` | The name of the domain. | |
| `-active` | Whether the domain is active (`true` or `false`). | |
| `-servers` | **ONTAP 9.0, 9.1**: A comma-separated list of IP addresses for the NIS servers that are used by the domain configuration. | |
| `-nis-servers` | **ONTAP 9.2**: A comma-separated list of IP addresses and host names for the NIS servers that are used by the domain configuration. | |

You provide these values with the `vserver services name-service ns-switch create` command when you specify the look-up order for name service sources.

| Field | Description | Your value |
|---|---|---|
| `-vserver` | The name of the SVM on which the name service look-up order is to be configured. | |

| | | |
|---|---|---|
| `-database` | The name service database: <br><br> • `hosts` for files and DNS name services <br><br> • `group` for files, LDAP, and NIS name services <br><br> • `passwd` for files, LDAP, and NIS name services <br><br> • `netgroup` for files, LDAP, and NIS name services <br><br> • `namemap` for files and LDAP name services | |
| `-sources` | The order in which to look up name service sources (in a comma-separated list): <br><br> • `files` <br><br> • `dns` <br><br> • `ldap` <br><br> • `nis` | |

## Configure SAML access

Beginning with ONTAP 9.3, you provide these values with the `security saml-sp create` command to configure SAML authentication.

| Field | Description | Your value |
|---|---|---|
| `-idp-uri` | The FTP address or HTTP address of the Identity Provider (IdP) host from where the IdP metadata can be downloaded. | |
| `-sp-host` | The host name or IP address of the SAML service provider host (ONTAP system). By default, the IP address of the cluster-management LIF is used. | |
| `-cert-ca` and `-cert-serial`, or `-cert-common-name` | The server certificate details of the service provider host (ONTAP system). You can enter either the service provider's certificate issuing certification authority (CA) and the certificate's serial number, or the Server Certificate Common Name. | |

| `-verify-metadata-server` | Whether the identity of the IdP metadata server must be validated (`true` or `false`). The best practice is to always set this value to `true`. | |
|---|---|---|

## Create login accounts

### Create login accounts overview

You can enable local or remote cluster and SVM administrator accounts. A local account is one in which the account information, public key, or security certificate resides on the storage system. AD account information is stored on a domain controller. LDAP and NIS accounts reside on LDAP and NIS servers.

#### Cluster and SVM administrators

A *cluster administrator* accesses the admin SVM for the cluster. The admin SVM and a cluster administrator with the reserved name `admin` are automatically created when the cluster is set up.

A cluster administrator with the default `admin` role can administer the entire cluster and its resources. The cluster administrator can create additional cluster administrators with different roles as needed.

An *SVM administrator* accesses a data SVM. The cluster administrator creates data SVMs and SVM administrators as needed.

SVM administrators are assigned the `vsadmin` role by default. The cluster administrator can assign different roles to SVM administrators as needed.

> ⓘ The following generic names cannot be used for remote cluster and SVM administrator accounts: "adm", "bin", "cli", "daemon", "ftp", "games", "halt", "lp", "mail", "man", "naroot", "netapp", "news", "nobody", "operator", "root", "shutdown", "sshd", "sync", "sys", "uucp", and "www".

#### Merged roles

If you enable multiple remote accounts for the same user, the user is assigned the union of all roles specified for the accounts. That is, if an LDAP or NIS account is assigned the `vsadmin` role, and the AD group account for the same user is assigned the `vsadmin-volume` role, the AD user logs in with the more inclusive `vsadmin` capabilities. The roles are said to be *merged*.

### Enable local account access

#### Enable local account access overview

A local account is one in which the account information, public key, or security certificate resides on the storage system. You can use the `security login create` command to enable local accounts to access an admin or data SVM.

**Enable password account access**

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with a password. You are prompted for the password after you enter the command.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

**Step**

1. Enable local administrator accounts to access an SVM using a password:

   `security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment`

   For complete command syntax, see the worksheet.

   The following command enables the cluster administrator account `admin1` with the predefined `backup` role to access the admin SVM`engCluster` using a password. You are prompted for the password after you enter the command.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

**Enable SSH public key accounts**

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSH public key.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

- You must associate the public key with the account before the account can access the SVM.

  Associating a public key with a user account

  You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

If you want to enable SSL FIPS mode on a cluster where administrator accounts authenticate with an SSH public key before accessing SVMs, you must ensure that the host key algorithm is supported before enabling FIPS.

**Note:** Host key algorithm support has changed in ONTAP 9.11.1 and later releases.

| ONTAP release | Supported key types | Unsupported key types |
|---|---|---|
| 9.11.1 and later | ecdsa-sha2-nistp256 | rsa-sha2-512<br>rsa-sha2-256<br>ssh-ed25519<br>ssh-dss<br>ssh-rsa |
| 9.10.1 and earlier | ecdsa-sha2-nistp256<br>ssh-ed25519 | ssh-dss<br>ssh-rsa |

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type before enabling FIPS, or the administrator authentication will fail.

For more information, see Configure network security using FIPS.

**Step**

1. Enable local administrator accounts to access an SVM using an SSH public key:

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   For complete command syntax, see the worksheet.

   The following command enables the SVM administrator account `svmadmin1` with the predefined `vsadmin-volume` role to access the SVM`engData1` using an SSH public key:

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

**After you finish**

If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

Associating a public key with a user account

**Enable SSH multifactor authentication (MFA)**

Beginning with ONTAP 9.3, you can use the `security login create` command to enhance security by requiring that administrators log in to an admin or data SVM with both an SSH public key and a user password.

Beginning with ONTAP 9.12.1, you can use Yubikey hardware authentication devices for SSH client MFA using the FIDO2 (Fast IDentity Online) or Personal Identity Verification (PIV) authentication standards.

Learn more about Multifactor Authentication in ONTAP 9 (TR-4647).

**Before you begin**

You must be a cluster administrator to perform this task.

**About this task**

- You must associate the public key with the account before the account can access the SVM.

  Associate a public key with a user account

  You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

  Modifying the role assigned to an administrator

- The user is always authenticated with public key authentication followed by password authentication.

**Step**

1. Require local administrator accounts to access an SVM using SSH MFA:

   `security login create -vserver SVM -user-or-group-name user_name -application ssh -authentication-method password|publickey -role admin -second -authentication-method password|publickey`

   The following command requires the SVM administrator account `admin2` with the predefined `admin` role to log in to the SVM`engData1` with both an SSH public key and a user password:

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

**After you finish**

If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

Associating a public key with a user account

**Enable SSL certificate accounts**

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSL certificate.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

- You must install a CA-signed server digital certificate before the account can access the SVM.

  Generating and installing a CA-signed server certificate

  You can perform this task before or after you enable account access.

- If you are unsure of the access control role you want to assign to the login account, you can add the role later with the `security login modify` command.

  Modifying the role assigned to an administrator

> **(i)** For cluster administrator accounts, certificate authentication is supported only with the `http` and `ontapi` applications. For SVM administrator accounts, certificate authentication is supported only with the `ontapi` application.

**Step**

1. Enable local administrator accounts to access an SVM using an SSL certificate:

   `security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment`

   For complete command syntax, see the ONTAP man pages by release.

   The following command enables the SVM administrator account `svmadmin2` with the default `vsadmin` role to access the SVM`engData2` using an SSL digital certificate.

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

**After you finish**

If you have not installed a CA-signed server digital certificate, you must do so before the account can access the SVM.

Generating and installing a CA-signed server certificate

**Enable Active Directory account access**

You can use the `security login create` command to enable Active Directory (AD) user or group accounts to access an admin or data SVM. Any user in the AD group can access the SVM with the role that is assigned to the group.

**What you'll need**

- The cluster time must be synchronized to within five minutes of the time on the AD domain controller.
- You must be a cluster administrator to perform this task.

**About this task**

- You must configure AD domain controller access to the cluster or SVM before the account can access the SVM.

[Configuring Active Directory domain controller access](#)

You can perform this task before or after you enable account access.

- Beginning with ONTAP 9.11.1, you can use [LDAP fast bind for nsswitch authentication](#) if it is supported by the AD LDAP server.
- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

[Modifying the role assigned to an administrator](#)

> (i) AD group account access is supported only with the `SSH` and `ontapi` applications.

**Step**

1. Enable AD user or group administrator accounts to access an SVM:

   `security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod domain -role role -comment comment [-is-ldap-fastbind true]`

   For complete command syntax, see the [worksheet](#).

   [Creating or modifying login accounts](#)

   The following command enables the AD cluster administrator account `DOMAIN1\guest1` with the predefined `backup` role to access the admin SVM`engCluster`.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role backup
   ```

   The following command enables the SVM administrator accounts in the AD group account `DOMAIN1\adgroup` with the predefined `vsadmin-volume` role to access the SVM`engData`.

   ```
   cluster1::>security login create -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vsadmin-volume
   ```

**After you finish**

If you have not configured AD domain controller access to the cluster or SVM, you must do so before the account can access the SVM.

[Configuring Active Directory domain controller access](#)

**Enable LDAP or NIS account access**

You can use the `security login create` command to enable LDAP or NIS user

accounts to access an admin or data SVM. If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

- Group accounts are not supported.

- You must configure LDAP or NIS server access to the SVM before the account can access the SVM.

  Configuring LDAP or NIS server access

  You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

  Modifying the role assigned to an administrator

- Beginning with ONTAP 9.4, multifactor authentication (MFA) is supported for remote users over LDAP or NIS servers.

- Beginning with ONTAP 9.11.1, you can use LDAP fast bind for nsswitch authentication if it is supported by the LDAP server.

- Because of a known LDAP issue, you should not use the `':'` (colon) character in any field of LDAP user account information (for example, `gecos`, `userPassword`, and so on). Otherwise, the lookup operation will fail for that user.

**Steps**

1. Enable LDAP or NIS user or group accounts to access an SVM:

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   For complete command syntax, see the worksheet.

   Creating or modifying login accounts

   The following command enables the LDAP or NIS cluster administrator account `guest2` with the predefined `backup` role to access the admin SVM`engCluster`.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   guest2 -application ssh -authmethod nsswitch -role backup
   ```

2. Enable MFA login for LDAP or NIS users:

   ```
   security login modify -user-or-group-name rem_usr1 -application ssh
   -authentication-method nsswitch -role admin -is-ns-switch-group no -second
   -authentication-method publickey
   ```

The authentication method can be specified as `publickey` and second authentication method as `nsswitch`.

The following example shows the MFA authentication being enabled:

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

**After you finish**

If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

Configuring LDAP or NIS server access

**Configure SAML authentication**

Beginning with ONTAP 9.3, you can configure Security Assertion Markup Language (SAML) authentication for web services. When SAML authentication is configured and enabled, users are authenticated by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP.

**What you'll need**

- You must have configured the IdP for SAML authentication.
- You must have the IdP URI.

**About this task**

- SAML authentication applies only to the `http` and `ontapi` applications.

  The `http` and `ontapi` applications are used by the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

- SAML authentication is applicable only for accessing the admin SVM.

**Steps**

1. Create a SAML configuration so that ONTAP can access the IdP metadata:

   `security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name`

   `idp_uri` is the FTP or HTTP address of the IdP host from where the IdP metadata can be downloaded.

   `ontap_host_name` is the host name or IP address of the SAML service provider host, which in this case is the ONTAP system. By default, the IP address of the cluster-management LIF is used.

   You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.

```
cluster_12::> security saml-sp create -idp-uri
https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify
-metadata-server false

Warning: This restarts the web server. Any HTTP/S connections that are
active
          will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.63.56.150/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server
domain to ensure that users are the same for different authentication
methods. See the "security login show" command for the Data ONTAP user
configuration.
```

The URL to access the ONTAP host metadata is displayed.

2. From the IdP host, configure the IdP with the ONTAP host metadata.

   For more information about configuring the IdP, see the IdP documentation.

3. Enable SAML configuration:

   `security saml-sp modify -is-enabled true`

   Any existing user that accesses the `http` or `ontapi` application is automatically configured for SAML authentication.

4. If you want to create users for the `http` or `ontapi` application after SAML is configured, specify SAML as the authentication method for the new users.

   a. Create a login method for new users with SAML authentication: `security login create -user -or-group-name user_name -application [http | ontapi] -authentication-method saml -vserver svm_name`

   ```
   cluster_12::> security login create -user-or-group-name admin1
   -application http -authentication-method saml -vserver  cluster_12
   ```

   b. Verify that the user entry is created:

   ```
   security login show
   ```

```
cluster_12::> security login show

Vserver: cluster_12

                                   Second
User/Group                         Authentication              Acct
Authentication
Name           Application Method           Role Name          Locked
Method
-------------- ----------- ------------- ---------------- ------
--------------
admin          console     password      admin                  no     none
admin          http        password      admin                  no     none
admin          http        saml          admin                  -      none
admin          ontapi      password      admin                  no     none
admin          ontapi      saml          admin                  -      none
admin          service-processor
                           password      admin                  no     none
admin          ssh         password      admin                  no     none
admin1         http        password      backup                 no     none
**admin1       http        saml          backup                 -
none**
```

## Manage access-control roles

### Manage access-control roles overview

The role assigned to an administrator determines the commands to which the administrator has access. You assign the role when you create the account for the administrator. You can assign a different role or define custom roles as needed.

### Modify the role assigned to an administrator

You can use the `security login modify` command to change the role of a cluster or SVM administrator account. You can assign a predefined or custom role.

**What you'll need**

You must be a cluster administrator to perform this task.

**Step**

1. Change the role of a cluster or SVM administrator:

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

For complete command syntax, see the .

The following command changes the role of the AD cluster administrator account `DOMAIN1\guest1` to the predefined `readonly` role.

```
cluster1::>security login modify -vserver engCluster -user-or-group-name
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

The following command changes the role of the SVM administrator accounts in the AD group account `DOMAIN1\adgroup` to the custom `vol_role` role.

```
cluster1::>security login modify -vserver engData -user-or-group-name
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

**Define custom roles**

You can use the `security login role create` command to define a custom role. You can execute the command as many times as necessary to achieve the exact combination of capabilities that you want to associate with the role.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

- A role, whether predefined or custom, grants or denies access to ONTAP commands or command directories.

  A command directory (`volume`, for example) is a group of related commands and command subdirectories. Except as described in this procedure, granting or denying access to a command directory grants or denies access to each command in the directory and its subdirectories.

- Specific command access or subdirectory access overrides parent directory access.

  If a role is defined with a command directory, and then is defined again with a different access level for a specific command or for a subdirectory of the parent directory, the access level that is specified for the command or subdirectory overrides that of the parent.

  > ⓘ You cannot assign an SVM administrator a role that gives access to a command or command directory that is available only to the `admin` cluster administrator—for example, the `security` command directory.

**Step**

1. Define a custom role:

```
security login role create -vserver SVM_name -role role -cmddirname
command_or_directory_name -access access_level -query query
```

For complete command syntax, see the worksheet.

The following commands grant the `vol_role` role full access to the commands in the `volume` command directory and read-only access to the commands in the `volume snapshot` subdirectory.

```
cluster1::>security login role create -role vol_role -cmddirname
"volume" -access all

cluster1::>security login role create -role vol_role -cmddirname "volume
snapshot" -access readonly
```

The following commands grant the `SVM_storage` role read-only access to the commands in the `storage` command directory, no access to the commands in the `storage encryption` subdirectory, and full access to the `storage aggregate plex offline` nonintrinsic command.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

**Predefined roles for cluster administrators**

The predefined roles for cluster administrators should meet most of your needs. You can create custom roles as necessary. By default, a cluster administrator is assigned the predefined `admin` role.

The following table lists the predefined roles for cluster administrators:

| This role… | Has this level of access… | To the following commands or command directories |
|------------|---------------------------|--------------------------------------------------|
| admin | all | All command directories ( `DEFAULT`) |

| admin-no-fsa (available beginning in ONTAP 9.12.1) | Read/Write | • All command directories (DEFAULT)<br>• `security login rest-role`<br>• `security login role` |
| --- | --- | --- |
| | Read only | • `security login rest-role create`<br>• `security login rest-role delete`<br>• `security login rest-role modify`<br>• `security login rest-role show`<br>• `security login role create`<br>• `security login role create`<br>• `security login role delete`<br>• `security login role modify`<br>• `security login role show`<br>• `volume activity-tracking`<br>• `volume analytics` |
| | None | `volume file show-disk-usage` |
| autosupport | all | • `set`<br>• `system node autosupport` |
| | none | All other command directories (DEFAULT) |

| backup | all | `vserver services ndmp` |
|---|---|---|
| | readonly | `volume` |
| | none | All other command directories (`DEFAULT`) |
| readonly | all | <ul><li>`security login password`<br><br>For managing own user account local password and key information only</li><li>`set`</li></ul> |
| | none | `security` |
| | readonly | All other command directories (`DEFAULT`) |
| none | none | All command directories ( `DEFAULT`) |

> (i) The `autosupport` role is assigned to the predefined `autosupport` account, which is used by AutoSupport OnDemand. ONTAP prevents you from modifying or deleting the `autosupport` account. ONTAP also prevents you from assigning the `autosupport` role to other user accounts.

**Predefined roles for SVM administrators**

The predefined roles for SVM administrators should meet most of your needs. You can create custom roles as necessary. By default, an SVM administrator is assigned the predefined `vsadmin` role.

The following table lists the predefined roles for SVM administrators:

| Role name | Capabilities |
|---|---|

| vsadmin | • Managing own user account local password and key information |
|---|---|
| | • Managing volumes, except volume moves |
| | • Managing quotas, qtrees, Snapshot copies, and files |
| | • Managing LUNs |
| | • Performing SnapLock operations, except privileged delete |
| | • Configuring protocols: NFS, SMB, iSCSI, and FC. including FCoE |
| | • Configuring services: DNS, LDAP, and NIS |
| | • Monitoring jobs |
| | • Monitoring network connections and network interface |
| | • Monitoring the health of the SVM |
| vsadmin-volume | • Managing own user account local password and key information |
| | • Managing volumes, including volume moves |
| | • Managing quotas, qtrees, Snapshot copies, and files |
| | • Managing LUNs |
| | • Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE |
| | • Configuring services: DNS, LDAP, and NIS |
| | • Monitoring network interface |
| | • Monitoring the health of the SVM |
| vsadmin-protocol | • Managing own user account local password and key information |
| | • Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE |
| | • Configuring services: DNS, LDAP, and NIS |
| | • Managing LUNs |
| | • Monitoring network interface |
| | • Monitoring the health of the SVM |

| vsadmin-backup | • Managing own user account local password and key information |
| --- | --- |
| | • Managing NDMP operations |
| | • Making a restored volume read/write |
| | • Managing SnapMirror relationships and Snapshot copies |
| | • Viewing volumes and network information |
| vsadmin-snaplock | • Managing own user account local password and key information |
| | • Managing volumes, except volume moves |
| | • Managing quotas, qtrees, Snapshot copies, and files |
| | • Performing SnapLock operations, including privileged delete |
| | • Configuring protocols: NFS and SMB |
| | • Configuring services: DNS, LDAP, and NIS |
| | • Monitoring jobs |
| | • Monitoring network connections and network interface |
| vsadmin-readonly | • Managing own user account local password and key information |
| | • Monitoring the health of the SVM |
| | • Monitoring network interface |
| | • Viewing volumes and LUNs |
| | • Viewing services and protocols |

## Manage administrator accounts

### Manage administrator accounts overview

Depending on how you have enabled account access, you may need to associate a public key with a local account, install a CA-signed server digital certificate, or configure AD, LDAP, or NIS access. You can perform all of these tasks before or after enabling account access.

### Associate a public key with an administrator account

For SSH public key authentication, you must associate the public key with an administrator account before the account can access the SVM. You can use the `security login publickey create` command to associate a key with an administrator account.

**Before you begin**

- You must have generated the SSH key.

- You must be a cluster or SVM administrator to perform this task.

**About this task**

If you authenticate an account over SSH with both a password and an SSH public key, the account is authenticated first with the public key.

**Step**

1. Associate a public key with an administrator account:

   ```
   security login publickey create -vserver SVM_name -username user_name -index
   index -publickey certificate -comment comment
   ```

   For complete command syntax, see the worksheet.

   Associating a public key with a user account

   The following command associates a public key with the SVM administrator account `svmadmin1` for the SVM `engData1`. The public key is assigned index number 5.

   ```
   cluster1::>security login publickey create -vserver engData1 -username
   svmadmin1 -index 5 -publickey
   "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J
   /vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIza
   FciDy7hgnmdj9eNGedGr/JNrftQbLD1hZybX+72DpQB0tYWBhe6eDJ1oPLob
   ZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
   ```

**Generate and install a CA-signed server certificate**

**Generate and install a CA-signed server certificate overview**

On production systems, it is a best practice to install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server. You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR), and the `security certificate install` command to install the certificate you receive back from the certificate authority.

**Generate a certificate signing request**

You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

**What you'll need**

You must be a cluster or SVM administrator to perform this task.

**Steps**

1. Generate a CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

The following command creates a CSR with a `2048`-bit private key generated by the `SHA256` hashing function for use by the `Software` group in the `IT` department of a company whose custom common name is `server1.companyname.com`, located in `Sunnyvale, California, USA`. The email address of the SVM contact administrator is `web@example.com`. The system displays the CSR and the private key in the output.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your certificate request and private key for
future reference.
```

2. Copy the certificate request from the CSR output, and send it in electronic form (such as email) to a trusted third-party CA for signing.

After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

**Install a CA-signed server certificate**

You can use the `security certificate install` command to install a CA-signed server certificate on an SVM. ONTAP prompts you for the certificate authority (CA) root and intermediate certificates that form the certificate chain of the server certificate.

**What you'll need**

You must be a cluster or SVM administrator to perform this task.

**Step**

1. Install a CA-signed server certificate: `security certificate install -vserver SVM_name -type certificate_type`

   For complete command syntax, see the worksheet.

   > ⓘ  ONTAP prompts you for the CA root and intermediate certificates that form the certificate chain of the server certificate. The chain starts with the certificate of the CA that issued the server certificate, and can range up to the root certificate of the CA. Any missing intermediate certificates result in the failure of server certificate installation.

   The following command installs the CA-signed `server` certificate and intermediate certificates on the SVM`engData2`.

   ```
   cluster1::>security certificate install -vserver engData2 -type server
   Please enter Certificate: Press <Enter> when done
   -----BEGIN CERTIFICATE-----
   MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
   cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
   BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
   WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
   EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
   MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
   -----END CERTIFICATE-----


   Please enter Private Key: Press <Enter> when done
   -----BEGIN RSA PRIVATE KEY-----
   MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
   C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
   PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
   z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANQa99SuSl8U
   DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
   AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
   aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
   -----END RSA PRIVATE KEY-----


   Do you want to continue entering root and/or intermediate certificates
   {y|n}: y
   ```

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate certificates
{y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1FowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate certificates
{y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

**Configure Active Directory domain controller access**

**Configure Active Directory domain controller access overview**

You must configure AD domain controller access to the cluster or SVM before an AD
account can access the SVM. If you have already configured a SMB server for a data
SVM, you can configure the SVM as a gateway, or *tunnel*, for AD access to the cluster. If
you have not configured a SMB server, you can create a computer account for the SVM
on the AD domain.

ONTAP supports the following domain controller authentication services:

- Kerberos

- LDAP

- Netlogon

- Local Security Authority (LSA)

ONTAP supports the following session key algorithms for secure Netlogon connections:

| Session key algorithm | Available in… |
|---|---|
| HMAC-SHA256, based on the Advanced Encryption Standard (AES) | ONTAP 9.10.1 and later |
| DES and HMAC-MD5 (when strong key is set) | All ONTAP 9 releases |

If you want to use AES session keys during Netlogon secure channel establishment in ONTAP 9.10.1 and later, you must enable them using the following command:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

The default is `false`.

In ONTAP releases earlier than 9.10.1, if the domain controller enforces AES for secure Netlogon services, the connection fails. The domain controller must be configured to accept strong key connections with ONTAP in these releases.

**Configure an authentication tunnel**

If you have already configured a SMB server for a data SVM, you can use the `security login domain-tunnel create` command to configure the SVM as a gateway, or *tunnel*, for AD access to the cluster.

**What you'll need**

- You must have configured a SMB server for a data SVM.

- You must have enabled an AD domain user account to access the admin SVM for the cluster.

- You must be a cluster administrator to perform this task.

Beginning with ONTAP 9.10.1, if you have an SVM gateway (domain tunnel) for AD access, you can use Kerberos for admin authentication if you have disabled NTLM in your AD domain. In earlier releases, Kerberos was not supported with admin authentication for SVM gateways. This functionality is available by default; no configuration is required.

**NOTE**

Kerberos authentication is always attempted first. In case of failure, NTLM authentication is then attempted.

**Step**

1. Configure a SMB-enabled data SVM as an authentication tunnel for AD domain controller access to the cluster:

   ```
   security login domain-tunnel create -vserver SVM_name
   ```

   For complete command syntax, see the worksheet.

> ⓘ The SVM must be running for the user to be authenticated.

The following command configures the SMB-enabled data SVM`engData` as an authentication tunnel.

```
cluster1::>security login domain-tunnel create -vserver engData
```

**Create an SVM computer account on the domain**

If you have not configured an SMB server for a data SVM, you can use the `vserver active-directory create` command to create a computer account for the SVM on the domain.

**What you'll need**

You must be a cluster or SVM administrator to perform this task.

**About this task**

After you enter the `vserver active-directory create` command, you are prompted to provide the credentials for an AD user account with sufficient privileges to add computers to the specified organizational unit in the domain. The password of the account cannot be empty.

**Step**

1. Create a computer account for an SVM on the AD domain:

   ```
   vserver active-directory create -vserver SVM_name -account-name
   NetBIOS_account_name -domain domain -ou organizational_unit
   ```

   For complete command syntax, see the worksheet.

   The following command creates a computer account named `ADSERVER1` on the domain `example.com` for the SVM `engData`. You are prompted to enter the AD user account credentials after you enter the command.

   ```
   cluster1::>vserver active-directory create -vserver engData -account
   -name ADSERVER1 -domain example.com

   In order to create an Active Directory machine account, you must supply
   the name and password of a Windows account with sufficient privileges to
   add computers to the "CN=Computers" container within the "example.com"
   domain.

   Enter the user name: Administrator

   Enter the password:
   ```

# Configure LDAP or NIS server access

## Configure LDAP or NIS server access overview

You must configure LDAP or NIS server access to an SVM before LDAP or NIS accounts can access the SVM. The switch feature lets you use LDAP or NIS as alternative name service sources.

## Configure LDAP server access

You must configure LDAP server access to an SVM before LDAP accounts can access the SVM. You can use the `vserver services name-service ldap client create` command to create an LDAP client configuration on the SVM. You can then use the `vserver services name-service ldap create` command to associate the LDAP client configuration with the SVM.

**What you'll need**

- You must have installed a CA-signed server digital certificate on the SVM.
- You must be a cluster or SVM administrator to perform this task.

**About this task**

Most LDAP servers can use the default schemas provided by ONTAP:

- MS-AD-BIS (the preferred schema for most Windows 2012 and later AD servers)
- AD-IDMU (Windows 2008, Windows 2012 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX LDAP servers)

It is best to use the default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema and modifying the copy. For more information, see the following documents.

- NFS configuration
- NetApp Technical Report 4835: How to Configure LDAP in ONTAP

**Steps**

1. Create an LDAP client configuration on an SVM: `vserver services name-service ldap client create -vserver SVM_name -client-config client_configuration -servers LDAP_server_IPs -schema schema -use-start-tls true|false`

   (i) Start TLS is supported for access to data SVMs only. It is not supported for access to admin SVMs.

   For complete command syntax, see the worksheet.

   The following command creates an LDAP client configuration named `corp` on the SVMengData. The client makes anonymous binds to the LDAP servers with the IP addresses `172.160.0.100` and `172.16.0.101`. The client uses the `RFC-2307` schema to make LDAP queries. Communication between the client and server is encrypted using Start TLS.

```
cluster1::>vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

> ⓘ  Beginning with ONTAP 9.2, the field `-ldap-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the LDAP server.

2. Associate the LDAP client configuration with the SVM: `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

   For complete command syntax, see the worksheet.

   The following command associates the LDAP client configuration `corp` with the SVM `engData`, and enables the LDAP client on the SVM.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```

> ⓘ  Beginning with ONTAP 9.2, the `vserver services name-service ldap create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

3. Validate the status of the name servers by using the vserver services name-service ldap check command.

   The following command validates LDAP servers on the SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                      |
| Client Configuration Name: c1                                     |
| LDAP Status: up                                                   |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                      |
```

   The name service check command is available beginning with ONTAP 9.2.

**Configure NIS server access**

You must configure NIS server access to an SVM before NIS accounts can access the SVM. You can use the `vserver services name-service nis-domain create` command to create an NIS domain configuration on an SVM.

**What you'll need**

- All configured servers must be available and accessible before you configure the NIS domain on the SVM.

- You must be a cluster or SVM administrator to perform this task.

**About this task**

You can create multiple NIS domains. Only one NIS domain can be set to `active` at a time.

**Step**

1. Create an NIS domain configuration on an SVM: `vserver services name-service nis-domain create -vserver SVM_name -domain client_configuration -active true|false -nis -servers NIS_server_IPs`

   For complete command syntax, see the worksheet.

   > (i)  Beginning with ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

   The following command creates an NIS domain configuration on the SVM `engData`. The NIS domain `nisdomain` is active on creation and communicates with an NIS server with the IP address `192.0.2.180`.

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
   ```

**Create a name service switch**

The name service switch feature lets you use LDAP or NIS as alternative name service sources. You can use the `vserver services name-service ns-switch modify` command to specify the look-up order for name service sources.

**What you'll need**

- You must have configured LDAP and NIS server access.
- You must be a cluster administrator or SVM administrator to perform this task.

**Step**

1. Specify the lookup order for name service sources:

   ```
   vserver services name-service ns-switch modify -vserver SVM_name -database
   name_service_switch_database -sources name_service_source_order
   ```

   For complete command syntax, see the worksheet.

   The following command specifies the lookup order of the LDAP and NIS name service sources for the `passwd` database on the `engData`SVM.

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

**Change an administrator password**

You should change your initial password immediately after logging into the system for the first time. If you are an SVM administrator, you can use the `security login password` command to change your own password. If you are a cluster administrator, you can use the `security login password` command to change any administrator's password.

**What you'll need**

- You must be a cluster or SVM administrator to change your own password.
- You must be a cluster administrator to change another administrator's password.

**About this task**

The new password must observe the following rules:

- It cannot contain the user name
- It must be at least eight characters long
- It must contain at least one letter and one number
- It cannot be the same as the last six passwords

> (i) You can use the `security login role config modify` command to modify the password rules for accounts associated with a given role. For more information, see the man page.`security login role config modify`

**Step**

1. Change an administrator password: `security login password -vserver SVM_name -username user_name`

   The following command changes the password of the administrator `admin1` for the SVM`vs1.example.com`. You are prompted to enter the current password, then enter and reenter the new password.

   ```
   vs1.example.com::>security login password -vserver engData -username
   admin1
   Please enter your current password:
   Please enter a new password:
   Please enter it again:
   ```

**Lock and unlock an administrator account**

You can use the `security login lock` command to lock an administrator account, and the `security login unlock` command to unlock the account.

**What you'll need**

You must be a cluster administrator to perform these tasks.

**Steps**

1. Lock an administrator account:

   `security login lock -vserver SVM_name -username user_name`

   The following command locks the administrator account `admin1` for the SVM `vs1.example.com`:

   > `cluster1::>security login lock -vserver engData -username admin1`

2. Unlock an administrator account:

   `security login unlock -vserver SVM_name -username user_name`

   The following command unlocks the administrator account `admin1` for the SVM `vs1.example.com`:

   > `cluster1::>security login unlock -vserver engData -username admin1`

**Manage failed login attempts**

Repeated failed login attempts sometimes indicate that an intruder is attempting to access the storage system. You can take a number of steps to ensure that an intrusion does not take place.

**How you will know that login attempts have failed**

The Event Management System (EMS) notifies you about failed login attempts every hour. You can find a record of failed login attempts in the `audit.log` file.

**What to do if repeated login attempts fail**

In the short term, you can take a number of steps to prevent an intrusion:

- Require that passwords be composed of a minimum number of uppercase characters, lowercase characters, special characters, and/or digits
- Impose a delay after a failed login attempt
- Limit the number of allowed failed login attempts, and lock out users after the specified number of failed attempts
- Expire and lock out accounts that are inactive for a specified number of days

You can use the `security login role config modify` command to perform these tasks.

Over the long term, you can take these additional steps:

- Use the `security ssh modify` command to limit the number of failed login attempts for all newly created SVMs.
- Migrate existing MD5-algorithm accounts to the more secure SHA-512 algorithm by requiring users to change their passwords.

**Enforce SHA-2 on administrator account passwords**

Administrator accounts created prior to ONTAP 9.0 continue to use MD5 passwords after the upgrade, until the passwords are manually changed. MD5 is less secure than SHA-2. Therefore, after upgrading, you should prompt users of MD5 accounts to change their passwords to use the default SHA-512 hash function.

**About this task**

The password hash functionality enables you to do the following:

- Display user accounts that match the specified hash function.
- Expire accounts that use a specified hash function (for example, MD5), forcing the users to change their passwords in their next login.
- Lock accounts whose passwords use the specified hash function.
- When reverting to a release earlier than ONTAP 9, reset the cluster administrator's own password for it to be compatible with the hash function (MD5) that is supported by the earlier release.

ONTAP accepts pre-hashed SHA-2 passwords only by using NetApp Manageability SDK (security-login-create and security-login-modify-password).

[Manageability enhancements](#)

**Steps**

1. Migrate the MD5 administrator accounts to the SHA-512 password hash function:

   a. Expire all MD5 administrator accounts: `security login expire-password -vserver * -username * -hash-function md5`

   Doing so forces MD5 account users to change their passwords upon next login.

   b. Ask users of MD5 accounts to log in through a console or SSH session.

   The system detects that the accounts are expired and prompts users to change their passwords. SHA-512 is used by default for the changed passwords.

2. For MD5 accounts whose users do not log in to change their passwords within a period of time, force the account migration:

   a. Lock accounts that still use the MD5 hash function (advanced privilege level): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

   After the number of days specified by `-lock-after`, users cannot access their MD5 accounts.

   b. Unlock the accounts when the users are ready to change their passwords: `security login unlock -vserver vserver_name -username user_name`

   c. Have users log in to their accounts through a console or SSH session and change their passwords when the system prompts them to do so.

## Manage multi-admin verification

**Multi-admin verification overview**

Beginning with ONTAP 9.11.1, you can use multi-admin verification (MAV) to ensure that certain operations, such as deleting volumes or Snapshot copies, can be executed only after approvals from designated administrators. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data.

Configuring multi-admin verification consists of:

- Creating one or more administrator approval groups.
- Enabling multi-admin verification functionality.
- Adding or modifying rules.

After initial configuration, these elements can be modified only by administrators in a MAV approval group (MAV administrators).

When multi-admin verification is enabled, the completion of every protected operation requires three steps:

- When a user initiates the operation, a request is generated.
- Before it can be executed, at least one MAV administrator must approve.
- Upon approval, the user completes the operation.

Multi-admin verification is not intended for use with volumes or workflows that involve heavy automation, because each automated task would require approval before the operation could be completed. If you want to use automation and MAV together, it's recommended to use queries for specific MAV operations. For example, you could apply `volume delete` MAV rules only to volumes where automation is not involved, and you could designate those volumes with a particular naming scheme.

> (i)  If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following Knowledge Base article: How to disable Multi-Admin Verification if MAV admin is unavailable.

**How multi-admin verification works**

Multi-admin verification consists of:

- A group of one or more administrators with approval and veto powers.
- A set of protected operations or commands in a *rules table*.
- A *rules engine* to identify and control execution of protected operations.

MAV rules are evaluated after role-based access control (RBAC) rules. Therefore, administrators who execute or approve protected operations must already possess the minimum RBAC privileges for those operations. Learn more about RBAC.

When multi-admin verification is enabled, system-defined rules (also known as *guard-rail* rules) establish a set of MAV operations to contain the risk of circumventing the MAV process itself. These operations cannot be removed from the rules table. Once MAV is enabled, operations designated by an asterisk ( * ) require approval by one or more administrators before execution, except for **show** commands.

- `security multi-admin-verify modify*`

Controls the configuration of multi-admin verification functionality.

- `security multi-admin-verify approval-group` operations*

  Control membership in the set of administrators with multi-admin verification credentials.

- `security multi-admin-verify rule` operations*

  Control the set of commands requiring multi-admin verification.

- `security multi-admin-verify request` operations

  Control the approval process.

In addition to the system-defined commands, the following commands are protected by default when multi-admin verification is enabled, but you can modify the rules to remove protection for these commands.

- `security login password`
- `security login unlock`
- `set`

The following commands can be protected in ONTAP 9.11.1 and later releases.

| | |
|---|---|
| `cluster peer delete` | `volume snapshot autodelete modify` |
| `event config modify` | `volume snapshot delete` |
| `security login create` | `volume snapshot policy add-schedule` |
| `security login delete` | `volume snapshot policy create` |
| `security login modify` | `volume snapshot policy delete` |
| `system node run` | `volume snapshot policy modify` |
| `system node systemshell` | `volume snapshot policy modify-schedule` |
| `volume delete` | `volume snapshot policy remove-schedule` |
| `volume flexcache delete` | `volume snapshot restore` |
| `volume snaplock modify` | `vserver peer delete` |

**How multi-admin approval works**

Any time a protected operation is entered on a MAV-protected cluster, an operation execution request is sent to the designated MAV administrator group.

You can configure:

- The names, contact information, and number of administrators in the MAV group.

A MAV administrator should have an RBAC role with cluster administrator privileges.

- The number of MAV administrator groups.
    - A MAV group is assigned for each protected operation rule.
    - For multiple MAV groups, you can configure which MAV group approves a given rule.
- The number of MAV approvals required to execute a protected operation.
- An *approval expiry* period within which a MAV administrator must respond to an approval request.
- An *execution expiry* period within which the requesting administrator must complete the operation.

Once these parameters are configured, MAV approval is required to modify them.

MAV administrators cannot approve their own requests to execute protected operations. Therefore:

- MAV should not be enabled on clusters with only one administrator.
- If there is only one person in the MAV group, that MAV administrator cannot enter protected operations; regular administrators must enter them and the MAV administrator can only approve.
- If you want MAV administrators to be able to execute protected operations, the number of MAV administrators must be one greater than the number of approvals required.
  For example, if two approvals are required for a protected operation, and you want MAV administrators to execute them, there must be three people in the MAV administrators group.

MAV administrators can receive approval requests in email alerts (using EMS) or they can query the request queue. When they receive a request, they can take one of three actions:

- Approve
- Reject (veto)
- Ignore (no action)

Email notifications are sent to all approvers associated with a MAV rule when:

- A request is created.
- A request is approved or vetoed.
- An approved request is executed.

If the requestor is in the same approval group for the operation, they will receive an email when their request is approved.

**Note:** A requestor can't approve their own requests, even if they are in the approval group. But they can get the email notifications. Requestors who are not in approval groups (that is, who are not MAV administrators) don't receive email notifications.

### How protected operation execution works

If execution is approved for a protected operation, the requesting user continues with the operation when prompted. If the operation is vetoed, the requesting user must delete the request before proceeding.

MAV rules are evaluated after RBAC permissions. As a result, a user without sufficient RBAC permissions for operation execution cannot initiate the MAV request process.

**Manage administrator approval groups**

Before enabling multi-admin verification (MAV), you must create an admin approval group containing one or more administrators to be granted approve or veto authority. Once you have enabled multi-admin verification, any modifications to approval group membership requires approval from one of the existing qualified administrators.

**About this task**

You can add existing administrators to a MAV group or create new administrators.

MAV functionality honors existing role-based access control (RBAC) settings. Potential MAV administrators must have sufficient privilege to execute protected operations before they are added to MAV administrator groups. Learn more about RBAC.

You can configure MAV to alert MAV administrators that approval requests are pending. To do so, you must configure email notifications—in particular, the `Mail From` and `Mail Server` parameters—or you can clear these parameters to disable notification. Without email alerts, MAV administrators must check the approval queue manually.

**System Manager procedure**

If you want to create a MAV approval group for the first time, see the System Manager procedure to enable multi-admin verification.

To modify an existing approval group or create an additional approval group:

1. Identify administrators to receive multi-admin verification.

    a. Click **Cluster > Settings.**

    b. Click → next to **Users and Roles.**

    c. Click ＋ Add under **Users.**

    d. Modify the roster as needed.

    For more information, see Control administrator access.

2. Create or modify the MAV approval group:

    a. Click **Cluster > Settings.**

    b. Click → next to **Multi-Admin Approval** in the **Security** section.
    (You will see the ⚙ icon if MAV is not yet configured.)

        ▪ Name: enter a group name.

        ▪ Approvers: select approvers from a list of users.

        ▪ Email address: enter email address(es).

        ▪ Default group: select a group.

MAV approval is required to edit an existing configuration once MAV is enabled.

**CLI procedure**

1. Verify that values have been set for the `Mail From` and `Mail Server` parameters. Enter:

```
event config show
```

The display should be similar to the following:

```
cluster01::> event config show
                        Mail From:  admin@localhost
                      Mail Server:  localhost
                        Proxy URL:  -
                       Proxy User:  -
  Publish/Subscribe Messaging Enabled:  true
```

To configure these parameters, enter:

```
event config modify -mail-from email_address -mail-server server_name
```

2. Identify administrators to receive multi-admin verification

| If you want to… | Enter this command |
| --- | --- |
| Display current administrators | `security login show` |
| Modify credentials of current administrators | `security login modify <parameters>` |
| Create new administrator accounts | `security login create -user-or-group -name admin_name -application ssh -authentication-method password` |

3. Create the MAV approval group:

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name
group_name -approvers approver1[,approver2…] [[-email address1], address1…]
```

- ◦ `-vserver` - Only the admin SVM is supported in this release.
- ◦ `-name` - The MAV group name, up to 64 characters.
- ◦ `-approvers` - The list of one or more approvers.
- ◦ `-email` - One or more email addresses that are notified when a request is created, approved, vetoed, or executed.

   **Example:** The following command creates a MAV group with two members and associated email addresses.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email
pavan@myfirm.com,julia@myfirm.com
```

4. Verify group creation and membership:

```
security multi-admin-verify approval-group show
```

**Example:**

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name             Approvers         Email
-------  ---------------  ------------------
-------------------------------------------------------------
svm-1    mav-grp1    pavan,julia       email
pavan@myfirm.com,julia@myfirm.com
```

Use these commands to modify your initial MAV group configuration.

**Note:** All require MAV administrator approval before execution.

| If you want to… | Enter this command |
|---|---|
| Modify the group characteristics or modify existing member information | `security multi-admin-verify approval-group modify [parameters]` |
| Add or remove members | `security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]] [-approvers-to-remove approver1[,approver2…]]` |
| Delete a group | `security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name` |

**Enable and disable multi-admin verification**

Multi-admin verification (MAV) must be enabled explicitly. Once you have enabled multi-admin verification, approval by administrators in a MAV approval group (MAV administrators) is required to delete it.

**About this task**

Once MAV is enabled, modifying or disabling MAV requires MAV administrator approval.

> ⓘ  If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following Knowledge Base article: How to disable Multi-Admin Verification if MAV admin is unavailable.

When you enable MAV, you can specify the following parameters globally.

**Approval groups**

A list of global approval groups. At least one group is required to enable MAV functionality.

**Required approvers**

The number of approvers required to execute a protected operation. The default and minimum number is 1.

**Note:** The required number of approvers must be less than the total number of unique approvers in the default approval groups.

**Approval expiry (hours, minutes, seconds)**

The period within which a MAV administrator must respond to an approval request. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).

**Execution expiry (hours, minutes, seconds)**

The period within which the requesting administrator must complete the:: operation. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).

You can also override any of these parameters for specific operation rules.

**System Manager procedure**

1. Identify administrators to receive multi-admin verification.

   a. Click **Cluster > Settings.**

   b. Click ➜ next to **Users and Roles.**

   c. Click ➕ Add under **Users.**

   d. Modify the roster as needed.

      For more information, see Control administrator access.

2. Enable multi-admin verification by creating at least one approval group and adding at least one rule.

   a. Click **Cluster > Settings.**

   b. Click ⚙ next to **Multi-Admin Approval** in the **Security** section.

   c. Click ➕ Add to add at least one approval group.

      ▪ Name – Enter a group name.

      ▪ Approvers – Select approvers from a list of users.

      ▪ Email address – Enter email address(es).

      ▪ Default group – Select a group.

   d. Add at least one rule.

      ▪ Operation – Select a supported command from the list.

      ▪ Query – Enter any desired command options and values.

      ▪ Optional parameters; leave blank to apply global settings, or assign a different value for specific rules to override the global settings.

         ▪ Required number of approvers

         ▪ Approval groups

e. Click **Advanced Settings** to view or modify defaults.

- Required number of approvers (default: 1)
- Execution request expiry (default: 1 hour)
- Approval request expiry (default: 1hour)
- Mail server*
- From email address*

    *These update the email settings managed under "Notification Management". You are prompted to set them if they have not yet been configured.

f. Click **Enable** to complete MAV initial configuration.

After initial configuration, the current MAV status is displayed in the **Multi-Admin Approval** tile.

- Status (enabled or not)
- Active operations for which approvals are required
- Number of open requests in pending state

You can display an existing configuration by clicking ➔. MAV approval is required to edit an existing configuration.

To disable multi-admin verification:

1. Click **Cluster > Settings.**
2. Click ⚙ next to **Multi-Admin Approval** in the **Security** section.
3. Click the Enabled toggle button.

    MAV approval is required to complete this operation.

**CLI procedure**

Before enabling MAV functionality at the CLI, at least one MAV administrator group must have been created.

| If you want to… | Enter this command |
|---|---|
| Enable MAV functionality | ```security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]```<br><br>**Example** : the following command enables MAV with 1 approval group, 2 required approvers, and default expiry periods.<br><br>```cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true```<br><br>Complete initial configuration by adding at least one operation rule. |
| Modify a MAV configuration (requires MAV approval) | ```security multi-admin-verify approval-group modify [-approval-groups group1 [,group2…]] [-required-approvers nn ] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]``` |
| Verify MAV functionality | ```security multi-admin-verify show```<br><br>**Example:**<br><br>```cluster-1::> security multi-admin-verify show`<br>`Is      Required  Execution`<br>`Approval Approval`<br>`Enabled Approvers Expiry    Expiry`<br>`Groups`<br>`------- --------- ---------`<br>`-------- ----------`<br>`true    2         1h        1h`<br>`mav-grp1``` |
| Disable MAV functionality (requires MAV approval) | ```security multi-admin-verify modify -enabled false``` |

**Manage protected operation rules**

You create multi-admin verification (MAV) rules to designate operations requiring approval. Whenever an operation is initiated, protected operations are intercepted and a request for approval is generated.

Rules can be created before enabling MAV by any administrator with appropriate RBAC capabilities, but once MAV is enabled, any modification to the rule set requires MAV approval.

You can create rules for the following commands in ONTAP 9.11.1.

| | |
|---|---|
| `cluster peer delete` | `volume snapshot autodelete modify` |
| `event config modify` | `volume snapshot delete` |
| `security login create` | `volume snapshot policy add-schedule` |
| `security login delete` | `volume snapshot policy create` |
| `security login modify` | `volume snapshot policy delete` |
| `system node run` | `volume snapshot policy modify` |
| `system node systemshell` | `volume snapshot policy modify-schedule` |
| `volume delete` | `volume snapshot policy remove-schedule` |
| `volume flexcache delete` | `volume snapshot restore` |
| | `vserver peer delete` |

In addition, the following commands are protected by default when MAV is enabled, but you can modify the rules to remove protection for these commands.

- `security login password`
- `security login unlock`
- `set`

The rules for MAV system-default commands – the `security multi-admin-verify` commands – cannot be altered.

When you create a rule, you can optionally specify the `-query` option to limit the request to a subset of the command functionality. For example, in the default set command, `-query` is set to `-privilege diag`, meaning that a request is generated for the set command only when -privilege diag is specified.

```
smci-vsim20::> security multi-admin-verify rule show
                                                  Required  Approval
Vserver Operation                                 Approvers Groups
------- ----------------------------------------- --------- -------------
vs01    set                                       -         -
           Query: -privilege diagnostic
```

By default, rules specify that a corresponding `security multi-admin-verify request create` "*protected_operation*" command is generated automatically when a protected operation is entered. You can modify this default to require that the `request create` command be entered separate.

By default, rules inherit the following global MAV settings, although you can specify rule-specific exceptions:

- Required Number of Approvers
- Approval Groups
- Approval Expiry period
- Execution Expiry period

**System Manager procedure**

If you want to add a protected operation rule for the first time, see the System Manager procedure to enable multi-admin verification.

To modify the existing rule set:

1. Click **Cluster > Settings**.
2. Click ⚙ next to **Multi-Admin Approval** in the **Security** section.
3. Click ✚ Add to add at least one rule; you can also modify or delete existing rules.
    - Operation – Select a supported command from the list.
    - Query – Enter any desired command options and values.
    - Optional parameters – Leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
        - Required number of approvers
        - Approval groups

**CLI procedure**

ⓘ  All `security multi-admin-verify rule` commands require MAV administrator approval before execution except `security multi-admin-verify rule show`.

| If you want to… | Enter this command |
|---|---|
| Create a rule | `security multi-admin-verify rule create -operation "protected_operation"` [`-query operation_subset`] [`parameters`] |

| If you want to… | Enter this command |
|---|---|
| Modify credentials of current administrators | `security login modify <parameters>`<br><br>**Example**: the following rule requires approval to delete the root volume.<br><br>`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0` |
| Modify a rule | `security multi-admin-verify rule modify -operation "protected_operation" [parameters]` |
| Delete a rule | `security multi-admin-verify rule delete -operation "protected_operation"` |
| Show rules | `security multi-admin-verify rule show` |

For command syntax details, see the `security multi-admin-verify rule` man pages.

**Request execution of protected operations**

When you initiate a protected operation or command on a cluster enabled for multi-admin verification (MAV), ONTAP automatically intercepts the operation and asks to generate a request, which must be approved by one or more administrators in a MAV approval group (MAV administrators). Alternatively, you can create a MAV request without the dialog.

If approved, you must then respond to the query to complete the operation within the request expiry period. If vetoed, or if the request or expiry periods are exceeded, you must delete the request and resubmit.

MAV functionality honors existing RBAC settings. That is, your administrator role must have sufficient privilege to execute a protected operation without regard to MAV settings. Learn more about RBAC.

If you are a MAV administrator, your requests to execute protected operations must also be approved by a MAV administrator.

**System Manager procedure**

When a user clicks on a menu item to initiate an operation and the operation is protected, a request for approval is generated and the user receives a notification similar to the following:

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

The **Multi-Admin Requests** window is available when MAV is enabled, showing pending requests based on the user's login ID and MAV role (approver or not). For each pending request, the following fields are displayed:

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

  If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- (Number of) Potential Approvers

When the request is approved, the requesting user can retry the operation within the expiry period.

If the user retries the operation without approval, a notification is displayed similar to the following:

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

**CLI procedure**

1. Enter the protected operation directly or using the MAV request command.

   **Examples – to delete a volume, enter one of the following commands:**

   ◦ volume delete

   ```
   cluster-1::*> volume delete -volume vol1 -vserver vs0

   Warning: This operation requires multi-admin verification. To create
   a
           verification request use "security multi-admin-verify
   request
           create".

           Would you like to create a request for this operation?
            {y|n}: y

   Error: command failed: The security multi-admin-verify request (index
   3) is
           auto-generated and requires approval.
   ```

   ◦ security multi-admin-verify request create "volume delete"

```
Error: command failed: The security multi-admin-verify request (index
3)
        requires approval.
```

2. Check the status of the request and respond to the MAV notice.

    a. If the request is approved, respond to the CLI message to complete the operation.

    **Example:**

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. If the request is vetoed, or the expiry period has passed, delete the request, and either resubmit or contact the MAV administrator.

**Example:**

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index
3) hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

**Manage protected operation requests**

When administrators in a MAV approval group (MAV administrators) are notified of a pending operation execution request, they must respond with an approve or veto message within a fixed time period (approval expiry). If a sufficient number of approvals are not received, the requester must delete the request and make another.

**About this task**

Approval requests are identified with index numbers, which are included in email messages and displays of the request queue.

The following information from the request queue can be displayed:

**Operation**

The protected operation for which the request is created.

**Query**

The object (or objects) upon which the user wants to apply the operation.

**State**

The current state of the request; pending, approved, rejected, expired, executed. If a request is rejected by one approver, no further actions are possible.

**Required approvers**

The number of MAV administrators that are required to approve the request. A user can set the required-approvers parameter for the operation rule. If a user does not set the required-approvers to the rule, then the required-approvers from the global setting is applied.

**Pending approvers**

The number of MAV administrators that are still required to approve the request for the request to be marked as approved.

**Approval expiry**

The period within which a MAV administrator must respond to an approval request. Any authorized user can set the approval-expiry for an operation rule. If approval-expiry is not set for the rule, then the approval-expiry from the global setting is applied.

**Execution expiry**

The period within which the requesting administrator must complete the operation. Any authorized user can set the execution-expiry for an operation rule. If execution-expiry is not set for the rule, then the execution-expiry from the global setting is applied.

**Users approved**

The MAV administrators who have approved the request.

**User vetoed**

The MAV administrators who have vetoed the request.

**Storage VM (vserver)**

The SVM with which the request is associated with. Only the admin SVM is supported in this release.

**User requested**

The username of the user who created the request.

**Time created**

The time when the request is created.

**Time approved**

The time when the request state changed to approved.

**Comment**

Any comments that are associated with the request.

**Users permitted**

The list of users permitted to perform the protected operation for which the request is approved. If `users-permitted` is empty, then any user with appropriate permissions can perform the operation.

All expired or executed requests are deleted when a limit of 1000 requests is reached, or when the expired

time is greater than 8hrs for expired requests. Vetoed requests are deleted once they are marked as expired.

**System Manager procedure**

MAV administrators receive email messages with details of the approval request, request expiry period, and a link to approve or reject the request. They can access an approval dialog by clicking the link in the email or navigate to **Events & Jobs>Requests** in System Manager.

The **Requests** window is available when multi-admin verification is enabled, showing pending requests based on the user's login ID and MAV role (approver or not).

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

  If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- (Number of) Potential Approvers

MAV administrators have additional controls in this window; they can approve, reject, or delete individual operations, or selected groups of operations. However, if the MAV administrator is the Requesting User, they cannot approve, reject or delete their own requests.

**CLI procedure**

1. When notified of pending requests by email, note the request's index number and approval expiry period. The index number can also be displayed using the **show** or **show-pending** options mentioned below.
2. Approve or veto the request.

| If you want to… | Enter this command |
| --- | --- |
| Approve a request | `security multi-admin-verify request approve` *nn* |
| Veto a request | `security multi-admin-verify request veto` *nn* |

| If you want to… | Enter this command |
|---|---|
| Show all requests, pending requests, or a single request | `security multi-admin-verify request { show | show-pending } [`*`nn`*`] { -fields `*`field1`*`[,`*`field2`*`…] | [-instance ] }`<br><br>You can show all requests in the queue or only pending requests. If you enter the index number, only information for that is displayed. You can display information about specific fields (by using the `-fields` parameter) or about all fields (by using the `-instance` parameter). |
| Delete a request | `security multi-admin-verify request delete `*`nn`* |

**Example:**

The following sequence approves a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```
          cluster1::> security multi-admin-verify request show-pending
                                   Pending
Index Operation        Query State    Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete   -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

      Request Index: 3
          Operation: volume delete
              Query: -
              State: approved
  Required Approvers: 2
   Pending Approvers: 0
    Approval Expiry: 2/25/2022 14:32:03
   Execution Expiry: 2/25/2022 14:35:36
          Approvals: mav-admin2
        User Vetoed: -
            Vserver: cluster-1
     User Requested: julia
       Time Created: 2/25/2022 13:32:03
      Time Approved: 2/25/2022 13:35:36
            Comment: -
    Users Permitted: -
```

**Example:**

The following sequence vetoes a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```
      cluster1::> security multi-admin-verify request show-pending
                                Pending
 Index Operation       Query State    Approvers Requestor
 ----- -------------- ----- ------- --------- ---------
     3 volume delete  -     pending 1         pavan


 cluster-1::> security multi-admin-verify request veto 3

 cluster-1::> security multi-admin-verify request show 3

        Request Index: 3
            Operation: volume delete
                Query: -
                State: vetoed
   Required Approvers: 2
    Pending Approvers: 0
      Approval Expiry: 2/25/2022 14:32:03
     Execution Expiry: 2/25/2022 14:35:36
            Approvals: mav-admin1
         User Vetoed: mav-admin2
              Vserver: cluster-1
       User Requested: pavan
         Time Created: 2/25/2022 13:32:03
        Time Approved: 2/25/2022 13:35:36
              Comment: -
      Users Permitted: -
```

# Ransomware protection

### Autonomous Ransomware Protection overview

Beginning with ONTAP 9.10.1, the Autonomous Ransomware Protection (ARP) feature uses workload analysis in NAS (NFS and SMB) environments to proactively detect and warn about abnormal activity that might indicate a ransomware attack.

When an attack is suspected, ARP also creates new Snapshot copies, in addition to existing protection from scheduled Snapshot copies.

The ARP feature is enabled with the following licenses.

| ONTAP releases | License |
| --- | --- |
| ONTAP 9.11.1 and later | Anti_ransomware |

| ONTAP releases | License |
|---|---|
| ONTAP 9.10.1 | MT_EK_MGMT (Multi-Tenant Key Management) |

- If you are upgrading to ONTAP 9.11.1 or later and ARP is already configured on your system, you do not need to purchase the new Anti-ransomware license. For new ARP configurations, the new license is required.

- If you are reverting from ONTAP 9.11.1 or later to ONTAP 9.10.1, and you have enabled ARP with the Anti-ransomware license, you will see a warning message and might need to reconfigure ARP. Learn about reverting ARP.

You can configure ARP on a per-volume basis using either ONTAP System Manager or the ONTAP command line interface (CLI).

### ONTAP ransomware protection strategy

An effective ransomware detection strategy should include more than a single layer of protection.

An analogy would be the safety features of a vehicle. You wouldn't want to rely on a single feature, such as a seatbelt, to completely protect you in an accident. Air bags, anti-lock brakes, and forward-collision warning are all additional safety features that will lead to a much better outcome. Ransomware protection should be viewed in the same way.

While ONTAP includes features like FPolicy, Snapshot copies, SnapLock, and Active IQ Digital Advisor to help protect from ransomware, the following information focuses on the ONTAP ARP on-box feature with machine-learning capabilities.

To learn more about ONTAP's other anti-ransomware features, see: TR-4572: NetApp Solution for Ransomware.

### What ONTAP ARP detects

There are two types of ransomware attacks:

1. Denial of service to files by encrypting data.
   The attacker withholds access to this data unless a ransom is paid.

2. Theft of sensitive proprietary data.
   The attacker threatens to release this data to the public domain unless a ransom is paid.

ONTAP ARP addresses the first type, with an anti-ransomware detection mechanism that is based on:

1. Identification of the incoming data as encrypted or plaintext.

2. Analytics, which detects

   - High data *entropy* (an evaluation of the randomness of data in a file)

   - A surge in abnormal volume activity with data encryption

   - An extension that does not conform to the normal extension type

> (i) No ransomware detection or prevention system can completely guarantee safety from a ransomware attack. While it's possible an attack might go undetected, NetApp ARP acts as an important additional layer of defense if anti-virus software has failed to detect an intrusion. ARP can detect the spread of most ransomware attacks after only a small number of files are encrypted, take action automatically to protect data, and alert you that a suspected attack is happening.

**How to recover data in ONTAP after a ransomware attack**

When an attack is suspected, the system takes a volume Snapshot copy at that point in time and locks that copy. If the attack is confirmed later, the volume can be restored to this proactively taken snapshot, minimizing the data loss.

Locked Snapshot copies cannot be deleted by normal means. However, if you decide later to mark the attack as a false positive, the locked copy will be deleted.

With the knowledge of the affected files and the time of attack, it is possible to selectively recover the affected files from various Snapshot copies, rather than simply reverting the whole volume to one of the snapshots.

ARP thus builds on proven ONTAP data protection and disaster recovery technology to respond to ransomware attacks. See the following topics for more information on recovering data.

- Recover from Snapshot copies (System Manager)
- Restoring files from Snapshot copies (CLI)
- Smart ransomware recovery

## Autonomous Ransomware Protection use cases and considerations

ONTAP platform support:

- The Autonomous Ransomware Protection (ARP) feature is available for all on-premises ONTAP systems beginning with ONTAP 9.10.1.
- ARP is not currently available for ONTAP Select.
- ARP is not currently available for Amazon FSx or the following Cloud Volumes ONTAP environments:
  - AWS
  - Azure
  - Google Cloud

Suitable workloads:

- Databases on NFS storage
- Windows or Linux home directories

  Because users could create files with extensions that weren't detected in the learning period, there is greater possibility of false positives in this workload.

- Images and video

  For example, health care records and Electronic Design Automation (EDA) data.

Beginning with ONTAP 9.12.1, ARP is available for these configurations:

- Volumes protected with SnapMirror
- SVMs protected with SnapMirror
- SVMs enabled for migration (SVM data mobility)

Unsuitable workloads:

- Workloads with a high frequency of file create or delete (hundreds of thousands of files in few seconds; for example, test/dev workloads)
- ARP depends on the ability to recognize an unusual surge in file create or delete activity. If the application itself is the source of the file activity, it cannot be effectively distinguished from ransomware activity
- Workloads where the application or the host encrypts data
  ARP depends on distinguishing incoming data as encrypted or unencrypted. If the application itself is encrypting the data, then the effectiveness of the feature is reduced. However, the feature can still work based on file activity (create, delete, and overwrite) and file type.

Unsupported system configurations:

- SAN environments
- ONTAP S3 environments
- VMDKs on NFS

Volume requirements:

- Less than 100% full
- Junction path must be active

Unsupported volume types:

- Offline volumes
- Restricted volumes
- SnapLock volumes
- FlexGroup volumes
- FlexCache volumes (the anti-ransomware feature is supported on origin FlexVol volumes but not on cache volumes)
- SAN-only volumes
- Volumes of stopped storage VMs
- Root volumes of storage VMs

**SnapMirror and ARP interoperability**

Beginning with ONTAP 9.12.1, ARP is supported on SnapMirror destination volumes. If a SnapMirror source volume is ARP-enabled, the SnapMirror destination volume automatically acquires the ARP configuration state (learning, enabled, etc), ARP training data, and ARP-created Snapshot of the source volume. No explicit enablement is required.

While the destination volume consists of read-only (RO) Snapshot copies, no ARP processing is done on its data. However, when the SnapMirror destination volume is converted to read-write (RW), ARP is automatically

enabled on the RW-converted destination volume. The destination volume does not require any additional learning procedure besides what is already recorded on the source volume.

In ONTAP 9.10.1 and 9.11.1, SnapMirror does not transfer the ARP configuration state, training data, and Snapshot copies from source to destination volumes. Hence when the SnapMirror destination volume is converted to RW, ARP on the destination volume must be explicitly enabled in learning mode after conversion.

### ARP performance and frequency considerations

The ARP feature can have a minimal impact on system performance as measured in throughput and peak IOPS. The impact of the anti-ransomware feature is highly dependent on volume workloads. For most typical or common workloads, the following configuration limits are recommended:

| Workload characteristics | Recommended volume limit per node | Performance degradation when per-node volume limit is exceeded * |
|---|---|---|
| Read-intensive or the data can be compressed. | 150 | 4% of maximum IOPS |
| Write-intensive and the data cannot be compressed. | 60 | 10% of maximum IOPS |

* System performance is not degraded beyond these percentages regardless of the number of volumes added in excess of the recommended limits.

Because ARP analytics are run in a prioritized sequence, as the number of protected volumes increases, analytics are run on each volume less frequently.

### How automatic Snapshot copies work when ransomware is detected

In order to obtain the best possible recovery point, ARP creates an automatic Snapshot copy as soon as it detects abnormal file activity. However, ARP does not immediately flag an alert; rather, analytics need to run and confirm that the suspicious activity matches a ransomware profile before generating an alert. This process could take up to 60 minutes. If the analytics determines the activity is not suspicious, then an alert is not generated, but the automatically created Snapshot copy remains present on the file system for a minimum of two days.

Beginning with ONTAP 9.11.1, you can control the number and retention period for ARP Snapshot copies that are automatically generated in response to suspected ransomware attacks. Learn how to modify options for automatic Snapshot copies.

## Enable Autonomous Ransomware Protection

Beginning with ONTAP 9.10.1, Autonomous Ransomware Protection (ARP) can be enabled on new or existing volumes. You first enable ARP in learning mode, in which the system analyzes the workload to characterize normal behavior. Then you switch to active mode, in which abnormal activity is flagged for your evaluation.

**What you'll need**
- A storage VM enabled for NFS or SMB (or both).
- The correct license is installed for your ONTAP version.

| ONTAP releases | License |
|---|---|
| ONTAP 9.8-9.10.1 | MT_EK_MGMT (Multi-Tenant Key Management) |
| ONTAP 9.11.1 and later | Anti_ransomware |

- An NAS workload with clients configured.

- The volume to be protected must have an active junction-path.

- Optional but recommended: The EMS system is configured to send email notifications, which will include notices of ARP activity. For more information, see Configure EMS events to send email notifications.

**About this task**

NetApp ARP includes an initial learning period (also known as "dry run"), in which an ONTAP system learns which file extensions are valid and uses the analyzed data to develop alert profiles. After running ARP in learning mode for enough time to assess workload characteristics, you can switch to active mode and start protecting your data. In active mode, if a file extension is flagged as abnormal, but then you evaluate it and mark it as a false positive, the alert profile is refined to so that the extension is not flagged as abnormal in future alerts.

Although you can switch from learning to active mode anytime, a learning period of 30 days is recommended. Switching early may lead to too many false positives. In the ONTAP CLI, you can use the `security anti-ransomware volume workload-behavior show` command to show file extensions detected to date. It is recommended that you not use this tool to shorten the learning period.

You can enable ARP on an existing volume, or you can create a new volume and enable ARP from the beginning.

> (i) In existing volumes, learning and active modes only apply to newly-written data, not to already existing data in the volume. The existing data is not scanned and analyzed, because the characteristics of earlier normal data traffic are assumed based on the new data after the volume is enabled for ARP.

To manage this feature in the ONTAP CLI, you can use the `security anti-ransomware volume` command. You can also use the `volume modify` command with the `-anti-ransomware` parameter.

**Example 1. Steps**

**System Manager**

1. Click **Storage > Volumes** and then select the volume you want to protect.

2. In the **Security** tab of the **Volumes** overview, click **Status** to switch from Disabled to Enabled in learning-mode in the **Anti-ransomware** box.

3. When the learning period is over, switch ARP to active mode.

   a. Click **Storage > Volumes** and then select the volume that is ready for active mode.

   b. In the **Security** tab of the **Volumes** overview, click **Switch** to active mode in the Anti-ransomware box.

4. You can always verify the ARP state of the volume in the **Anti-ransomware** box.
   To display ARP status for all volumes: In the **Volumes** pane, click **Show/Hide**, then ensure that **Anti-ransomware** status is checked.

**CLI**

1. Modify an existing volume to enable ransomware protection in learning mode:

   ```
   security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
   ```

   You can also enable ransomware with the `volume modify` command:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   dry-run
   ```

   At the CLI, you can also create a new volume with anti-ransomware protection enabled before provisioning data.

   ```
   volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size
   nn -anti-ransomware-state dry-run -junction-path /path_name
   ```

   > ⓘ You should always enable ARP initially in the dry-run state. Beginning with the active state can lead to excessive false positive reports.

2. When the learning period is over, modify the protected volume to switch to active mode:

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   You can also switch to active mode with the modify volume command:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Verify the ARP state of the volume.

   ```
   security anti-ransomware volume show
   ```

# Enable Autonomous Ransomware Protection by default in new volumes

Beginning with ONTAP 9.10.1, you can configure storage VMs (SVMs) such that new volumes are enabled by default for Autonomous Ransomware Protection (ARP) in learning mode.

**What you'll need**

- The correct license is installed for your ONTAP version.

| ONTAP releases | License |
|---|---|
| ONTAP 9.11.1 and later | Anti_ransomware |
| ONTAP 9.8-9.10.1 | MT_EK_MGMT (Multi-Tenant Key Management) |

**About this task**

New volumes are created by default with ARP in disabled mode, but you can change this setting in System Manager and at the CLI. Volumes enabled by default are set to ARP in learning mode.

> (i) Enabling ARP by default for new volumes in an SVM does not automatically enable ARP for existing volumes in that SVM. Learn how to enable ARP in an existing volume.

**Example 2. Steps**

**System Manager**

1. Click **Storage > Storage VMs** and then select the storage VM for default anti-virus.

2. In the **Settings** tab, [in the **Security** section], click ✏ in the **Anti-ransomware** box, then check the box to enable ARP for NAS volumes.

**CLI**

1. Modify an existing SVM to enable ARP by default in new volumes:
   ```
   vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
   ```

   At the CLI, you can also create a new SVM with ARP enabled by default for new volumes.
   ```
   vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]
   ```

# Pause Autonomous Ransomware Protection to exclude workload events from analysis

If you are expecting unusual workload events, you can temporarily suspend and resume Autonomous Ransomware Protection (ARP) analysis at any time.

**What you'll need**

- ARP is running in learning or active mode.

**About this task**

During an ARP pause, no events are logged nor are any actions for new writes. However, the analytics operation continues for earlier logs in the background.

> ⓘ Do not use the anti-ransomware disable function to pause analytics. Doing so disables ARP on the volume and all the existing information around learned workload behavior is lost. This would require a restart of the learning period.

**Example 3. Steps**

**System Manager**

1. Click **Storage > Volumes** and then select the volume where you want to pause ARP.

2. In the Security tab of the Volumes overview, click **Pause anti-ransomware** in the **Anti-ransomware** box.

**CLI**

Pause ARP on a volume:

```
security anti-ransomware volume pause -vserver svm_name -volume vol_name
```

To resume processing, use the `resume` parameter.

```
security anti-ransomware volume resume -vserver svm_name -volume vol_name
```

## Respond to abnormal activity.

When Autonomous Ransomware Protection (ARP) detects abnormal activity in a protected volume, it issues a warning. You should evaluate the notification to determine whether the activity is expected and acceptable, or whether an attack is under way.

**What you'll need**

- ARP is running in active mode.

**About this task**

ARP displays a list of suspected files when it detects any combination of high data entropy, abnormal volume activity with data encryption, and unusual file extensions.

When the warning is issued, you can respond by marking the file activity in one of two ways:

- False positive

  The identified file type is expected in your workload and can be ignored.

- Potential ransomware attack

  The identified file type is unexpected in your workload and should be treated as a potential attack.

In both cases, normal monitoring resumes after updating and clearing the notices; ARP records your evaluation, logs are updated with the new file types and using them for future analysis. However, in the case of a suspected attack, you must determine whether it is an attack, respond to it if it is, and restore protected data

before clearing the notices. Learn more about how to recover from a ransomware attack.

ⓘ | There are no notices to clear if you restored an entire volume.

**Example 4. Steps**

**System Manager**

1. When you receive an "abnormal activity" notification, click on the link or navigate to the **Security** tab of the **Volumes** overview.

   Warnings are displayed in the Overview pane of the Events window.

2. When a "Detected abnormal volume activity" message is displayed, view the suspect files.

   In the **Security** tab, click View **Suspected File Types**.

3. In the **Suspected File Types** dialog box, examine each file type and mark it as either "False Positive" or "Potential Ransomware attack".

| If you selected this value… | Take this action… |
|---|---|
| False Positive | Click **Update** and **Clear Suspect File Types** to record your decision and resume normal anti-ransomware monitoring. |
| Potential Ransomware Attack | Respond to the attack and restore protected data. Then click **Update** and **Clear Suspect File Types** to record your decision and resume normal ARP monitoring.<br>There are no suspect file types to clear if you restored an entire volume. |

**CLI**

1. When you receive a notification of a suspected ransomware attack, verify the time and severity of the attack:

   `security anti-ransomware volume show -vserver svm_name -volume vol_name`

   Sample output:

   ```
   Vserver Name: vs0
   Volume Name: vol1
   State: enabled
   Attack Probability: moderate
   Attack Timeline: 9/14/2021 01:03:23
   Number of Attacks: 1
   ```

   You can also check EMS messages:

   `event log show -message-name callhome.arw.activity.seen`

2. Generate an attack report and note the output location:

   `security anti-ransomware volume attack generate-report -volume vol_name -dest-path file_location/`

   Sample output:

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
"vs0:vol1/"
```

3. View the report on an admin client system. For example:

```
[root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
```

4. Take one of the following actions based on your evaluation of the file extensions:

   ◦ False positive

   Enter the following command to record your decision – adding the new extension to the list of
   those allowed – and resume normal anti-ransomware monitoring:
   `anti-ransomware volume attack clear-suspect -vserver` *svm_name* `-volume`
   *vol_name* [*extension identifiers*] `-false-positive true`

   Use one of the following parameters to identify the extensions:
   [`-seq-no` *integer*] Sequence number of the file in the suspect list.
   [`-extension` *text*, … ] File extensions
   [`-start-time` *date_time* `-end-time` *date_time*] Starting and ending times for the range
   of files to be cleared, in the form "MM/DD/YYYY HH:MM:SS".

   ◦ Potential ransomware attack

   Respond to the attack and restore data. Then enter the following command to record your
   decision and resume normal ARP monitoring:

   `anti-ransomware volume attack clear-suspect -vserver` *svm_name* `-volume`
   *vol_name* [*extension identifiers*] `-false-positive false`

   Use one of the following parameters to identify the extensions:
   [`-seq-no` *integer*] Sequence number of the file in the suspect list
   [`-extension` *text*, … ] File extension
   [`-start-time` *date_time* `-end-time` *date_time*] Starting and ending times for the range
   of files to be cleared, in the form "MM/DD/YYYY HH:MM:SS".

   There are no suspect file types to clear if you restored an entire volume.

## Restore data after a ransomware attack

Snapshot copies named "Anti_ransomware_backup" are created when Autonomous
Ransomware Protection (ARP) detects a potential attack. You can restore data from
these ARP copies or from other Snapshot copies.

**About this task**

If the volume has SnapMirror relationships, manually replicate all mirror copies of the volume immediately after you restore from a Snapshot copy. Not doing so can result in unusable mirror copies that must be deleted and recreated.

**What you'll need**

- ARP enabled

- Reports from potential ransomware attacks

**Steps**

You can use System Manager or the ONTAP CLI to restore your data.

**System Manager**

1. If you want to restore data from earlier Snapshot copies, instead of from the ARP copies, you must do the following to release the anti-ransomware Snapshot lock. If you want to restore from the ARP copies, it is not necessary to release the lock and you can skip this step.

| If a system attack was identified do this… | If a system attack was not identified do this… |
|---|---|
| a. Click **Storage > Volumes**.<br><br>b. Select **Security**, and click **View Suspected File Types**<br><br>c. Mark the files as "False Positive" .<br><br>d. Click **Update** and **Clear Suspect File Types** | To release the Snapshot lock, you must restore from the ARP copies before you restore from earlier Snapshot copies.<br><br>Follow steps 2-3 to restore data from the ARP copies, then repeat the process to restore from earlier Snapshot copies. |

2. Display the Snapshot copies in volumes:

   Click **Storage > Volumes**, select the volume, and click **Snapshot Copies**.

3. Click ⋮ next to the Snapshot copy you want to restore, and select **Restore**.

**CLI**

1. If you want to restore data from earlier Snapshot copies, instead of from the ARP copies, you must do the following to release the anti-ransomware Snapshot lock. If you want to restore from the ARP copies, it is not necessary to release the lock and you can skip this step.

   ```
   It is only necessary to release the anti-ransomware Snaplock before
   restoring from earlier Snapshot copies if you are using the `volume
   snap restore`` command as outline below.  If you are restoring data
   using Flex Clone, Single File Snap Restore or other methods, this is
   not necessary.
   ```

| If a system attack was identified do this… | If a system attack was not identified do this… |
|---|---|
| Mark the attack as a "false positive" and "clear suspect".<br><br>`anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`<br><br>Use one of the following parameters to identify the extensions:<br>`[-seq-no integer]` Sequence number of the file in the suspect list.<br>`[-extension text, … ]` File extensions<br>`[-start-time date_time -end-time date_time]` Starting and ending times for the range of files to be cleared, in the form "MM/DD/YYYY HH:MM:SS". | To release the Snapshot lock, you must restore from the ARP copies before you restore from earlier Snapshot copies.<br><br>Follow steps 2-3 to restore data from the ARP copies, then repeat the process to restore from earlier Snapshot copies. |

2. List the Snapshot copies in a volume:

   `volume snapshot show -vserver SVM -volume volume`

   The following example shows the Snapshot copies in `vol1`:

   ```
   clus1::> volume snapshot show -vserver vs1 -volume vol1

   Vserver Volume Snapshot                    State     Size   Total% Used%
   ------- ------ ---------- ----------- ------   -----  ------ -----
   vs1   vol1   hourly.2013-01-25_0005  valid   224KB    0%    0%
                daily.2013-01-25_0010    valid    92KB     0%    0%
                hourly.2013-01-25_0105   valid   228KB     0%    0%
                hourly.2013-01-25_0205   valid   236KB     0%    0%
                hourly.2013-01-25_0305   valid   244KB     0%    0%
                hourly.2013-01-25_0405   valid   244KB     0%    0%
                hourly.2013-01-25_0505   valid   244KB     0%    0%

   7 entries were displayed.
   ```

3. Restore the contents of a volume from a Snapshot copy:

   `volume snapshot restore -vserver SVM -volume volume -snapshot snapshot`

   The following example restores the contents of `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

## Modify options for automatic Snapshot copies

Beginning with ONTAP 9.11.1, you can use the CLI to control the number and retention period for Autonomous Ransomware Protection (ARP) Snapshot copies that are automatically generated in response to suspected ransomware attacks.

**Note**: The `vserver options` command is a hidden command. To view the man page, enter `man vserver options` at the ONTAP CLI.

The following options for automatic Snapshot copies can be modified:

**arw.snap.max.count**

  Specifies the maximum number of ARP Snapshot copies that can exist in a volume at any given time. Older copies are deleted to ensure that the total number of ARP Snapshot copies are within this specified limit.

**arw.snap.create.interval.hours**

  Specifies the interval (in hours) between ARP Snapshot copies. A new Snapshot copy will be created when an attack is suspected and the copy created previously is older than this specified interval.

**arw.snap.normal.retain.interval.hours**

  Specifies the duration (in hours) for which an ARP Snapshot copy is retained. When an ARP Snapshot copy becomes this old, any other ARP Snapshot copy created before the latest copy to reach this age is deleted. No ARP Snapshot copy can be older than this duration.

**arw.snap.max.retain.interval.days**

  Specifies the maximum duration (in days) for which an ARP Snapshot copy can be retained. Any ARP Snapshot copy older than this duration will be deleted if there is no attack reported on the volume.

**arw.snap.create.interval.hours.post.max.count**

  Specifies the interval (in hours) between ARP Snapshot copies when the volume already contains the maximum number of ARP Snapshot copies. When the maximum number is reached, an ARP Snapshot copy is deleted to make room for a new copy. The new ARP Snapshot copy creation speed can be reduced to retain the older copy using this option. If the volume already contains maximum number of ARP Snapshot copies, then this interval specified in this option is used for next ARP Snapshot copy creation, instead of arw.snap.create.interval.hours.

**arw.surge.snap.interval.days**

  Specifies the interval (in days) between ARP surge Snapshot copies. A new ARP Snapshot surge copy is created when there is a surge in IO traffic and the last created ARP Snapshot copy is older than this specified interval. This option also specifies the duration (in days) for which an ARP surge Snapshot copy is retained.

### CLI procedure

To show all current ARP Snapshot copy settings, enter:
```
vserver options -vserver svm_name arw*
```

To show selected current ARP Snapshot copy settings, enter:

```
vserver options -vserver svm_name -option-name arw_setting_name
```

To modify ARP Snapshot copy settings, enter:

```
vserver options -vserver svm_name -option-name arw_setting_name -option-value
arw_setting_value
```

# Antivirus configuration

## Antivirus configuration overview

You can use NetApp virus scanning, called *Vscan*, to protect data from being compromised by viruses or other malicious code. It shows you how to use on-access scanning to check for viruses when clients access files over SMB, and how to use on-demand scanning to check for viruses immediately or on a schedule.

You can work with Vscan by using the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool. Vscan is not supported by System Manager.

**Related information**

[NetApp Technical Report 4286: Antivirus Solution for Clustered Data ONTAP McAfee](#)

[NetApp Technical Report 4304: Antivirus Solution for Clustered Data ONTAP Symantec](#)

[NetApp Technical Report 4312: Antivirus Solution for Clustered Data ONTAP Trend Micro](#)

## About NetApp antivirus protection

### About NetApp virus scanning

You can use integrated antivirus functionality on NetApp storage systems to protect data from being compromised by viruses or other malicious code. NetApp virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

#### How virus scanning works

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors. The ONTAP Antivirus Connector, provided by NetApp and installed on the external server, handles communication between the storage system and the antivirus software.

- You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files over SMB. File operation is suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a scan from the server.

  On-access scanning is not supported for NFS.

- You can use *on-demand scanning* to check files for viruses immediately or on a schedule. You might want to run scans only in off-peak hours, for example. The external server updates the scan status of the checked files, so that file-access latency for those files (assuming they have not been modified) is typically reduced when they are next accessed over SMB.

You can use on-demand scanning for any path in the SVM namespace, even for volumes that are exported only through NFS.

You typically enable both scanning modes on an SVM. In either mode, the antivirus software takes remedial action on infected files based on your settings in the software.



**Virus scanning workflow**

You must create a scanner pool and apply a scanner policy before you can enable scanning. You typically enable both on-access and on-demand scanning on an SVM.

ⓘ   You must have completed the CIFS configuration.
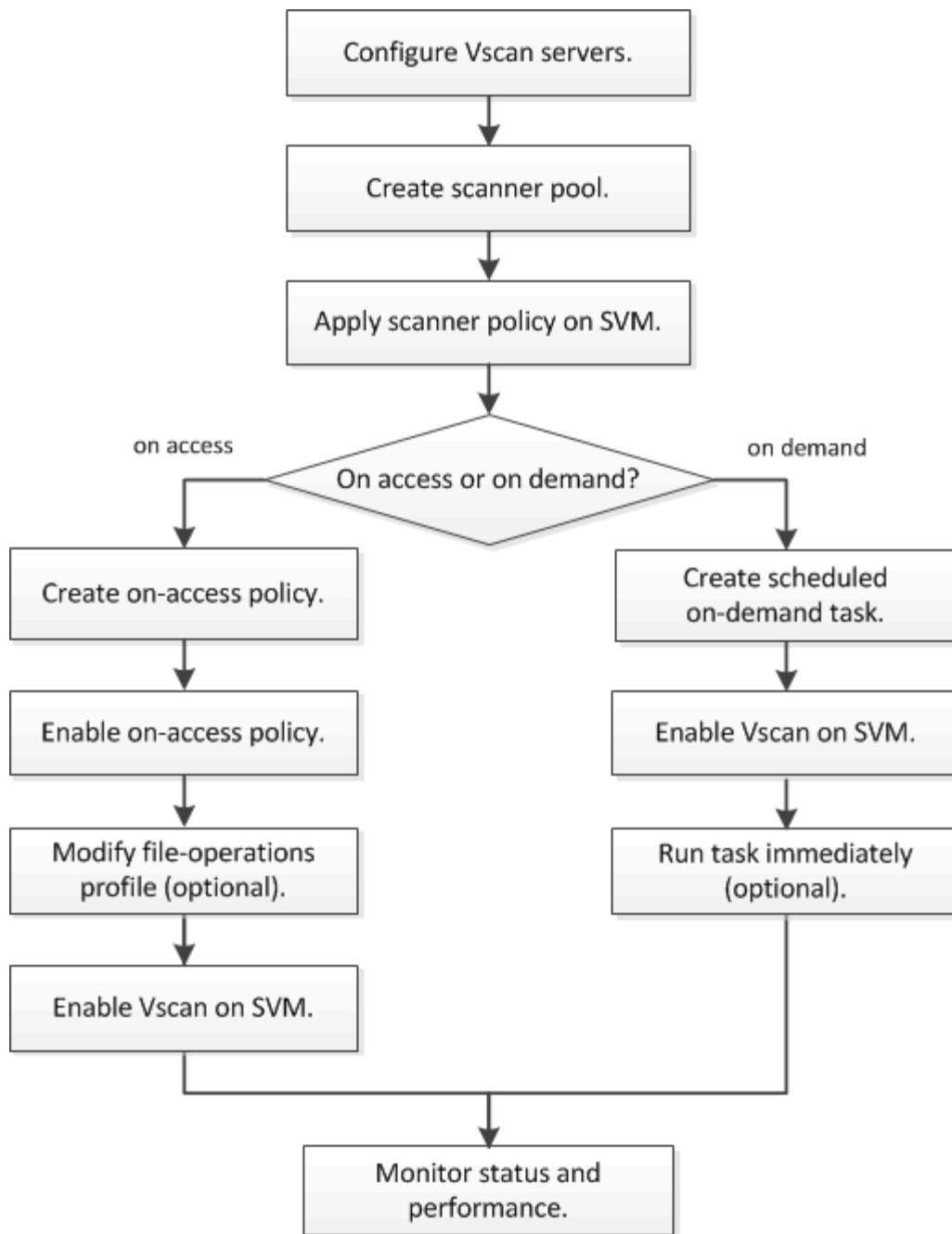
**Antivirus architecture**

The NetApp antivirus architecture consists of a Vscan server and a set of ONTAP configurables.

**Vscan server components**

You must install the following components on the Vscan server.

- **ONTAP Antivirus Connector**

  The ONTAP Antivirus Connector provided by NetApp handles communication between ONTAP and the Vscan server.

- **Antivirus software**

  ONTAP-compliant third-party antivirus software scans files for viruses or other malicious code. You specify the remedial actions to be taken on infected files when you configure the software.

**ONTAP configurables**

You must configure the following items on the NetApp storage system.

- **Scanner pool**

  A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. It also defines a scan request timeout period, after which the scan request is sent to an alternative Vscan server if one is available.

  > ⓘ It is a best practice to set the timeout period in the antivirus software on the Vscan server to five seconds less than the scanner-pool request timeout period, to avoid situations in which file access is delayed or denied altogether because the timeout period on the software is greater than the timeout period for the scan request.

- **Privileged user**

  A privileged user is a domain user account that a Vscan server uses to connect to the SVM. The account must be included in the list of privileged users defined in the scanner pool.

- **Scanner policy**

  A scanner policy determines whether a scanner pool is active. A scanner policy can have one of the following values:

  - `Primary` specifies that the scanner pool is active.

  - `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool is connected.

  - `Idle` specifies that the scanner pool is inactive.
    Scanner policies are system-defined. You cannot create a custom scanner policy.

- **On-access policy**

  An on-access policy defines the scope of an on-access scan. You can specify the maximum size of the files to be scanned, the extensions of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan.

  By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access:

  - `scan-ro-volume` enables scanning of read-only volumes.

  - `scan-execute-access` restricts scanning to files opened with execute access.

    > ⓘ "Execute access" is not identical with "execute permission." A given client will have "execute access" on an executable file only if the file was opened with "execute intent."

  You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan

servers are available for virus scanning.

- **On-demand task**

  An on-demand task defines the scope of an on-demand scan. You can specify the maximum size of the files to be scanned, the extensions and paths of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. Files in subdirectories are scanned by default.

  You use a cron schedule to specify when the task runs. You can use the `vserver vscan on-demand-task run` command to run the task immediately.

- **Vscan file-operations profile (on-access scanning only)**

  The `-vscan-fileop-profile` parameter for the `vserver cifs share create` command defines which operations on a SMB share can trigger virus scanning. By default, the parameter is set to `standard`, which is the NetApp best practice.

  You can adjust this parameter as necessary when you create or modify a SMB share:

  - `no-scan` specifies that virus scans are never triggered for the share.

  - `standard` specifies that virus scans can be triggered by open, close, and rename operations.

  - `strict` specifies that virus scans can be triggered by open, read, close, and rename operations.

    The `strict` profile provides enhanced security for situations in which multiple clients access a file simultaneously. If one client closes a file after writing a virus to it, and the same file remains open on a second client, `strict` ensures that a read operation on the second client triggers a scan before the file is closed.

    You should be careful to restrict the `strict` profile to shares containing files that you anticipate will be accessed simultaneously. Because the profile generates more scan requests than the others, it may affect performance adversely.

  - `writes-only` specifies that virus scans can be triggered only when a file that has been modified is closed.

    > ⓘ    If a client application performs a rename operation, the file is closed with the new name and is not scanned. If such operations pose a security concern in your environment, you should use the `standard` or `strict` profile.

    Because `writes-only` generates fewer scan requests than the other profiles (except `no-scan`), it typically improves performance.

    Keep in mind, though, that if you use this profile for a share, the scanner must be configured to delete or quarantine an unrepairable infected file, so that it cannot be accessed by clients later. If, for example, a client closes a file after writing a virus to it, and the file is not repaired, deleted, or quarantined, any client that accesses the file *without* writing to it will be infected.

## Vscan server installation and configuration

You must set up one or more Vscan servers to ensure that files on your system are scanned for viruses. Follow the instructions provided by your vendor to install and

configure the antivirus software on the server. Follow the instructions in the readme file provided by NetApp to install and configure the ONTAP Antivirus Connector.

> ⓘ For disaster recovery and MetroCluster configurations, you must set up separate Vscan servers for the local and partner clusters.

**Antivirus software requirements**

- For information about antivirus software requirements, see the vendor documentation.
- For information about the vendors, software, and versions supported by Vscan, see the NetAppInteroperability Matrix.

  mysupport.netapp.com/matrix

**ONTAP Antivirus Connector requirements**

- You can download the ONTAP Antivirus Connector from the Software Download page on the NetApp Support Site. NetApp Downloads: Software
- For information about the Windows versions supported by the ONTAP Antivirus Connector, see the NetAppInteroperability Matrix.

  mysupport.netapp.com/matrix

  > ⓘ You can install different versions of Windows servers for different Vscan servers in a cluster.

- .NET 3.0 or later must be installed on the Windows server.
- SMB 2.0 must be enabled on the Windows server.

# Configure scanner pools

**Configure scanner pools overview**

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. A scanner policy determines whether a scanner pool is active.

> ⓘ If you use an export policy on a SMB server, you must add each Vscan server to the export policy.

**Create a scanner pool on a single cluster**

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. You can create a scanner pool for an individual SVM or for all of the SVMs in a cluster.

**What you'll need**

- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured the ONTAP Antivirus Connector with the SVM management LIF or the SVM data LIF.
- For scanner pools defined for all of the SVMs in a cluster, you must have configured the ONTAP Antivirus

Connector with the cluster management LIF.

**About this task**

The list of privileged users must include the domain user account the Vscan server uses to connect to the SVM.

**Steps**

1. Create a scanner pool:

   `vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users`

   ◦ Specify a data SVM for a pool defined for an individual SVM, and specify a cluster admin SVM for a pool defined for all of the SVMs in a cluster.

   ◦ Specify an IP address or FQDN for each Vscan server host name.

   ◦ Specify the domain and user name for each privileged user.
   For a complete list of options, see the man page for the command.

   The following command creates a scanner pool named `SP` on the `vs1`SVM:

   ```
   cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
   SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
   cifs\u1,cifs\u2
   ```

2. Verify that the scanner pool was created: `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `SP` scanner pool:

   ```
   cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
   SP

                                   Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: idle
                            Current Status: off
           Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: vserver
         List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
    List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
    27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
   ```

   You can also use the `vserver vscan scanner-pool show` command to view all of the scanner pools

on an SVM. For complete command syntax, see the man page for the command.

**Create scanner pools in MetroCluster configurations**

You must create primary and secondary scanner pools on each cluster in a MetroCluster configuration, corresponding to the primary and secondary SVMs on the cluster.

**What you'll need**

- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured the ONTAP Antivirus Connector with the SVM management LIF or the SVM data LIF.
- For scanner pools defined for all of the SVMs in a cluster, you must have configured the ONTAP Antivirus Connector with the cluster management LIF.

**About this task**

MetroCluster configurations protect data by implementing two physically separate mirrored clusters. Each cluster synchronously replicates the data and SVM configuration of the other. A primary SVM on the local cluster serves data when the cluster is online. A secondary SVM on the local cluster serves data when the remote cluster is offline.

This means that you must create primary and secondary scanner pools on each cluster in a MetroCluster configuration, corresponding to the primary and secondary SVMs on the cluster. The secondary pool becomes active when the cluster begins serving data from the secondary SVM. The following illustration shows a typical MetroCluster configuration.
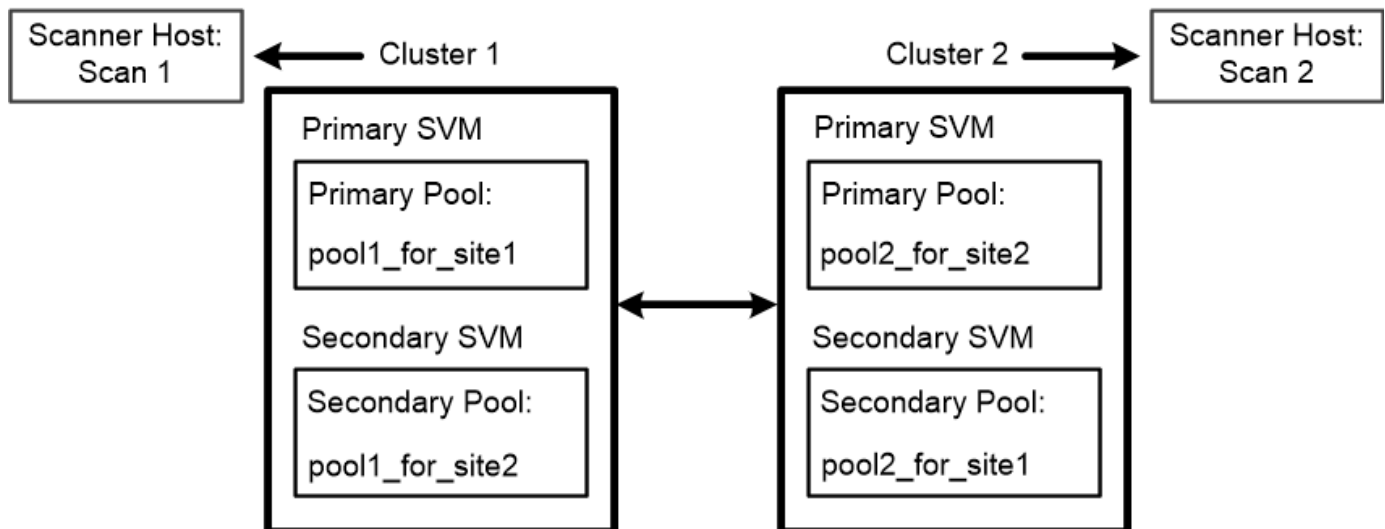


> ⓘ The list of privileged users must include the domain user account the Vscan server uses to connect to the SVM.

**Steps**

1. Create a scanner pool:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
privileged_users
```

- Specify a data SVM for a pool defined for an individual SVM, and specify a cluster admin SVM for a pool defined for all the SVMs in a cluster.
- Specify an IP address or FQDN for each Vscan server host name.
- Specify the domain and user name for each privileged user.

> ℹ️ You must create all scanner pools from the cluster containing the primary SVM.

For a complete list of options, see the man page for the command.

The following commands create primary and secondary scanner pools on each cluster in a MetroCluster configuration:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Verify that the scanner pools were created: `vserver vscan scanner-pool show -vserver` `data_SVM|cluster_admin_SVM` `-scanner-pool` `scanner_pool`

For a complete list of options, see the man page for the command.

The following command displays the details for the scanner pool `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                               Scanner Pool: pool1_for_site1
                             Applied Policy: idle
                             Current Status: off
          Cluster on Which Policy Is Applied: -
                    Scanner Pool Config Owner: vserver
            List of IPs of Allowed Vscan Servers:
     List of Host Names of Allowed Vscan Servers: scan1
                      List of Privileged Users: cifs\u1,cifs\u2
```

You can also use the `vserver vscan scanner-pool show` command to view all of the scanner pools on an SVM. For complete command syntax, see the man page for the command.

**Apply a scanner policy on a single cluster**

A scanner policy determines whether a scanner pool is active. You must make a scanner pool active before the Vscan servers that are defined in the scanner pool can connect to an SVM.

**About this task**

- You can apply only one scanner policy to a scanner pool.

- If you created a scanner pool for all of the SVMs in a cluster, you must apply a scanner policy on each SVM individually.

- For disaster recovery and MetroCluster configurations, you must apply a scanner policy to the scanner pools for the local cluster and partner cluster.

  In the policy that you create for the local cluster, you must specify the local cluster in the `cluster` parameter. In the policy that you create for the partner cluster, you must specify the partner cluster in the `cluster` parameter. The partner cluster can then take over virus scanning operations in case of a disaster.

**Steps**

1. Apply a scanner policy:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   A scanner policy can have one of the following values:

   ◦ `Primary` specifies that the scanner pool is active.

   ◦ `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool are connected.

- ◦ `Idle` specifies that the scanner pool is inactive.

The following example shows that the scanner pool named `SP` on the `vs1` SVM is active:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP  -scanner-policy primary
```

2. Verify that the scanner pool is active:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

For a complete list of options, see the man page for the command.

The following command displays the details for the `SP` scanner pool:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                  Vserver: vs1
                             Scanner Pool: SP
                           Applied Policy: primary
                           Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                Scanner Pool Config Owner: vserver
         List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. For the complete command syntax, see the man page for the command.

**Apply scanner policies in MetroCluster configurations**

A scanner policy determines whether a scanner pool is active. You must apply a scanner policy to the primary and secondary scanner pools on each cluster in a MetroCluster configuration.

**About this task**

- You can apply only one scanner policy to a scanner pool.
- If you created a scanner pool for all of the SVMs in a cluster, you must apply a scanner policy on each SVM individually.

**Steps**

1. Apply a scanner policy:

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on
```

A scanner policy can have one of the following values:

- ° `Primary` specifies that the scanner pool is active.

- ° `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool is connected.

- ° `Idle` specifies that the scanner pool is inactive.

> ⓘ    You must apply all scanner policies from the cluster containing the primary SVM.

The following commands apply scanner policies to the primary and secondary scanner pools on each cluster in a MetroCluster configuration:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Verify that the scanner pool is active:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

For a complete list of options, see the man page for the command.

The following command displays the details for the scanner pool `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                      Vserver: cifssvm1
                                 Scanner Pool: pool1_for_site1
                               Applied Policy: primary
                               Current Status: on
             Cluster on Which Policy Is Applied: cluster1
                     Scanner Pool Config Owner: vserver
          List of IPs of Allowed Vscan Servers:
   List of Host Names of Allowed Vscan Servers: scan1
                       List of Privileged Users: cifs\u1,cifs\u2
```

You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. For complete command syntax, see the man page for the command.

**Commands for managing scanner pools**

You can modify and delete scanner pools, and manage privileged users and Vscan servers for a scanner pool. You can view summary and details for a scanner pool.

| If you want to… | Enter the following command… |
|---|---|
| Modify a scanner pool | `vserver vscan scanner-pool modify` |
| Delete a scanner pool | `vserver vscan scanner-pool delete` |
| Add privileged users to a scanner pool | `vserver vscan scanner-pool privileged-users add` |
| Delete privileged users from a scanner pool | `vserver vscan scanner-pool privileged-users remove` |
| Add Vscan servers to a scanner pool | `vserver vscan scanner-pool servers add` |
| Delete Vscan servers from a scanner pool | `vserver vscan scanner-pool servers remove` |
| View summary and details for a scanner pool | `vserver vscan scanner-pool show` |
| View privileged users for a scanner pool | `vserver vscan scanner-pool privileged-users show` |
| View Vscan servers for all scanner pools | `vserver vscan scanner-pool servers show` |

For more information about these commands, see the man pages.

## Configure on-access scanning

### Create an on-access policy

An on-access policy defines the scope of an on-access scan. You can specify the maximum size of the files to be scanned, the extensions of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. You can create an on-access policy for an individual SVM or for all the SVMs in a cluster.

**About this task**

By default, ONTAP creates an on-access policy named "default_CIFS" and enables it for all the SVMs in a cluster.

You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan servers are available for virus scanning. Keep in mind that any file that qualifies for scan exclusion based on the `paths-to-exclude`, `file-ext-to-exclude`, or `max-file-size` parameters is not considered for scanning even if the `scan-mandatory` option is set to on.

> (i) For potential issues related to the `scan-mandatory` option, see Potential connectivity issues involving the scan-mandatory option.

By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access.

**Steps**

1. Create an on-access policy:

   ```
   vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
   -policy-name policy_name -protocol CIFS -max-file-size
   max_size_of_files_to_scan –filters [scan-ro-volume,][scan-execute-access]
   -file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
   extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
   -exclude paths_of_files_to_exclude -scan-mandatory on|off
   ```

   ◦ Specify a data SVM for a policy defined for an individual SVM, a cluster admin SVM for a policy defined for all the SVMs in a cluster.

   ◦ The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.

   ◦ Set `-scan-files-with-no-ext` to true to scan files without extensions.
     The following command creates an on-access policy named `Policy1` on the `vs1`SVM:

   ```
   cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
   -name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
   -file-ext-to-include "mp*","tx*" -file-ext-to-exclude "mp3","txt" -scan
   -files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
   ```

2. Verify that the on-access policy has been created: `vserver vscan on-access-policy show`

```
-instance data_SVM|cluster_admin_SVM -policy-name policy_name
```

For a complete list of options, see the man page for the command.

The following command displays the details for the `Policy1` policy:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                              Vserver: vs1
                               Policy: Policy1
                        Policy Status: off
                  Policy Config Owner: vserver
                 File-Access Protocol: CIFS
                              Filters: scan-ro-volume
                       Mandatory Scan: on
  Max File Size Allowed for Scanning: 3GB
              File Paths Not to Scan: \vol\a b\, \vol\a,b\
         File Extensions Not to Scan: mp3, txt
             File Extensions to Scan: mp*, tx*
         Scan Files with No Extension: false
```

**Enable an on-access policy**

You must enable an on-access policy on an SVM before its files can be scanned. If you created an on-access policy for all the SVMs in a cluster, you must enable the policy on each SVM individually. You can enable only one on-access policy on an SVM at a time.

**Steps**

1. Enable an on-access policy:

   ```
   vserver vscan on-access-policy enable -vserver data_SVM -policy-name
   policy_name
   ```

   The following command enables an on-access policy named `Policy1` on the `vs1`SVM:

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. Verify that the on-access policy is enabled: `vserver vscan on-access-policy show -instance data_SVM -policy-name policy_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `Policy1` on-access policy:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                             Vserver: vs1
                              Policy: Policy1
                       Policy Status: on
                 Policy Config Owner: vserver
                File-Access Protocol: CIFS
                             Filters: scan-ro-volume
                      Mandatory Scan: on
 Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
        File Extensions Not to Scan: mp3, txt
            File Extensions to Scan: mp*, tx*
         Scan Files with No Extension: false
```

**Modify the Vscan file-operations profile for an SMB share**

The Vscan file-operations profile for an SMB share defines which operations on the share
can trigger scanning. By default, the parameter is set to `standard`. You can adjust the
parameter as necessary when you create or modify an SMB share.

**About this task**

For more information on the available values for a Vscan file-operations profile, see "Vscan file-operations
profile."

Vscan file-operations profile (on-access scanning only)

> (i) Virus scanning is not performed on a SMB share for which the `continuously-available`
> parameter is set to `Yes`.

**Step**

1. Modify the value of the Vscan file-operations profile for a SMB share: `vserver cifs share modify`
   `-vserver` *data_SVM* `-share-name` *share* `-path` *share_path* `-vscan-fileop-profile no-`
   `scan|standard|strict|writes-only`

   For a complete list of options, see the man page for the command.

   The following command changes the Vscan file operations profile for a SMB share to `strict`:

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

**Commands for managing on-access policies**

You can modify, disable, or delete an on-access policy. You can view a summary and details for the policy.

| If you want to… | Enter the following command… |
|---|---|
| Modify an on-access policy | `vserver vscan on-access-policy modify` |
| Disable an on-access policy | `vserver vscan on-access-policy disable` |
| Delete an on-access policy | `vserver vscan on-access-policy delete` |
| View summary and details for an on-access policy | `vserver vscan on-access-policy show` |
| Add to the list of paths to exclude | `vscan on-access-policy paths-to-exclude add` |
| Delete from the list of paths to exclude | `vscan on-access-policy paths-to-exclude remove` |
| View the list of paths to exclude | `vscan on-access-policy paths-to-exclude show` |
| Add to the list of file extensions to exclude | `vscan on-access-policy file-ext-to-exclude add` |
| Delete from the list of file extensions to exclude | `vscan on-access-policy file-ext-to-exclude remove` |
| View the list of file extensions to exclude | `vscan on-access-policy file-ext-to-exclude show` |
| Add to the list of file extensions to include | `vscan on-access-policy file-ext-to-include add` |
| Delete from the list of file extensions to include | `vscan on-access-policy file-ext-to-include remove` |
| View the list of file extensions to include | `vscan on-access-policy file-ext-to-include show` |

For more information about these commands, see the man pages.

## Configure on-demand scanning

### Configure on-demand scanning overview

You can use on-demand scanning to check files for viruses immediately or on a schedule. You might want to run scans only in off-peak hours, for example, or you might want to scan very large files that were excluded from an on-access scan.

You can use a cron schedule to specify when the task runs:

- You can assign a schedule when you create a task.

- You can create a task without assigning a schedule, and use the `vserver vscan on-demand-task schedule` command to assign a schedule.

- You can use the `vserver vscan on-demand-task run` command to run a task immediately, whether or not you have assigned a schedule.

Only one task can be scheduled at a time on an SVM.

> ⓘ   On-demand scanning does not support scanning of symbolic links or stream files.

### Create an on-demand task

An on-demand task defines the scope of an on-demand scan. You can specify the maximum size of the files to be scanned, the extensions and paths of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. Files in subdirectories are scanned by default.

**Steps**

1. Create an on-demand task:

   ```
   vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
   -scan-paths paths_of_files_to_scan -report-directory report_directory_path
   -report-expiry-time expiration_time_for_report -schedule cron_schedule -max
   -file-size max_size_of_files_to_scan -paths-to-exclude
   paths_of_files_to_exclude -file-ext-to-exclude extensions_of_files_to_exclude
   -file-ext-to-include extensions_of_files_to_include -scan-files-with-no-ext
   true|false -directory-recursion true|false
   ```

   - The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.

   - Set `-scan-files-with-no-ext` to true to scan files without extensions.
     For a complete list of options, see the man page for the command.

   The following command creates an on-access task named `Task1` on the `vs1`SVM:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

> (i) You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

2. Verify that the on-demand task has been created: `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `Task1` task:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                          Vserver: vs1
                        Task Name: Task1
              List of Scan Paths: /vol1/, /vol2/cifs/
           Report Directory Path: /report
                     Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
           File Paths Not to Scan: /vol1/cold-files/
      File Extensions Not to Scan: mp3, mp4
          File Extensions to Scan: vmdk?, mp*
     Scan Files with No Extension: false
          Request Service Timeout: 5m
                  Cross Junction: true
             Directory Recursion: true
                   Scan Priority: low
                Report Log Level: info
       Expiration Time for Report: -
```

**After you finish**

You must enable scanning on the SVM before the task is scheduled to run.

**Schedule an on-demand task**

If you have created an on-demand task without assigning a schedule, or if you want to

assign a different schedule to a task, you can use the `vserver vscan on-demand-task schedule` command to assign a schedule to the task.

**About this task**

The schedule assigned with the `vserver vscan on-demand-task schedule` command overrides a schedule already assigned with the `vserver vscan on-demand-task create` command.

**Steps**

1. Schedule an on-demand task:

   `vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name -schedule cron_schedule`

   The following command schedules an on-access task named `Task2` on the `vs2`SVM:

   ```
   cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
   -name Task2 -schedule daily
   [Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
   command to view the status.
   ```

   > ⓘ  You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

2. Verify that the on-demand task has been scheduled: `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `Task 2` task:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                              Vserver: vs2
                            Task Name: Task2
                   List of Scan Paths: /vol1/, /vol2/cifs/
               Report Directory Path: /report
                         Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
               File Paths Not to Scan: /vol1/cold-files/
          File Extensions Not to Scan: mp3, mp4
               File Extensions to Scan: vmdk, mp*
       Scan Files with No Extension: false
             Request Service Timeout: 5m
                        Cross Junction: true
                  Directory Recursion: true
                        Scan Priority: low
                     Report Log Level: info
```

**After you finish**

You must enable scanning on the SVM before the task is scheduled to run.

**Run an on-demand task immediately**

You can run an on-demand task immediately, whether or not you have assigned a
schedule.

**What you'll need**

You must have enabled scanning on the SVM.

**Step**

1. Run an on-demand task immediately:

   ```
   vserver vscan on-demand-task run -vserver data_SVM -task-name task_name
   ```

   The following command runs an on-access task named `Task1` on the `vs1`SVM:

   ```
   cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
   Task1
   [Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
   command to view the status.
   ```

   > ℹ️ You can use the `job show` command to view the status of the job. You can use the `job`
   > `pause` and `job resume` commands to pause and restart the job, or the `job stop`
   > command to end the job.

**Commands for managing on-demand tasks**

You can modify, delete, or unschedule an on-demand task. You can view a summary and details for the task, and manage reports for the task.

| If you want to… | Enter the following command… |
|---|---|
| Modify an on-demand task | `vserver vscan on-demand-task modify` |
| Delete an on-demand task | `vserver vscan on-demand-task delete` |
| Unschedule an on-demand task | `vserver vscan on-demand-task unschedule` |
| View summary and details for an on-demand task | `vserver vscan on-demand-task show` |
| View on-demand reports | `vserver vscan on-demand-task report show` |
| Delete on-demand reports | `vserver vscan on-demand-task report delete` |

For more information about these commands, see the man pages.

## Enable virus scanning on an SVM

You must enable virus scanning on an SVM before an on-access or on-demand scan can run. The Vscan configuration must exist.

**Steps**

1. Enable virus scanning on an SVM:

   `vserver vscan enable -vserver data_SVM`

   > ⓘ You can use the `vserver vscan disable` command to disable virus scanning if necessary.

   The following command enables virus scanning on the `vs1`SVM:

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. Verify that virus scanning is enabled on the SVM:

   `vserver vscan show -vserver data_SVM`

   For a complete list of options, see the man page for the command.

   The following command displays the Vscan status of the `vs1`SVM:

```
cluster1::> vserver vscan show -vserver vs1

                              Vserver: vs1
                         Vscan Status: on
```

## Reset the status of scanned files

Occasionally, you might want to reset the scan status of successfully scanned files on an SVM by using the `vserver vscan reset` command to discard the cached information for the files. You might want to use this command to restart the virus scanning processing in case of a misconfigured scan, for example.

**About this task**

After you run the `vserver vscan reset` command, all eligible files will be scanned the next time they are accessed.

> (i) This command can affect performance adversely, depending on the number and size of the files to be rescanned.

**Step**

1. Reset the status of scanned files:

   `vserver vscan reset -vserver data_SVM`

   The following command resets the status of scanned files on the `vs1`SVM:

   ```
   cluster1::> vserver vscan reset -vserver vs1
   ```

## View Vscan event log information

You can use the `vserver vscan show-events` command to view event log information about infected files, updates to Vscan servers, and the like. You can view event information for the cluster or for given nodes, SVMs, or Vscan servers.

**What you'll need**

Advanced privileges are required for this task.

**Steps**

1. Change to advanced privilege level:

   `set -privilege advanced`

2. View Vscan event log information:

   `vserver vscan show-events`

For a complete list of options, see the man page for the command.

The following command displays event log information for the cluster `cluster1`:

```
cluster1::*> vserver vscan show-events

Vserver      Node              Server           Event Type         Event Time
-----------  ---------------   ---------------  -----------------
----------------
vs1          Cluster-01        192.168.1.1      file-infected      9/5/2014
11:37:38
vs1          Cluster-01        192.168.1.1      scanner-updated    9/5/2014
11:37:08
vs1          Cluster-01        192.168.1.1      scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

## Troubleshoot connectivity issues

### Potential connectivity issues involving the scan-mandatory option

You can use the `vserver vscan connection-status show` commands to view information about Vscan server connections that you might find helpful in troubleshooting connectivity issues.

By default, the `scan-mandatory` option for on-access scanning denies file access when a Vscan server connection is not available for scanning. Although this option offers important safety features, it can lead to problems in a few situations.

- Before enabling client access, you must ensure that at least one Vscan server is connected to an SVM on each node that has a LIF. If you need to connect servers to SVMs after enabling client access, you must turn off the `scan-mandatory` option on the SVM to ensure that file access is not denied because a Vscan server connection is not available. You can turn the option back on after the server has been connected.

- If a target LIF hosts all the Vscan server connections for an SVM, the connection between the server and the SVM will be lost if the LIF is migrated. To ensure that file access is not denied because a Vscan server connection is not available, you must turn off the `scan-mandatory` option before migrating the LIF. You can turn the option back on after the LIF has been migrated.

Each SVM should have at least two Vscan servers assigned to it. It is a best practice to connect Vscan servers to the storage system over a different network from the one used for client access.

### Commands for viewing Vscan server connection status

You can use the `vserver vscan connection-status show` commands to view summary and detailed information about Vscan server connection status.

| If you want to… | Enter the following command… |
|---|---|
| View a summary of Vscan server connections | `vserver vscan connection-status show` |
| View details for Vscan server connections | `vserver vscan connection-status show-all` |
| View details for connected Vscan servers | `vserver vscan connection-status show-connected` |
| View details for available Vscan servers that are not connected | `vserver vscan connection-status show-not-connected` |

For more information about these commands, see the man pages.

# NAS auditing and security tracing

## SMB and NFS auditing and security tracing overview

You can use the file access auditing features available for the SMB and NFS protocols with ONTAP, such as native auditing and file policy management using FPolicy.

You should design and implement auditing of SMB and NFS file access events under the following circumstances:

- Basic SMB and NFS protocol file access has been configured.
- You want to create and maintain an auditing configuration using one of the following methods:
  - Native ONTAP functionality
  - External FPolicy servers

## Audit NAS events on SVMs

### Audit NAS events on SVMs overview

Auditing for NAS events is a security measure that enables you to track and log certain SMB and NFS events on storage virtual machines (SVMs). This helps you track potential security problems and provides evidence of any security breaches. You can also stage and audit Active Directory central access policies to see what the result of implementing them would be.

### SMB events

You can audit the following events:

- SMB file and folder access events

  You can audit SMB file and folder access events on objects stored on FlexVol volumes belonging to the auditing-enabled SVMs.

- SMB logon and logoff events

  You can audit SMB logon and logoff events for SMB servers on SVMs.

- Central access policy staging events

  You can audit the effective access of objects on SMB servers using permissions applied through proposed central access policies. Auditing through the staging of central access policies enables you to see what the effects are of central access policies before they are deployed.

  Auditing of central access policy staging is set up using Active Directory GPOs; however, the SVM auditing configuration must be configured to audit central access policy staging events.

  Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.

**NFS events**

You can audit file and directory events by utilizing NFSv4 ACL's on objects stored on SVMs.

**How auditing works**

**Basic auditing concepts**

To understand auditing in ONTAP, you should be aware of some basic auditing concepts.

- **Staging files**

  The intermediate binary files on individual nodes where audit records are stored prior to consolidation and conversion. Staging files are contained in staging volumes.

- **Staging volume**

  A dedicated volume created by ONTAP to store staging files. There is one staging volume per aggregate. Staging volumes are shared by all audit-enabled storage virtual machines (SVMs) to store audit records of data access for data volumes in that particular aggregate. Each SVM's audit records are stored in a separate directory within the staging volume.

  Cluster administrators can view information about staging volumes, but most other volume operations are not permitted. Only ONTAP can create staging volumes. ONTAP automatically assigns a name to staging volumes. All staging volume names begin with `MDV_aud_` followed by the UUID of the aggregate containing that staging volume (for example: `MDV_aud_1d0131843d4811e296fc123478563412.`)

- **System volumes**

  A FlexVol volume that contains special metadata, such as metadata for file services audit logs. The admin SVM owns system volumes, which are visible across the cluster. Staging volumes are a type of system volume.

- **Consolidation task**

  A task that gets created when auditing is enabled. This long-running task on each SVM takes the audit records from staging files across the member nodes of the SVM. This task merges the audit records in

sorted chronological order, and then converts them to a user-readable event log format specified in the auditing configuration—either the EVTX or XML file format. The converted event logs are stored in the audit event log directory that is specified in the SVM auditing configuration.

**How the ONTAP auditing process works**

The ONTAP auditing process is different from the Microsoft auditing process. Before you configure auditing, you should understand how the ONTAP auditing process works.

Audit records are initially stored in binary staging files on individual nodes. If auditing is enabled on an SVM, every member node maintains staging files for that SVM. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

**Process when auditing is enabled on an SVM**

Auditing can only be enabled on SVMs. When the storage administrator enables auditing on the SVM, the auditing subsystem checks whether staging volumes are present. A staging volume must exist for each aggregate that contains data volumes owned by the SVM. The auditing subsystem creates any needed staging volumes if they do not exist.

The auditing subsystem also completes other prerequisite tasks before auditing is enabled:

* The auditing subsystem verifies that the log directory path is available and does not contain symlinks.

  The log directory must already exist as a path within the SVM's namespace. It is recommended to create a new volume or qtree to hold the audit log files. The auditing subsystem does not assign a default log file location. If the log directory path specified in the auditing configuration is not a valid path, auditing configuration creation fails with the `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` error.

  Configuration creation fails if the directory exists but contains symlinks.

* Auditing schedules the consolidation task.

  After this task is scheduled, auditing is enabled. The SVM auditing configuration and the log files persist across a reboot or if the NFS or SMB servers are stopped or restarted.

**Event log consolidation**

Log consolidation is a scheduled task that runs on a routine basis until auditing is disabled. When auditing is disabled, the consolidation task verifies that all of the remaining logs are consolidated.

**Guaranteed auditing**

By default, auditing is guaranteed. ONTAP guarantees that all auditable file access events (as specified by configured audit policy ACLs) are recorded, even if a node is unavailable. A requested file operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed to the disk in the staging files, either because of insufficient space or because of other issues, client operations are denied.

> **ⓘ** An administrator, or account user with privilege level access, can bypass the file audit logging operation by using NetApp Manageability SDK or REST APIs. You can determine if any file actions have been taken using NetApp Manageability SDK or REST APIs by reviewing the command history logs stored in the `audit.log` file.
>
> For more information about command history audit logs, see the "Managing audit logging for management activities" section in System administration.

**Consolidation process when a node is unavailable**

If a node containing volumes belonging to an SVM with auditing enabled is unavailable, the behavior of the auditing consolidation task depends on whether the node's storage failover (SFO) partner (or the HA partner in the case of a two-node cluster) is available:

- If the staging volume is available through the SFO partner, the staging volumes last reported from the node are scanned, and consolidation proceeds normally.
- If the SFO partner is not available, the task creates a partial log file.

  When a node is not reachable, the consolidation task consolidates the audit records from the other available nodes of that SVM. To identify that it is not complete, the task adds the suffix `.partial` to the consolidated file name.

- After the unavailable node is available, the audit records in that node are consolidated with the audit records from the other nodes at that time.
- All audit records are preserved.

**Event log rotation**

Audit event log files are rotated when they reach a configured threshold log size or on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

**Process when auditing is disabled on the SVM**

When auditing is disabled on the SVM, the consolidation task is triggered one final time. All outstanding, recorded audit records are logged in a user-readable format. Existing event logs stored in the event log directory are not deleted when auditing is disabled on the SVM and are available for viewing.

After all existing staging files for that SVM are consolidated, the consolidation task is removed from the schedule. Disabling the auditing configuration for the SVM does not remove the auditing configuration. A storage administrator can reenable auditing at any time.

The auditing consolidation job, which gets created when auditing is enabled, monitors the consolidation task and re-creates it if the consolidation task exits because of an error. Previously, users could delete the auditing consolidation job by using job manager commands such as `job delete`. Users are no longer allowed to delete the auditing consolidation job.

**Auditing requirements and considerations**

Before you configure and enable auditing on your storage virtual machine (SVM), you need to be aware of certain requirements and considerations.

- The maximum number of auditing-enabled SVMs supported in a cluster is 50.

- Auditing is not tied to SMB or NFS licensing.

  You can configure and enable auditing even if SMB and NFS licenses are not installed on the cluster.

- NFS auditing supports security ACEs (type U).

- For NFS auditing, there is no mapping between mode bits and auditing ACEs.

  When converting ACLs to mode bits, auditing ACEs are skipped. When converting mode bits to ACLs, auditing ACEs are not generated.

- The directory specified in the auditing configuration must exist.

  If it does not exist, the command to create the auditing configuration fails.

- The directory specified in the auditing configuration must meet the following requirements:

  ◦ The directory must not contain symbolic links.

    If the directory specified in the auditing configuration contains symbolic links, the command to create the auditing configuration fails.

  ◦ You must specify the directory by using an absolute path.

    You should not specify a relative path, for example, `/vs1/../`.

- Auditing is dependent on having available space in the staging volumes.

  You must be aware of and have a plan for ensuring that there is sufficient space for the staging volumes in aggregates that contain audited volumes.

- Auditing is dependent on having available space in the volume containing the directory where converted event logs are stored.

  You must be aware of and have a plan for ensuring that there is sufficient space in the volumes used to store event logs. You can specify the number of event logs to retain in the auditing directory by using the `-rotate-limit` parameter when creating an auditing configuration, which can help to ensure that there is enough available space for the event logs in the volume.

- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, Dynamic Access Control must be enabled to generate central access policy staging events.

  Dynamic Access Control is not enabled by default.

**Aggregate space considerations when enabling auditing**

When an auditing configuration is created and auditing is enabled on at least one storage virtual machine (SVM) in the cluster, the auditing subsystem creates staging volumes on all existing aggregates and on all new aggregates that are created. You need to be aware of certain aggregate space considerations when you enable auditing on the cluster.

Staging volume creation might fail due to non-availability of space in an aggregate. This might happen if you create an auditing configuration and existing aggregates do not have enough space to contain the staging volume.

You should ensure that there is enough space on existing aggregates for the staging volumes before enabling auditing on an SVM.

**Limitations for the size of audit records on staging files**

The size of an audit record on a staging file cannot be greater than 32 KB.

### When large audit records can occur

Large audit records might occur during management auditing in one of the following scenarios:

- Adding or deleting users to or from groups with a large number of users.
- Adding or deleting a file-share access control list (ACL) on a file-share with a large number of file-share users.
- Other scenarios.

Disable management auditing to avoid this issue. To do this, modify the audit configuration and remove the following from the list of audit event types:

- file-share
- user-account
- security-group
- authorization-policy-change

   After removal, they will not be audited by the file services auditing subsystem.

### The effects of audit records that are too large

- If the size of an audit record is too large (over 32 KB), the audit record is not created and the auditing subsystem generates an event management system (EMS) message similar to the following:

   ```
   File Services Auditing subsystem failed the operation or truncated an audit
   record because it was greater than max_audit_record_size value. Vserver
   UUID=%s, event_id=%u, size=%u
   ```

   If auditing is guaranteed, the file operation fails because its audit record cannot be created.

- If the size of the audit record is more than 9,999 bytes, the same EMS message as above is displayed. A partial audit record is created with the larger key value missing.

- If the audit record exceeds 2,000 characters, the following error message shows instead of the actual value:

   ```
   The value of this field was too long to display.
   ```

**What the supported audit event log formats are**

Supported file formats for the converted audit event logs are `EVTX` and `XML` file formats.

You can specify the type of file format when you create the auditing configuration. By default, ONTAP converts the binary logs to the `EVTX` file format.

**View audit event logs**

You can use audit event logs to determine whether you have adequate file security and whether there have been improper file and folder access attempts. You can view and process audit event logs saved in the `EVTX` or `XML` file formats.

- `EVTX` file format

  You can open the converted `EVTX` audit event logs as saved files using Microsoft Event Viewer.

  There are two options that you can use when viewing event logs using Event Viewer:

  - General view

    Information that is common to all events is displayed for the event record. In this version of ONTAP, the event-specific data for the event record is not displayed. You can use the detailed view to display event-specific data.

  - Detailed view

    A friendly view and an XML view are available. The friendly view and the XML view display both the information that is common to all events and the event-specific data for the event record.

- `XML` file format

  You can view and process `XML` audit event logs on third-party applications that support the `XML` file format. XML viewing tools can be used to view the audit logs provided you have the XML schema and information about definitions for the XML fields. For more information about the XML schema and definitions, see the [ONTAP Auditing Schema Reference](#).

**How active audit logs are viewed using Event Viewer**

If the audit consolidation process is running on the cluster, the consolidation process appends new records to the active audit log file for audit-enabled storage virtual machines (SVMs). This active audit log can be accessed and opened over an SMB share in Microsoft Event Viewer.

In addition to viewing existing audit records, Event Viewer has a refresh option that enables you to refresh the content in the console window. Whether the newly appended logs are viewable in Event Viewer depends on whether oplocks are enabled on the share used to access the active audit log.

| Oplocks setting on the share | Behavior |
|---|---|
| Enabled | Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation does not refresh the log with new events appended by the consolidation process. |
| Disabled | Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation refreshes the log with new events appended by the consolidation process. |

ⓘ This information is applicable only for `EVTX` event logs. `XML` event logs can be viewed through SMB in a browser or through NFS using any XML editor or viewer.

## SMB events that can be audited

**SMB events that can be audited overview**

ONTAP can audit certain SMB events, including certain file and folder access events, certain logon and logoff events, and central access policy staging events. Knowing which access events can be audited is helpful when interpreting results from the event logs.

The following additional SMB events can be audited in ONTAP 9.2 and later:

| Event ID (EVT/EVTX) | Event | Description | Category |
|---|---|---|---|
| 4670 | Object permissions were changed | OBJECT ACCESS: Permissions changed. | File Access |
| 4907 | Object auditing settings were changed | OBJECT ACCESS: Audit settings changed. | File Access |
| 4913 | Object Central Access Policy was changed | OBJECT ACCESS: CAP changed. | File Access |

The following SMB events can be audited in ONTAP 9.0 and later:

| Event ID (EVT/EVTX) | Event | Description | Category |
|---|---|---|---|
| 540/4624 | An account was successfully logged on | LOGON/LOGOFF: Network (SMB) logon. | Logon and Logoff |
| 529/4625 | An account failed to log on | LOGON/LOGOFF: Unknown user name or bad password. | Logon and Logoff |
| 530/4625 | An account failed to log on | LOGON/LOGOFF: Account logon time restriction. | Logon and Logoff |
| 531/4625 | An account failed to log on | LOGON/LOGOFF: Account currently disabled. | Logon and Logoff |
| 532/4625 | An account failed to log on | LOGON/LOGOFF: User account has expired. | Logon and Logoff |
| 533/4625 | An account failed to log on | LOGON/LOGOFF: User cannot log on to this computer. | Logon and Logoff |
| 534/4625 | An account failed to log on | LOGON/LOGOFF: User not granted logon type here. | Logon and Logoff |

| 535/4625 | An account failed to log on | LOGON/LOGOFF: User's password has expired. | Logon and Logoff |
|---|---|---|---|
| 537/4625 | An account failed to log on | LOGON/LOGOFF: Logon failed for reasons other than above. | Logon and Logoff |
| 539/4625 | An account failed to log on | LOGON/LOGOFF: Account locked out. | Logon and Logoff |
| 538/4634 | An account was logged off | LOGON/LOGOFF: Local or network user logoff. | Logon and Logoff |
| 560/4656 | Open Object/Create Object | OBJECT ACCESS: Object (file or directory) open. | File Access |
| 563/4659 | Open Object with the Intent to Delete | OBJECT ACCESS: A handle to an object (file or directory) was requested with the Intent to Delete. | File Access |
| 564/4660 | Delete Object | OBJECT ACCESS: Delete Object (file or directory). ONTAP generates this event when a Windows client attempts to delete the object (file or directory). | File Access |
| 567/4663 | Read Object/Write Object/Get Object Attributes/Set Object Attributes | OBJECT ACCESS: Object access attempt (read, write, get attribute, set attribute). **Note:** For this event, ONTAP audits only the first SMB read and first SMB write operation (success or failure) on an object. This prevents ONTAP from creating excessive log entries when a single client opens an object and performs many successive read or write operations to the same object. | File Access |
| NA/4664 | Hard link | OBJECT ACCESS: An attempt was made to create a hard link. | File Access |
| NA/4818 | Proposed central access policy does not grant the same access permissions as the current central access policy | OBJECT ACCESS: Central Access Policy Staging. | File Access |

| NA/NA Data ONTAP Event ID 9999 | Rename Object | OBJECT ACCESS: Object renamed. This is an ONTAP event. It is not currently supported by Windows as a single event. | File Access |
|---|---|---|---|
| NA/NA Data ONTAP Event ID 9998 | Unlink Object | OBJECT ACCESS: Object unlinked. This is an ONTAP event. It is not currently supported by Windows as a single event. | File Access |

**Additional information about Event 4656**

The `HandleID` tag in the audit `XML` event contains the handle of the object (file or directory) accessed. The `HandleID` tag for the EVTX 4656 event contains different information depending on whether the open event is for creating a new object or for opening an existing object:

- If the open event is an open request to create a new object (file or directory), the `HandleID` tag in the audit XML event shows an empty `HandleID` (for example: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  The `HandleID` is empty because the OPEN (for creating a new object) request gets audited before the actual object creation happens and before a handle exists. Subsequent audited events for the same object have the right object handle in the `HandleID` tag.

- If the open event is an open request to open an existing object, the audit event will have the assigned handle of that object in the `HandleID` tag (for example: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

**Determine what the complete path to the audited object is**

The object path printed in the `<ObjectName>` tag for an audit record contains the name of the volume (in parentheses) and the relative path from the root of the containing volume. If you want to determine the complete path of the audited object, including the junction path, there are certain steps you must take.

**Steps**

1. Determine what the volume name and relative path to audited object is by looking at the `<ObjectName>` tag in the audit event.

   In this example, the volume name is "data1" and the relative path to the file is `/dir1/file.txt`:

   ```
   <Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
   ```

2. Using the volume name determined in the previous step, determine what the junction path is for the volume containing the audited object:

   In this example, the volume name is "data1" and the junction path for the volume containing the audited object is `/data/data1`:

   ```
   volume show -junction -volume data1
   ```

```
                                   Junction                        Junction
    Vserver    Volume      Language Active   Junction Path     Path Source
    --------- ------------ -------- -------- ----------------- -----------
    vs1       data1        en_US.UTF-8
                                    true     /data/data1       RW_volume
```

3. Determine the full path to the audited object by appending the relative path found in the `<ObjectName>` tag to the junction path for the volume.

   In this example, the junction path for the volume:

   `/data/data1/dir1/file.text`

**Considerations when auditing symlinks and hard links**

# There are certain considerations you must keep in mind when auditing symlinks and hard links.

An audit record contains information about the object being audited including the path to the audited object, which is identified in the `ObjectName` tag. You should be aware of how paths for symlinks and hard links are recorded in the `ObjectName` tag.

## Symlinks

A symlink is a file with a separate inode that contains a pointer to the location of a destination object, known as the target. When accessing an object through a symlink, ONTAP automatically interprets the symlink and follows the actual canonical protocol agnostic path to the target object in the volume.

In the following example output, there are two symlinks, both pointing to a file named `target.txt`. One of the symlinks is a relative symlink and one is an absolute symlink. If either of the symlinks are audited, the `ObjectName` tag in the audit event contains the path to the file `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

## Hard links

A hard link is a directory entry that associates a name with an existing file on a file system. The hard link points to the inode location of the original file. Similar to how ONTAP interprets symlinks, ONTAP interprets the hard link and follows the actual canonical path to the target object in the volume. When access to a hard link object is audited, the audit event records this absolute canonical path in the `ObjectName` tag rather than the hard link path.

**Considerations when auditing alternate NTFS data streams**

## There are certain considerations you must keep in mind when auditing files with NTFS alternate data streams.

The location of an object being audited is recorded in an event record using two tags, the `ObjectName` tag (the path) and the `HandleID` tag (the handle). To properly identify which stream requests are being logged, you must be aware of what ONTAP records in these fields for NTFS alternate data streams:

- EVTX ID: 4656 events (open and create audit events)
  - The path of the alternate data stream is recorded in the `ObjectName` tag.
  - The handle of the alternate data stream is recorded in the `HandleID` tag.
- EVTX ID: 4663 events (all other audit events, such as read, write, getattr, and so on)
  - The path of the base file, not the alternate data stream, is recorded in the `ObjectName` tag.
  - The handle of the alternate data stream is recorded in the `HandleID` tag.

**Example**

The following example illustrates how to identify EVTX ID: 4663 events for alternate data streams using the `HandleID` tag. Even though the `ObjectName` tag (path) recorded in the read audit event is to the base file path, the `HandleID` tag can be used to identify the event as an audit record for the alternate data stream.

Stream file names take the form `base_file_name:stream_name`. In this example, the `dir1` directory contains a base file with an alternate data stream having the following paths:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

> ⓘ   The output in the following event example is truncated as indicated; the output does not display all of the available output tags for the events.

For an EVTX ID 4656 (open audit event), the audit record output for the alternate data stream records the alternate data stream name in the `ObjectName` tag:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

For an EVTX ID 4663 (read audit event), the audit record output for the same alternate data stream records the base file name in the `ObjectName` tag; however, the handle in the `HandleID` tag is the alternative data stream's handle and can be used to correlate this event with the alternative data stream:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

**NFS file and directory access events that can be audited**

ONTAP can audit certain NFS file and directory access events. Knowing what access events can be audited is helpful when interpreting results from the converted audit event logs.

You can audit the following NFS file and directory access events:

- READ
- OPEN
- CLOSE
- READDIR
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

To reliably audit NFS RENAME events, you should set audit ACEs on directories instead of files because file permissions are not checked for a RENAME operation if the directory permissions are sufficient.

**Plan the auditing configuration**

Before you configure auditing on storage virtual machines (SVMs), you must understand which configuration options are available and plan the values that you want to set for each option. This information can help you configure the auditing configuration that meets your business needs.

There are certain configuration parameters that are common to all auditing configurations.

Additionally, there are certain parameters that you can use to specify which methods are used when rotating the consolidated and converted audit logs. You can specify one of the three following methods when you configure auditing:

- Rotate logs based on log size

  This is the default method used to rotate logs.

- Rotate logs based on a schedule
- Rotate logs based on log size and schedule (whichever event occurs first)

  ⓘ    At least one of the methods for log rotation should always be set.

**Parameters common to all auditing configurations**

There are two required parameters that you must specify when you create the auditing configuration. There are also three optional parameters that you can specify:

| Type of information | Option | Required | Include | Your values |
|---|---|---|---|---|
| *SVM name*<br><br>Name of the SVM on which to create the auditing configuration. The SVM must already exist. | `-vserver vserver_name` | Yes | Yes | |
| *Log destination path*<br><br>Specifies the directory where the converted audit logs are stored, typically a dedicated volume or qtree. The path must already exist in the SVM namespace.<br><br>The path can be up to 864 characters in length and must have read-write permissions.<br><br>If the path is not valid, the audit configuration command fails.<br><br>If the SVM is an SVM disaster recovery source, the log destination path cannot be on the root volume. This is because root volume content is not replicated to the disaster recovery destination.<br><br>You cannot use a FlexCache volume as a log destination (ONTAP 9.7 and later). | `-destination text` | Yes | Yes | |

| Categories of events to audit | `-events {file-ops\|cifs-logon-logoff\|cap-staging\|file-share \|audit-policy-change \|user-account\|security-group\|authorization-policy-change}` | No | | |
|---|---|---|---|---|
| Specifies the categories of events to audit. The following event categories can be audited: | | | | |

Specifies the categories of events to audit. The following event categories can be audited:

- File access events (both SMB and NFSv4)

- SMB logon and logoff events

- Central access policy staging events

  Central access policy staging events are a new advanced auditing event available beginning with Windows 2012 Active Directory domains. Central access policy staging events log information about changes to central access policies configured in Active Directory.

- File share category events

- Audit policy change events

- Local user account management events

- Security group management events

- Authorization policy change events

The default is to audit file access and SMB logon and logoff events.

**Note:** Before you can specify `cap-staging` as an event category, a SMB server must exist on the SVM. Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.

| Log file output format | `-format {xml\|evtx}` | No | | |
|---|---|---|---|---|

Determines the output format of the audit logs. The output format can be either ONTAP-specific `XML` or Microsoft Windows `EVTX` log format. By default, the output format is `EVTX`.

| | | | | |
|---|---|---|---|---|
| *Log files rotation limit*<br><br>Determines how many audit log files to retain before rotating the oldest log file out. For example, if you enter a value of `5`, the last five log files are retained.<br><br>A value of `0` indicates that all the log files are retained. The default value is 0. | `-rotate-limit integer` | No | | |

**Parameters used for determining when to rotate audit event logs**

### Rotate logs based on log size

The default is to rotate audit logs based on size.

- The default log size is 100 MB

- If you want to use the default log rotation method and the default log size, you do not need to configure any specific parameters for log rotation.

- If you want to rotate the audit logs based on a log size alone, use the following command to unset the `-rotate-schedule-minute` parameter: `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

If you do not want to use the default log size, you can configure the `-rotate-size` parameter to specify a custom log size:

| Type of information | Option | Required | Include | Your values |
|---|---|---|---|---|
| *Log file size limit*<br><br>Determines the audit log file size limit. | `-rotate-size { integer[KB\|MB\|GB\|TB\|PB]}` | No | | |

### Rotate logs based on a schedule

If you choose to rotate the audit logs based on a schedule, you can schedule log rotation by using the time-based rotation parameters in any combination.

- If you use time-based rotation, the `-rotate-schedule-minute` parameter is mandatory.

- All other time-based rotation parameters are optional.

- The rotation schedule is calculated by using all the time-related values.

  For example, if you specify only the `-rotate-schedule-minute` parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all months of the year.

- If you specify only one or two time-based rotation parameters (for example, `-rotate-schedule-month` and `-rotate-schedule-minutes`), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months.

  For example, you can specify that the audit log is to be rotated during the months January, March, and

August on all Mondays, Wednesdays, and Saturdays at 10:30 a.m.

- If you specify values for both `-rotate-schedule-dayofweek` and `-rotate-schedule-day`, they are considered independently.

  For example, if you specify `-rotate-schedule-dayofweek` as Friday and `-rotate-schedule-day` as 13, then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.

- If you want to rotate the audit logs based on a schedule alone, use the following command to unset the `-rotate-size` parameter: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

You can use the following list of available auditing parameters to determine what values to use for configuring a schedule for audit event log rotations:

| Type of information | Option | Required | Include | Your values |
|---|---|---|---|---|
| *Log rotation schedule: Month*<br><br>Determines the monthly schedule for rotating audit logs.<br><br>Valid values are `January` through `December`, and `all`. For example, you can specify that the audit log is to be rotated during the months January, March, and August. | `-rotate-schedule-month`<br>`chron_month` | No | | |
| *Log rotation schedule: Day of week*<br><br>Determines the daily (day of week) schedule for rotating audit logs.<br><br>Valid values are `Sunday` through `Saturday`, and `all`. For example, you can specify that the audit log is to be rotated on Tuesdays and Fridays, or during all the days of a week. | `-rotate-schedule`<br>`-dayofweek`<br>`chron_dayofweek` | No | | |
| *Log rotation schedule: Day*<br><br>Determines the day of the month schedule for rotating the audit log.<br><br>Valid values range from `1` through `31`. For example, you can specify that the audit log is to be rotated on the 10th and 20th days of a month, or all days of a month. | `-rotate-schedule-day`<br>`chron_dayofmonth` | No | | |

| | | | | |
|---|---|---|---|---|
| *Log rotation schedule: Hour*<br><br>Determines the hourly schedule for rotating the audit log.<br><br>Valid values range from `0` (midnight) to `23` (11:00 p.m.). Specifying `all` rotates the audit logs every hour. For example, you can specify that the audit log is to be rotated at 6 (6 a.m.) and 18 (6 p.m.). | `-rotate-schedule-hour chron_hour` | No | | |
| *Log rotation schedule: Minute*<br><br>Determines the minute schedule for rotating the audit log.<br><br>Valid values range from `0` to `59`. For example, you can specify that the audit log is to be rotated at the 30th minute. | `-rotate-schedule-minute chron_minute` | Yes, if configuring schedule-based log rotation; otherwise, no. | | |

**Rotate logs based on log size and schedule**

You can choose to rotate the log files based on log size and a schedule by setting both the `-rotate-size` parameter and the time-based rotation parameters in any combination. For example: if `-rotate-size` is set to 10 MB and `-rotate-schedule-minute` is set to 15, the log files rotate when the log file size reaches 10 MB or on the 15th minute of every hour (whichever event occurs first).

**Create a file and directory auditing configuration on SVMs**

**Create the auditing configuration**

Creating a file and directory auditing configuration on your storage virtual machine (SVM) includes understanding the available configuration options, planning the configuration, and then configuring and enabling the configuration. You can then display information about the auditing configuration to confirm that the resultant configuration is the desired configuration.

Before you can begin auditing file and directory events, you must create an auditing configuration on the storage virtual machine (SVM).

**Before you begin**

If you plan on creating an auditing configuration for central access policy staging, a SMB server must exist on the SVM.

- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled.

  Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.

- If the arguments of a field in a command is invalid, for example, invalid entries for fields, duplicate entries, and non-existent entries, then the command fails before the audit phase.

  Such failures do not generate an audit record.

### About this task

If the SVM is an SVM disaster recovery source, the destination path cannot be on the root volume.

### Step

1. Using the information in the planning worksheet, create the auditing configuration to rotate audit logs based on log size or a schedule:

| If you want to rotate audit logs by… | Enter… |
| --- | --- |
| Log size | `vserver audit create -vserver vserver_name -destination path -events [{file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-account|security-group|authorization-policy-change}] [-format {xml|evtx}] [-rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]` |
| A schedule | `vserver audit create -vserver vserver_name -destination path -events [{file-ops|cifs-logon-logoff|cap-staging}] [-format {xml|evtx}] [-rotate-limit integer] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-day chron_dayofmonth] [-rotate-schedule-hour chron_hour] -rotate-schedule-minute chron_minute`<br><br> The `-rotate-schedule-minute` parameter is required if you are configuring time-based audit log rotation. |

### Examples

The following example creates an auditing configuration that audits file operations and SMB logon and logoff events (the default) using size-based rotation. The log format is EVTX (the default). The logs are stored in the /audit_log directory. The log file size limit is 200 MB. The logs are rotated when they reach 200 MB in size:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

The following example creates an auditing configuration that audits file operations and SMB logon and logoff events (the default) using size-based rotation. The log format is `EVTX` (the default). The log file size limit is `100 MB` (the default), and the log rotation limit is `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-limit 5
```

The following example creates an auditing configuration that audits file operations, CIFS logon and logoff events, and central access policy staging events using time-based rotation. The log format is `EVTX` (the default). The audit logs are rotated monthly, at 12:30 p.m. on all days of the week. The log rotation limit is `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

**Enable auditing on the SVM**

After you finish setting up the auditing configuration, you must enable auditing on the storage virtual machine (SVM).

**What you'll need**

The SVM audit configuration must already exist.

**About this task**

When an SVM disaster recovery ID discard configuration is first started (after the SnapMirror initialization is complete) and the SVM has an auditing configuration, ONTAP automatically disables the auditing configuration. Auditing is disabled on the read-only SVM to prevent the staging volumes from filling up. You can enable auditing only after the SnapMirror relationship is broken and the SVM is read-write.

**Step**

1. Enable auditing on the SVM:

   ```
   vserver audit enable -vserver vserver_name
   ```

   ```
   vserver audit enable -vserver vs1
   ```

**Verify the auditing configuration**

After completing the auditing configuration, you should verify that auditing is configured properly and is enabled.

**Steps**

1. Verify the auditing configuration:

   ```
   vserver audit show -instance -vserver vserver_name
   ```

The following command displays in list form all auditing configuration information for storage virtual machine (SVM) vs1:

```
vserver audit show -instance -vserver vs1
```

```
                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
             Categories of Events to Audit: file-ops
                          Log Format: evtx
                  Log File Size Limit: 200MB
         Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                   Rotation Schedules: -
            Log Files Rotation Limit: 0
```

**Configure file and folder audit policies**

**Configure file and folder audit policies**

Implementing auditing on file and folder access events is a two-step process. First, you must create and enable an auditing configuration on storage virtual machines (SVMs). Second, you must configure audit policies on the files and folders that you want to monitor. You can configure audit policies to monitor both successful and failed access attempts.

You can configure both SMB and NFS audit policies. SMB and NFS audit policies have different configuration requirements and audit capabilities.

If the appropriate audit policies are configured, ONTAP monitors SMB and NFS access events as specified in the audit policies only if the SMB or NFS servers are running.

**Configure audit policies on NTFS security-style files and directories**

Before you can audit file and directory operations, you must configure audit policies on the files and directories for which you want to collect audit information. This is in addition to setting up and enabling the audit configuration. You can configure NTFS audit policies by using the Windows Security tab or by using the ONTAP CLI.

**Configuring NTFS audit policies using the Windows Security tab**

You can configure NTFS audit policies on files and directories by using the **Windows Security** tab in the Windows Properties window. This is the same method used when configuring audit policies on data residing on a Windows client, which enables you to use

the same GUI interface that you are accustomed to using.

**What you'll need**

Auditing must be configured on the storage virtual machine (SVM) that contains the data to which you are applying system access control lists (SACLs).

**About this task**

Configuring NTFS audit policies is done by adding entries to NTFS SACLs that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI. The security descriptor can contain discretionary access control lists (DACLs) for applying file and folder access permissions, SACLs for file and folder auditing, or both SACLs and DACLs.

To set NTFS audit policies using the Windows Security tab, complete the following steps on a Windows host:

**Steps**

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.

2. Complete the **Map Network Drive** box:

   a. Select a **Drive** letter.

   b. In the **Folder** box, type the SMB server name that contains the share, holding the data you want to audit and the name of the share.

      You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

      If your SMB server name is "SMB_SERVER" and your share is named "share1", you should enter `\\SMB_SERVER\share1`.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to enable auditing access.

4. Right-click the file or directory, and then select **Properties**.

5. Select the **Security** tab.

6. Click **Advanced**.

7. Select the **Auditing** tab.

8. Perform the desired actions:

| If you want to…. | Do the following |
|---|---|
| Set up auditing for a new user or group | a. Click **Add**.<br>b. In the Enter the object name to select box, type the name of the user or group that you want to add.<br>c. Click **OK**. |

| Remove auditing from a user or group | a. In the Enter the object name to select box, select the user or group that you want to remove. |
| --- | --- |
| | b. Click **Remove**. |
| | c. Click **OK**. |
| | d. Skip the rest of this procedure. |
| Change auditing for a user or group | a. In the Enter the object name to select box, select the user or group that you want to change. |
| | b. Click **Edit**. |
| | c. Click **OK**. |

If you are setting up auditing on a user or group or changing auditing on an existing user or group, the Auditing Entry for <object> box opens.

9. In the **Apply to** box, select how you want to apply this auditing entry.

   You can select one of the following:

   - **This folder, subfolders and files**
   - **This folder and subfolders**
   - **This folder only**
   - **This folder and files**
   - **Subfolders and files only**
   - **Subfolders only**
   - **Files only**
     If you are setting up auditing on a single file, the **Apply to** box is not active. The **Apply to** box setting defaults to **This object only**.

     > ⓘ  Because auditing takes SVM resources, select only the minimal level that provides the auditing events that meet your security requirements.

10. In the **Access** box, select what you want audited and whether you want to audit successful events, failure events, or both.

    - To audit successful events, select the Success box.
    - To audit failure events, select the Failure box.

    Select only the actions that you need to monitor to meet your security requirements. For more information about these auditable events, see your Windows documentation. You can audit the following events:

    - **Full control**
    - **Traverse folder / execute file**
    - **List folder / read data**
    - **Read attributes**
    - **Read extended attributes**

- Create files / write data
- Create folders / append data
- Write attributes
- Write extended attributes
- Delete subfolders and files
- Delete
- Read permissions
- Change permissions
- Take ownership

11. If you do not want the auditing setting to propagate to subsequent files and folders of the original container, select the **Apply these auditing entries to objects and/or containers within this container only** box.

12. Click **Apply**.

13. After you finish adding, removing, or editing auditing entries, click **OK**.

   The Auditing Entry for <object> box closes.

14. In the **Auditing** box, select the inheritance settings for this folder.

   Select only the minimal level that provides the auditing events that meet your security requirements. You can choose one of the following:

   - Select the Include inheritable auditing entries from this object's parent box.
   - Select the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box.
   - Select both boxes.
   - Select neither box.
     If you are setting SACLs on a single file, the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box is not present in the Auditing box.

15. Click **OK**.

   The Auditing box closes.

### Configure NTFS audit policies using the ONTAP CLI

You can configure audit policies on files and folders using the ONTAP CLI. This enables you to configure NTFS audit policies without needing to connect to the data using an SMB share on a Windows client.

You can configure NTFS audit policies by using the `vserver security file-directory` command family.

You can only configure NTFS SACLs using the CLI. Configuring NFSv4 SACLs is not supported with this ONTAP command family. See the man pages for more information about using these commands to configure and add NTFS SACLs to files and folders.

### Configure auditing for UNIX security style files and directories

You configure auditing for UNIX security style files and directories by adding audit ACEs

to NFSv4.x ACLs. This allows you to monitor certain NFS file and directory access events for security purposes.

**About this task**

For NFSv4.x, both discretionary and system ACEs are stored in the same ACL. They are not stored in separate DACLs and SACLs. Therefore, you must exercise caution when adding audit ACEs to an existing ACL to avoid overwriting and losing an existing ACL. The order in which you add the audit ACEs to an existing ACL does not matter.

**Steps**

1. Retrieve the existing ACL for the file or directory by using the `nfs4_getfacl` or equivalent command.

   For more information about manipulating ACLs, see the man pages of your NFS client.

2. Append the desired audit ACEs.

3. Apply the updated ACL to the file or directory by using the `nfs4_setfacl` or equivalent command.

**Display information about audit policies applied to files and directories**

### Display information about audit policies using the Windows Security tab

You can display information about audit policies that have been applied to files and directories by using the Security tab in the Windows Properties window. This is the same method used for data residing on a Windows server, which enables customers to use the same GUI interface that they are accustomed to using.

**About this task**

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

To display information about SACLs that have been applied to NTFS files and folders, complete the following steps on a Windows host.

**Steps**

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.

2. Complete the **Map Network Drive** dialog box:

   a. Select a **Drive** letter.

   b. In the **Folder** box, type the IP address or SMB server name of the storage virtual machine (SVM) containing the share that holds both the data you would like to audit and the name of the share.

      If your SMB server name is "SMB_SERVER" and your share is named "share1", you should enter `\\SMB_SERVER\share1`.

      > ⓘ  You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you display auditing information.

4. Right-click on the file or directory, and select **Properties**.

5. Select the **Security** tab.

6. Click **Advanced**.

7. Select the **Auditing** tab.

8. Click **Continue**.

   The Auditing box opens. The **Auditing entries** box displays a summary of users and groups that have SACLs applied to them.

9. In the **Auditing entries** box select the user or group whose SACL entries you want displayed.

10. Click **Edit**.

    The Auditing entry for <object> box opens.

11. In the **Access** box, view the current SACLs that are applied to the selected object.

12. Click **Cancel** to close the **Auditing entry for <object>** box.

13. Click **Cancel** to close the **Auditing** box.

**Display information about NTFS audit policies on FlexVol volumes using the CLI**

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the information to validate your security configuration or to troubleshoot auditing issues.

**About this task**

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

You must provide the name of the storage virtual machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

- NTFS security-style volumes and qtrees use only NTFS system access control lists (SACLs) for audit policies.

- Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.

  Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.

- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, the output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4 SACLs and Storage-Level Access Guard NTFS SACLs.

- If the path that is entered in the command is to data with NTFS effective security, the output also displays

information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

- When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information.

  NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.

- ACL output is displayed only for files and folders with NTFS or NFSv4 security.

  This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

**Step**

1. Display file and directory audit policy settings with the desired level of detail:

| If you want to display information… | Enter the following command… |
|---|---|
| In summary form | `vserver security file-directory show -vserver vserver_name -path path` |
| As a detailed list | `vserver security file-directory show -vserver vserver_name -path path -expand-mask true` |

**Examples**

The following example displays the audit policy information for the path `/corp` in SVM vs1. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                    Vserver: vs1
                  File Path: /corp
          File Inode Number: 357
             Security Style: ntfs
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
       Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
              Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8014
                             Owner:DOMAIN\Administrator
                             Group:BUILTIN\Administrators
                             SACL - ACEs
                                ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                                SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                             DACL - ACEs
                                ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                                ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                                ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                                ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

The following example displays the audit policy information for the path `/datavol1` in SVM vs1. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                  Vserver: vs1
                File Path: /datavol1
        File Inode Number: 77
           Security Style: ntfs
          Effective Style: ntfs
           DOS Attributes: 10
  DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
             Unix User Id: 0
            Unix Group Id: 0
           Unix Mode Bits: 777
  Unix Mode Bits in Text: rwxrwxrwx
                     ACLs: NTFS Security Descriptor
                           Control:0xaa14
                           Owner:BUILTIN\Administrators
                           Group:BUILTIN\Administrators
                           SACL - ACEs
                             AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                           DACL - ACEs
                             ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                             ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                           Storage-Level Access Guard security
                           SACL (Applies to Directories):
                             AUDIT-EXAMPLE\Domain Users-0x120089-FA
                             AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           DACL (Applies to Directories):
                             ALLOW-EXAMPLE\Domain Users-0x120089
                             ALLOW-EXAMPLE\engineering-0x1f01ff
                             ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                           SACL (Applies to Files):
                             AUDIT-EXAMPLE\Domain Users-0x120089-FA
                             AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           DACL (Applies to Files):
                             ALLOW-EXAMPLE\Domain Users-0x120089
                             ALLOW-EXAMPLE\engineering-0x1f01ff
                             ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

**Ways to display information about file security and audit policies**

You can use the wildcard character (*) to display information about file security and audit policies of all files and directories under a given path or a root volume.

The wildcard character (*) can be used as the last subcomponent of a given directory path below which you want to display information of all files and directories.

If you want to display information of a particular file or directory named as "*", then you need to provide the complete path inside double quotes (" ").

**Example**

The following command with the wildcard character displays the information about all files and directories below the path /1/ of SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                      Vserver: vs1
                    File Path: /1/1
               Security Style: mixed
              Effective Style: ntfs
               DOS Attributes: 10
       DOS Attributes in Text: ----D---
       Expanded Dos Attributes: -
                 Unix User Id: 0
                Unix Group Id: 0
               Unix Mode Bits: 777
       Unix Mode Bits in Text: rwxrwxrwx
                         ACLs: NTFS Security Descriptor
                               Control:0x8514
                               Owner:BUILTIN\Administrators
                               Group:BUILTIN\Administrators
                               DACL - ACEs
                               ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                      Vserver: vs1
                    File Path: /1/1/abc
               Security Style: mixed
              Effective Style: ntfs
               DOS Attributes: 10
       DOS Attributes in Text: ----D---
       Expanded Dos Attributes: -
                 Unix User Id: 0
                Unix Group Id: 0
               Unix Mode Bits: 777
       Unix Mode Bits in Text: rwxrwxrwx
                         ACLs: NTFS Security Descriptor
                               Control:0x8404
                               Owner:BUILTIN\Administrators
                               Group:BUILTIN\Administrators
                               DACL - ACEs
                               ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

The following command displays the information of a file named as "*" under the path `/vol1/a` of SVM vs1. The path is enclosed within double quotes (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 1002
          Unix Group Id: 65533
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                             AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                         DACL - ACEs
                             ALLOW-EVERYONE@-0x1f00a9-FI|DI
                             ALLOW-OWNER@-0x1f01ff-FI|DI
                             ALLOW-GROUP@-0x1200a9-IG
```

**CLI change events that can be audited**

**CLI change events that can be audited overview**

ONTAP can audit certain CLI change events, including certain SMB-share events, certain audit policy events, certain local security group events, local user group events, and authorization policy events. Understanding which change events can be audited is helpful when interpreting results from the event logs.

You can manage storage virtual machine (SVM) auditing CLI change events by manually rotating the audit logs, enabling or disabling auditing, displaying information about auditing change events, modifying auditing change events, and deleting auditing change events.

As an administrator, if you execute any command to change configuration related to the SMB-share, local user-group, local security-group, authorization-policy, and audit-policy events, a record generates and the corresponding event gets audited:

| Auditing Category | Events | Event IDs | Run this command… |
|---|---|---|---|

| Mhost Auditing | policy-change | [4719] Audit configuration changed | `vserver audit disable|enable|modify` |
| --- | --- | --- | --- |
| | file-share | [5142] Network share was added | `vserver cifs share create` |
| | | [5143] Network share was modified | `vserver cifs share modify` `vserver cifs share create|modify|delete` `vserver cifs share add|remove` |
| | | [5144] Network share deleted | `vserver cifs share delete` |

Auditing

140

| | | Rename | `and-groups local-user rename` |
|---|---|---|---|
| | security-group | [4731] Local Security Group created | `vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create` |
| | | [4734] Local Security Group deleted | `vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete` |
| | | [4735] Local Security Group Modified | `vserver cifs users-and-groups local-group rename|modify` `vserver services name-service unix-group modify` |
| | | [4732] User added to Local Group | `vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser` |
| | | [4733] User Removed from Local Group | `vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser` |
| | authorization-policy-change | [4704] User Rights Assigned | `vserver cifs users-and-groups privilege add-privilege` |
| | | [4705] User Rights Removed | `vserver cifs users-and-groups privilege remove-privilege|reset-privilege` |

**Manage file-share event**

When a file-share event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated. The file-share events are generated when the SMB network share is modified using `vserver cifs share` related commands.

The file-share events with the event-ids 5142, 5143, and 5144 are generated when a SMB network share is added, modified, or deleted for the SVM. The SMB network share configuration is modified using the `cifs share access control create|modify|delete` commands.

The following example displays a file-share event with the ID 5143 is generated, when a share object called 'audit_dest' is created:

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

**Manage audit-policy-change event**

When an audit-policy-change event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated. The audit-policy-change events are generated when an audit policy is modified using `vserver audit` related commands.

The audit-policy-change event with the event-id 4719 is generated whenever an audit policy is disabled, enabled, or modified and helps to identify when a user attempts to disable auditing to cover the tracks. It is configured by default and requires diagnostic privilege to disable.

The following example displays an audit-policy change event with the ID 4719 generated, when an audit is disabled:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

**Manage user-account event**

When a user-account event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The user-account events with event-ids 4720, 4722, 4724, 4725, 4726, 4738, and 4781 are generated when a local SMB or NFS user is created or deleted from the system, local user account is enabled, disabled or modified, and local SMB user password is reset or changed. The user-account events are generated when a user account is modified using `vserver cifs users-and-groups <local user>` and `vserver services name-service <unix user>` commands.

The following example displays a user account event with the ID 4720 generated, when a local SMB user is created:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

The following example displays a user account event with the ID 4781 generated, when the local SMB user created in the preceding example is renamed:

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

**Manage security-group event**

When a security-group event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The security-group events with event-ids 4731, 4732, 4733, 4734, and 4735 are generated when a local SMB or NFS group is created or deleted from the system, and local user is added or removed from the group. The security-group-events are generated when a user account is modified using `vserver cifs users-and-groups <local-group>` and `vserver services name-service <unix-group>` commands.

The following example displays a security group event with the ID 4731 generated, when a local UNIX security group is created:

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
    ...
    ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

**Manage authorization-policy-change event**

When authorization-policy-change event is configured for a storage virtual machine
(SVM) and an audit is enabled, audit events are generated.

The authorization-policy-change events with the event-ids 4704 and 4705 are generated whenever the
authorization rights are granted or revoked for an SMB user and SMB group. The authorization-policy-change
events are generated when the authorization rights are assigned or revoked using `vserver cifs users-and-groups privilege` related commands.

The following example displays an authorization policy event with the ID 4704 generated, when the
authorization rights for a SMB user group are assigned:

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

**Manage auditing configurations**

**Manually rotate the audit event logs**

Before you can view the audit event logs, the logs must be converted to user-readable formats. If you want to view the event logs for a specific storage virtual machine (SVM) before ONTAP automatically rotates the log, you can manually rotate the audit event logs on an SVM.

**Step**

1. Rotate the audit event logs by using the `vserver audit rotate-log` command.

   `vserver audit rotate-log -vserver vs1`

   The audit event log is saved in the SVM audit event log directory with the format specified by the auditing configuration (`XML` or `EVTX`), and can be viewed by using the appropriate application.

**Enable and disable auditing on SVMs**

You can enable or disable auditing on storage virtual machines (SVMs). You might want to temporarily stop file and directory auditing by disabling auditing. You can enable auditing at any time (if an auditing configuration exists).

**What you'll need**

Before you can enable auditing on the SVM, the SVM's auditing configuration must already exist.

**About this task**

Disabling auditing does not delete the auditing configuration.

**Steps**

1. Perform the appropriate command:

| If you want auditing to be… | Enter the command… |
|---|---|
| Enabled | `vserver audit enable -vserver vserver_name` |
| Disabled | `vserver audit disable -vserver vserver_name` |

2. Verify that auditing is in the desired state:

```
vserver audit show -vserver vserver_name
```

**Examples**

The following example enables auditing for SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                            Vserver: vs1
                    Auditing state: true
              Log Destination Path: /audit_log
        Categories of Events to Audit: file-ops, cifs-logon-logoff
                        Log Format: evtx
                Log File Size Limit: 100MB
          Log Rotation Schedule: Month: -
 Log Rotation Schedule: Day of Week: -
            Log Rotation Schedule: Day: -
           Log Rotation Schedule: Hour: -
         Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

The following example disables auditing for SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1

                                 Vserver: vs1
                          Auditing state: false
                     Log Destination Path: /audit_log
             Categories of Events to Audit: file-ops, cifs-logon-logoff
                              Log Format: evtx
                       Log File Size Limit: 100MB
          Log Rotation Schedule: Month: -
    Log Rotation Schedule: Day of Week: -
            Log Rotation Schedule: Day: -
           Log Rotation Schedule: Hour: -
         Log Rotation Schedule: Minute: -
                       Rotation Schedules: -
              Log Files Rotation Limit: 10
```

**Display information about auditing configurations**

You can display information about auditing configurations. The information can help you determine whether the configuration is what you want in place for each SVM. The displayed information also enables you to verify whether an auditing configuration is enabled.

**About this task**

You can display detailed information about auditing configurations on all SVMs or you can customize what information is displayed in the output by specifying optional parameters. If you do not specify any of the optional parameters, the following is displayed:

- SVM name to which the auditing configuration applies
- The audit state, which can be `true` or `false`

  If the audit state is `true`, auditing is enabled. If the audit state is `false`, auditing is disabled.

- The categories of events to audit
- The audit log format
- The target directory where the auditing subsystem stores consolidated and converted audit logs

**Step**

1. Display information about the auditing configuration by using the `vserver audit show` command.

   For more information about using the command, see the man pages.

**Examples**

The following example displays a summary of the auditing configuration for all SVMs:

```
cluster1::> vserver audit show

 Vserver      State  Event Types Log Format Target Directory
 -----------  ------ ----------- ---------- --------------------
 vs1          false  file-ops    evtx       /audit_log
```

The following example displays, in list form, all auditing configuration information for all SVMs:

```
cluster1::> vserver audit show -instance

                           Vserver: vs1
                    Auditing state: true
              Log Destination Path: /audit_log
        Categories of Events to Audit: file-ops
                        Log Format: evtx
                Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                Rotation Schedules: -
           Log Files Rotation Limit: 0
```

**Commands for modifying auditing configurations**

If you want to change an auditing setting, you can modify the current configuration at any time, including modifying the log path destination and log format, modifying the categories of events to audit, how to automatically save log files, and specify the maximum number of log files to save.

| If you want to… | Use this command… |
|---|---|
| Modify the log destination path | `vserver audit modify` with the `-destination` parameter |
| Modify the category of events to audit | `vserver audit modify` with the `-events` parameter<br><br>ⓘ To audit central access policy staging events, the Dynamic Access Control (DAC) SMB server option must be enabled on the storage virtual machine (SVM). |

| Modify the log format | `vserver audit modify` with the `-format` parameter |
| --- | --- |
| Enabling automatic saves based on internal log file size | `vserver audit modify` with the `-rotate-size` parameter |
| Enabling automatic saves based on a time interval | `vserver audit modify` with the `-rotate-schedule-month`, `-rotate-schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour`, and `-rotate-schedule-minute` parameters |
| Specifying the maximum number of saved log files | `vserver audit modify` with the `-rotate-limit` parameter |

**Delete an auditing configuration**

In you no longer want to audit file and directory events on the storage virtual machine (SVM) and do not want to maintain an auditing configuration on the SVM, you can delete the auditing configuration.

**Steps**

1. Disable the auditing configuration:

   `vserver audit disable -vserver vserver_name`

   `vserver audit disable -vserver vs1`

2. Delete the auditing configuration:

   `vserver audit delete -vserver vserver_name`

   `vserver audit delete -vserver vs1`

**What the process is when reverting**

If you plan to revert the cluster, you should be aware of the revert process ONTAP follows when there are auditing-enabled storage virtual machines (SVMs) in the cluster. You must take certain actions before reverting.

**Reverting to a version of ONTAP that does not support the auditing of SMB logon and logoff events and central access policy staging events**

Support for auditing of SMB logon and logoff events and for central access policy staging events starts with clustered Data ONTAP 8.3. If you are reverting to a version of ONTAP that does not support these event types and you have auditing configurations that monitor these event types, you must change the auditing configuration for those audit-enabled SVMs before reverting. You must modify the configuration so that only file-op events are audited.

## Troubleshoot auditing and staging volume space issues

Issues can arise when there is insufficient space on either the staging volumes or on the volume containing the audit event logs. If there is insufficient space, new audit records cannot be created, which prevents clients from accessing data, and access requests fail. You should know how to troubleshoot and resolve these volume space issues.

### Troubleshoot space issues related to the event log volumes

If volumes containing event log files run out of space, auditing cannot convert log records into log files. This results in client access failures. You must know how to troubleshoot space issues related to event log volumes.

- storage virtual machine (SVM) and cluster administrators can determine whether there is insufficient volume space by displaying information about volume and aggregate usage and configuration.
- If there is insufficient space in the volumes containing event logs, SVM and cluster administrators can resolve the space issues by either removing some of the event log files or by increasing the size of the volume.

> **ⓘ** If the aggregate that contains the event log volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only a cluster administrator can increase the size of an aggregate.

- The destination path for the event log files can be changed to a directory on another volume by modifying the auditing configuration.

> **ⓘ** Data access is denied in the following cases:
>
> - If the destination directory is deleted.
> - If the file limit on a volume, which hosts the destination directory, reaches to its maximum level.

Learn more about:

- How to view information about volumes and increasing volume size.
- How to view information about aggregates and managing aggregates.

### Troubleshoot space issues related to the staging volumes

If any of the volumes containing staging files for your storage virtual machine (SVM) runs out of space, auditing cannot write log records into staging files. This results in client access failures. To troubleshoot this issue, you need to determine whether any of the staging volumes used in the SVM are full by displaying information about volume usage.

If the volume containing the consolidated event log files has sufficient space but there are still client access failures due to insufficient space, then the staging volumes might be out of space. The SVM administrator must contact you to determine whether the staging volumes that contain staging files for the SVM have insufficient space. The auditing subsystem generates an EMS event if auditing events cannot be generated due to insufficient space in a staging volume. The following message is displayed: `No space left on device`. Only you can view information about staging volumes; SVM administrators cannot.

All staging volume names begin with `MDV_aud_` followed by the UUID of the aggregate containing that staging

volume. The following example shows four system volumes on the admin SVM, which were automatically
created when a file services auditing configuration was created for a data SVM in the cluster:

```
cluster1::> volume show -vserver cluster1
Vserver    Volume         Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                         aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                         root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                         aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                         aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

If there is insufficient space in the staging volumes, you can resolve the space issues by increasing the size of
the volume.

> ⓘ If the aggregate that contains the staging volume is full, then the size of the aggregate must be
> increased before you can increase the size of the volume. Only you can increase the size of an
> aggregate; SVM administrators cannot.

If one or more aggregates have an available space of less than 2 GB, the SVM audit creation fails. When the
SVM audit creation fails, the staging volumes that were created are deleted.

## Use FPolicy for file monitoring and management on SVMs

### How FPolicy works

**What the two parts of the FPolicy solution are**

FPolicy is a file access notification framework that is used to monitor and manage file
access events on storage virtual machines (SVMs).

There are two parts to an FPolicy solution. The ONTAP FPolicy framework manages activities on the cluster
and sends notifications to external FPolicy servers. External FPolicy servers process notifications sent by
ONTAP FPolicy.

The ONTAP framework creates and maintains the FPolicy configuration, monitors file events, and sends
notifications to external FPolicy servers. ONTAP FPolicy provides the infrastructure that allows communication
between external FPolicy servers and storage virtual machine (SVM) nodes.

The FPolicy framework connects to external FPolicy servers and sends notifications for certain file system events to the FPolicy servers when these events occur as a result of client access. The external FPolicy servers process the notifications and send responses back to the node. What happens as a result of the notification processing depends on the application and whether the communication between the node and the external servers is asynchronous or synchronous.

**What synchronous and asynchronous notifications are**

FPolicy sends notifications to external FPolicy servers via the FPolicy interface. The notifications are sent either in synchronous or asynchronous mode. The notification mode determines what ONTAP does after sending notifications to FPolicy servers.

- **Asynchronous notifications**

  With asynchronous notifications, the node does not wait for a response from the FPolicy server, which enhances overall throughput of the system. This type of notification is suitable for applications where the FPolicy server does not require that any action be taken as a result of notification evaluation. For example, asynchronous notifications are used when the storage virtual machine (SVM) administrator wants to monitor and audit file access activity.

  If an FPolicy server operating in asynchronous mode experiences a network outage, FPolicy notifications generated during the outage are stored on the storage node. When the FPolicy server comes back online, it is alerted of the stored notifications and can fetch them from the storage node. The length of time the notifications can be stored during an outage is configurable up to 10 minutes.

- **Synchronous notifications**

  When configured to run in synchronous mode, the FPolicy server must acknowledge every notification before the client operation is allowed to continue. This type of notification is used when an action is required based on the results of notification evaluation. For example, synchronous notifications are used when the SVM administrator wants to either allow or deny requests based on criteria specified on the external FPolicy server.

**Synchronous and asynchronous applications**

There are many possible uses for FPolicy applications, both asynchronous and synchronous.

Asynchronous applications are ones where the external FPolicy server does not alter access to files or directories or modify data on the storage virtual machine (SVM). For example:

- File access and audit logging
- Storage resource management

Synchronous applications are ones where data access is altered or data is modified by the external FPolicy server. For example:

- Quota management
- File access blocking
- File archiving and hierarchical storage management
- Encryption and decryption services
- Compression and decompression services

You can use the SDK for FPolicy to identify and implement other applications as well.

**Roles that cluster components play with FPolicy implementation**

The cluster, the contained storage virtual machines (SVMs), and data LIFs all play a role in an FPolicy implementation.

- **cluster**

  The cluster contains the FPolicy management framework and maintains and manages information about all FPolicy configurations in the cluster.

- **SVM**

  An FPolicy configuration is defined at the SVM level. The scope of the configuration is the SVM, and it only operates on SVM resources. One SVM configuration cannot monitor and send notifications for file access requests that are made for data residing on another SVM.

  FPolicy configurations can be defined on the admin SVM. After configurations are defined on the admin SVM, they can be seen and used in all SVMs.

- **data LIFs**

  Connections to the FPolicy servers are made through data LIFs belonging to the SVM with the FPolicy configuration. The data LIFs used for these connections can fail over in the same manner as data LIFs used for normal client access.

**How FPolicy works with external FPolicy servers**

**How FPolicy works with external FPolicy servers overview**

After FPolicy is configured and enabled on the storage virtual machine (SVM), FPolicy runs on every node on which the SVM participates. FPolicy is responsible for establishing and maintaining connections with external FPolicy servers (FPolicy servers), for notification processing, and for managing notification messages to and from FPolicy servers.

Additionally, as part of connection management, FPolicy has the following responsibilities:

- Ensures that file notification flows through the correct LIF to the FPolicy server.
- Ensures that when multiple FPolicy servers are associated with a policy, load balancing is done when sending notifications to the FPolicy servers.
- Attempts to reestablish the connection when a connection to an FPolicy server is broken.
- Sends the notifications to FPolicy servers over an authenticated session.
- Manages the passthrough-read data connection established by the FPolicy server for servicing client requests when passthrough-read is enabled.

**How control channels are used for FPolicy communication**

FPolicy initiates a control channel connection to an external FPolicy server from the data LIFs of each node participating on a storage virtual machine (SVM). FPolicy uses control

channels for transmitting file notifications; therefore, an FPolicy server might see multiple control channel connections based on SVM topology.

**How privileged data access channels are used for synchronous communication**

With synchronous use cases, the FPolicy server accesses data residing on the storage virtual machine (SVM) through a privileged data access path. Access through the privileged path exposes the complete file system to the FPolicy server. It can access data files to collect information, to scan files, read files, or write into files.

Because the external FPolicy server can access the entire file system from the root of the SVM through the privileged data channel, the privileged data channel connection must be secure.

**How FPolicy connection credentials are used with privileged data access channels**

The FPolicy server makes privileged data access connections to cluster nodes by using a specific Windows user credential that is saved with the FPolicy configuration. SMB is the only supported protocol for making a privileged data access channel connection.

If the FPolicy server requires privileged data access, the following conditions must be met:

- A SMB license must be enabled on the cluster.
- The FPolicy server must run under the credentials configured in the FPolicy configuration.

When making a data channel connection, FPolicy uses the credential for the specified Windows user name. Data access is made over the admin share ONTAP_ADMIN$.

**What granting super user credentials for privileged data access means**

ONTAP uses the combination of the IP address and the user credential configured in the FPolicy configuration to grant super user credentials to the FPolicy server.

Super user status grants the following privileges when the FPolicy server accesses data:

- Avoid permission checks

  The user avoids checks on files and directory access.

- Special locking privileges

  ONTAP allows read, write, or modify access to any file regardless of existing locks. If the FPolicy server takes byte range locks on the file, it results in immediate removal of existing locks on the file.

- Bypass any FPolicy checks

  Access does not generate any FPolicy notifications.

**How FPolicy manages policy processing**

There might be multiple FPolicy policies assigned to your storage virtual machine (SVM); each with a different priority. To create an appropriate FPolicy configuration on the SVM, it

is important to understand how FPolicy manages policy processing.

Each file access request is initially evaluated to determine which policies are monitoring this event. If it is a monitored event, information about the monitored event along with interested policies is passed to FPolicy where it is evaluated. Each policy is evaluated in order of the assigned priority.

You should consider the following recommendations when configuring policies:

- When you want a policy to always be evaluated before other policies, configure that policy with a higher priority.

- If the success of requested file access operation on a monitored event is a prerequisite for a file request that is evaluated against another policy, give the policy that controls the success or failure of the first file operation a higher priority.

  For example, if one policy manages FPolicy file archiving and restore functionality and a second policy manages file access operations on the online file, the policy that manages file restoration must have a higher priority so that the file is restored before the operation managed by the second policy can be allowed.

- If you want all policies that might apply to a file access operation to be evaluated, give synchronous policies a lower priority.

You can reorder policy priorities for existing policies by modifying the policy sequence number. However, to have FPolicy evaluate policies based on the modified priority order, you must disable and reenable the policy with the modified sequence number.

**What the node-to-external FPolicy server communication process is**

To properly plan your FPolicy configuration, you should understand what the node-to-external FPolicy server communication process is.

Every node that participates on each storage virtual machine (SVM) initiates a connection to an external FPolicy server (FPolicy server) using TCP/IP. Connections to the FPolicy servers are set up using node data LIFs; therefore, a participating node can set up a connection only if the node has an operational data LIF for the SVM.

Each FPolicy process on participating nodes attempts to establish a connection with the FPolicy server when the policy is enabled. It uses the IP address and port of the FPolicy external engine specified in the policy configuration.

The connection establishes a control channel from each of the nodes participating on each SVM to the FPolicy server through the data LIF. In addition, if IPv4 and IPv6 data LIF addresses are present on the same participating node, FPolicy attempts to establish connections for both IPv4 and IPv6. Therefore, in a scenario where the SVM extends over multiple nodes or if both IPv4 and IPv6 addresses are present, the FPolicy server must be ready for multiple control channel setup requests from the cluster after the FPolicy policy is enabled on the SVM.

For example, if a cluster has three nodes—Node1, Node2, and Node3—and SVM data LIFs are spread across only Node2 and Node3, control channels are initiated only from Node2 and Node3, irrespective of the distribution of data volumes. Say that Node2 has two data LIFs—LIF1 and LIF2—that belong to the SVM and that the initial connection is from LIF1. If LIF1 fails, FPolicy attempts to establish a control channel from LIF2.

Node without SVM data LIF

Nodes with SVM data LIFs
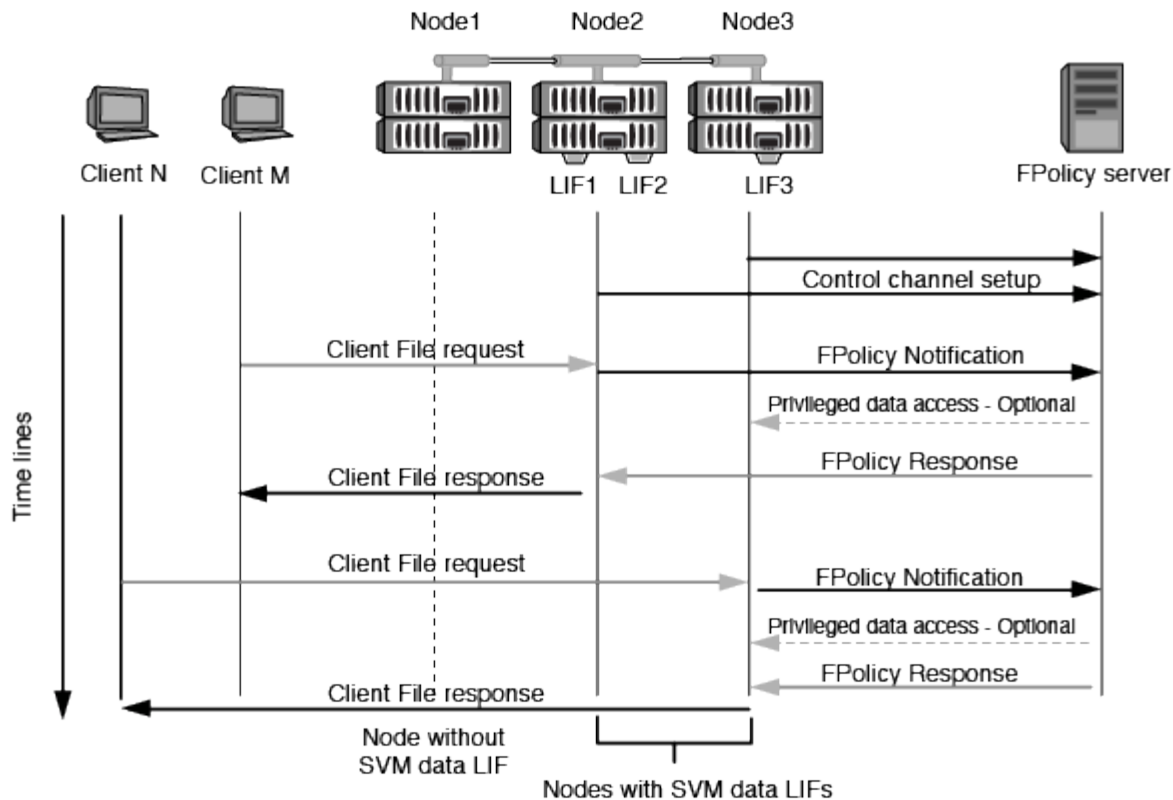
## How FPolicy manages external communication during LIF migration or failover

Data LIFs can be migrated to data ports in the same node or to data ports on a remote node.

When a data LIF fails over or is migrated, a new control channel connection is made to the FPolicy server. FPolicy can then retry SMB and NFS client requests that timed out, with the result that new notifications are sent to the external FPolicy servers. The node rejects FPolicy server responses to original, timed-out SMB and NFS requests.

## How FPolicy manages external communication during node failover

If the cluster node that hosts the data ports used for FPolicy communication fails, ONTAP breaks the connection between the FPolicy server and the node.

The impact of cluster failover to the FPolicy server can be mitigated by configuring the LIF manager to migrate the data port used in FPolicy communication to another active node. After the migration is complete, a new connection is established using the new data port.

If the LIF manager is not configured to migrate the data port, the FPolicy server must wait for the failed node to come up. After the node is up, a new connection is initiated from that node with a new Session ID.

> The FPolicy server detects broken connections with the keep-alive protocol message. The timeout for purging the session ID is determined when configuring FPolicy. The default keep-alive timeout is two minutes.

### How FPolicy services work across SVM namespaces

ONTAP provides a unified storage virtual machine (SVM) namespace. Volumes across the cluster are joined together by junctions to provide a single, logical file system. The

FPolicy server is aware of the namespace topology and provides FPolicy services across the namespace.

The namespace is specific to and contained within the SVM; therefore, you can see the namespace only from the SVM context. Namespaces have the following characteristics:

- A single namespace exists in each SVM, with the root of the namespace being the root volume, represented in the namespace as slash (/).

- All other volumes have junction points below the root (/).

- Volume junctions are transparent to clients.

- A single NFS export can provide access to the complete namespace; otherwise, export policies can export specific volumes.

- SMB shares can be created on the volume or on qtrees within the volume, or on any directory within the namespace.

- The namespace architecture is flexible.

  Examples of typical namespace architectures are as follows:

    ◦ A namespace with a single branch off of the root

    ◦ A namespace with multiple branches off of the root

    ◦ A namespace with multiple unbranched volumes off of the root

**FPolicy configuration types**

There are two basic FPolicy configuration types. One configuration uses external FPolicy servers to process and act upon notifications. The other configuration does not use external FPolicy servers; instead, it uses the ONTAP internal, native FPolicy server for simple file blocking based on extensions.

- **External FPolicy server configuration**

  The notification is sent to the FPolicy server, which screens the request and applies rules to determine whether the node should allow the requested file operation. For synchronous policies, the FPolicy server then sends a response to the node to either allow or block the requested file operation.

- **Native FPolicy server configuration**

  The notification is screened internally. The request is allowed or denied based on file extension settings configured in the FPolicy scope.

  **Note**: File extension requests that are denied are not logged.

**When to create a native FPolicy configuration**

Native FPolicy configurations use the ONTAP internal FPolicy engine to monitor and block file operations based on the file's extension. This solution does not require external FPolicy servers (FPolicy servers). Using a native file blocking configuration is appropriate when this simple solution is all that is needed.

Native file blocking enables you to monitor any file operations that match configured operation and filtering events and then deny access to files with particular extensions. This is the default configuration.

This configuration provides a means to block file access based only on the file's extension. For example, to block files that contain `mp3` extensions, you configure a policy to provide notifications for certain operations with target file extensions of `mp3`. The policy is configured to deny `mp3` file requests for operations that generate notifications.

The following applies to native FPolicy configurations:

- The same set of filters and protocols that are supported by FPolicy server-based file screening are also supported for native file blocking.

- Native file blocking and FPolicy server-based file screening applications can be configured at the same time.

  To do so, you can configure two separate FPolicy policies for the storage virtual machine (SVM), with one configured for native file blocking and one configured for FPolicy server-based file screening.

- The native file blocking feature only screens files based on the extensions and not on the content of the file.

- In the case of symbolic links, native file blocking uses the file extension of the root file.

Learn more about FPolicy: Native File Blocking.

**When to create a configuration that uses external FPolicy servers**

FPolicy configurations that use external FPolicy servers to process and manage notifications provide robust solutions for use cases where more than simple file blocking based on file extension is needed.

You should create a configuration that uses external FPolicy servers when you want to do such things as monitor and record file access events, provide quota services, perform file blocking based on criteria other than simple file extensions, provide data migration services using hierarchical storage management applications, or provide a fine-grained set of policies that monitor only a subset of data in the storage virtual machine (SVM).

**How FPolicy passthrough-read enhances usability for hierarchical storage management**

Passthrough-read enables the FPolicy server (functioning as the hierarchical storage management (HSM) server) to provide read access to offline files without having to recall the file from the secondary storage system to the primary storage system.

When an FPolicy server is configured to provide HSM to files residing on a SMB server, policy-based file migration occurs where the files are stored offline on secondary storage and only a stub file remains on primary storage. Even though a stub file appears as a normal file to clients, it is actually a sparse file that is the same size of the original file. The sparse file has the SMB offline bit set and points to the actual file that has been migrated to secondary storage.

Typically when a read request for an offline file is received, the requested content must be recalled back to primary storage and then accessed through primary storage. The need to recall data back to primary storage has several undesirable effects. Among the undesirable effects is the increased latency to client requests caused by the need to recall the content before responding to the request and the increased space consumption needed for recalled files on the primary storage.

FPolicy passthrough-read allows the HSM server (the FPolicy server) to provide read access to migrated, offline files without having to recall the file from the secondary storage system to the primary storage system. Instead of recalling the files back to primary storage, read requests can be serviced directly from secondary storage.

( i ) Copy Offload (ODX) is not supported with FPolicy passthrough-read operation.

Passthrough-read enhances usability by providing the following benefits:

- Read requests can be serviced even if the primary storage does not have sufficient space to recall requested data back to primary storage.

- Better capacity and performance management when a surge of data recall might occur, such as if a script or a backup solution needs to access many offline files.

- Read requests for offline files in Snapshot copies can be serviced.

  Because Snapshot copies are read-only, the FPolicy server cannot restore the original file if the stub file is located in a Snapshot copy. Using passthrough-read eliminates this problem.

- Policies can be set up that control when read requests are serviced through access to the file on secondary storage and when the offline file should be recalled to primary storage.

  For example, a policy can be created on the HSM server that specifies the number of times the offline file can be accessed in a specified period of time before the file is migrated back to primary storage. This type of policy avoids recalling files that are rarely accessed.

**How read requests are managed when FPolicy passthrough-read is enabled**

You should understand how read requests are managed when FPolicy passthrough-read is enabled so that you can optimally configure connectivity between the storage virtual machine (SVM) and the FPolicy servers.

When FPolicy passthrough-read is enabled and the SVM receives a request for an offline file, FPolicy sends a notification to the FPolicy server (HSM server) through the standard connection channel.

After receiving the notification, the FPolicy server reads the data from the file path sent in the notification and sends the requested data to the SVM through the passthrough-read privileged data connection that is established between the SVM and the FPolicy server.

After the data is sent, the FPolicy server then responds to the read request as an ALLOW or DENY. Based on whether the read request is allowed or denied, ONTAP either sends the requested information or sends an error message to the client.

**Requirements, considerations, and best practices for configuring FPolicy**

Before you create and configure FPolicy configurations on your SVMs, you need to be aware of certain requirements, considerations, and best practices for configuring FPolicy.

FPolicy features are configured either through the command line interface (CLI) or through APIs.

**Requirements for setting up FPolicy**

Before you configure and enable FPolicy on your storage virtual machine (SVM), you need to be aware of certain requirements.

- All nodes in the cluster must be running a version of ONTAP that supports FPolicy.

- If you are not using the ONTAP native FPolicy engine, you must have external FPolicy servers (FPolicy servers) installed.

- The FPolicy servers must be installed on a server accessible from the data LIFs of the SVM where FPolicy

policies are enabled.

> ℹ️ Beginning with ONTAP 9.8, ONTAP provides a client LIF service for outbound FPolicy connections with the addition of the `data-fpolicy-client` service. Learn more about LIFs and service policies.

- The IP address of the FPolicy server must be configured as a primary or secondary server in the FPolicy policy external engine configuration.

- If the FPolicy servers access data over a privileged data channel, the following additional requirements must be met:

  - SMB must be licensed on the cluster.

    Privileged data access is accomplished using SMB connections.

  - A user credential must be configured for accessing files over the privileged data channel.

  - The FPolicy server must run under the credentials configured in the FPolicy configuration.

  - All data LIFs used to communicate with the FPolicy servers must be configured to have `cifs` as one of the allowed protocols.

    This includes the LIFs used for passthrough-read connections.

**Best practices and recommendations when setting up FPolicy**

When setting up FPolicy on storage virtual machines (SVMs), you need to be familiar with configuration best practices and recommendations to ensure that your FPolicy configuration provides robust monitoring performance and results that meet your requirements.

- External FPolicy servers (FPolicy servers) should be placed in close proximity to the cluster with high-bandwidth connectivity to provide minimal latency and high-bandwidth connectivity.

- The FPolicy external engine should be configured with more than one FPolicy server to provide resiliency and high availability of FPolicy server notification processing, especially if policies are configured for synchronous screening.

- It is recommended that you disable the FPolicy policy before making any configuration changes.

  For example, if you want to add or modify an IP address in the FPolicy external engine configured for the enabled policy, you should first disable the policy.

- The cluster node-to-FPolicy server ratio should be optimized to ensure that FPolicy servers are not overloaded, which can introduce latencies when the SVM responds to client requests.

  The optimal ratio depends on the application for which the FPolicy server is being used.

**Passthrough-read upgrade and revert considerations**

There are certain upgrade and revert considerations that you must know about before upgrading to an ONTAP release that supports passthrough-read or before reverting to a release that does not support passthrough-read.

**Upgrading**

After all nodes are upgraded to a version of ONTAP that supports FPolicy passthrough-read, the cluster is capable of using the passthrough-read functionality; however, passthrough-read is disabled by default on existing FPolicy configurations. To use passthrough-read on existing FPolicy configurations, you must disable the FPolicy policy and modify the configuration, and then reenable the configuration.

**Reverting**

Before reverting to a version of ONTAP that does not support FPolicy passthrough-read, the following conditions must be met:

- All the policies using passthrough-read must be disabled, and then the affected configurations must be modified so that they do not use passthrough-read.
- FPolicy functionality must be disabled on the cluster by disabling every FPolicy policy on the cluster.

**What the steps for setting up an FPolicy configuration are**

Before FPolicy can monitor file access, an FPolicy configuration must be created and enabled on the storage virtual machine (SVM) for which FPolicy services are required.

The steps for setting up and enabling an FPolicy configuration on the SVM are as follows:

1. Create an FPolicy external engine.

   The FPolicy external engine identifies the external FPolicy servers (FPolicy servers) that are associated with a specific FPolicy configuration. If the internal "native" FPolicy engine is used to create a native file-blocking configuration, you do not need to create an FPolicy external engine.

2. Create an FPolicy event.

   An FPolicy event describes what the FPolicy policy should monitor. Events consist of the protocols and file operations to monitor, and can contain a list of filters. Events use filters to narrow the list of monitored events for which the FPolicy external engine must send notifications. Events also specify whether the policy monitors volume operations.

3. Create an FPolicy policy.

   The FPolicy policy is responsible for associating, with the appropriate scope, the set of events that need to be monitored and for which of the monitored events notifications must be sent to the designated FPolicy server (or to the native engine if no FPolicy servers are configured). The policy also defines whether the FPolicy server is allowed privileged access to the data for which it receives notifications. An FPolicy server needs privileged access if the server needs to access the data. Typical use cases where privileged access is needed include file blocking, quota management, and hierarchical storage management. The policy is where you specify whether the configuration for this policy uses an FPolicy server or the internal "native" FPolicy server.

   A policy specifies whether screening is mandatory. If screening is mandatory and all FPolicy servers are down or no response is received from the FPolicy servers within a defined timeout period, then file access is denied.

   A policy's boundaries are the SVM. A policy cannot apply to more than one SVM. However, a specific SVM can have multiple FPolicy policies, each with the same or different combination of scope, event, and external server configurations.

4. Configure the policy scope.

   The FPolicy scope determines which volumes, shares, or export-policies the policy acts on or excludes from monitoring. A scope also determines which file extensions should be included or excluded from FPolicy monitoring.

   > ℹ️  Exclude lists take precedence over include lists.

5. Enable the FPolicy policy.

   When the policy is enabled, the control channels and, optionally, the privileged data channels are connected. The FPolicy process on the nodes on which the SVM participates begin monitoring file and folder access and, for events that match configured criteria, sends notifications to the FPolicy servers (or to the native engine if no FPolicy servers are configured).

   > ℹ️  If the policy uses native file blocking, an external engine is not configured or associated with the policy.

**Plan the FPolicy configuration**

**Plan the FPolicy external engine configuration**

Before you configure the FPolicy external engine (external engine), you must understand what it means to create an external engine and which configuration parameters are available. This information helps you to determine which values to set for each parameter.

**Information that is defined when creating the FPolicy external engine**

The external engine configuration defines the information that FPolicy needs to make and manage connections to the external FPolicy servers (FPolicy servers), including the following information:

- SVM name
- Engine name
- The IP addresses of the primary and secondary FPolicy servers and the TCP port number to use when making the connection to the FPolicy servers
- Whether the engine type is asynchronous or synchronous
- How to authenticate the connection between the node and the FPolicy server

  If you choose to configure mutual SSL authentication, then you must also configure parameters that provide SSL certificate information.

- How to manage the connection using various advanced privilege settings

  This includes parameters that define such things as timeout values, retry values, keep-alive values, maximum request values, sent and receive buffer size values, and session timeout values.

The `vserver fpolicy policy external-engine create` command is used to create an FPolicy external engine.

**What the basic external engine parameters are**

You can use the following table of basic FPolicy configuration parameters to help you plan your configuration:

| Type of information | Option |
|---|---|
| *SVM*<br><br>Specifies the SVM name that you want to associate with this external engine.<br><br>Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM. | `-vserver vserver_name` |
| *Engine name*<br><br>Specifies the name to assign to the external engine configuration. You must specify the external engine name later when you create the FPolicy policy. This associates the external engine with the policy.<br><br>The name can be up to 256 characters long.<br><br>(i) The name should be up to 200 characters long if configuring the external engine name in a MetroCluster or SVM disaster recovery configuration.<br><br>The name can contain any combination of the following ASCII-range characters:<br><br>• `a` through `z`<br>• `A` through `Z`<br>• `0` through `9`<br>• "_", "-", and "." | `-engine-name engine_name` |

| | |
|---|---|
| *Primary FPolicy servers*<br><br>Specifies the primary FPolicy servers to which the node sends notifications for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses.<br><br>If more than one primary server IP address is specified, every node on which the SVM participates creates a control connection to every specified primary FPolicy server at the time the policy is enabled. If you configure multiple primary FPolicy servers, notifications are sent to the FPolicy servers in a round-robin fashion.<br><br>If the external engine is used in a MetroCluster or SVM disaster recovery configuration, you should specify the IP addresses of the FPolicy servers at the source site as primary servers. The IP addresses of the FPolicy servers at the destination site should be specified as secondary servers. | `-primary-servers IP_address,...` |
| *Port number*<br><br>Specifies the port number of the FPolicy service. | `-port integer` |
| *Secondary FPolicy servers*<br><br>Specifies the secondary FPolicy servers to which to send file access events for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses.<br><br>Secondary servers are used only when none of the primary servers are reachable. Connections to secondary servers are established when the policy is enabled, but notifications are sent to secondary servers only if none of the primary servers are reachable. If you configure multiple secondary servers, notifications are sent to the FPolicy servers in a round-robin fashion. | `-secondary-servers IP_address,...` |
| *External engine type*<br><br>Specifies whether the external engine operates in synchronous or asynchronous mode. By default, FPolicy operates in synchronous mode.<br><br>When set to `synchronous`, file request processing sends a notification to the FPolicy server, but then does not continue until after receiving a response from the FPolicy server. At that point, request flow either continues or processing results in denial, depending on whether the response from the FPolicy server permits the requested action.<br><br>When set to `asynchronous`, file request processing sends a notification to the FPolicy server, and then continues. | `-extern-engine-type external_engine_type` The value for this parameter can be one of the following:<br><br>• `synchronous`<br><br>• `asynchronous` |

| | |
|---|---|
| *SSL option for communication with FPolicy server*<br><br>Specifies the SSL option for communication with the FPolicy server. This is a required parameter. You can choose one of the options based on the following information:<br><br>• When set to `no-auth`, no authentication takes place.<br><br>   The communication link is established over TCP.<br><br>• When set to `server-auth`, the SVM authenticates the FPolicy server using SSL server authentication.<br><br>• When set to `mutual-auth`, mutual authentication takes place between the SVM and the FPolicy server; the SVM authenticates the FPolicy server, and the FPolicy server authenticates the SVM.<br><br>   If you choose to configure mutual SSL authentication, then you must also configure the `-certificate-common-name`, `-certificate-serial`, and `-certifcate-ca` parameters. | `-ssl-option {no-auth |server-auth|mutual-auth}` |
| *Certificate FQDN or custom common name*<br><br>Specifies the certificate name used if SSL authentication between the SVM and the FPolicy server is configured. You can specify the certificate name as an FQDN or as a custom common name.<br><br>If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-common-name` parameter. | `-certificate-common -name text` |
| *Certificate serial number*<br><br>Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.<br><br>If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-serial` parameter. | `-certificate-serial text` |
| *Certificate authority*<br><br>Specifies the CA name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.<br><br>If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-ca` parameter. | `-certificate-ca text` |

**What the advanced external engine options are**

You can use the following table of advanced FPolicy configuration parameters as you plan whether to customize your configuration with advanced parameters. You use these parameters to modify communication behavior between the cluster nodes and the FPolicy servers:

| Type of information | Option |
|---|---|
| *Timeout for canceling a request*<br><br>Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) that the node waits for a response from the FPolicy server.<br><br>If the timeout interval passes, the node sends a cancel request to the FPolicy server. The node then sends the notification to an alternate FPolicy server. This timeout helps in handling an FPolicy server that is not responding, which can improve SMB/NFS client response. Also, canceling requests after a timeout period can help in releasing system resources because the notification request is moved from a down/bad FPolicy server to an alternate FPolicy server.<br><br>The range for this value is `0` through `100`. If the value is set to `0`, the option is disabled and cancel request messages are not sent to the FPolicy server. The default is `20s`. | `-reqs-cancel-timeout` `integer[h|m|s]` |
| *Timeout for aborting a request*<br><br>Specifies the timeout in hours (`h`), minutes (`m`), or seconds (`s`) for aborting a request.<br><br>The range for this value is `0` through `200`. | `-reqs-abort-timeout ` `` `integer[h|m|s]`` |
| *Interval for sending status requests*<br><br>Specifies the interval in hours (`h`), minutes (`m`), or seconds (`s`) after which a status request is sent to the FPolicy server.<br><br>The range for this value is `0` through `50`. If the value is set to `0`, the option is disabled and status request messages are not sent to the FPolicy server. The default is `10s`. | `-status-req-interval` `integer[h|m|s]` |
| *Maximum outstanding requests on the FPolicy server*<br><br>Specifies the maximum number of outstanding requests that can be queued on the FPolicy server.<br><br>The range for this value is `1` through `10000`. The default is `50`. | `-max-server-reqs integer` |

| | |
|---|---|
| *Timeout for disconnecting a nonresponsive FPolicy server*<br><br>Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) after which the connection to the FPolicy server is terminated.<br><br>The connection is terminated after the timeout period only if the FPolicy server's queue contains the maximum allowed requests and no response is received within the timeout period. The maximum allowed number of requests is either `50` (the default) or the number specified by the `max-server-reqs-` parameter.<br><br>The range for this value is `1` through `100`. The default is `60s`. | `-server-progress` `-timeout integer[h\|m\|s]` |
| *Interval for sending keep-alive messages to the FPolicy server*<br><br>Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) at which keep-alive messages are sent to the FPolicy server.<br><br>Keep-alive messages detect half-open connections.<br><br>The range for this value is `10` through `600`. If the value is set to `0`, the option is disabled and keep-alive messages are prevented from being sent to the FPolicy servers. The default is `120s`. | `-keep-alive-interval-` `integer[h\|m\|s]` |
| *Maximum reconnect attempts*<br><br>Specifies the maximum number of times the SVM attempts to reconnect to the FPolicy server after the connection has been broken.<br><br>The range for this value is `0` through `20`. The default is `5`. | `-max-connection-retries` `integer` |
| *Receive buffer size*<br><br>Specifies the receive buffer size of the connected socket for the FPolicy server.<br><br>The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the receive buffer is set to a value defined by the system.<br><br>For example, if the default receive buffer size of the socket is 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the receive buffer. | `-recv-buffer-size` `integer` |

| | |
|---|---|
| *Send buffer size*<br><br>Specifies the send buffer size of the connected socket for the FPolicy server.<br><br>The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the send buffer is set to a value defined by the system.<br><br>For example, if the default send buffer size of the socket is set to 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the send buffer. | `-send-buffer-size integer` |
| *Timeout for purging a session ID during reconnection*<br><br>Specifies the interval in hours (`h`), minutes (`m`), or seconds (`s`) after which a new session ID is sent to the FPolicy server during reconnection attempts.<br><br>If the connection between the storage controller and the FPolicy server is terminated and reconnection is made within the `-session-timeout` interval, the old session ID is sent to FPolicy server so that it can send responses for old notifications.<br><br>The default value is set to 10 seconds. | `-session-timeout [integerh][integerm][integers]` |

**Additional information about configuring FPolicy external engines to use SSL authenticated connections**

You need to know some additional information if you want to configure the FPolicy external engine to use SSL when connecting to FPolicy servers.

**SSL server authentication**

If you choose to configure the FPolicy external engine for SSL server authentication, before creating the external engine, you must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.

**Mutual authentication**

If you configure FPolicy external engines to use SSL mutual authentication when connecting storage virtual machine (SVM) data LIFs to external FPolicy servers, before creating the external engine, you must install the public certificate of the CA that signed the FPolicy server certificate along with the public certificate and key file for authentication of the SVM. You must not delete this certificate while any FPolicy policies are using the installed certificate.

If the certificate is deleted while FPolicy is using it for mutual authentication when connecting to an external FPolicy server, you cannot reenable a disabled FPolicy policy that uses that certificate. The FPolicy policy cannot be reenabled in this situation even if a new certificate with the same settings is created and installed on the SVM.

If the certificate has been deleted, you need to install a new certificate, create new FPolicy external engines that use the new certificate, and associate the new external engines with the FPolicy policy that you want to reenable by modifying the FPolicy policy.

**Install certificates for SSL**

The public certificate of the CA that is used to sign the FPolicy server certificate is installed by using the `security certificate install` command with the `-type` parameter set to `client_ca`. The private key and public certificate required for authentication of the SVM is installed by using the `security certificate install` command with the `-type` parameter set to `server`.

**Certificates do not replicate in SVM disaster recovery relationships with a non-ID-preserve configuration**

Security certificates used for SSL authentication when making connections to FPolicy servers do not replicate to SVM disaster recovery destinations with non-ID-preserve configurations. Although the FPolicy external-engine configuration on the SVM is replicated, security certificates are not replicated. You must manually install the security certificates on the destination.

When you set up the SVM disaster recovery relationship, the value you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), all of the FPolicy configuration details are replicated, including the security certificate information. You must install the security certificates on the destination only if you set the option to `false` (non-ID-preserve).

**Restrictions for cluster-scoped FPolicy external engines with MetroCluster and SVM disaster recovery configurations**

You can create a cluster-scoped FPolicy external engine by assigning the cluster storage virtual machine (SVM) to the external engine. However, when creating a cluster-scoped external engine in a MetroCluster or SVM disaster recovery configuration, there are certain restrictions when choosing the authentication method that the SVM uses for external communication with the FPolicy server.

There are three authentication options that you can choose when creating external FPolicy servers: no authentication, SSL server authentication, and SSL mutual authentication. Although there are no restrictions when choosing the authentication option if the external FPolicy server is assigned to a data SVM, there are restrictions when creating a cluster-scoped FPolicy external engine:

| Configuration | Permitted? |
|---|---|
| MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with no authentication (SSL is not configured) | Yes |
| MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with SSL server or SSL mutual authentication | No |

- If a cluster-scoped FPolicy external engine with SSL authentication exists and you want to create a MetroCluster or SVM disaster recovery configuration, you must modify this external engine to use no authentication or remove the external engine before you can create the MetroCluster or SVM disaster recovery configuration.

- If the MetroCluster or SVM disaster recovery configuration already exists, ONTAP prevents you from creating a cluster-scoped FPolicy external engine with SSL authentication.

**Complete the FPolicy external engine configuration worksheet**

You can use this worksheet to record the values that you need during the FPolicy external engine configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the external engine.

**Information for a basic external engine configuration**

You should record whether you want to include each parameter setting in the external engine configuration and then record the value for the parameters that you want to include.

| Type of information | Required | Include | Your values |
|---|---|---|---|
| Storage virtual machine (SVM) name | Yes | Yes | |
| Engine name | Yes | Yes | |
| Primary FPolicy servers | Yes | Yes | |
| Port number | Yes | Yes | |
| Secondary FPolicy servers | No | | |
| External engine type | No | | |
| SSL option for communication with external FPolicy server | Yes | Yes | |
| Certificate FQDN or custom common name | No | | |
| Certificate serial number | No | | |
| Certificate authority | No | | |

**Information for advanced external engine parameters**

To configure an external engine with advanced parameters, you must enter the configuration command while in advanced privilege mode.

| Type of information | Required | Include | Your values |
|---|---|---|---|
| Timeout for canceling a request | No | | |
| Timeout for aborting a request | No | | |

| | | | |
|---|---|---|---|
| Interval for sending status requests | No | | |
| Maximum outstanding requests on the FPolicy server | No | | |
| Timeout for disconnecting a nonresponsive FPolicy server | No | | |
| Interval for sending keep-alive messages to the FPolicy server | No | | |
| Maximum reconnect attempts | No | | |
| Receive buffer size | No | | |
| Send buffer size | No | | |
| Timeout for purging a session ID during reconnection | No | | |

**Plan the FPolicy event configuration**

**Plan the FPolicy event configuration overview**

Before you configure FPolicy events, you must understand what it means to create an FPolicy event. You must determine which protocols you want the event to monitor, which events to monitor, and which event filters to use. This information helps you plan the values that you want to set.

**What it means to create an FPolicy event**

Creating the FPolicy event means defining information that the FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server. The FPolicy event configuration defines the following configuration information:

- Storage virtual machine (SVM) name
- Event name
- Which protocols to monitor

  FPolicy can monitor SMB, NFSv3, and NFSv4 file access operations.

- Which file operations to monitor

  Not all file operations are valid for each protocol.

- Which file filters to configure

  Only certain combinations of file operations and filters are valid. Each protocol has its own set of supported combinations.

- Whether to monitor volume mount and unmount operations

> ℹ️ There is a dependency with three of the parameters (`-protocol`, `-file-operations`, `-filters`). The following combinations are valid for the three parameters:
>
>   - You can specify the `-protocol` and `-file-operations` parameters.
>   - You can specify all three of the parameters.
>   - You can specify none of the parameters.

**What the FPolicy event configuration contains**

You can use the following list of available FPolicy event configuration parameters to help you plan your configuration:

| Type of information | Option |
|---|---|
| *SVM*<br><br>Specifies the SVM name that you want to associate with this FPolicy event.<br><br>Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM. | `-vserver vserver_name` |
| *Event name*<br><br>Specifies the name to assign to the FPolicy event. When you create the FPolicy policy you associate the FPolicy event with the policy using the event name.<br><br>The name can be up to 256 characters long.<br><br>> ℹ️ The name should be up to 200 characters long if configuring the event in a MetroCluster or SVM disaster recovery configuration.<br><br>The name can contain any combination of the following ASCII-range characters:<br><br>- `a` through `z`<br>- `A` through `Z`<br>- `0` through `9`<br>- " _ ", "-", and "." | `-event-name event_name` |

| | |
|---|---|
| *Protocol*<br><br>Specifies which protocol to configure for the FPolicy event. The list for `-protocol` can include one of the following values:<br><br>• `cifs`<br><br>• `nfsv3`<br><br>• `nfsv4`<br><br>   ⓘ  If you specify `-protocol`, then you must specify a valid value in the `-file-operations` parameter. As the protocol version changes, the valid values might change. | `-protocol protocol` |
| *File operations*<br><br>Specifies the list of file operations for the FPolicy event.<br><br>The event checks the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. You can list one or more file operations by using a comma-delimited list. The list for `-file-operations` can include one or more of the following values:<br><br>• `close` for file close operations<br><br>• `create` for file create operations<br><br>• `create-dir` for directory create operations<br><br>• `delete` for file delete operations<br><br>• `delete_dir` for directory delete operations<br><br>• `getattr` for get attribute operations<br><br>• `link` for link operations<br><br>• `lookup` for lookup operations<br><br>• `open` for file open operations<br><br>• `read` for file read operations<br><br>• `write` for file write operations<br><br>• `rename` for file rename operations<br><br>• `rename_dir` for directory rename operations<br><br>• `setattr` for set attribute operations<br><br>• `symlink` for symbolic link operations<br><br>   ⓘ  If you specify `-file-operations`, then you must specify a valid protocol in the `-protocol` parameter. | `-file-operations file_operations,...` |

| | |
|---|---|
| *Filters*<br><br>Specifies the list of filters for a given file operation for the specified protocol. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following:<br><br>(i) If you specify the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.<br><br>• `monitor-ads` option to filter the client request for alternate data stream.<br><br>• `close-with-modification` option to filter the client request for close with modification.<br><br>• `close-without-modification` option to filter the client request for close without modification.<br><br>• `first-read` option to filter the client request for first read.<br><br>• `first-write` option to filter the client request for first write.<br><br>• `offline-bit` option to filter the client request for offline bit set.<br><br>Setting this filter results in the FPolicy server receiving notification only when offline files are accessed.<br><br>• `open-with-delete-intent` option to filter the client request for open with delete intent.<br><br>Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to delete it. This is used by file systems when the `FILE_DELETE_ON_CLOSE` flag is specified.<br><br>• `open-with-write-intent` option to filter client request for open with write intent.<br><br>Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to write something in it.<br><br>• `write-with-size-change` option to filter the client request for write with size change. | `-filters filter, …` |

| | |
|---|---|
| *Filters* continued<br><br>  • `setattr-with-owner-change` option to filter the client setattr requests for changing owner of a file or a directory.<br><br>  • `setattr-with-group-change` option to filter the client setattr requests for changing the group of a file or a directory.<br><br>  • `setattr-with-sacl-change` option to filter the client setattr requests for changing the SACL on a file or a directory.<br><br>    This filter is available only for the SMB and NFSv4 protocols.<br><br>  • `setattr-with-dacl-change` option to filter the client setattr requests for changing the DACL on a file or a directory.<br><br>    This filter is available only for the SMB and NFSv4 protocols.<br><br>  • `setattr-with-modify-time-change` option to filter the client setattr requests for changing the modification time of a file or a directory.<br><br>  • `setattr-with-access-time-change` option to filter the client setattr requests for changing the access time of a file or a directory.<br><br>  • `setattr-with-creation-time-change` option to filter the client setattr requests for changing the creation time of a file or a directory.<br><br>    This option is available only for the SMB protocol.<br><br>  • `setattr-with-mode-change` option to filter the client setattr requests for changing the mode bits on a file or a directory.<br><br>  • `setattr-with-size-change` option to filter the client setattr requests for changing the size of a file.<br><br>  • `setattr-with-allocation-size-change` option to filter the client setattr requests for changing the allocation size of a file.<br><br>    This option is available only for the SMB protocol.<br><br>  • `exclude-directory` option to filter the client requests for directory operations.<br><br>    When this filter is specified, the directory operations are not monitored. | `-filters filter,...` |
| *Is volume operation required*<br><br>Specifies whether monitoring is required for volume mount and unmount operations. The default is `false`. | `-volume-operation {true\|false}` |

**List of supported file operation and filter combinations that FPolicy can monitor for SMB**

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring SMB file access

operations.

The list of supported file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

| Supported file operations | Supported filters |
|---|---|
| close | monitor-ads, offline-bit, close-with-modification, close-without-modification, close-with-read, exclude-directory |
| create | monitor-ads, offline-bit |
| create_dir | Currently no filter is supported for this file operation. |
| delete | monitor-ads, offline-bit |
| delete_dir | Currently no filter is supported for this file operation. |
| getattr | offline-bit, exclude-dir |
| open | monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir |
| read | monitor-ads, offline-bit, first-read |
| write | monitor-ads, offline-bit, first-write, write-with-size-change |
| rename | monitor-ads, offline-bit |
| rename_dir | Currently no filter is supported for this file operation. |
| setattr | monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory |

**Supported file operation and filter combinations that FPolicy can monitor for NFSv3**

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv3 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

| Supported file operations | Supported filters |
|---|---|

| create | offline-bit |
|--------|-------------|
| create_dir | Currently no filter is supported for this file operation. |
| delete | offline-bit |
| delete_dir | Currently no filter is supported for this file operation. |
| link | offline-bit |
| lookup | offline-bit, exclude-dir |
| read | offline-bit, first-read |
| write | offline-bit, first-write, write-with-size-change |
| rename | offline-bit |
| rename_dir | Currently no filter is supported for this file operation. |
| setattr | offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory |
| symlink | offline-bit |

**Supported file operation and filter combinations that FPolicy can monitor for NFSv4**

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv4 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv4 file access events is provided in the following table:

| Supported file operations | Supported filters |
|---------------------------|-------------------|
| close | offline-bit, exclude-directory |
| create | offline-bit |
| create_dir | Currently no filter is supported for this file operation. |
| delete | offline-bit |

| delete_dir | Currently no filter is supported for this file operation. |
|---|---|
| getattr | offline-bit, exclude-directory |
| link | offline-bit |
| lookup | offline-bit, exclude-directory |
| open | offline-bit, exclude-directory |
| read | offline-bit, first-read |
| write | offline-bit, first-write, write-with-size-change |
| rename | offline-bit |
| rename_dir | Currently no filter is supported for this file operation. |
| setattr | offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory |
| symlink | offline-bit |

**Complete the FPolicy event configuration worksheet**

You can use this worksheet to record the values that you need during the FPolicy event configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy event.

You should record whether you want to include each parameter setting in the FPolicy event configuration and then record the value for the parameters that you want to include.

| Type of information | Required | Include | Your values |
|---|---|---|---|
| Storage virtual machine (SVM) name | Yes | Yes | |
| Event name | Yes | Yes | |
| Protocol | No | | |
| File operations | No | | |
| Filters | No | | |

| Volume operation | No | | |
|---|---|---|---|

**Plan the FPolicy policy configuration**

### Plan the FPolicy policy configuration overview

Before you configure the FPolicy policy, you must understand which parameters are required when creating the policy as well as why you might want to configure certain optional parameters. This information helps you to determine which values to set for each parameter.

When creating an FPolicy policy you associate the policy with the following:

- The storage virtual machine (SVM)
- One or more FPolicy events
- An FPolicy external engine

You can also configure several optional policy settings.

### What the FPolicy policy configuration contains

You can use the following list of available FPolicy policy required and optional parameters to help you plan your configuration:

| Type of information | Option | Required | Default |
|---|---|---|---|
| *SVM name*<br><br>Specifies the name of the SVM on which you want to create an FPolicy policy. | `-vserver vserver_name` | Yes | None |

| Policy name | -policy-name policy_name | Yes | None |
|---|---|---|---|
| Specifies the name of the FPolicy policy.<br><br>The name can be up to 256 characters long.<br><br>(i) The name should be up to 200 characters long if configuring the policy in a MetroCluster or SVM disaster recovery configuration.<br><br>The name can contain any combination of the following ASCII-range characters:<br><br>• a through z<br>• A through Z<br>• 0 through 9<br>• "_", "-", and "." | | | |
| Event names | -events event_name, ... | Yes | None |
| Specifies a comma-delimited list of events to associate with the FPolicy policy.<br><br>• You can associate more than one event to a policy.<br>• An event is specific to a protocol.<br>• You can use a single policy to monitor file access events for more than one protocol by creating an event for each protocol that you want the policy to monitor, and then associating the events to the policy.<br>• The events must already exist. | | | |

| | | | |
|---|---|---|---|
| *External engine name*<br><br>Specifies the name of the external engine to associate with the FPolicy policy.<br><br>• An external engine contains information required by the node to send notifications to an FPolicy server.<br><br>• You can configure FPolicy to use the ONTAP native external engine for simple file blocking or to use an external engine that is configured to use external FPolicy servers (FPolicy servers) for more sophisticated file blocking and file management.<br><br>• If you want to use the native external engine, you can either not specify a value for this parameter or you can specify `native` as the value.<br><br>• If you want to use FPolicy servers, the configuration for the external engine must already exist. | `-engine engine_name` | Yes (unless the policy uses the internal ONTAP native engine) | `native` |
| *Is mandatory screening required*<br><br>Specifies whether mandatory file access screening is required.<br><br>• The mandatory screening setting determines what action is taken on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period.<br><br>• When set to `true`, file access events are denied.<br><br>• When set to `false`, file access events are allowed. | `-is-mandatory {true\|false}` | No | `true` |

| *Allow privileged access*<br><br>Specifies whether you want the FPolicy server to have privileged access to the monitored files and folders by using a privileged data connection.<br><br>If configured, FPolicy servers can access files from the root of the SVM containing the monitored data using the privileged data connection.<br><br>For privileged data access, SMB must be licensed on the cluster and all the data LIFs used to connect to the FPolicy servers must be configured to have `cifs` as one of the allowed protocols.<br><br>If you want to configure the policy to allow privileged access, you must also specify the user name for the account that you want the FPolicy server to use for privileged access. | `-allow -privileged -access {yes\|no}` | No (unless passthrough-read is enabled) | `no` |
|---|---|---|---|
| *Privileged user name*<br><br>Specifies the user name of the account the FPolicy servers use for privileged data access.<br><br>• The value for this parameter should use the "domain\user name" format.<br><br>• If `-allow-privileged-access` is set to `no`, any value set for this parameter is ignored. | `-privileged -user-name user_name` | No (unless privileged access is enabled) | None |

| Allow passthrough-read<br><br>Specifies whether the FPolicy servers can provide passthrough-read services for files that have been archived to secondary storage (offline files) by the FPolicy servers:<br><br>• Passthrough-read is a way to read data for offline files without restoring the data to the primary storage.<br><br>   Passthrough-read reduces response latencies because there is no need to recall files back to primary storage before responding to the read request. Additionally, passthrough-read optimizes storage efficiency by eliminating the need to consume primary storage space with files that are recalled solely to satisfy read requests.<br><br>• When enabled, the FPolicy servers provide the data for the file over a separate privileged data channel opened specifically for passthrough-reads.<br><br>• If you want to configure passthrough-read, the policy must also be configured to allow privileged access. | `-is-passthrough`<br>`-read-enabled`<br>`{true\|false}` | No | `false` |
|---|---|---|---|

**Requirement for FPolicy scope configurations if the FPolicy policy uses the native engine**

If you configure the FPolicy policy to use the native engine, there is a specific requirement for how you define the FPolicy scope configured for the policy.

The FPolicy scope defines the boundaries on which the FPolicy policy applies, for example whether the FPolicy applies to specified volumes or shares. There are a number of parameters that further restrict the scope to which the FPolicy policy applies. One of these parameters, `-is-file-extension-check-on` `-directories-enabled`, specifies whether to check file extensions on directories. The default value is `false`, which means that file extensions on directories are not checked.

When an FPolicy policy that uses the native engine is enabled on a share or volume and the `-is-file` `-extension-check-on-directories-enabled` parameter is set to `false` for the scope of the policy, directory access is denied. With this configuration, because the file extensions are not checked for directories, any directory operation is denied if it falls under the scope of the policy.

To ensure that directory access succeeds when using the native engine, you must set the `-is-file` `-extension-check-on-directories-enabled parameter` to `true` when creating the scope.

With this parameter set to `true`, extension checks happen for directory operations and the decision whether to

allow or deny access is taken based on the extensions included or excluded in the FPolicy scope configuration.

**Complete the FPolicy policy worksheet**

You can use this worksheet to record the values that you need during the FPolicy policy configuration process. You should record whether you want to include each parameter setting in the FPolicy policy configuration and then record the value for the parameters that you want to include.

| Type of information | Include | Your values |
|---|---|---|
| Storage virtual machine (SVM) name | Yes | |
| Policy name | Yes | |
| Event names | Yes | |
| External engine name | | |
| Is mandatory screening required? | | |
| Allow privileged access | | |
| Privileged user name | | |
| Is passthrough-read enabled? | | |

**Plan the FPolicy scope configuration**

**Plan the FPolicy scope configuration overview**

Before you configure the FPolicy scope, you must understand what it means to create a scope. You must understand what the scope configuration contains. You also need to understand what the scope rules of precedence are. This information can help you plan the values that you want to set.

**What it means to create an FPolicy scope**

Creating the FPolicy scope means defining the boundaries on which the FPolicy policy applies. The storage virtual machine (SVM) is the basic boundary. When you create a scope for an FPolicy policy, you must define the FPolicy policy to which it will apply, and you must designate to which SVM you want to apply the scope.

There are a number of parameters that further restrict the scope within the specified SVM. You can restrict the scope by specifying what to include in the scope or by specifying what to exclude from the scope. After you apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

Notifications are generated for file access events where matches are found in the "include" options. Notifications are not generated for file access events where matches are found in the "exclude" options.

The FPolicy scope configuration defines the following configuration information:

- SVM name
- Policy name
- The shares to include or exclude from what gets monitored
- The export policies to include or exclude from what gets monitored
- The volumes to include or exclude from what gets monitored
- The file extensions to include or exclude from what gets monitored
- Whether to do file extension checks on directory objects

> (i) There are special considerations for the scope for a cluster FPolicy policy. The cluster FPolicy policy is a policy that the cluster administrator creates for the admin SVM. If the cluster administrator also creates the scope for that cluster FPolicy policy, the SVM administrator cannot create a scope for that same policy. However, if the cluster administrator does not create a scope for the cluster FPolicy policy, then any SVM administrator can create the scope for that cluster policy. If the SVM administrator creates a scope for that cluster FPolicy policy, the cluster administrator cannot subsequently create a cluster scope for that same cluster policy. This is because the cluster administrator cannot override the scope for the same cluster policy.

**What the scope rules of precedence are**

The following rules of precedence apply to scope configurations:

- When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include`.

- When an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include`.

- An administrator can specify both `-file-extensions-to-include` and `-file-extensions-to-exclude` lists.

  The `-file-extensions-to-exclude` parameter is checked before the `-file-extensions-to-include` parameter is checked.

**What the FPolicy scope configuration contains**

You can use the following list of available FPolicy scope configuration parameters to help you plan your configuration:

> (i) When configuring what shares, export policies, volumes, and file extensions to include or exclude from the scope, the include and exclude parameters can include metacharacters such as "?" and "*". The use of regular expressions is not supported.

| Type of information | Option |
|---|---|

| | |
|---|---|
| *SVM*<br><br>Specifies the SVM name on which you want to create an FPolicy scope.<br><br>Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM. | `-vserver vserver_name` |
| *Policy name*<br><br>Specifies the name of the FPolicy policy to which you want to attach the scope. The FPolicy policy must already exist. | `-policy-name policy_name` |
| *Shares to include*<br><br>Specifies a comma-delimited list of shares to monitor for the FPolicy policy to which the scope is applied. | `-shares-to-include share_name, ...` |
| *Shares to exclude*<br><br>Specifies a comma-delimited list of shares to exclude from monitoring for the FPolicy policy to which the scope is applied. | `-shares-to-exclude share_name, ...` |
| *Volumes to include* Specifies a comma-delimited list of volumes to monitor for the FPolicy policy to which the scope is applied. | `-volumes-to-include volume_name, ...` |
| *Volumes to exclude*<br><br>Specifies a comma-delimited list of volumes to exclude from monitoring for the FPolicy policy to which the scope is applied. | `-volumes-to-exclude volume_name, ...` |
| *Export policies to include*<br><br>Specifies a comma-delimited list of export policies to monitor for the FPolicy policy to which the scope is applied. | `-export-policies-to -include export_policy_name, ...` |
| *Export policies to exclude*<br><br>Specifies a comma-delimited list of export policies to exclude from monitoring for the FPolicy policy to which the scope is applied. | `-export-policies-to -exclude export_policy_name, ...` |
| *File extensions to include*<br><br>Specifies a comma-delimited list of file extensions to monitor for the FPolicy policy to which the scope is applied. | `-file-extensions-to -include file_extensions, ...` |

| File extension to exclude | `-file-extensions-to-exclude file_extensions, ...` |
|---|---|
| Specifies a comma-delimited list of file extensions to exclude from monitoring for the FPolicy policy to which the scope is applied. | |
| *Is file extension check on directory enabled ?* | `-is-file-extension-check-on-directories-enabled {true\| false\|}` |
| Specifies whether the file name extension checks apply to directory objects as well. If this parameter is set to `true`, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to `false`, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match. | |
| If the FPolicy policy to which the scope is assigned is configured to use the native engine, this parameter must be set to `true`. | |

**Complete the FPolicy scope worksheet**

You can use this worksheet to record the values that you need during the FPolicy scope configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy scope.

You should record whether you want to include each parameter setting in the FPolicy scope configuration and then record the value for the parameters that you want to include.

| Type of information | Required | Include | Your values |
|---|---|---|---|
| Storage virtual machine (SVM) name | Yes | Yes | |
| Policy name | Yes | Yes | |
| Shares to include | No | | |
| Shares to exclude | No | | |
| Volumes to include | No | | |
| Volumes to exclude | No | | |
| Export policies to include | No | | |
| Export policies to exclude | No | | |
| File extensions to include | No | | |
| File extension to exclude | No | | |

| Is file extension check on directory enabled? | No | | |
|---|---|---|---|

**Create the FPolicy configuration**

### Create the FPolicy external engine

You must create an external engine to start creating an FPolicy configuration. The external engine defines how FPolicy makes and manages connections to external FPolicy servers. If your configuration uses the internal ONTAP engine (the native external engine) for simple file blocking, you do not need to configure a separate FPolicy external engine and do not need to perform this step.

**What you'll need**

The external engine worksheet should be completed.

**About this task**

If the external engine is used in a MetroCluster configuration, you should specify the IP addresses of the FPolicy servers at the source site as primary servers. The IP addresses of the FPolicy servers at the destination site should be specified as secondary servers.

**Steps**

1. Create the FPolicy external engine by using the `vserver fpolicy policy external-engine create` command.

   The following command creates an external engine on storage virtual machine (SVM) vs1.example.com. No authentication is required for external communications with the FPolicy server.

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. Verify the FPolicy external engine configuration by using the `vserver fpolicy policy external-engine show` command.

   The following command display information about all external engines configured on SVM vs1.example.com:

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

```
                                  Primary          Secondary
External
Vserver            Engine         Servers          Servers          Port Engine
Type
--------------     -----------    -------------    -----------      ------
-----------
vs1.example.com    engine1        10.1.1.2,        -                6789
synchronous

                                  10.1.1.3
```

The following command displays detailed information about the external engine named "engine1" on SVM vs1.example.com:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
-name engine1
```

```
                                Vserver: vs1.example.com
                                 Engine: engine1
                 Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
            Port Number of FPolicy Service: 6789
               Secondary FPolicy Servers: -
                     External Engine Type: synchronous
 SSL Option for External Communication: no-auth
             FQDN or Custom Common Name: -
           Serial Number of Certificate: -
                  Certificate Authority: -
```

**Create the FPolicy event**

As part of creating an FPolicy policy configuration, you need to create an FPolicy event. You associate the event with the FPolicy policy when it is created. An event defines which protocol to monitor and which file access events to monitor and filter.

**Before you begin**

You should complete the FPolicy event worksheet.

**Steps**

1. Create the FPolicy event by using the `vserver fpolicy policy event create` command.

   ```
   vserver fpolicy policy event create -vserver-name vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. Verify the FPolicy event configuration by using the `vserver fpolicy policy event show` command.

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

```
                    Event               File                         Is Volume
Vserver             Name      Protocols Operations      Filters      Operation
---------------     --------- --------- ------------- ---------
------------
vs1.example.com     event1    cifs      open, close,  -            false
                                        read, write
```

**Create the FPolicy policy**

When you create the FPolicy policy, you associate an external engine and one or more events to the policy. The policy also specifies whether mandatory screening is required, whether the FPolicy servers have privileged access to data on the storage virtual machine (SVM), and whether passthrough-read for offline files is enabled.

**What you'll need**

- The FPolicy policy worksheet should be completed.
- If you plan on configuring the policy to use FPolicy servers, the external engine must exist.
- At least one FPolicy event that you plan on associating with the FPolicy policy must exist.
- If you want to configure privileged data access, a SMB server must exist on the SVM.

**Steps**

1. Create the FPolicy policy:

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name
   policy_name -engine engine_name -events event_name,… [-is-mandatory
   {true|false}] [-allow-privileged-access {yes|no}] [-privileged-user-name
   domain\user_name] [-is-passthrough-read-enabled {true|false}]
   ```

   ◦ You can add one or more events to the FPolicy policy.

   ◦ By default, mandatory screening is enabled.

   ◦ If you want to allow privileged access by setting the `-allow-privileged-access` parameter to `yes`, you must also configure a privileged user name for privileged access.

   ◦ If you want to configure passthrough-read by setting the `-is-passthrough-read-enabled` parameter to `true`, you must also configure privileged data access.

   The following command creates a policy named "policy1" that has the event named "event1" and the external engine named "engine1" associated with it. This policy uses default values in the policy configuration:
   ```
   vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1
   -events event1 -engine engine1
   ```

   The following command creates a policy named "policy2" that has the event named "event2" and the external engine named "engine2" associated with it. This policy is configured to use privileged access using the specified user name. Passthrough-read is enabled:
   ```
   vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
   -events event2 -engine engine2 -allow-privileged-access yes -privileged-
   ```

```
user-name example\archive_acct -is-passthrough-read-enabled true
```

The following command creates a policy named "native1" that has the event named "event3" associated with it. This policy uses the native engine and uses default values in the policy configuration:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. Verify the FPolicy policy configuration by using the `vserver fpolicy policy show` command.

   The following command displays information about the three configured FPolicy policies, including the following information:

   ◦ The SVM associated with the policy

   ◦ The external engine associated with the policy

   ◦ The events associated with the policy

   ◦ Whether mandatory screening is required

   ◦ Whether privileged access is required
   ```
   vserver fpolicy policy show
   ```

```
   Vserver         Policy     Events    Engine    Is Mandatory Privileged
                   Name                                         Access
  --------------   --------- --------- --------- ------------
  -----------
  vs1.example.com  policy1    event1    engine1   true         no
  vs1.example.com  policy2    event2    engine2   true         yes
  vs1.example.com  native1    event3    native    true         no
```

**Create the FPolicy scope**

After creating the FPolicy policy, you need to create an FPolicy scope. When creating the scope, you associate the scope with an FPolicy policy. A scope defines the boundaries on which the FPolicy policy applies. Scopes can include or exclude files based on shares, export policies, volumes, and file extensions.

**What you'll need**

The FPolicy scope worksheet must be completed. The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event.

**Steps**

1. Create the FPolicy scope by using the `vserver fpolicy policy scope create` command.

   ```
   vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
   policy1 -volumes-to-include datavol1,datavol2
   ```

2. Verify the FPolicy scope configuration by using the `vserver fpolicy policy scope show` command.

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
                      Vserver: vs1.example.com
                       Policy: policy1
            Shares to Include: -
            Shares to Exclude: -
           Volumes to Include: datavol1, datavol2
           Volumes to Exclude: -
    Export Policies to Include: -
    Export Policies to Exclude: -
     File Extensions to Include: -
     File Extensions to Exclude: -
```

**Enable the FPolicy policy**

After you are through configuring an FPolicy policy configuration, you enable the FPolicy policy. Enabling the policy sets its priority and starts file access monitoring for the policy.

**What you'll need**

The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event. The FPolicy policy scope must exist and must be assigned to the FPolicy policy.

**About this task**

The priority is used when multiple policies are enabled on the storage virtual machine (SVM) and more than one policy has subscribed to the same file access event. Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them when enabling the policy.

> ⓘ  A policy cannot be enabled on the admin SVM.

**Steps**

1. Enable the FPolicy policy by using the `vserver fpolicy enable` command.

   ```
   vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
   -sequence-number 1
   ```

2. Verify that the FPolicy policy is enabled by using the `vserver fpolicy show` command.

   ```
   vserver fpolicy show -vserver vs1.example.com
   ```

   ```
                                  Sequence
    Vserver          Policy Name     Number  Status   Engine
    ---------------  ---------------- -------- -------- ---------
    vs1.example.com  policy1                1  on       engine1
   ```

**Modify FPolicy configurations**

**Commands for modifying FPolicy configurations**

You can modify FPolicy configurations by modifying the elements that make up the configuration. You can modify external engines, FPolicy events, FPolicy scopes, and FPolicy policies. You can also enable or disable FPolicy policies. When you disable the FPolicy policy, file monitoring is discontinued for that policy.

It is recommended to disable the FPolicy policy before modifying the configuration.

| If you want to modify… | Use this command… |
|---|---|
| External engines | `vserver fpolicy policy external-engine modify` |
| Events | `vserver fpolicy policy event modify` |
| Scopes | `vserver fpolicy policy scope modify` |
| Policies | `vserver fpolicy policy modify` |

See the man pages for the commands for more information.

**Enable or disable FPolicy policies**

You can enable FPolicy policies after the configuration is complete. Enabling the policy sets its priority and starts file access monitoring for the policy. You can disable FPolicy policies if you want to stop file access monitoring for the policy.

**What you'll need**
Before enabling FPolicy policies, the FPolicy configuration must be completed.

**About this task**
- The priority is used when multiple policies are enabled on the storage virtual machine (SVM) and more than one policy has subscribed to the same file access event.
- Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them when enabling the policy.
- If you want to change the priority of an FPolicy policy, you must disable the policy and then reenable it using the new sequence number.

**Step**
1. Perform the appropriate action:

| If you want to… | Enter the following command… |
|---|---|
| Enable an FPolicy policy | `vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer` |

| Disable an FPolicy policy | `vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name` |

## Display information about FPolicy configurations

**How the show commands work**

It is helpful when displaying information about the FPolicy configuration to understand how the `show` commands work.

A `show` command without additional parameters displays information in a summary form. Additionally, every `show` command has the same two mutually exclusive optional parameters, `-instance` and `-fields`.

When you use the `-instance` parameter with a `show` command, the command output displays detailed information in a list format. In some cases, the detailed output can be lengthy and include more information than you need. You can use the `-fields fieldname[,fieldname…]` parameter to customize the output so that it displays information only for the fields you specify. You can identity which fields that you can specify by entering `?` after the `-fields` parameter.

> ⓘ The output of a `show` command with the `-fields` parameter might display other relevant and necessary fields related to the requested fields.

Every `show` command has one or more optional parameters that filter that output and enable you to narrow the scope of information displayed in command output. You can identity which optional parameters are available for a command by entering `?` after the `show` command.

The `show` command supports UNIX-style patterns and wildcards to enable you to match multiple values in command-parameters arguments. For example, you can use the wildcard operator (*), the NOT operator (!), the OR operator (|), the range operator (integer…integer), the less-than operator (<), the greater-than operator (>), the less-than or equal to operator (<=), and the greater-than or equal to operator (>=) when specifying values.

For more information about using UNIX-style patterns and wildcards, see the Using the ONTAP command-line interface.

**Commands for displaying information about FPolicy configurations**

You use the `fpolicy show` commands to display information about the FPolicy configuration, including information about FPolicy external engines, events, scopes, and policies.

| If you want to display information about FPolicy… | Use this command… |
|---|---|
| External engines | `vserver fpolicy policy external-engine show` |
| Events | `vserver fpolicy policy event show` |

| Scopes | `vserver fpolicy policy scope show` |
|--------|-------------------------------------|
| Policies | `vserver fpolicy policy show` |

See the man pages for the commands for more information.

**Display information about FPolicy policy status**

You can display information about the status for FPolicy policies to determine whether a policy is enabled, what external engine it is configured to use, what the sequence number is for the policy, and to which storage virtual machine (SVM) the FPolicy policy is associated.

**About this task**

If you do not specify any parameters, the command displays the following information:

- SVM name
- Policy name
- Policy sequence number
- Policy status

In addition to displaying information about policy status for FPolicy policies configured on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output, or `-fields ?` to determine what fields you can use.

**Step**

1. Display filtered information about FPolicy policy status by using the appropriate command:

| If you want to display status information about policies… | Enter the command… |
|-----------------------------------------------------------|--------------------|
| On the cluster | `vserver fpolicy show` |
| That have the specified status | `vserver fpolicy show -status {on|off}` |
| On a specified SVM | `vserver fpolicy show -vserver vserver_name` |
| With the specified policy name | `vserver fpolicy show -policy-name policy_name` |
| That use the specified external engine | `vserver fpolicy show -engine engine_name` |

**Example**

The following example displays the information about FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show
                                        Sequence
Vserver               Policy Name         Number   Status      Engine
-------------------   -------------------  -------- ---------   ---------
FPolicy               cserver_policy      -        off         eng1
vs1.example.com       v1p1                -        off         eng2
vs1.example.com       v1p2                -        off         native
vs1.example.com       v1p3                -        off         native
vs1.example.com       cserver_policy      -        off         eng1
vs2.example.com       v1p1                3        on          native
vs2.example.com       v1p2                1        on          eng3
vs2.example.com       cserver_policy      2        on          eng1
```

**Display information about enabled FPolicy policies**

You can display information about enabled FPolicy policies to determine what FPolicy external engine it is configured to use, what the priority is for the policy, and to which storage virtual machine (SVM) the FPolicy policy is associated.

**About this task**

If you do not specify any parameters, the command displays the following information:

- SVM name
- Policy name
- Policy priority

You can use command parameters to filter the command's output by specified criteria.

**Step**

1. Display information about enabled FPolicy policies by using the appropriate command:

| If you want to display information about enabled policies… | Enter the command… |
|---|---|
| On the cluster | `vserver fpolicy show-enabled` |
| On a specified SVM | `vserver fpolicy show-enabled -vserver vserver_name` |
| With the specified policy name | `vserver fpolicy show-enabled -policy-name policy_name` |
| With the specified sequence number | `vserver fpolicy show-enabled -priority integer` |

**Example**

The following example displays the information about enabled FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

**Manage FPolicy server connections**

**Connect to external FPolicy servers**

To enable file processing, you might need to manually connect to an external FPolicy server if the connection has previously been terminated. A connection is terminated after the server timeout is reached or due to some error. Alternatively, the administrator might manually terminate a connection.

**About this task**

If a fatal error occurs, the connection to the FPolicy server can be terminated. After resolving the issue that caused the fatal error, you must manually reconnect to the FPolicy server.

**Steps**

1. Connect to the external FPolicy server by using the `vserver fpolicy engine-connect` command.

   For more information about the command, see the man pages.

2. Verify that the external FPolicy server is connected by using the `vserver fpolicy show-engine` command.

   For more information about the command, see the man pages.

**Disconnect from external FPolicy servers**

You might need to manually disconnect from an external FPolicy server. This might be desirable if the FPolicy server has issues with notification request processing or if you need to perform maintenance on the FPolicy server.

**Steps**

1. Disconnect from the external FPolicy server by using the `vserver fpolicy engine-disconnect` command.

   For more information about the command, see the man pages.

2. Verify that the external FPolicy server is disconnected by using the `vserver fpolicy show-engine` command.

For more information about the command, see the man pages.

**Display information about connections to external FPolicy servers**

You can display status information about connections to external FPolicy servers (FPolicy servers) for the cluster or for a specified storage virtual machine (SVM). This information can help you determine which FPolicy servers are connected.

**About this task**

If you do not specify any parameters, the command displays the following information:

- SVM name
- Node name
- FPolicy policy name
- FPolicy server IP address
- FPolicy server status
- FPolicy server type

In addition to displaying information about FPolicy connections on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output. You can enter `?` after the `-fields` parameter to find out which fields you can use.

**Step**

1. Display filtered information about connection status between the node and the FPolicy server by using the appropriate command:

| If you want to display connection status information about FPolicy servers… | Enter… |
|---|---|
| That you specify | `vserver fpolicy show-engine -server IP_address` |
| For a specified SVM | `vserver fpolicy show-engine -vserver vserver_name` |
| That are attached with a specified policy | `vserver fpolicy show-engine -policy-name policy_name` |

| With the server status that you specify | `vserver fpolicy show-engine -server-status status`<br><br>The server status can be one of the following:<br><br>- `connected`<br>- `disconnected`<br>- `connecting`<br>- `disconnecting` |
|---|---|
| With the specified type | `vserver fpolicy show-engine -server-type type`<br><br>The FPolicy server type can be one of the following:<br><br>- `primary`<br>- `secondary` |
| That were disconnected with the specified reason | `vserver fpolicy show-engine -disconnect-reason text`<br><br>Disconnect can be due to multiple reasons. The following are common reasons for disconnect:<br><br>- `Disconnect command received from CLI.`<br>- `Error encountered while parsing notification response from FPolicy server.`<br>- `FPolicy Handshake failed.`<br>- `SSL handshake failed.`<br>- `TCP Connection to FPolicy server failed.`<br>- `The screen response message received from the FPolicy server is not valid.` |

**Example**

This example displays information about external engine connections to FPolicy servers on SVM vs1.example.com:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                              Server-       Server-
Vserver         Policy      Node          Server     status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1    node1        10.1.1.2      connected     primary
vs1.example.com policy1    node1        10.1.1.3      disconnected  primary
vs1.example.com policy1    node2        10.1.1.2      connected     primary
vs1.example.com policy1    node2        10.1.1.3      disconnected  primary
```

This example displays information only about connected FPolicy servers:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

**Display information about the FPolicy passthrough-read connection status**

You can display information about FPolicy passthrough-read connection status to external
FPolicy servers (FPolicy servers) for the cluster or for a specified storage virtual machine
(SVM). This information can help you determine which FPolicy servers have
passthrough-read data connections and for which FPolicy servers the passthrough-read
connection is disconnected.

**About this task**

If you do not specify any parameter, the command displays the following information:

- SVM name
- FPolicy policy name
- Node name
- FPolicy server IP address
- FPolicy passthrough-read connection status

In addition to displaying information about FPolicy connections on the cluster or a specific SVM, you can use
command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively,
you can use the `-fields` parameter to display only the indicated fields in the command output. You can enter
`?` after the `-fields` parameter to find out which fields you can use.

**Step**

1. Display filtered information about connection status between the node and the FPolicy server by using the

appropriate command:

| If you want to display connection status information about… | Enter the command… |
|---|---|
| FPolicy passthrough-read connection status for the cluster | `vserver fpolicy show-passthrough-read-connection` |
| FPolicy passthrough-read connection status for a specified SVM | `vserver fpolicy show-passthrough-read-connection -vserver vserver_name` |
| FPolicy passthrough-read connection status for a specified policy | `vserver fpolicy show-passthrough-read-connection -policy-name policy_name` |
| Detailed FPolicy passthrough-read connection status for a specified policy | `vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance` |
| FPolicy passthrough-read connection status for the status that you specify | `vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` The server status can be one of the following:<br><br>• `connected`<br><br>• `disconnected` |

**Example**

The following command displays information about passthrough-read connections from all FPolicy servers on the cluster:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                        FPolicy           Server
Vserver           Policy Name   Node          Server            Status
---------------   ------------  -----------   -----------------
--------------
vs2.example.com   pol_cifs_2    FPolicy-01    2.2.2.2           disconnected
vs1.example.com   pol_cifs_1    FPolicy-01    1.1.1.1           connected
```

The following command displays detailed information about passthrough-read connections from FPolicy servers configured in the "pol_cifs_1" policy:

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                              Node: FPolicy-01
                                           Vserver: vs1.example.com
                                            Policy: pol_cifs_1
                                            Server: 1.1.1.1
            Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                     Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

## Use security tracing to verify or troubleshoot file and directory access

### How security traces work

You can add permission tracing filters to instruct ONTAP to log information about why the SMB and NFS servers on a storage virtual machine (SVM) allows or denies a client or user's request to perform an operation. This can be useful when you want to verify that your file access security scheme is appropriate or when you want to troubleshoot file access issues.

Security traces allow you to configure a filter that detects client operations over SMB and NFS on the SVM, and trace all access checks matching that filter. You can then view the trace results, which provides a convenient summary of the reason that access was allowed or denied.

When you want to verify the security settings for SMB or NFS access on files and folders on your SVM or if you are faced with an access problem, you can quickly add a filter to turn on permission tracing.

The following list outlines important facts about how security traces works:

- ONTAP applies security traces at the SVM level.
- Each incoming request is screened to see if it matches filtering criteria of any enabled security traces.
- Traces are performed for both file and folder access requests.
- Traces can filter based on the following criteria:
  - Client IP
  - SMB or NFS path
  - Windows name
  - UNIX name
- Requests are screened for *Allowed* and *Denied* access response results.
- Each request matching filtering criteria of enabled traces is recorded in the trace results log.
- The storage administrator can configure a timeout on a filter to automatically disable it.

- If a request matches multiple filters, the results from the filter with the highest index number is recorded.
- The storage administrator can print results from the trace results log to determine why an access request was allowed or denied.

**Types of access checks security traces monitor**

Access checks for a file or folder are done based on multiple criteria. Security traces monitor operations on all these criteria.

The types of access checks that security traces monitor include the following:

- Volume and qtree security style
- Effective security of the file system containing the files and folders on which operations are requested
- User mapping
- Share-level permissions
- Export-level permissions
- File-level permissions
- Storage-Level Access Guard security

**Considerations when creating security traces**

You should keep several considerations in mind when you create security traces on storage virtual machines (SVMs). For example, you need to know on which protocols you can create a trace, which security-styles are supported, and what the maximum number of active traces is.

- You can only create security traces on SVMs.
- Each security trace filter entry is SVM specific.

  You must specify the SVM on which you want to run the trace.

- You can add permission tracing filters for SMB and NFS requests.
- You must set up the SMB or NFS server on the SVM on which you want to create trace filters.
- You can create security traces for files and folders residing on NTFS, UNIX, and mixed security-style volumes and qtrees.
- You can add a maximum of 10 permission tracing filters per SVM.
- You must specify a filter index number when creating or modifying a filter.

  Filters are considered in order of the index number. The criteria in a filter with a higher index number is considered before the criteria with a lower index number. If the request being traced matches criteria in multiple enabled filters, only the filter with the highest index number is triggered.

- After you have created and enabled a security trace filter, you must perform some file or folder requests on a client system to generate activity that the trace filter can capture and log in the trace results log.
- You should add permission tracing filters for file access verification or troubleshooting purposes only.

  Adding permission tracing filters has a minor effect on controller performance.

When you are done with verification or troubleshooting activity, you should disable or remove all permission tracing filters. Furthermore, the filtering criteria you select should be as specific as possible so that ONTAP does not send a large number of trace results to the log.

## Perform security traces

### Perform security traces overview

Performing a security trace involves creating a security trace filter, verifying the filter criteria, generating access requests on an SMB or NFS client that match filter criteria, and viewing the results.

After you are finished using a security filter to capture trace information, you can modify the filter and reuse it, or disable it if you no longer need it. After viewing and analyzing the filter trace results, you can then delete them if they are no longer needed.

### Create security trace filters

You can create security trace filters that detect SMB and NFS client operations on storage virtual machines (SVMs)and trace all access checks matching the filter. You can use the results from security traces to validate your configuration or to troubleshoot access issues.

**About this task**

There are two required parameters for the vserver security trace filter create command:

| Required parameters | Description |
| --- | --- |
| `-vserver vserver_name` | *SVM name*<br><br>The name of the SVM that contains the files or folders on which you want to apply the security trace filter. |
| `-index index_number` | *Filter index number*<br><br>The index number you want to apply to the filter. You are limited to a maximum of 10 trace filters per SVM. The allowed values for this parameter are 1 through 10. |

A number of optional filter parameters enable you to customize the security trace filter so that you can narrow down the results produced by the security trace:

| Filter parameter | Description |
| --- | --- |
| `-client-ip IP_Address` | This filter specifies the IP address from which the user is accessing the SVM. |

| | |
|---|---|
| `-path path` | This filter specifies the path on which to apply the permission trace filter. The value for `-path` can use either of the following formats:<br><br>    • The complete path, starting from the root of the share or export<br><br>    • A partial path, relative to the root of the share<br><br>You must use NFS style directory UNIX-style directory separators in the path value. |
| `-windows-name win_user_name` or `-unix -name``unix_user_name` | You can specify either the Windows user name or UNIX user name whose access requests you want to trace. The user name variable is case insensitive. You cannot specify both a Windows user name and a UNIX user name in the same filter.<br><br>ⓘ  Even though you can trace SMB and NFS access events, the mapped UNIX user and the mapped UNIX users' groups might be used when performing access checks on mixed or UNIX security-style data. |
| `-trace-allow {yes\|no}` | Tracing for deny events is always enabled for a security trace filter. You can optionally trace allow events. To trace allow events, you set this parameter to `yes`. |
| `-enabled {enabled\|disabled}` | You can enable or disable the security trace filter. By default, the security trace filter is enabled. |
| `-time-enabled integer` | You can specify a timeout for the filter, after which it is disabled. |

**Steps**

1. Create a security trace filter:

   ```
   vserver security trace filter create -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   `filter_parameters` is a list of optional filter parameters.

   For more information, see the man pages for the command.

2. Verify the security trace filter entry:

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

**Examples**

The following command creates a security trace filter for any user accessing a file with a share path `\\server\share1\dir1\dir2\file.txt` from the IP address 10.10.10.7. The filter uses a complete path for the `-path` option. The client's IP address used to access data is 10.10.10.7. The filter times out after 30 minutes:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver   Index   Client-IP            Path            Trace-Allow
Windows-Name
--------  -----   -----------   ---------------------   -----------
-------------
vs1         1     10.10.10.7    /dir1/dir2/file.txt            no       -
```

The following command creates a security trace filter using a relative path for the -path option. The filter traces access for a Windows user named "joe". Joe is accessing a file with a share path \\server\share1\dir1\dir2\file.txt. The filter traces allow and deny events:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                          Vserver: vs1
                     Filter Index: 2
         Client IP Address to Match: -
                             Path: /dir1/dir2/file.txt
                Windows User Name: mydomain\joe
                   UNIX User Name: -
                Trace Allow Events: yes
                   Filter Enabled: enabled
          Minutes Filter is Enabled: 60
```

**Display information about security trace filters**

You can display information about security trace filters configured on your storage virtual machine (SVM). This enables you to see which types of access events each filter traces.

**Step**

1. Display information about security trace filter entries by using the `vserver security trace filter show` command.

   For more information about using this command, see the man pages.

**Examples**

The following command displays information about all security trace filters on SVM vs1:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver   Index   Client-IP              Path                Trace-Allow
Windows-Name
--------  -----   -----------   ---------------------   -----------
-------------
vs1        1      -             /dir1/dir2/file.txt           yes       -
vs1        2      -             /dir3/dir4/                   no
mydomain\joe
```

**Display security trace results**

You can display the security trace results generated for file operations that match security trace filters. You can use the results to validate your file access security configuration or to troubleshoot SMB and NFS file access issues.

**What you'll need**

An enabled security trace filter must exist and operations must have been performed from an SMB or NFS client that matches the security trace filter to generate security trace results.

**About this task**

You can display a summary of all security trace results, or you can customize what information is displayed in the output by specifying optional parameters. This can be helpful when the security trace results contain a large number of records.

If you do not specify any of the optional parameters, the following is displayed:

- storage virtual machine (SVM) name
- Node name
- Security trace index number
- Security style
- Path
- Reason
- User name

  The user name is displayed depending on how the trace filter is configured:

| If the filter is configured… | Then… |
|---|---|
| With a UNIX user name | The security trace result displays the UNIX user name. |
| With a Windows user name | The security trace result displays the Windows user name. |
| Without a user name | The security trace result displays the Windows user name. |

You can customize the output by using optional parameters. Some of the optional parameters that you can use to narrow the results returned in the command output include the following:

| Optional parameter | Description |
|---|---|
| `-fields field_name, ...` | Displays output on the fields you choose. You can use this parameter either alone or in combination with other optional parameters. |
| `-instance` | Displays detailed information about security trace events. Use this parameter with other optional parameters to display detailed information about specific filter results. |
| `-node node_name` | Displays information only about events on the specified node. |
| `-vserver vserver_name` | Displays information only about events on the specified SVM. |
| `-index integer` | Displays information about the events that occurred as a result of the filter corresponding to the specified index number. |
| `-client-ip IP_address` | Displays information about the events that occurred as a result of file access from the specified client IP address. |
| `-path path` | Displays information about the events that occurred as a result of file access to the specified path. |
| `-user-name user_name` | Displays information about the events that occurred as a result of file access by the specified Windows or UNIX user. |
| `-security-style security_style` | Displays information about the events that occurred on file systems with the specified security style. |

See the man page for information about other optional parameters that you can use with the command.

**Step**

1. Display security trace filter results by using the `vserver security trace trace-result show` command.

   `vserver security trace trace-result show -user-name domain\user`

```
Vserver: vs1

Node      Index   Filter Details          Reason
--------  ------- --------------------    -----------------------------
node1     3       User:domain\user        Access denied by explicit ACE
                  Security Style:mixed
                  Path:/dir1/dir2/


node1     5       User:domain\user        Access denied by explicit ACE
                  Security Style:unix
                  Path:/dir1/
```

**Modify security trace filters**

If you want to change the optional filter parameters used to determine which access events are traced, you can modify existing security trace filters.

**About this task**

You must identify which security trace filter you want to modify by specifying the storage virtual machine (SVM) name on which the filter is applied and the index number of the filter. You can modify all the optional filter parameters.

**Steps**

1. Modify a security trace filter:

   `vserver security trace filter modify -vserver vserver_name -index index_numberfilter_parameters`

   ◦ `vserver_name` is the name of the SVM on which you want to apply a security trace filter.

   ◦ `index_number` is the index number that you want to apply to the filter. The allowed values for this parameter are 1 through 10.

   ◦ `filter_parameters` is a list of optional filter parameters.

2. Verify the security trace filter entry:

   `vserver security trace filter show -vserver vserver_name -index index_number`

**Example**

The following command modifies the security trace filter with the index number 1. The filter traces events for any user accessing a file with a share path `\\server\share1\dir1\dir2\file.txt` from any IP address. The filter uses a complete path for the `-path` option. The filter traces allow and deny events:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                Vserver: vs1
                           Filter Index: 1
              Client IP Address to Match: -
                                   Path: /dir1/dir2/file.txt
                       Windows User Name: -
                          UNIX User Name: -
                      Trace Allow Events: yes
                          Filter Enabled: enabled
                Minutes Filter is Enabled: 60
```

**Delete security trace filters**

When you no longer need a security trace filter entry, you can delete it. Because you can
have a maximum of 10 security trace filters per storage virtual machine (SVM), deleting
unneeded filters enables you to create new filters if you have reached the maximum.

**About this task**

To uniquely identify the security trace filter that you want to delete, you must specify the following:

- The name of the SVM to which the trace filter is applied
- The filter index number of the trace filter

**Steps**

1. Identify the filter index number of the security trace filter entry you want to delete:

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver    Index   Client-IP            Path                  Trace-Allow
   Windows-Name
   -------- -----   -----------   --------------------   -----------
   -------------
   vs1        1      -             /dir1/dir2/file.txt          yes        -
   vs1        2      -             /dir3/dir4/                  no
   mydomain\joe
   ```

2. Using the filter index number information from the previous step, delete the filter entry:

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number
   ```

   ```
   vserver security trace filter delete -vserver vs1 -index 1
   ```

3. Verify that the security trace filter entry is deleted:

```
vserver security trace filter show -vserver vserver_name

vserver security trace filter show -vserver vs1
```

```
Vserver   Index   Client-IP              Path                  Trace-Allow
Windows-Name
--------  -----   -----------  ----------------------   -----------
------------
vs1        2      -                     /dir3/dir4/                 no
mydomain\joe
```

**Delete security trace records**

After you finish using a filter trace record to verify file access security or to troubleshoot SMB or NFS client access issues, you can delete the security trace record from the security trace log.

**About this task**

Before you can delete a security trace record, you must know the record's sequence number.

ⓘ Each storage virtual machine (SVM) can store a maximum of 128 trace records. If the maximum is reached on the SVM, the oldest trace records are automatically deleted as new ones are added. If you do not want to manually delete trace records on this SVM, you can let ONTAP automatically delete the oldest trace results after the maximum is reached to make room for new results.

**Steps**

1. Identify the sequence number of the record you want to delete:

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. Delete the security trace record:

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name -seqnum integer

vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
999
```

   ◦ `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.

     This is a required parameter.

   ◦ `-vserver vserver_name` is the name of the SVM on which the permission tracing event that you want to delete occurred.

This is a required parameter.

- ◦ `-seqnum integer` is the sequence number of the log event that you want to delete.

  This is a required parameter.

**Delete all security trace records**

If you do not want to keep any of the existing security trace records, you can delete all of the records on a node with a single command.

**Step**

1. Delete all security trace records:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name *
   ```

   - ◦ `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.
   - ◦ `-vserver vserver_name` is the name of the storage virtual machine (SVM) on which the permission tracing event that you want to delete occurred.

**Interpret security trace results**

Security trace results provide the reason that a request was allowed or denied. Output displays the result as a combination of the reason for allowing or denying access and the location within the access checking pathway where access is either allowed or denied. You can use the results to isolate and identify why actions are or are not allowed.

**Finding information about the lists of result types and filter details**

You can find the lists of result types and filter details that can be included in the security trace results in the man pages for the `vserver security trace trace-result show` command.

**Example of output from the** `Reason` **field in an** `Allow` **result type**

The following is an example of the output from the `Reason` field that appears in the trace results log in an `Allow` result type:

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

**Example of output from the** `Reason` **field in an** `Allow` **result type**

The following is an example of the output from the `Reason` field that appears in the trace results log in a `Deny` result type:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

**Example of output from the** `Filter details` **field**

The following is an example of the output from the `Filter details` field in the trace results log, which list the effective security style of the file system containing files and folders that match the filter criteria:

```
Security Style: MIXED and ACL
```

## Where to find additional information

After you have successfully tested SMB client access, you can perform advanced SMB configuration or add SAN access. After you have successfully tested NFS client access, you can perform advanced NFS configuration or add SAN access. When protocol access is complete, you should protect the root volume of SVM.

**SMB configuration**

You can further configure SMB access using the following:

- SMB management

  Describes how to configure and manage file access using the SMB protocol.

- NetApp Technical Report 4191: Best Practices Guide for Clustered Data ONTAP 8.2 Windows File Services

  Provides a brief overview of SMB implementation and other Windows File Services features with recommendations and basic troubleshooting information for ONTAP.

- NetApp Technical Report 3740: SMB 2 Next-Generation CIFS Protocol in Data ONTAP

  Describes SMB 2 features, configuration details, and its implementation in ONTAP.

**NFS configuration**

You can further configure NFS access using the following:

- NFS management

  Describes how to configure and manage file access using the NFS protocol.

- NetApp Technical Report 4067: NFS Best Practice and Implementation Guide

  Serves as an NFSv3 and NFSv4 operational guide and provides an overview of ONTAP operating system with a focus on NFSv4.

- NetApp Technical Report 4668: Name Services Best Practices Guide

Provides a comprehensive list of best practices, limits, recommendations, and considerations when configuring LDAP, NIS, DNS, and local user and group files for authentication purposes.

- NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory
- NetApp Technical Report 4835: How to Configure LDAP in ONTAP
- NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation

Describes the best practices that should be followed while implementing NFSv4 components on AIX, Linux, or Solaris clients attached to systems running ONTAP.

**Root volume protection**

After configuring protocols on the SVM, you should ensure that its root volume is protected:

- Data protection

Describes how to create a load-sharing mirror to protect the SVM root volume, which is a NetApp best practice for NAS-enabled SVMs. Also describes how to quickly recover from volume failures or losses by promoting the SVM root volume from a load-sharing mirror.

# Manage encryption with System Manager

## Encrypt stored data using software-based encryption

Use volume encryption to ensure that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Volume encryption does not require special disks; it works with all HDDs and SSDs.

Volume encryption requires a key manager. You can configure the Onboard Key Manager using System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

After the key manager is configured, new volumes are encrypted by default.

**Steps**
1. Click **Cluster > Settings**.
2. Under **Encryption**, click ⚙ to configure the Onboard Key Manager for the first time.
3. To encrypt existing volumes, click **Storage > Volumes**.
4. On the desired volume, click ⋮ and then click **Edit**.
5. Select **Enable encryption**.

## Encrypt stored data using self-encrypting drives

Use disk encryption to ensure that all data in a local tier cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Disk encryption requires special self-encrypting HDDs or SSDs.

Disk encryption requires a key manager. You can configure the onboard key manager using System Manager.

You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

If ONTAP detects self-encrypting disks, it prompts you to configure the onboard key manager when you create the local tier.

**Steps**

1. Under **Encryption**, click ⚙ to configure the onboard key manager.

2. If you see a message that disks need to be rekeyed, click ⋮, and then click **Rekey Disks**.

# Manage encryption with the CLI

## NetApp Encryption overview with the CLI

NetApp offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

- Software-based encryption using NetApp Volume Encryption (NVE) supports data encryption one volume at a time

- Hardware-based encryption using NetApp Storage Encryption (NSE) supports full-disk encryption (FDE) of data as it is written.

You can work with encryption if the following apply:

- You want to use best practices, not explore every available option.

- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.

## Configure NetApp Volume Encryption

### Configure NetApp Volume Encryption overview

NetApp Volume Encryption (NVE) is a software-based technology for encrypting data at rest one volume at a time. An encryption key accessible only to the storage system ensures that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen.

### Understanding NVE

Both data, including Snapshot copies, and metadata are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume. An external key management server or Onboard Key Manager serves keys to nodes:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). It is a best practice to configure external key management servers on a different storage system from your data.

- The Onboard Key Manager is a built-in tool that serves keys to nodes from the same storage system as your data.

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume

encryption (VE) license and use an onboard or external key manager. Whenever an external or onboard key manager is configured there is a change in how the encryption of data at rest is configured for brand new aggregates and brand new volumes. Brand new aggregates will have NetApp Aggregate Encryption (NAE) enabled by default. Brand new volumes that are not part of an NAE aggregate will have NetApp Volume Encryption (NVE) enabled by default. If a data storage virtual machine (SVM) is configured with its own key-manager using multi-tenant key management, then the volume created for that SVM is automatically configured with NVE.

You can enable encryption on a new or existing volume. NVE supports the full range of storage efficiency features, including deduplication and compression.

> ⓘ  If you are using SnapLock, you can enable encryption only on new, empty SnapLock volumes. You cannot enable encryption on an existing SnapLock volume.

You can use NVE on any type of aggregate (HDD, SSD, hybrid, array LUN), with any RAID type, and in any supported ONTAP implementation, including ONTAP Select. You can also use NVE with hardware-based encryption to "double encrypt" data on self-encrypting drives.

> ⓘ  AFF A220, AFF A800, FAS2720, FAS2750, and later systems store core dumps on their boot device. When NVE is enabled on these systems, the core dump is also encrypted.

**Aggregate-level encryption**

Ordinarily, every encrypted volume is assigned a unique key. When the volume is deleted, the key is deleted with it.

Beginning with ONTAP 9.6, you can use *NetApp Aggregate Encryption (NAE)* to assign keys to the containing aggregate for the volumes to be encrypted. When an encrypted volume is deleted, the keys for the aggregate are preserved. The keys are deleted if the entire aggregate is deleted.

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager.

NVE and NAE volumes can coexist on the same aggregate. Volumes encrypted under aggregate-level encryption are NAE volumes by default. You can override the default when you encrypt the volume.

You can use the `volume move` command to convert an NVE volume to an NAE volume, and vice versa. You can replicate an NAE volume to an NVE volume.

You cannot use `secure purge` commands on an NAE volume.

**When to use external key management servers**

Although it is less expensive and typically more convenient to use the onboard key manager, you should set up KMIP servers if any of the following are true:

- Your encryption key management solution must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
- You need a multi-cluster solution, with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location

different from the data.

**Scope of external key management**

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.

- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a named SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.

- Beginning with ONTAP 9.10.1, you can use Azure Key Vault and Google Cloud KMS to protect NVE keys only for data vservers.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

A list of validated external key managers is available in the NetApp Interoperability Matrix Tool (IMT). You can find this list by entering the term "key managers" into the IMT's search feature.

**Support details**

The following table shows NVE support details:

| Resource or feature | Support details |
|---|---|
| Platforms | AES-NI offload capability required. See the Hardware Universe (HWU) to verify that NVE and NAE are supported for your platform. |
| Encryption | Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you add a volume encryption (VE) license and have an onboard or external key manager configured. If you need to create an unencrypted aggregate, use the following command: <br><br> `storage aggregate create -encrypt-with-aggr-key false` <br><br> If you need to create a plain text volume, use the following command: <br><br> `volume create -encrypt false` <br><br> Encryption is not enabled by default when: <br><br> • VE license is not installed. <br> • Key manager is not configured. <br> • Platform or software does not support encryption. <br> • Hardware encryption is enabled. |

| | |
|---|---|
| ONTAP | All ONTAP implementations. Support for ONTAP Cloud is available in ONTAP 9.5 and later. |
| Devices | HDD, SSD, hybrid, array LUN. |
| RAID | RAID0, RAID4, RAID-DP, RAID-TEC. |
| Volumes | Data volumes and existing root volumes. You cannot encrypt data on an SVM root volume or MetroCluster metadata volumes. |
| Aggregate-level encryption | Beginning with ONTAP 9.6, NVE supports aggregate-level encryption (NAE):<br><br>• You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication.<br><br>• You cannot rekey an aggregate-level encryption volume.<br><br>• Secure-purge is not supported on aggregate-level encryption volumes.<br><br>• In addition to data volumes, NAE supports encryption of SVM root volumes and the MetroCluster metadata volume. NAE does not support encryption of the root volume. |
| SVM scope | Beginning with ONTAP 9.6, NVE supports SVM scope for external key management only, not for Onboard Key Manager. MetroCluster is supported beginning with ONTAP 9.8. |
| Storage efficiency | Deduplication, compression, compaction, FlexClone. Clones use the same key as the parent, even after splitting the clone from the parent. You are warned to rekey the split clone. |
| Replication | • For volume replication, the destination volume must have been enabled for encryption. Encryption can be configured for the source and unconfigured for the destination, and vice versa.<br><br>• For SVM replication, the destination volume is automatically encrypted, unless the destination does not contain a node that supports volume encryption, in which case replication succeeds, but the destination volume is not encrypted.<br><br>• For MetroCluster configurations, each cluster pulls external key management keys from its configured key servers. OKM keys are replicated to the partner site by the configuration replication service. |
| Compliance | Beginning with ONTAP 9.2, SnapLock is supported in both Compliance and Enterprise modes, for new volumes only. You cannot enable encryption on an existing SnapLock volume. |
| FlexGroups | Beginning with ONTAP 9.2, FlexGroups are supported. Destination aggregates must be of the same type as source aggregates, either volume-level or aggregate-level. Beginning with ONTAP 9.5, in-place rekey of FlexGroup volumes is supported. |

| 7-Mode transition | Beginning with 7-Mode Transition Tool 3.3, you can use the 7-Mode Transition Tool CLI to perform copy-based transition to NVE-enabled destination volumes on the clustered system. |
| --- | --- |

**Related information**

FAQ - NetApp Volume Encryption and NetApp Aggregate Encryption

**NetApp Volume Encryption workflow**

You must configure key management services before you can enable volume encryption. You can enable encryption on a new volume or on an existing volume.
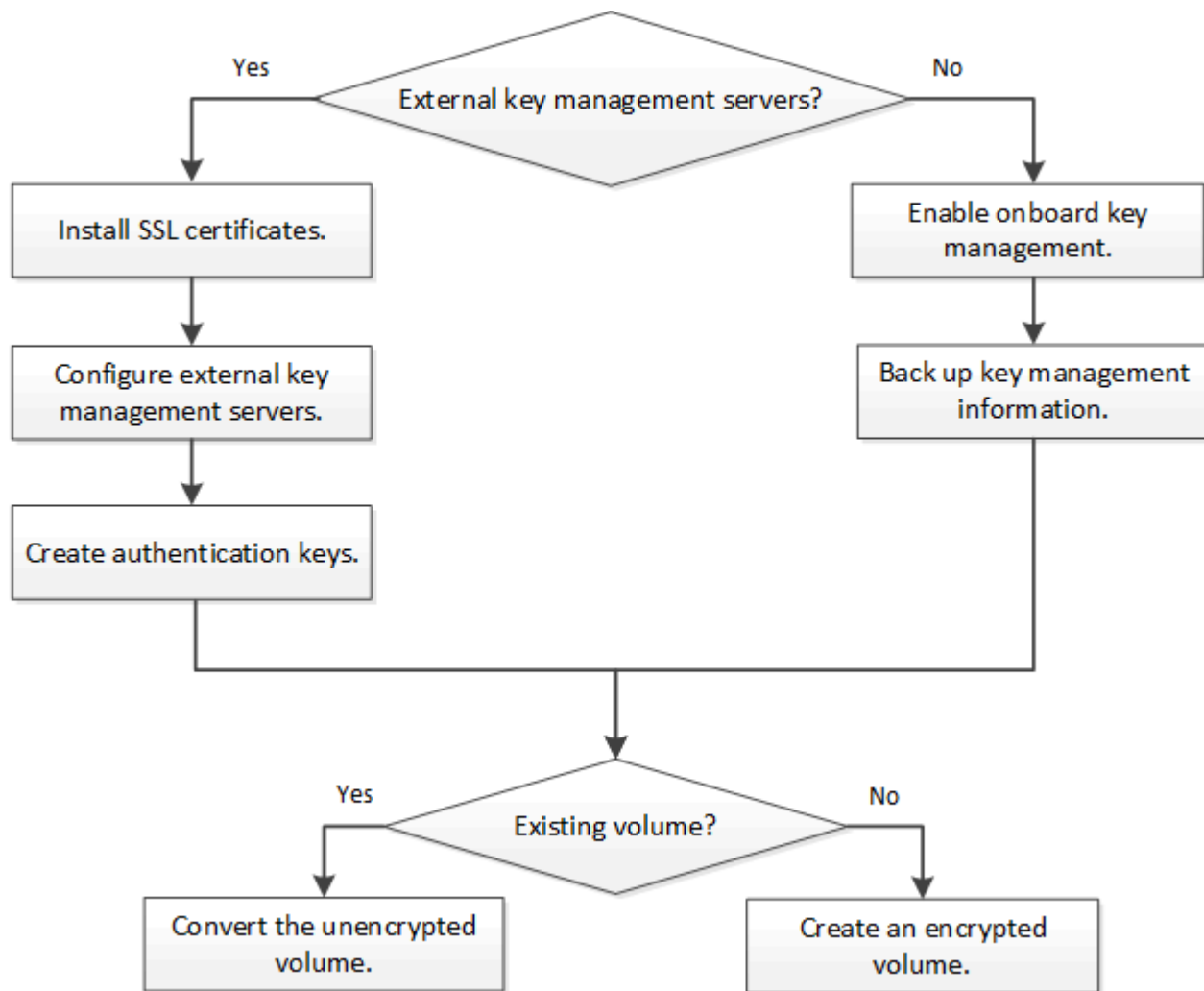


You must install the VE license and configure key management services before you can encrypt data with NVE. Before installing the license, you should determine whether your ONTAP version supports NVE.

**Configure NVE**

**Determine whether your cluster version supports NVE**

You should determine whether your cluster version supports NVE before you install the license. You can use the `version` command to determine the cluster version.

**About this task**

The cluster version is the lowest version of ONTAP running on any node in the cluster.

**Step**

1. Determine whether your cluster version supports NVE:

   `version -v`

   NVE is not supported if the command output displays the text "1Ono-DARE" (for "no Data At Rest Encryption"), or if you are using a platform that is not listed in Support details.

   The following command determines whether NVE is supported on `cluster1`.

   ```
   cluster1::> version -v
   NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
   ```

   The output of `1Ono-DARE` indicates that NVE is not supported on your cluster version.

**Install the license**

A VE license entitles you to use the feature on all nodes in the cluster. You must install the license before you can encrypt data with NVE.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

You should have received the VE license key from your sales representative.

**Steps**

1. Install the VE license for a node:

   `system license add -license-code license_key`

   The following command installs the license with the key AAAAAAAAAAAAAAAAAAAAAAAAAAAA.

   ```
   cluster1::> system license add -license-code
   AAAAAAAAAAAAAAAAAAAAAAAAAAAA
   ```

2. Verify that the license is installed by displaying all the licenses on the cluster:

   `system license show`

   For complete command syntax, see the man page for the command.

   The following command displays all the licenses on `cluster1`:

```
cluster1::> system license show
```

The VE license package name is "VE".

### Configure external key management

### Configure external key management overview

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).

> (i) For ONTAP 9.1 and earlier versions, node management LIFs must be assigned to ports that are configured with the node management role before you can use the external key manager.

NetApp Volume Encryption (NVE) supports Onboard Key Manager in ONTAP 9.1 and later. Beginning in ONTAP 9.3, NVE supports external key management (KMIP) and Onboard Key Manager. Beginning in ONTAP 9.10.1, you can use Azure Key Vault or Google Cloud Key Manager Service to protect your NVE keys. Beginning in ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See Configure clustered key servers.

### Install SSL certificates on the cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

**What you'll need**

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.
- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.

  The SSL KMIP client certificate must not be password-protected.

- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.
- In a MetroCluster environment, you must install the KMIP SSL certificate on both clusters.

> (i) You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

**About this task**

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

**Steps**

1. Install the SSL KMIP client certificates for the cluster:

```
security certificate install -vserver admin_svm_name -type client
```

You are prompted to enter the SSL KMIP public and private certificates.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

**Enable external key management in ONTAP 9.6 and later (NVE)**

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. Beginning with ONTAP 9.6, you have the option to configure a separate external key manager to secure the keys that a data SVM uses to access encrypted data.

Beginning in ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see Configure clustered external key servers.

**Before you begin**

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster or SVM administrator to perform this task.
- If you want to enable external key management for a MetroCluster environment, MetroCluster must be fully configured before enabling external key management.
- In a MetroCluster environment, you must install the KMIP SSL certificate on both clusters.

**About this task**

You can connect up to four KMIP servers to a cluster or SVM. A minimum of two servers is recommended for redundancy and disaster recovery.

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a data SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.
- For multitenant environments, install a license for *MT_EK_MGMT* by using the following command:

```
system license add -license-code <MT_EK_MGMT license code>
```

For complete command syntax, see the man page for the command.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM,

ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

You can configure onboard key management at the cluster scope and external key management at the SVM scope. You can use the `security key-manager key migrate` command to migrate keys from onboard key management at the cluster scope to external key managers at the SVM scope.

**Steps**

1. Configure key manager connectivity for the cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > ⓘ
   > - The `security key-manager external enable` command replaces the `security key-manager setup` command. If you run the command at the cluster login prompt, *admin_SVM* defaults to the admin SVM of the current cluster. You must be the cluster administrator to configure cluster scope. You can run the `security key-manager external modify` command to change the external key management configuration.
   > - In a MetroCluster environment, if you are configuring external key management for the admin SVM, you must repeat the `security key-manager external enable` command on the partner cluster.

   The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

   ```
   clusterl::> security key-manager external enable -vserver cluster1 -key
   -servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. Configure a key manager an SVM:

   ```
   security key-manager external enable -vserver SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > ⓘ
   > - If you run the command at the SVM login prompt, SVM defaults to the current SVM. You must be a cluster or SVM administrator to configure SVM scope. You can run the `security key-manager external modify` command to change the external key management configuration.
   > - In a MetroCluster environment, if you are configuring external key management for a data SVM, you do not have to repeat the `security key-manager external enable` command on the partner cluster.

   The following command enables external key management for `svm1` with a single key server listening on the default port 5696:

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Repeat the last step for any additional SVMs.

> (i) You can also use the `security key-manager external add-servers` command to configure additional SVMs. The `security key-manager external add-servers` command replaces the `security key-manager add` command. For complete command syntax, see the man page.

4. Verify that all configured KMIP servers are connected:

```
security key-manager external show-status -node node_name
```

> (i) The `security key-manager external show-status` command replaces the `security key-manager show -status` command. For complete command syntax, see the man page.

```
cluster1::> security key-manager external show-status

Node   Vserver  Key Server                                         Status
----   -------  -------------------------------------  ------------
node1
       svm1
                keyserver.svm1.com:5696                            available
       cluster1
                10.0.0.10:5696                                     available
                fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
                ks1.local:15696                                    available
node2
       svm1
                keyserver.svm1.com:5696                            available
       cluster1
                10.0.0.10:5696                                     available
                fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
                ks1.local:15696                                    available

8 entries were displayed.
```

**Enable external key management in ONTAP 9.5 and earlier**

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two

servers is recommended for redundancy and disaster recovery.

**What you'll need**

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.
- In a MetroCluster environment, you must install the KMIP SSL certificate on both clusters.

**About this task**

ONTAP configures KMIP server connectivity for all nodes in the cluster.

**Steps**

1. Configure key manager connectivity for cluster nodes:

   ```
   security key-manager setup
   ```

   The key manager setup starts.

   > ℹ️ In a MetroCluster environment, you must run this command on both clusters.

2. Enter the appropriate response at each prompt.

3. Add a KMIP server:

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   > ℹ️ In a MetroCluster environment, you must run this command on both clusters.

4. Add an additional KMIP server for redundancy:

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   > ℹ️ In a MetroCluster environment, you must run this command on both clusters.

5. Verify that all configured KMIP servers are connected:

   ```
   security key-manager show -status
   ```

   For complete command syntax, see the man page.

```
cluster1::> security key-manager show -status

Node            Port     Registered Key Manager   Status
-------------   ----     ----------------------   ---------------
cluster1-01     5696     20.1.1.1                 available
cluster1-01     5696     20.1.1.2                 available
cluster1-02     5696     20.1.1.1                 available
cluster1-02     5696     20.1.1.2                 available
```

**Manage keys with Azure Key Vault or Google Cloud KMS**

Beginning in ONTAP 9.10.1, you can use Azure Key Vault (AKV) and Google Cloud Platform's Key Management Service (Cloud KMS) to protect your ONTAP encryption keys in a Azure- or Google Cloud Platform-deployed application.

AKV and Cloud KMS can be used to protect NetApp Volume Encryption (NVE) keys only for data SVMs.

Key management with AKV or Cloud KMS can be enabled with the CLI or the ONTAP REST API.

When using AKV or Cloud KMS, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com for Azure; oauth2.googleapis.com for Cloud KMS). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

**Prerequisites**
- The ONTAP cluster's nodes must support NVE
- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed
- You must be a cluster or SVM administrator

**Limitations**
- AKV and Cloud KMS are not available for NSE and NAE. External KMIPs can be used instead
- AKV and Cloud KMS are not available for MetroCluster configurations.
- AKV and Cloud KMS can only be configured on a data SVM

**Enable external key management with the CLI**

Enabling external key management depends on the specific key manager you use. If you are enabling AKV in a Cloud Volumes ONTAP, note that there is a separate procedure. Choose the tab of the key manager and environment that suits your needs:

**Azure**

**Enable Azure Key Vault for ONTAP**

1. Before you begin, you need to obtain the appropriate authentication credentials from your Azure account, either a client secret or certificate.
   You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`.

2. Set privileged level to advanced
   ```
   set -priv advanced
   ```

3. Enable AKV on the SVM
   ```
   security key-manager external azure enable -client-id client_id -tenant-id
   tenant_id -name -key-id key_id -authentication-method {certificate|client-
   secret}
   ```
   When prompted, enter either the client certificate or client secret from your Azure account.

4. Verify AKV is enabled correctly:
   ```
   security key-manager external azure show vserver SVM_name
   ```
   If the service reachability is not OK, establish the connectivity to the AKV key management service via data SVM LIF.

**Google Cloud**

**Enable Cloud KMS with the CLI for ONTAP**

1. Before you begin, you need to obtain the private key for the Google Cloud KMS account key file in a JSON format. This can be found in your GCP account.
   You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`.

2. Set privileged level to advanced
   ```
   set -priv advanced
   ```

3. Enable Cloud KMS on the SVM
   ```
   security key-manager external gcp enable -vserver data_svm_name -project-id
   project_id-key-ring-name key_ring_name -key-ring-location key_ring_location
   -key-name key_name
   ```
   When prompted, enter the contents of the JSON file with the Service Account Private Key

4. Verify that Cloud KMS is configured with the correct parameters:
   ```
   security key-manager external gcp show vserver SVM_name
   ```
   The status of `kms_wrapped_key_status` will be "`UNKNOWN`" if no encrypted volumes have been created.
   If the service reachability is not OK, establish the connectivity to the GCP key management service via data SVM LIF.

If one or more encrypted volumes is already configured for a data SVM and the corresponding NVE keys are managed by the admin SVM onboard key manager, those keys should be migrated to the external key management service. To do this with the CLI, run the command:

```
security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM
```
New encrypted volumes cannot be created for the tenant's data vserver until all NVE keys of the data SVM are successfully migrated.

**Enable onboard key management in ONTAP 9.6 and later (NVE)**

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

**What you'll need**

- You must be a cluster administrator to perform this task.

- You must configure the MetroCluster environment before you configure an external key manager.

**About this task**

You must run the `security key-manager onboard sync` command each time you add a node to the cluster.

If you have a MetroCluster configuration you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. You can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

When configuring ONTAP data at rest encryption, to meet the requirements for Commercial Solutions for Classified (CSfC) you must use NSE with NVE and ensure the Onboard Key Manager is enabled in Common Criteria mode. Refer to the CSfC Solution Brief for more information on CSfC.

> (i) When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:
>
> - The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.
>
>   If you fail to enter the correct cluster passphrase at boot, encrypted volumes are not mounted. To correct this, you must reboot the node and enter the correct cluster passphrase. Once booted, the system allows up to 5 consecutive attempts to correctly enter the cluster passphrase in a 24-hour period for any command that requires the cluster passphrase as a parameter. If the limit is reached (for example, you have failed to correctly enter the cluster passphrase 5 times in a row) then you must either wait for the 24-hour timeout period to elapse, or you must reboot the node, in order to reset the limit.
>
> - System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.
>
>   The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The image update process proceeds to the next step if validation succeeds; otherwise, the image update fails. See the "cluster image" man page for information concerning system updates.

(i) The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. Under normal operating conditions, volatile memory contents will be cleared within 30s when a system is halted.

**Steps**

1. Start the key manager setup:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

(i) Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. The `-cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

The following example starts the key manager setup command on cluster1 without requiring that the passphrase be entered after every reboot:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for "cc-mode", a passphrase between 64 and 256 characters.

(i) If the specified "cc-mode" passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

3. At the passphrase confirmation prompt, reenter the passphrase.

4. Verify that the authentication keys have been created:

```
security key-manager key query -key-type NSE-AK
```

(i) The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page.

The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
        Vserver: cluster1
   Key Manager: onboard
          Node: node1
```

```
Key Tag                              Key Type  Restored
-----------------------------------  --------  --------
node1                                NSE-AK    yes
    Key ID:
00000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                NSE-AK    yes
    Key ID:
00000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000


      Vserver: svm1
   Key Manager: onboard
         Node: node1
   Key Server: keyserver.svm1.com:5965

Key Tag                              Key Type  Restored
-----------------------------------  --------  --------
eb9f8311-e8d8-487e-9663-7642d7788a75 VEK       yes
    Key ID:
00000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e00000000
00000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb VEK       yes
    Key ID:
00000000000000002000000000004064f2e1533356a470385274a9c3ffb97700000000
00000000


      Vserver: cluster1
   Key Manager: onboard
         Node: node2

Key Tag                              Key Type  Restored
-----------------------------------  --------  --------
node1                                NSE-AK    yes
    Key ID:
00000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                NSE-AK    yes
    Key ID:
00000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000


      Vserver: svm1
   Key Manager: onboard
         Node: node2
   Key Server: keyserver.svm1.com:5965
```

```
Key Tag                                 Key Type   Restored
--------------------------------------  --------   --------
eb9f8311-e8d8-487e-9663-7642d7788a75    VEK        yes
    Key ID:
000000000000000002000000000000004001cb18336f7c8223743d3e75c6a7726e00000000
00000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb    VEK        yes
    Key ID:
000000000000000002000000000000004064f2e1533356a470385274a9c3ffb97700000000
00000000
```

**After you finish**

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up the information manually for use in case of a disaster.

**Enable onboard key management in ONTAP 9.5 and earlier (NVE)**

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

**What you'll need**

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.

- You must configure the MetroCluster environment before you configure the Onboard Key Manager.

**About this task**

You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.

- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume`

`move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

> (i) After a failed passphrase attempt, you must reboot the node again.

**Steps**

1. Start the key manager setup:

   `security key-manager setup -enable-cc-mode yes|no`

   > (i) Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc -mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted.

   The following example starts setting up the key manager on cluster1 without requiring that the passphrase be entered after every reboot:

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. Enter `yes` at the prompt to configure onboard key management.

3. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for "cc-mode", a passphrase between 64 and 256 characters.

   > (i) If the specified "cc-mode" passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

4. At the passphrase confirmation prompt, reenter the passphrase.

5. Verify that keys are configured for all nodes:

   `security key-manager key show`

   For the complete command syntax, see the man page.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                             Used By
-----------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
0000000000000000200000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                             Used By
-----------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
0000000000000000200000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

**After you finish**

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See Back up onboard key management information manually.

**Enable onboard key management in newly added nodes**

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

(i) For ONTAP 9.5 and earlier, you must run the `security key-manager setup` command each time you add a node to the cluster.

For ONTAP 9.6 and later, you must run the `security key-manager sync` command each time you add a node to the cluster.

If you add a node to a cluster that has onboard key management configured, you will run this command to refresh the missing keys.

If you have a MetroCluster configuration, review these guidelines:

- Beginning with ONTAP 9.6, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.

- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

> (i) After a failed passphrase attempt, you must reboot the node again.

**Encrypt volume data with NVE**

### Encrypt volume data with NVE overview

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default when you have the VE license and onboard or external key management. For ONTAP 9.6 and earlier, you can enable encryption on a new volume or on an existing volume. You must have installed the VE license and enabled key management before you can enable volume encryption. NVE is FIPS-140-2 level 1 compliant.

### Enable aggregate-level encryption with VE license

Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you have the VE license and onboard or external key management. Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

An aggregate enabled for aggregate-level encryption is called an *NAE aggregate* (for NetApp Aggregate Encryption). All volumes in an NAE aggregate must be encrypted with NAE or NVE encryption. With aggregate-level encryption, volumes you create in the aggregate are encrypted with NAE encryption by default. You can override the default to use NVE encryption instead.

Plain text volumes are not supported in NAE aggregates.

**Steps**

1. Enable or disable aggregate-level encryption:

| To… | Use this command… |
|------|-------------------|
| Create an NAE aggregate with ONTAP 9.7 or later | `storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* |
| Create an NAE aggregate with ONTAP 9.6 | `storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with` `-aggr-key true` |
| Convert a non-NAE aggregate to an NAE aggregate | `storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with` `-aggr-key true` |
| Convert an NAE aggregate to a non-NAE aggregate | `storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with` `-aggr-key false` |

For complete command syntax, see the man pages.

The following command enables aggregate-level encryption on `aggr1`:

- ◦ ONTAP 9.7 or later:

  ```
  cluster1::> storage aggregate create -aggregate aggr1
  ```

- ◦ ONTAP 9.6 or earlier:

  ```
  cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
  -aggr-key true
  ```

2. Verify that the aggregate is enabled for encryption:

   ```
   storage aggregate show -fields encrypt-with-aggr-key
   ```

   For complete command syntax, see the man page.

   The following command verifies that `aggr1` is enabled for encryption:

   ```
   cluster1::> storage aggregate show -fields encrypt-with-aggr-key
   aggregate            encrypt-aggr-key
   -------------------- ----------------
   aggr0_vsim4          false
   aggr1                true
   2 entries were displayed.
   ```

**After you finish**

Run the `volume create` command to create the encrypted volumes.

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically "pushes" an encryption key to the server when you encrypt a volume.

**Enable encryption on a new volume**

You can use the `volume create` command to enable encryption on a new volume.

**About this task**

You can encrypt volumes using NetApp Volume Encryption (NVE) and, beginning with ONTAP 9.6, NetApp Aggregate Encryption (NAE). To learn more about NAE and NVE, refer to the volume encryption overview.

The procedure to enable encryption on a new volume in ONTAP varies based on the version of ONTAP you are using and your specific configuration:

- Beginning with ONTAP 9.4, if you enable `cc-mode` when you set up the Onboard Key Manager, volumes you create with the `volume create` command are automatically encrypted, whether or not you specify `-encrypt true`.

- In ONTAP 9.6 and earlier releases, you must use `-encrypt true` with `volume create` commands to enable encryption (provided you did not enable `cc-mode`).

- If you want to create an NAE volume in ONTAP 9.6, you must enable NAE at the aggregate level. Refer to Enable aggregate-level encryption with the VE license for more details on this task.

- Beginning with ONTAP 9.7, newly created volumes are encrypted by default when you have the VE license and onboard or external key management. By default, new volumes created in an NAE aggregate will be of type NAE rather than NVE.

  ◦ In ONTAP 9.7 and later releases, if you add `-encrypt true` to the `volume create` command to create a volume in an NAE aggregate, the volume will have NVE encryption instead of NAE. All volumes in an NAE aggregate must be encrypted with either NVE or NAE.

ⓘ  Plaintext volumes are not supported in NAE aggregates.

**Steps**

1. Create a new volume and specify whether encryption is enabled on the volume. If the new volume is in an NAE aggregate, by default the volume will be an NAE volume:

| To create… | Use this command… |
|---|---|
| An NAE volume | `volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name` |

| An NVE volume | `volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true +` |
|---|---|
| | (i) In ONTAP 9.6 and earlier where NAE is not supported, `-encrypt true` specifies that the volume should be encrypted with NVE. In ONTAP 9.7 and later where volumes are created in NAE aggregates, `-encrypt true` overrides the default encryption type of NAE to create an NVE volume instead. |
| A plain text volume | `volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false` |

For complete command syntax, refer to the command reference page for `volume create`.

2. Verify that volumes are enabled for encryption:

`volume show -is-encrypted true`

For complete command syntax, see the command reference.

**Result**

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically "pushes" an encryption key to the server when you encrypt a volume.

**Enable encryption on an existing volume with the volume encryption conversion start command**

Beginning with ONTAP 9.3, you can use the `volume encryption conversion start` command to enable encryption of an existing volume "in place," without having to move the volume to a different location.

**About this task**

Once you start a conversion operation, it must complete. If you encounter a performance issue during the operation, you can run the `volume encryption conversion pause` command to pause the operation, and the `volume encryption conversion resume` command to resume the operation.

(i) You cannot use `volume encryption conversion start` to convert a SnapLock volume.

**Steps**

1. Enable encryption on an existing volume:

`volume encryption conversion start -vserver SVM_name -volume volume_name`

For complete command syntax, see the man page for the command.

The following command enables encryption on the existing volume `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

The system creates an encryption key for the volume. The data on the volume is encrypted.

2. Verify the status of the conversion operation:

`volume encryption conversion show`

For complete command syntax, see the man page for the command.

The following command displays the status of the conversion operation:

```
cluster1::> volume encryption conversion show

Vserver   Volume   Start Time          Status
-------   ------   ------------------  ---------------------------
vs1       vol1     9/18/2017 17:51:41  Phase 2 of 2 is in progress.
```

3. When the conversion operation is complete, verify that the volume is enabled for encryption:

`volume show -is-encrypted true`

For complete command syntax, see the man page for the command.

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate   State    Type  Size   Available   Used
-------   ------   ---------   -----    ----  -----  ---------   ----
vs1       vol1     aggr2       online    RW   200GB    160.0GB   20%
```

**Result**

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically "pushes" an encryption key to the server when you encrypt a volume.

**Enable encryption on an existing volume with the volume move start command**

You can use the `volume move start` command to enable encryption by moving an existing volume. You must use `volume move start` in ONTAP 9.2 and earlier. You can use the same aggregate or a different aggregate.

**What you'll need**

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

Delegating authority to run the volume move command

**About this task**

Beginning with ONTAP 9.8, you can use `volume move start` to enable encryption on a SnapLock or

FlexGroup volume.

Beginning with ONTAP 9.4, if you enable "cc-mode" when you set up the Onboard Key Manager, volumes you create with the `volume move start` command are automatically encrypted. You need not specify `-encrypt -destination true`.

Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be moved. A volume encrypted with a unique key is called an *NVE volume*. A volume encrypted with an aggregate-level key is called an *NAE volume* (for NetApp Aggregate Encryption). Plaintext volumes are not supported in NAE aggregates.

**Steps**

1. Move an existing volume and specify whether encryption is enabled on the volume:

| To convert… | Use this command… |
|---|---|
| A plaintext volume to an NVE volume | `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true` |
| An NVE or plaintext volume to an NAE volume (assuming aggregate-level encryption is enabled on the destination) | `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true` |
| An NAE volume to an NVE volume | `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false` |
| An NAE volume to a plaintext volume | `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false` |
| An NVE volume to a plaintext volume | `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false` |

For complete command syntax, see the man page for the command.

The following command converts a plaintext volume named `vol1` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Assuming aggregate-level encryption is enabled on the destination, the following command converts an NVE or plaintext volume named `vol1` to an NAE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

The following command converts an NAE volume named `vol2` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

The following command converts an NAE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

The following command converts an NVE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. View the encryption type of cluster volumes:

   `volume show -fields encryption-type none|volume|aggregate`

   The `encryption-type` field is available in ONTAP 9.6 and later.

   For complete command syntax, see the man page for the command.

   The following command displays the encryption type of volumes in `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver   volume  encryption-type
-------   ------  ---------------
vs1       vol1    none
vs2       vol2    volume
vs3       vol3    aggregate
```

3. Verify that volumes are enabled for encryption:

   `volume show -is-encrypted true`

   For complete command syntax, see the man page for the command.

   The following command displays the encrypted volumes on `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  ----- ---------  ----
vs1      vol1    aggr2      online   RW  200GB   160.0GB  20%
```

**Result**

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically "pushes" an encryption key to the server when you encrypt a volume.

**Enable node root volume encryption**

Beginning with ONTAP 9.8, you can use NetApp Volume Encryption to protect the root volume of your node.

**What you'll need**

- Your system must be using an HA configuration.

  Root volume encryption is not supported on single node configurations.

- Your node root volume must already be created.

- Your system must have an onboard key manager or an external key management server using the Key Management Interoperability Protocol (KMIP).

> ⓘ **About this task**
>
> This procedure applies to the node root volume. It does not apply to SVM root volumes. SVM root volumes can be protected through aggregate-level encryption.

Once root volume encryption begins, it must complete. You cannot pause the operation. Once encryption is complete, you cannot assign a new key to the root volume and you cannot perform a secure-purge operation.

**Steps**

1. Encrypt the root volume:

   `volume encryption conversion start -vserver SVM_name -volume root_vol_name`

2. Verify the status of the conversion operation:

   `volume encryption conversion show`

3. When the conversion operation is complete, verify that the volume is encrypted:

   `volume show -fields`

   The following shows example output for an encrypted volume.

```
::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
vserver     volume is-encrypted
---------- ------ ------------
xyz        vol0    true
```

## Configure NetApp hardware-based encryption

### Configure NetApp hardware-based encryption overview

NetApp hardware-based encryption supports full-disk encryption (FDE) of data as it is written. The data cannot be read without an encryption key stored on the firmware. The encryption key, in turn, is accessible only to an authenticated node.

### Understanding NetApp hardware-based encryption

A node authenticates itself to a self-encrypting drive using an authentication key retrieved from an external key management server or Onboard Key Manager:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). It is a best practice to configure external key management servers on a different storage system from your data.

- The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data.

You can use NetApp Volume Encryption with hardware-based encryption to "double encrypt" data on self-encrypting drives.

AFF A220, AFF A800, FAS2720, FAS2750, and later systems store core dumps on their boot device. When self-encrypting drives are enabled on these systems, the core dump is also encrypted.

> (i) If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow the instructions in the topic Returning a FIPS drive or SED to unprotected mode for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

### Supported self-encrypting drive types

Two types of self-encrypting drives are supported:

- Self-encrypting FIPS-certified SAS or NVMe drives are supported on all FAS and AFF systems. These drives, called *FIPS drives,* conform to the requirements of Federal Information Processing Standard Publication 140-2, level 2. The certified capabilities enable protections in addition to encryption, such as preventing denial-of-service attacks on the drive. FIPS drives cannot be mixed with other types of drives on the same node or HA pair.

- Beginning with ONTAP 9.6, self-encrypting NVMe drives that have not undergone FIPS testing are supported on AFF A800, A320, and later systems. These drives, called *SEDs*, offer the same encryption capabilities as FIPS drives, but can be mixed with non-encrypting drives on the same node or HA pair.

- All FIPS validated drives use a firmware cryptographic module that has been through FIPS validation. The FIPS drive cryptographic module does not use any keys that are generated outside of the drive (the

authentication passphrase that is input to the drive is used by the drive's firmware cryptographic module to obtain a key encryption key).

ⓘ     Non-encrypting drives are drives that are not SEDs or FIPS drives.

**When to use external key management**

Although it is less expensive and typically more convenient to use the onboard key manager, you should use external key management if any of the following are true:

- Your organization's policy requires a key management solution that uses a FIPS 140-2 Level 2 (or higher) cryptographic module.
- You need a multi-cluster solution, with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location different from the data.

**Support details**

The following table shows important hardware encryption support details. See the Interoperability Matrix for the latest information about supported KMIP servers, storage systems, and disk shelves.

| Resource or feature | Support details |
|---|---|
| Non-homogeneous disk sets | • FIPS drives cannot be mixed with other types of drives on the same node or HA pair. Conforming HA pairs can coexist with non-conforming HA pairs in the same cluster.<br>• SEDs can be mixed with non-encrypting drives on the same node or HA pair. |
| Drive type | • FIPS drives can be SAS or NVMe drives.<br>• SEDs must be NVMe drives. |
| 10 Gb network interfaces | Beginning with ONTAP 9.3, KMIP key management configurations support 10 Gb network interfaces for communications with external key management servers. |
| Ports for communication with the key management server | Beginning with ONTAP 9.3, you can use any storage controller port for communication with the key management server. Otherwise, you should use port e0M for communication with key management servers. Depending on the storage controller model, certain network interfaces might not be available during the boot process for communication with key management servers. |
| MetroCluster (MCC) | • NVMe drives support MCC.<br>• SAS drives do not support MCC. |

**Related information**

- NetApp Hardware Universe
- NetApp Volume Encryption and NetApp Aggregate Encryption

## Hardware-based encryption workflow

You must configure key management services before the cluster can authenticate itself to the self-encrypting drive. You can use an external key management server or an onboard key manager.
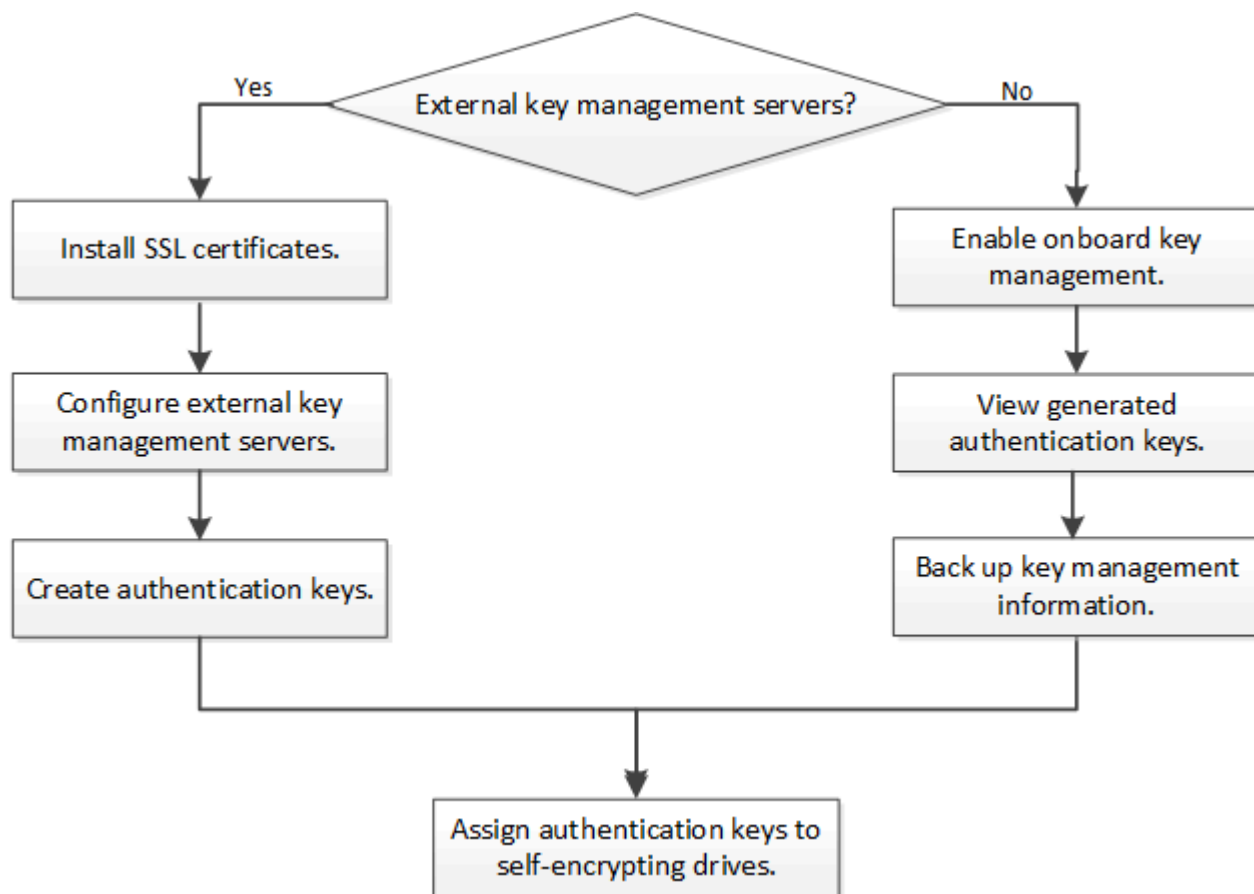


## Configure external key management

### Configure external key management overview

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).

For ONTAP 9.1 and earlier versions, node management LIFs must be assigned to ports that are configured with the node management role before you can use the external key manager.

NetApp Volume Encryption (NVE) can be implemented with Onboard Key Manager in ONTAP 9.1 and later. In ONTAP 9.3 and later, NVE can be implemented with external key management (KMIP) and Onboard Key Manager. Beginning in ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See Configure clustered key servers.

### Collect network information in ONTAP 9.2 and earlier

If you are using ONTAP 9.2 or earlier, you should fill out the network configuration

worksheet before enabling external key management.

ℹ️ Beginning with ONTAP 9.3, the system discovers all needed network information automatically.

| Item | Notes | Value |
|------|-------|-------|
| Key management network interface name | | |
| Key management network interface IP address | IP address of node management LIF, in IPv4 or IPv6 format | |
| Key management network interface IPv6 network prefix length | If you are using IPv6, the IPv6 network prefix length | |
| Key management network interface subnet mask | | |
| Key management network interface gateway IP address | | |
| IPv6 address for the cluster network interface | Required only if you are using IPv6 for the key management network interface | |
| Port number for each KMIP server | Optional. The port number must be the same for all KMIP servers. If you do not provide a port number, it defaults to port 5696, which is the Internet Assigned Numbers Authority (IANA) assigned port for KMIP. | |
| Key tag name | Optional. The key tag name is used to identify all keys belonging to a node. The default key tag name is the node name. | |

**Related information**

NetApp Technical Report 3954: NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager

NetApp Technical Report 4074: NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure

**Install SSL certificates on the cluster**

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public

certificate for the root certificate authority (CA) of the KMIP server.

**What you'll need**

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.
- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.

  The SSL KMIP client certificate must not be password-protected.

- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.
- In a MetroCluster environment, you must install the KMIP SSL certificate on both clusters.

> ⓘ    You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

**About this task**

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

**Steps**

1. Install the SSL KMIP client certificates for the cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   You are prompted to enter the SSL KMIP public and private certificates.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

**Enable external key management in ONTAP 9.6 and later (HW-based)**

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

Beginning in ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see Configure clustered external key servers.

**Before you begin**

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.
- In a MetroCluster environment, you must install the KMIP SSL certificate on both clusters.

**Steps**

1. Configure key manager connectivity for the cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > ⓘ
   > ◦ The `security key-manager external enable` command replaces the `security key-manager setup` command. You can run the `security key-manager external modify` command to change the external key management configuration. For complete command syntax, see the man pages.
   > ◦ In a MetroCluster environment, if you are configuring external key management for the admin SVM, you must repeat the `security key-manager external enable` command on the partner cluster.

   The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

   ```
   clusterl::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. Verify that all configured KMIP servers are connected:

   ```
   security key-manager external show-status -node node_name -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

   > ⓘ The `security key-manager external show-status` command replaces the `security key-manager show -status` command. For complete command syntax, see the man page.

```
cluster1::> security key-manager external show-status

Node   Vserver  Key Server                                           Status
----   -------  -------------------------------------------
             ------------
node1
       cluster1
                 10.0.0.10:5696                                      available
                 fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
                 ks1.local:15696                                    available
node2
       cluster1
                 10.0.0.10:5696                                      available
                 fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
                 ks1.local:15696                                    available

6 entries were displayed.
```

**Enable external key management in ONTAP 9.5 and earlier**

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

**What you'll need**

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.
- In a MetroCluster environment, you must install the KMIP SSL certificate on both clusters.

**About this task**

ONTAP configures KMIP server connectivity for all nodes in the cluster.

**Steps**

1. Configure key manager connectivity for cluster nodes:

   `security key-manager setup`

   The key manager setup starts.

   ⓘ  In a MetroCluster environment, you must run this command on both clusters.

2. Enter the appropriate response at each prompt.

3. Add a KMIP server:

   `security key-manager add -address key_management_server_ipaddress`

```
clusterl::> security key-manager add -address 20.1.1.1
```

> ℹ️ In a MetroCluster environment, you must run this command on both clusters.

4. Add an additional KMIP server for redundancy:

`security key-manager add -address key_management_server_ipaddress`

```
clusterl::> security key-manager add -address 20.1.1.2
```

> ℹ️ In a MetroCluster environment, you must run this command on both clusters.

5. Verify that all configured KMIP servers are connected:

`security key-manager show -status`

For complete command syntax, see the man page.

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager   Status
-------------   ----      ----------------------   ---------------
cluster1-01     5696      20.1.1.1                 available
cluster1-01     5696      20.1.1.2                 available
cluster1-02     5696      20.1.1.1                 available
cluster1-02     5696      20.1.1.2                 available
```

**Configure clustered external key servers**

Beginning in ONTAP 9.11.1, you can configure connectivity to clustered external key management servers on an SVM. With clustered key servers, you can designate primary and secondary key servers on a SVM. When registering keys, ONTAP will first attempt to access a primary key server before sequentially attempting to access secondary servers until the operation completes successfully, preventing duplication of keys.

External key servers can be used for NSE, NVE, NAE, and SED keys. An SVM can support up to four primary external KMIP servers. Each primary server can support up to three secondary key servers.

**Before you begin**

- KMIP key management is already enabled for the SVM.
- This process only supports key servers that use KMIP. For a list of supported key servers, check the NetApp Interoperability Matrix Tool.
- All nodes in the cluster must be running ONTAP 9.11.1 or later.

- The order of servers list arguments in the `-secondary-key-servers` parameter reflects the access order of the external key management (KMIP) servers.

## Create a clustered key server

The configuration procedure depends on whether or not you have configured a primary key server.

**Add primary and secondary key servers to an SVM**

1. Confirm that no key management has been enabled for the cluster:
   `security key-manager external show -vserver vserver_name`
   If the SVM already has the maximum of four primary key servers enabled, you must remove one of the existing primary key servers before adding a new one.

2. Enable the primary key manager:
   `security key-manager external enable -vserver vserver_name -key-servers server_ip -client-cert client_cert_name -server-ca-certs server_ca_cert_names`

3. Modify the primary key server to add secondary key servers. The `-secondary-key-servers` parameter accepts a comma-separated list of up to three key servers.
   `security key-manager external modify-server -vserver vserver_name -key-servers primary_key_server -secondary-key-servers list_of_key_servers`

**Add secondary key servers to an existing primary key server**

1. Modify the primary key server to add secondary key servers. The `-secondary-key-servers` parameter accepts a comma-separated list of up to three key servers.
   `security key-manager external modify-server -vserver vserver_name -key-servers primary_key_server -secondary-key-servers list_of_key_servers`
   For more information about secondary key servers, see Modifying secondary key servers.

## Modify clustered key servers

You can modify external key servers clusters by changing the status (primary or secondary) of particular key servers, add and removing secondary key servers, or by changing the access order of secondary key servers.

## Converting primary and secondary key servers

To convert a primary key server into a secondary key server, you must first remove it from the SVM with the `security key-manager external remove-servers` command.

To convert a secondary key server into a primary key server, you must first remove the secondary key server from its existing primary key server. See Modifying secondary key servers. If you convert a secondary key server to a primary server while removing an existing key, attempting to add a new server before completing the removal and conversion can result in the the duplication of keys.

## Modifying secondary key servers

Secondary key servers are managed with the `-secondary-key-servers` parameter of the `security key-manager external modify-server` command. The `-secondary-key-servers` parameter accepts a comma-separated list. The specified order of the secondary key servers in the list determines the access sequence for the secondary key servers. The access order can be modified by running the command `security key-manager external modify-server` with the secondary key servers entered in a

different sequence.

To remove a secondary key server, the `-secondary-key-servers` arguments should include the key servers you want to keep while omitting the one to be removed. To remove all secondary key servers, use the argument `–`, signifying none.

For additional information, refer to the `security key-manager external` page in the ONTAP command reference.

**Create authentication keys in ONTAP 9.6 and later**

You can use the `security key-manager key create` command to create the authentication keys for a node and store them on the configured KMIP servers.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

ONTAP creates authentication keys for all nodes in the cluster.

- This command is not supported when Onboard Key Manager is enabled. However, two authentication keys are created automatically when Onboard Key Manager is enabled. The keys can be viewed with the following command:

  `security key-manager key query -key-type NSE-AK`

- You receive a warning if the configured key management servers are already storing more than 128 authentication keys.

- You can use the `security key-manager key delete` command to delete any unused keys. The `security key-manager key delete` command fails if the given key is currently in use by ONTAP. (You must have privileges greater than "admin" to use this command.)

  > In a MetroCluster environment, before you delete a key, you must make sure that the key is not in use on the partner cluster. You can use the following commands on the partner cluster to check that the key is not in use:
  >
  > ° `storage encryption disk show -data-key-id` *key-id*
  > ° `storage encryption disk show -fips-key-id` *key-id*

**Steps**

1. Create the authentication keys for cluster nodes:

   `security key-manager key create -key-tag passphrase_label -prompt-for-key true|false`

Setting `prompt-for-key=true` causes the system to prompt the cluster administrator for the passphrase to use when authenticating encrypted drives. Otherwise, the system automatically generates a 32-byte passphrase. The `security key-manager key create` command replaces the `security key-manager create-key` command. For complete command syntax, see the man page.

The following example creates the authentication keys for `cluster1`, automatically generating a 32-byte passphrase:

```
cluster1::> security key-manager key create
Key ID:
000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

2. Verify that the authentication keys have been created:

```
security key-manager key query -node node
```

The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page. The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager key query
        Vserver: cluster1
    Key Manager: external
          Node: node1

Key Tag                              Key Type   Restored
------------------------------------ --------   --------
node1                                NSE-AK     yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                NSE-AK     yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000


        Vserver: cluster1
    Key Manager: external
          Node: node2

Key Tag                              Key Type   Restored
------------------------------------ --------   --------
node2                                NSE-AK     yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                NSE-AK     yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

**Create authentication keys in ONTAP 9.5 and earlier**

You can use the `security key-manager create-key` command to create the authentication keys for a node and store them on the configured KMIP servers.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

ONTAP creates authentication keys for all nodes in the cluster.

- This command is not supported when onboard key management is enabled.

- You receive a warning if the configured key management servers are already storing more than 128 authentication keys.

  You can use the key management server software to delete any unused keys, then run the command again.

**Steps**

1. Create the authentication keys for cluster nodes:

   `security key-manager create-key`

   For complete command syntax, see the man page for the command.

   > ⓘ The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

   The following example creates the authentication keys for `cluster1`:

   ```
   cluster1::> security key-manager create-key
       (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. Verify that the authentication keys have been created:

   `security key-manager query`

   For complete command syntax, see the man page.

   The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager query

   (security key-manager query)

         Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
-------------   --------  --------
cluster1-01     NSE-AK    yes
      Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


         Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
-------------   --------  --------
cluster1-02     NSE-AK    yes
      Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

**Assign a data authentication key to a FIPS drive or SED (external key management)**

You can use the `storage encryption disk modify` command to assign a data authentication key to a FIPS drive or SED. Cluster nodes use this key to lock or unlock encrypted data on the drive.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

A self-encrypting drive is protected from unauthorized access only if its authentication key ID is set to a non-default value. The manufacturer secure ID (MSID), which has key ID 0x0, is the standard default value for SAS drives. For NVMe drives, the standard default value is a null key, represented as a blank key ID. When you assign the key ID to a self-encrypting drive, the system changes its authentication key ID to a non-default value.

**Steps**

1. Assign a data authentication key to a FIPS drive or SED:

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   For complete command syntax, see the man page for the command.

> **(i)** You can use the `security key-manager query -key-type NSE-AK` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

Info: Starting modify on 14 disks.
        View the status of the operation by using the
        storage encryption disk show-status command.
```

2. Verify that the authentication keys have been assigned:

`storage encryption disk show`

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
[...]
```

### Configure onboard key management

**Enable onboard key management in ONTAP 9.6 and later**

You can use the Onboard Key Manager to authenticate cluster nodes to a FIPS drive or SED. The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data. The Onboard Key Manager is FIPS-140-2 level 1 compliant.

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

**What you'll need**

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.

- You must configure the MetroCluster environment before the Onboard key manager is configured.

**About this task**

You must run the `security key-manager onboard enable` command each time you add a node to the cluster. In MetroCluster configurations, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Except in MetroCluster, you can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

> When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:
>
> - The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.
>
>   If NetApp Storage Encryption (NSE) is enabled and you fail to enter the correct cluster passphrase at boot, the system cannot authenticate to its drives and automatically reboots. To correct this, you must enter the correct cluster passphrase at the boot prompt. Once booted, the system allows up to 5 consecutive attempts to correctly enter the cluster passphrase in a 24-hour period for any command that requires the cluster passphrase as a parameter. If the limit is reached (for example, you have failed to correctly enter the cluster passphrase 5 times in a row) then you must either wait for the 24-hour timeout period to elapse, or you must reboot the node, in order to reset the limit.
>
> - System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.
>
>   The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The image update process proceeds to the next step if validation succeeds; otherwise, the image update fails. See the "cluster image" man page for information concerning system updates.

> The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. Under normal operating conditions, volatile memory contents will be cleared within 30s when a system is halted.

**Steps**

1. Start the key manager setup command:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   > Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. The `-cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

   The following example starts the key manager setup command on cluster1 without requiring that the passphrase be entered after every reboot:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for "cc-mode", a passphrase between 64 and 256 characters.

> (i)   If the specified "cc-mode" passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

3. At the passphrase confirmation prompt, reenter the passphrase.

4. Verify that the authentication keys have been created:

`security key-manager key query -node node`

> (i)   The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page.

The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager key query
        Vserver: cluster1
    Key Manager: onboard
            Node: node1

Key Tag                                  Key Type   Restored
-------------------------------------    --------   --------
node1                                    NSE-AK     yes
    Key ID:
000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK     yes
    Key ID:
000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000


        Vserver: cluster1
    Key Manager: onboard
            Node: node2

Key Tag                                  Key Type   Restored
-------------------------------------    --------   --------
node1                                    NSE-AK     yes
    Key ID:
000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK     yes
    Key ID:
000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

**After you finish**

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up the information manually for use in case of a disaster.

**Enable onboard key management in ONTAP 9.5 and earlier**

You can use the Onboard Key Manager to authenticate cluster nodes to a FIPS drive or SED. The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data. The Onboard Key Manager is FIPS-140-2 level 1 compliant.

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting

disk.

**What you'll need**

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.

- You must configure the MetroCluster environment before the Onboard Key Manager is configured.

**About this task**

You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.

- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

> (i) After a failed passphrase attempt, you must reboot the node again.

**Steps**

1. Start the key manager setup:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > (i) Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc -mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted.

   The following example starts setting up the key manager on cluster1 without requiring that the passphrase be entered after every reboot:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Enter `yes` at the prompt to configure onboard key management.

3. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for "cc-mode", a passphrase between 64 and 256 characters.

> (i) If the specified "cc-mode" passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

4. At the passphrase confirmation prompt, reenter the passphrase.

5. Verify that keys are configured for all nodes:

`security key-manager key show`

For the complete command syntax, see the man page.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                           Used By
----------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
----------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

**After you finish**

All key management information is automatically backed up to the replicated database (RDB) for the cluster.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See Back up onboard key management information manually.

**Assign a data authentication key to a FIPS drive or SED (onboard key management)**

You can use the `storage encryption disk modify` command to assign a data authentication key to a FIPS drive or SED. Cluster nodes use this key to access data on the drive.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

A self-encrypting drive is protected from unauthorized access only if its authentication key ID is set to a non-default value. The manufacturer secure ID (MSID), which has key ID 0x0, is the standard default value for SAS drives. For NVMe drives, the standard default value is a null key, represented as a blank key ID. When you assign the key ID to a self-encrypting drive, the system changes its authentication key ID to a non-default value.

**Steps**

1. Assign a data authentication key to a FIPS drive or SED:

   ```
   storage encryption disk modify -disk disk_ID -data-key-id key_ID
   ```

   For complete command syntax, see the man page for the command.

   > (i) You can use the `security key-manager key query -key-type NSE-AK` command to view key IDs.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. Verify that the authentication keys have been assigned:

   ```
   storage encryption disk show
   ```

   For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
---------------------------------------------------------------
0.0.0   data
0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

**Assign a FIPS 140-2 authentication key to a FIPS drive**

You can use the `storage encryption disk modify` command with the `-fips-key`
`-id` option to assign a FIPS 140-2 authentication key to a FIPS drive. Cluster nodes use
this key for drive operations other than data access, such as preventing denial-of-service
attacks on the drive.

**What you'll need**

The drive firmware must support FIPS 140-2 compliance. The NetApp Interoperability Matrix Tool contains
information about supported drive firmware versions.

**About this task**

Your security setup may require you to use different keys for data authentication and FIPS 140-2
authentication. If that is not the case, you can use the same authentication key for FIPS compliance that you
use for data access.

**Steps**

1. You must first ensure you have assigned a data authentication key. This can be done with using an
   external key manager or an onboard key manager. Verify the key is assigned with the command `storage`
   `encryption disk show`.

2. Assign a FIPS 140-2 authentication key to SEDs:

   `storage encryption disk modify -disk` *disk_id* `-fips-key-id`
   *fips_authentication_key_id*

   You can use the `security key-manager query` command to view key IDs.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   6A1E21D80000000001000000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. Verify that the authentication key has been assigned:

```
storage encryption disk show -fips
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
         ----------------------------------------------------------------
2.10.0  full
6A1E21D80000000001000000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D80000000001000000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

**Enable cluster-wide FIPS-compliant mode for KMIP server connections**

You can use the `security config modify` command with the `-is-fips-enabled` option to enable cluster-wide FIPS-compliant mode for data in flight. Doing so forces the cluster to use OpenSSL in FIPS mode when connecting to KMIP servers.

**Before you begin**
- The storage controller must be configured in FIPS-compliant mode.
- All KMIP servers must support TLSv1.2. The system requires TLSv1.2 to complete the connection to the KMIP server when cluster-wide FIPS-compliant mode is enabled.

**About this task**

When you enable cluster-wide FIPS-compliant mode, the cluster will automatically use only TLS1.2 and FIPS-validated cipher suites. Cluster-wide FIPS-compliant mode is disabled by default.

You must reboot cluster nodes manually after modifying the cluster-wide security configuration.

**Steps**
1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Verify that TLSv1.2 is supported:

   ```
   security config show -supported-protocols
   ```

   For complete command syntax, see the man page.

```
cluster1::> security config show
         Cluster                                              Cluster
Security
Interface FIPS Mode  Supported Protocols    Supported Ciphers Config
Ready
--------- ---------- ---------------------- -----------------
---------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:        yes
                                            !aNULL:!EXP:
                                            !eNULL
```

3. Enable cluster-wide FIPS-compliant mode:

```
security config modify -is-fips-enabled true -interface SSL
```

For complete command syntax, see the man page.

4. Reboot cluster nodes manually.

5. Verify that cluster-wide FIPS-compliant mode is enabled:

```
security config show
```

```
cluster1::> security config show
         Cluster                                              Cluster
Security
Interface FIPS Mode  Supported Protocols    Supported Ciphers Config
Ready
--------- ---------- ---------------------- -----------------
---------------
SSL       true       TLSv1.2, TLSv1.1       ALL:!LOW:         yes
                                            !aNULL:!EXP:
                                            !eNULL:!RC4
```

## Manage NetApp encryption

### Unencrypt volume data

You can use the `volume move start` command to move and unencrypt volume data.

**What you'll need**

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

[Delegating authority to run the volume move command](#)

**Steps**

1. Move an existing encrypted volume and unencrypt the data on the volume:

   ```
   volume move start -vserver SVM_name -volume volume_name -destination-aggregate
   aggregate_name -encrypt-destination false
   ```

   For complete command syntax, see the man page for the command.

   The following command moves an existing volume named `vol1` to the destination aggregate `aggr3` and unencrypts the data on the volume:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   The system deletes the encryption key for the volume. The data on the volume is unencrypted.

2. Verify that the volume is disabled for encryption:

   ```
   volume show -encryption
   ```

   For complete command syntax, see the man page for the command.

   The following command displays whether volumes on `cluster1` are encrypted:

   ```
   cluster1::> volume show -encryption

   Vserver   Volume   Aggregate   State    Encryption State
   -------   ------   ---------   -----    ----------------
   vs1       vol1     aggr1       online   none
   ```

**Move an encrypted volume**

You can use the `volume move start` command to move an encrypted volume. The moved volume can reside on the same aggregate or a different aggregate.

**What you'll need**

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

Delegating authority to run the volume move command

**About this task**

The move will fail if the destination node or destination volume does not support volume encryption.

The `-encrypt-destination` option for `volume move start` defaults to true for encrypted volumes. Requiring you to specify explicitly that you do not want the destination volume to be encrypted ensures that you do not inadvertently unencrypt the data on the volume.

**Steps**

1. Move an existing encrypted volume and leave the data on the volume encrypted:

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name`

   For complete command syntax, see the man page for the command.

   The following command moves an existing volume named `vol1` to the destination aggregate `aggr3` and leaves the data on the volume encrypted:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. Verify that the volume is enabled for encryption:

   `volume show -is-encrypted true`

   For complete command syntax, see the man page for the command.

   The following command displays the encrypted volumes on `cluster1`:

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State   Type  Size   Available   Used
   -------  ------  ---------  -----   ----  -----  ---------   ----
   vs1      vol1    aggr3      online   RW   200GB    160.0GB   20%
   ```

**Delegate authority to run the volume move command**

You can use the `volume move` command to encrypt an existing volume, move an encrypted volume, or unencrypt a volume. Cluster administrators can run `volume move` command themselves, or they can delegate the authority to run the command to SVM administrators.

**About this task**

By default, SVM administrators are assigned the `vsadmin` role, which does not include the authority to move volumes. You must assign the `vsadmin-volume` role to SVM administrators to enable them to run the `volume move` command.

**Step**

1. Delegate authority to run the `volume move` command:

   `security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role vsadmin-volume`

   For complete command syntax, see the man page for the command.

The following command grants the SVM administrator authority to run the `volume move` command.

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

**Change the encryption key for a volume with the volume encryption rekey start command**

It is a security best practice to change the encryption key for a volume periodically. Beginning with ONTAP 9.3, you can use the `volume encryption rekey start` command to change the encryption key.

**About this task**

Once you start a rekey operation, it must complete. There is no returning to the old key. If you encounter a performance issue during the operation, you can run the `volume encryption rekey pause` command to pause the operation, and the `volume encryption rekey resume` command to resume the operation.

Until the rekey operation finishes, the volume will have two keys. New writes and their corresponding reads will use the new key. Otherwise, reads will use the old key.

> ⓘ You cannot use `volume encryption rekey start` to rekey a SnapLock volume.

**Steps**

1. Change an encryption key:

   `volume encryption rekey start -vserver SVM_name -volume volume_name`

   The following command changes the encryption key for `vol1` on SVM`vs1`:

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. Verify the status of the rekey operation:

   `volume encryption rekey show`

   For complete command syntax, see the man page for the command.

   The following command displays the status of the rekey operation:

   ```
   cluster1::> volume encryption rekey show

   Vserver    Volume   Start Time           Status
   -------    ------   ------------------   --------------------------
   vs1        vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. When the rekey operation is complete, verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State   Type  Size  Available  Used
-------  ------  ---------  -----   ----  ----- ---------  ----
vs1      vol1    aggr2      online   RW   200GB   160.0GB  20%
```

**Change the encryption key for a volume with the volume move start command**

It is a security best practice to change the encryption key for a volume periodically. You can use the `volume move start` command to change the encryption key. You must use `volume move start` in ONTAP 9.2 and earlier. The moved volume can reside on the same aggregate or a different aggregate.

**What you'll need**

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

Delegating authority to run the volume move command

**About this task**

You cannot use `volume move start` to rekey a SnapLock or FlexGroup volume.

**Steps**

1. Move an existing volume and change the encryption key:

   ```
   volume move start -vserver SVM_name -volume volume_name -destination-aggregate
   aggregate_name -generate-destination-key true
   ```

   For complete command syntax, see the man page for the command.

   The following command moves an existing volume named **vol1** to the destination aggregate **aggr2** and changes the encryption key:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr2 -generate-destination-key true
   ```

   A new encryption key is created for the volume. The data on the volume remains encrypted.

2. Verify that the volume is enabled for encryption:

   ```
   volume show -is-encrypted true
   ```

For complete command syntax, see the man page for the command.

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  ----- ---------  ----
vs1      vol1    aggr2      online  RW   200GB    160.0GB  20%
```

**Rotate authentication keys for NetApp Storage Encryption**

You can rotate authentication keys when using NetApp Storage Encryption (NSE).

**About this task**

Rotating authentication keys in an NSE environment is supported if you are using External Key Manager (KMIP).

> (i) Rotating authentication keys in an NSE environment is not supported for Onboard Key Manager (OKM).

**Steps**

1. Use the `security key-manager create-key` command to generate new authentication keys.

   You need to generate new authentication keys before you can change the authentication keys.

2. Use the `storage encryption disk modify -disk * -data-key-id` command to change the authentication keys.

**Delete an encrypted volume**

You can use the `volume delete` command to delete an encrypted volume.

**What you'll need**

- You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

  [Delegating authority to run the volume move command](#)

- The volume must be offline.

**Step**

1. Delete an encrypted volume:

   `volume delete -vserver SVM_name -volume volume_name`

   For complete command syntax, see the man page for the command.

   The following command deletes an encrypted volume named `vol1`:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Enter `yes` when you are prompted to confirm deletion.

The system deletes the encryption key for the volume after 24 hours.

Use `volume delete` with the `-force true` option to delete a volume and destroy the corresponding encryption key immediately. This command requires advanced privileges. For more information, see the man page.

**After you finish**

You can use the `volume recovery-queue` command to recover a deleted volume during the retention period after issuing the `volume delete` command:

`volume recovery-queue SVM_name -volume volume_name`

How to use the Volume Recovery feature

**Securely purge data on an encrypted volume**

**Securely purge data on an encrypted volume overview**

Beginning with ONTAP 9.4, you can use secure purge to non-disruptively scrub data on NVE-enabled volumes. Scrubbing data on an encrypted volume ensures that it cannot be recovered from the physical media, for example, in cases of "spillage," where data traces may have been left behind when blocks were overwritten, or for securely deleting a vacating tenant's data.

Secure purge works only for previously deleted files on NVE-enabled volumes. You cannot scrub an unencrypted volume. You must use KMIP servers to serve keys, not the onboard key manager.

**Considerations for using secure purge**

- Volumes created in an aggregate enabled for NetApp Aggregate Encryption (NAE) do not support secure purge.
- Secure purge works only for previously deleted files on NVE-enabled volumes.
- You cannot scrub an unencrypted volume.
- You must use KMIP servers to serve keys, not the onboard key manager.

Secure purge functions differently depending upon your version of ONTAP.

**ONTAP 9.8 and later**

- Secure purge is supported by MetroCluster and FlexGroup.

- If the volume being purged is the source of a SnapMirror relationship, you do not have to break the SnapMirror relationship to perform a secure purge.

- The re-encryption method is different for volumes using SnapMirror data protection versus volumes not using SnapMirror data protection (DP) or those using SnapMirror extended data protection..

  - By default, volumes using SnapMirror data protection (DP) mode re-encrypt data using the volume move re-encryption method.

  - By default, volumes not using SnapMirror data protection or volumes using SnapMirror extended data protection (XDP) mode use the in-place re-encryption method.

  - These defaults can be changed using the `secure purge re-encryption-method [volume-move|in-place-rekey]` command.

- By default, all Snapshot copies in FlexVol volumes are automatically deleted during the secure purge operation. By default, Snapshots in FlexGroup volumes and volumes using SnapMirror data protection are not automatically deleted during the secure purge operation. These defaults can be changed using the `secure purge delete-all-snapshots [true|false]` command.

**ONTAP 9.7 and earlier:**

- Secure purge does not support the following:

  - FlexClone

  - SnapVault

  - FabricPool

- If the volume being purged is the source of a SnapMirror relationship, you must break the SnapMirror relationship before you can purge the volume.

  If there are busy Snapshot copies in the volume, you must release the Snapshot copies before you can purge the volume. For example, you may need to split a FlexClone volume from its parent.

- Successfully invoking the secure-purge feature triggers a volume move that re-encrypts the remaining, unpurged data with a new key.

  The moved volume remains on the current aggregate. The old key is automatically destroyed, ensuring that purged data cannot be recovered from the storage media.

**Securely purge data on an encrypted volume without a SnapMirror relationship**

Beginning with ONTAP 9.4, you can use secure-purge to non-disruptively "scrub" data on NVE-enabled volumes.

**What you'll need**

- You must be a cluster administrator to perform this task.

- Advanced privileges are required for this task.

**About this task**

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status

of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

> ⓘ In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

**Steps**

1. Delete the files or the LUN you want to securely purge.

   ◦ On a NAS client, delete the files you want to securely purge.

   ◦ On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.

2. On the storage system, change to advanced privilege level:

   `set -privilege advanced`

3. If the files you want to securely purge are in snapshots, delete the snapshots:

   `snapshot delete -vserver SVM_name -volume vol_name -snapshot`

4. Securely purge the deleted files:

   `volume encryption secure-purge start -vserver SVM_name -volume volume_name`

   The following command securely purges the deleted files on `vol1` on SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Verify the status of the secure-purge operation:

   `volume encryption secure-purge show`

**Securely purge data on an encrypted volume with an Asynchronous SnapMirror relationship**

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively "scrub" data on NVE-enabled volumes with an Asynchronous SnapMirror relationship.

**What you'll need**

- You must be a cluster administrator to perform this task.

- Advanced privileges are required for this task.

**About this task**

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

> **ⓘ** In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

**Steps**

1. On the storage system, change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Delete the files or the LUN you want to securely purge.

   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.

3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Repeat this step on each volume in your Asynchronous SnapMirror relationship.

4. If the files you want to securely purge are in Snapshot copies, delete the Snapshot copies:

   ```
   snapshot delete -vserver SVM_name -volume vol_name -snapshot
   ```

5. If the files you want to securely purge are in the base Snapshot copies, do the following:

   a. Create a Snapshot copy on the destination volume in the Asynchronous SnapMirror relationship:

   ```
   volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
   vol_name
   ```

   b. Update SnapMirror to move the base Snapshot copy forward:

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   Repeat this step for each volume in the Asynchronous SnapMirror relationship.

   c. Repeat steps (a) and (b) equal to the number of base Snapshot copies plus one.

   For example, if you have two base Snapshot copies, you should repeat steps (a) and (b) three times.

   d. Verify that the base Snapshot copy is present:

   ```
   snapshot show -vserver SVM_name -volume vol_name`
   ```

   e. Delete the base Snapshot copy:

   ```
   snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot
   ```

6. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Repeat this step on each volume in the Asynchronous SnapMirror relationship.

The following command securely purges the deleted files on "vol1" on SVM "vs1":

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. Verify the status of the secure purge operation:

```
volume encryption secure-purge show
```

**Scrub data on an encrypted volume with a Synchronous SnapMirror relationship**

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively "scrub" data on NVE-enabled volumes with a Synchronous SnapMirror relationship.

**What you'll need**
- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

**About this task**

A secure purge might take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

> ⓘ In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

**Steps**
1. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

2. Delete the files or the LUN you want to securely purge.
   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.

3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
-prepare true
```

Repeat this step for the other volume in your Synchronous SnapMirror relationship.

4. If the files you want to securely purge are in Snapshot copies, delete the Snapshot copies:

```
snapshot delete -vserver SVM_name -volume vol_A -snapshot snapshot
```

5. If the secure purge file is in the base or common Snapshot copies, update the SnapMirror to move the common Snapshot copy forward:

```
snapmirror update -source-snapshot snapshot_name -destination-path destination_path
```

There are two common Snapshot copies, so this command must be issued twice.

6. If the secure purge file is in the application-consistent Snapshot copy, delete the Snapshot copy on both volumes in the Synchronous SnapMirror relationship:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot
```

Perform this step on both volumes.

7. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Repeat this step on each volume in the synchronous SnapMirror relationship.

The following command securely purges the deleted files on "vol1" on SMV "vs1".

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

8. Verify the status of the secure purge operation:

```
volume encryption secure-purge show
```

**Change the onboard key management passphrase**

It is a security best practice to change the onboard key management passphrase periodically. You should copy the new onboard key management passphrase to a secure location outside the storage system for future use.

**What you'll need**
- You must be a cluster or SVM administrator to perform this task.
- Advanced privileges are required for this task.

**Steps**
1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Change the onboard key management passphrase:

| For this ONTAP version… | Use this command… |
| --- | --- |
| ONTAP 9.6 and later | `security key-manager onboard update-passphrase` |
| ONTAP 9.5 and earlier | `security key-manager update-passphrase` |

For complete command syntax, see the man pages.

The following ONTAP 9.6 command lets you change the onboard key management passphrase for `cluster1`:

```
clusterl::> security key-manager onboard update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key management for Vserver "cluster1".
Do you want to continue? {y|n}: y
Enter current passphrase:
Enter new passphrase:
```

3. Enter `y` at the prompt to change the onboard key management passphrase.

4. Enter the current passphrase at the current passphrase prompt.

5. At the new passphrase prompt, enter a passphrase between 32 and 256 characters, or for "cc-mode", a passphrase between 64 and 256 characters.

   If the specified "cc-mode" passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

6. At the passphrase confirmation prompt, reenter the passphrase.

**After you finish**

In a MetroCluster environment, you must update the passphrase on the partner cluster:

- In ONTAP 9.5 and earlier, you must run `security key-manager update-passphrase` with the same passphrase on the partner cluster.

- In ONTAP 9.6 and later, you are prompted to run `security key-manager onboard sync` with the same passphrase on the partner cluster.

You should copy the onboard key management passphrase to a secure location outside the storage system for future use.

You should back up key management information manually whenever you change the onboard key management passphrase.

Backing up onboard key management information manually

**Back up onboard key management information manually**

You should copy onboard key management information to a secure location outside the

storage system whenever you configure the Onboard Key Manager passphrase.

**What you'll need**

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

**About this task**

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up key management information manually for use in case of a disaster.

**Steps**

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Display the key management backup information for the cluster:

| For this ONTAP version… | Use this command… |
| --- | --- |
| ONTAP 9.6 and later | `security key-manager onboard show-backup` |
| ONTAP 9.5 and earlier | `security key-manager backup show` |

For complete command syntax, see the man pages.

+
The following 9.6 command displays the key management backup information for `cluster1`:

+

```
cluster1::> security key-manager onboard show-backup

                 --------------------------BEGIN BACKUP--------------------------
        TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAA
        QAAAAAAAABvOlH0AAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
        dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAACgAAAAAAAA
        3WTh7gAAAAAAAAAAAAAIAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAA
        IgAAAAAAAoAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAJAGr3tJA/LRzU
        QRHwv+1aWvAAAAAAAAACQAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
        BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
        AQAAAMAAAAYAQAAAAAADA5/ccAAAAAIgAAAAAAAoAAAAAAAAEOTcR0AAAAA
        AAAAAAAAAAAACAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAACIAAAAAAAA
        KAAAAAAAAACI8z/bAAAAAAAAAAAAAAgAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
        AAAAAAAAAAkAAAAAAAIAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
        LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAwAAABgBAAAAAAAA
        1cNLLwAAAAiAAAAAAAACgAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAkA
        ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAIgAAAAAAAoAAAAAAAAJ4/cQsAAAAA
        AAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAACQAAAAAAAA
        gAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
        rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                 --------------------------END BACKUP--------------------------
```

1. Copy the backup information to a secure location outside the storage system for use in case of a disaster.

**Restore onboard key management encryption keys**

If need to restore an onboard key management encryption key, you first verify that a key needs to be restored, then you can set up the Onboard Key Manager to restore the key.

**Before you begin**

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.

**Steps for ONTAP 9.6 and later**

1. Verify that the key needs to be restored:
   `security key-manager key query -node node`

2. If you are running ONTAP 9.8 and later, and your root volume is encrypted, complete Steps if the root volume is encrypted.

   If you are running ONTAP 9.6 or 9.7, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

3. Restore the key:
   `security key-manager onboard sync`

   For complete command syntax, see the man pages.

   The following ONTAP 9.6 command synchronize the keys in the onboard key hierarchy:

   ```
   cluster1::> security key-manager onboard sync

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   ```

4. At the passphrase prompt, enter the onboard key management passphrase for the cluster.

**Steps for ONTAP 9.5 and earlier**

1. Verify that the key needs to be restored:
   `security key-manager key show`

2. If you are running ONTAP 9.8 and later, and your root volume is encrypted, complete these steps:

   If you are running ONTAP 9.6 or 9.7, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

3. Restore the key:
   `security key-manager setup -node node`

   For complete command syntax, see the man pages.

4. At the passphrase prompt, enter the onboard key management passphrase for the cluster.

**Steps if the root volume is encrypted**

If you are running ONTAP 9.8 and later, and your root volume is encrypted, you must set an onboard key management recovery passphrase with the boot menu. This process is also necessary if you do a boot media replacement.

1. Boot the node to the boot menu and select option `(10) Set onboard key management recovery secrets`.

2. Enter `y` to use this option.

3. At the prompt, enter the onboard key management passphrase for the cluster.

4. At the prompt, enter the backup key data.

   The node returns to the boot menu.

5. From the boot menu, select option `(1) Normal Boot.`

**Restore external key management encryption keys**

You can manually restore external key management encryption keys and "push" them to a different node. You might want to do this if you are restarting a node that was down temporarily when you created the keys for the cluster.

**What you'll need**

You must be a cluster or SVM administrator to perform this task.

**About this task**

In ONTAP 9.6 and later, you can use the `security key-manager key query -node node_name` command to verify if your key needs to be restored.

In ONTAP 9.5 and earlier, you can use the `security key-manager key show` command to verify if your key needs to be restored.

**Steps**

1. If you are running ONTAP 9.8 or later and your root volume is encrypted, do the following:

   If you are running ONTAP 9.7 or earlier, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

   a. Set the bootargs:

      `setenv kmip.init.ipaddr <ip-address>`

      `setenv kmip.init.netmask <netmask>`

      `setenv kmip.init.gateway <gateway>`

      `setenv kmip.init.interface e0M`

      `boot_ontap`

   b. Boot the node to the boot menu and select option `(11) Configure node for external key management.`

   c. Follow prompts to enter management certificate.

      After all management certificate information is entered, the system returns to the boot menu.

   d. From the boot menu, select option `(1) Normal Boot.`

2. Restore the key:

| For this ONTAP version… | Use this command… |
|---|---|
| ONTAP 9.6 and later | `security key-manager external restore -vserver SVM -node node -key-server host_name|IP_address:port -key-id key_id -key-tag key_tag` |
| ONTAP 9.5 and earlier | `security key-manager restore -node node -address IP_address -key-id key_id -key-tag key_tag` |

> ⓘ  `node` defaults to all nodes. For complete command syntax, see the man pages. This command is not supported when onboard key management is enabled.

The following ONTAP 9.6 command restores external key management authentication keys to all nodes in `cluster1`:

```
cluster1::> security key-manager external restore
```

**Replace SSL certificates**

All SSL certificates have an expiration date. You must update your certificates before they expire to prevent loss of access to authentication keys.

**Before you begin**
- You must have obtained the replacement public certificate and private key for the cluster (KMIP client certificate).
- You must have obtained the replacement public certificate for the KMIP server (KMIP server-ca certificate).
- You must be a cluster or SVM administrator to perform this task.
- In a MetroCluster environment, you must replace the KMIP SSL certificate on both clusters.

> ⓘ  You can install the replacement client and server certificates on the KMIP server before or after installing the certificates on the cluster.

**Steps**
1. Install the new KMIP server-ca certificate:

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. Install the new KMIP client certificate:

   ```
   security certificate install -type client -vserver <>
   ```

3. Update the key manager configuration to use the newly installed certificates:

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   If you are running ONTAP 9.6 or later in a MetroCluster environment, and you want to modify the key

manager configuration on the admin SVM, you must run the command on both clusters in the configuration.

> (i) Updating the key manager configuration to use the newly installed certificates will return an error if the public/private keys of the new client certificate are different from the keys previously installed. See the Knowledge Base article The new client certificate public or private keys are different from the existing client certificate for instructions on how to override this error.

**Replace a FIPS drive or SED**

You can replace a FIPS drive or SED the same way you replace an ordinary disk. Make sure to assign new data authentication keys to the replacement drive. For a FIPS drive, you may also want to assign a new FIPS 140-2 authentication key.

> (i) If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow the instructions in the topic Returning a FIPS drive or SED to unprotected mode for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

**What you'll need**

- You must know the key ID for the authentication key used by the drive.

- You must be a cluster administrator to perform this task.

**Steps**

1. Ensure that the disk has been marked as failed:

   `storage disk show -broken`

   For complete command syntax, see the man page.

   ```
   cluster1::> storage disk show -broken
   Original Owner: cluster1-01
     Checksum Compatibility: block

                                                                 Usable
   Physical
       Disk    Outage Reason HA Shelf Bay Chan    Pool   Type     RPM      Size
   Size
       ------  ----  ------------  ----  ---  ----  ------  -----   -----   -------
   -------
       0.0.0   admin   failed   0b    1    0     A   Pool0   FCAL  10000   132.8GB
   133.9GB
       0.0.7   admin   removed 0b    2    6     A   Pool1   FCAL  10000   132.8GB
   134.2GB
       [...]
   ```

2. Remove the failed disk and replace it with a new FIPS drive or SED, following the instructions in the hardware guide for your disk shelf model.

3. Assign ownership of the newly replaced disk:

```
storage disk assign -disk disk_name -owner node
```

For complete command syntax, see the man page.

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Confirm that the new disk has been assigned:

```
storage encryption disk show
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
-----------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. Assign the data authentication keys to the FIPS drive or SED.

   Assigning a data authentication key to a FIPS drive or SED (external key management)

6. If necessary, assign a FIPS 140-2 authentication key to the FIPS drive.

   Assigning a FIPS 140-2 authentication key to a FIPS drive

**Make data on a FIPS drive or SED inaccessible**

**Make data on a FIPS drive or SED inaccessible overview**

If you want to make data on a FIPS drive or SED permanently inaccessible, but keep the drive's unused space available for new data, you can sanitize the disk. If you want to make data permanently inaccessible and you do not need to reuse the drive, you can destroy it.

- Disk sanitization

When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

- Disk destroy

When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the disk irreversibly. Doing so renders the disk permanently unusable and the data on it permanently inaccessible.

You can sanitize or destroy individual self-encrypting drives, or all the self-encrypting drives for a node.

### Sanitize a FIPS drive or SED

If you want to make data on a FIPS drive or SED permanently inaccessible, and use the drive for new data, you can use the `storage encryption disk sanitize` command to sanitize the drive.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

**Steps**

1. Migrate any data that needs to be preserved to an aggregate on another disk.

2. Delete the aggregate on the FIPS drive or SED to be sanitized:

   `storage aggregate delete -aggregate aggregate_name`

   For complete command syntax, see the man page.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identify the disk ID for the FIPS drive or SED to be sanitized:

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
----------------------------------------------------------------
0.0.0    data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1    data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.2   data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. If a FIPS drive is running in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID 0x0:

   `storage encryption disk modify -disk `*`disk_id`*` -fips-key-id 0x0`

   You can use the `security key-manager query` command to view key IDs.

   ```
   cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

   Info: Starting modify on 1 disk.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

5. Sanitize the drive:

   `storage encryption disk sanitize -disk `*`disk_id`*

   You can use this command to sanitize hot spare or broken disks only. To sanitize all disks regardless of type, use the `-force-all-state` option. For complete command syntax, see the man page.

   ⓘ   You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

   ```
   cluster1::> storage encryption disk sanitize -disk 1.10.2

   Warning: This operation will cryptographically sanitize 1 spare or
   broken self-encrypting disk on 1 node.
           To continue, enter sanitize disk: sanitize disk

   Info: Starting sanitize on 1 disk.
         View the status of the operation using the
         storage encryption disk show-status command.
   ```

**Destroy a FIPS drive or SED**

If you want to make data on a FIPS drive or SED permanently inaccessible and you do not need to reuse the drive, you can use the `storage encryption disk destroy` command to destroy the disk.

**What you'll need**

You must be a cluster administrator to perform this task.

**About this task**

When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the drive irreversibly. Doing so renders the disk virtually unusable and the data on it permanently inaccessible. However, you can reset the disk to its factory-configured settings using the physical secure ID (PSID) printed on the disk's label. For more information, see Returning a FIPS drive or SED to service when authentication keys are lost.

> (i) You should not destroy a FIPS drive or SED unless you have the Non-Returnable Disk Plus service (NRD Plus). Destroying a disk voids its warranty.

**Steps**

1. Migrate any data that needs to be preserved to an aggregate on another different disk.

2. Delete the aggregate on the FIPS drive or SED to be destroyed:

   `storage aggregate delete -aggregate aggregate_name`

   For complete command syntax, see the man page.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identify the disk ID for the FIPS drive or SED to be destroyed:

   `storage encryption disk show`

   For complete command syntax, see the man page.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   -------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Destroy the disk:

```
storage encryption disk destroy -disk disk_id
```

For complete command syntax, see the man page.

> ℹ️ You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

**Emergency shredding of data on a FIPS drive or SED**

In case of a security emergency, you can instantly prevent access to a FIPS drive or SED, even if power is not available to the storage system or the KMIP server.

**What you'll need**

- If you are using a KMIP server that has no available power, the KMIP server must be configured with an easily destroyed authentication item (for example, a smart card or USB drive).

- You must be a cluster administrator to perform this task.

**Step**

1. Perform emergency shredding of data on a FIPS drive or SED:

| If… | Then… |
|---|---|

| Power is available to the storage system and you have time to take the storage system offline gracefully | a. If the storage system is configured as an HA pair, disable takeover. |
| --- | --- |
| | b. Take all aggregates offline and delete them. |
| | c. Set the privilege level to advanced: |
| | `set -privilege advanced` |
| | d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID: |
| | `storage encryption disk modify -disk * -fips-key -id 0x0` |
| | e. Halt the storage system. |
| | f. Boot into maintenance mode. |
| | g. Sanitize or destroy the disks: |
| | ◦ If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks: |
| | `disk encrypt sanitize -all` |
| | ◦ If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks: |
| | `disk encrypt destroy disk_id1 disk_id2 …` |
| | ⓘ The `disk encrypt sanitize` and `disk encrypt destroy` commands are reserved for maintenance mode only. These commands must be run on each HA node, and are not available for broken disks. |
| | h. Repeat these steps for the partner node. This leaves the storage system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it. |

| Power is available to the storage system and you must shred the data immediately | a. **If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:** | a. **If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:** |
|---|---|---|
| | b. If the storage system is configured as an HA pair, disable takeover. | b. If the storage system is configured as an HA pair, disable takeover. |
| | c. Set the privilege level to advanced:<br><br>`set -privilege advanced` | c. Set the privilege level to advanced:<br><br>`set -privilege advanced` |
| | d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:<br><br>`storage encryption disk modify -disk * -fips-key-id 0x0`<br><br>e. Sanitize the disk:<br><br>`storage encryption disk sanitize -disk * -force-all-states true` | d. Destroy the disks:<br>`storage encryption disk destroy -disk * -force-all-states true` |
| | The storage system panics, leaving the system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it. | |
| Power is available to the KMIP server but not to the storage system | a. Log in to the KMIP server.<br><br>b. Destroy all keys associated with the FIPS drives or SEDs that contain the data you want to prevent access to.<br>This prevents access to disk encryption keys by the storage system. | |
| Power is not available to the KMIP server or the storage system | Destroy the authentication item for the KMIP server (for example, the smart card). This prevents access to disk encryption keys by the storage system. | |

For complete command syntax, see the man pages.

**Return a FIPS drive or SED to service when authentication keys are lost**

The system treats a FIPS drive or SED as broken if you lose the authentication keys for it permanently and cannot retrieve them from the KMIP server. Although you cannot access

or recover the data on the disk, you can take steps to make the SED's unused space available again for data.

**Before you begin**

You must be a cluster administrator to perform this task.

**About this task**

You should use this process only if you are certain that the authentication keys for the FIPS drive or SED are permanently lost and that you cannot recover them.

If the disks are partitioned, they must first be unpartitioned before you can start this process. include::../_include/unpartition-disk.adoc[]

**Steps**

1. Return a FIPS drive or SED to service:

| If the SEDS are… | Use these steps… |
|---|---|
| Not in FIPS-compliance mode, or in FIPS-compliance mode and the FIPS key is available | a. Set the privilege level to advanced:<br>`set -privilege advanced`<br><br>b. Reset the FIPS key to the default manufacture secure ID 0x0:<br>`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`<br><br>c. Verify the operation succeeded:<br>`storage encryption disk show-status`<br>If the operation failed, use the PSID process in this topic.<br><br>d. Sanitize the broken disk:<br>`storage encryption disk sanitize -disk disk_id`<br>Verify the operation succeeded with the command `storage encryption disk show-status` before proceeding to the next step.<br><br>e. Unfail the sanitized disk:<br>`storage disk unfail -spare true -disk disk_id`<br><br>f. Check whether the disk has an owner:<br>`storage disk show -disk disk_id`<br><br>g. If the disk does not have an owner, assign one, then unfail the disk again:<br>`storage disk assign -owner node -disk disk_id`<br>`storage disk unfail -spare true -disk disk_id`<br><br>h. Verify that the disk is now a spare and ready to be reused in an aggregate:<br>`storage disk show -disk disk_id` |

| In FIPS-compliance mode, the FIPS key is not available, and the SEDs have a PSID printed on the label | a. Obtain the PSID of the disk from the disk label.<br><br>b. Set the privilege level to advanced:<br>`set -privilege advanced`<br><br>c. Reset the disk to its factory-configured settings:<br>`storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id`<br>Verify the operation succeeded with the command `storage encryption disk show-status` before proceeding to the next step.<br><br>d. Unfail the sanitized disk:<br>`storage disk unfail -spare true -disk disk_id`<br><br>e. Check whether the disk has an owner:<br>`storage disk show -disk disk_id`<br><br>f. If the disk does not have an owner, assign one, then unfail the disk again:<br>`storage disk assign -owner node -disk disk_id`<br>`storage disk unfail -spare true -disk disk_id`<br><br>g. Verify that the disk is now a spare and ready to be reused in an aggregate:<br>`storage disk show -disk disk_id` |

For complete command syntax, see the man pages.

**Return a FIPS drive or SED to unprotected mode**

A FIPS drive or SED is protected from unauthorized access only if the authentication key ID for the node is set to a value other than the default. You can return a FIPS drive or SED to unprotected mode by using the `storage encryption disk modify` command to set the key ID to the default.

If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow this process for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

**What you'll need**

You must be a cluster administrator to perform this task.

**Steps**

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. If a FIPS drive is running in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID 0x0:

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Confirm the operation succeeded with the command:

`storage encryption disk show-status`

Repeat the show-status command until the numbers in "Disks Begun" and "Disks Done" are the same.

```
cluster1:: storage encryption disk show-status

             FIPS    Latest   Start                   Execution   Disks
Disks Disks
Node         Support Request  Timestamp               Time (sec)  Begun
Done  Successful
-------      ------- -------- ------------------      ----------  ------
------  ----------
cluster1     true    modify   1/18/2022 15:29:38      3               14      5
5
1 entry was displayed.
```

3. Set the data authentication key ID for the node back to the default MSID 0x0:

`storage encryption disk modify -disk disk_id -data-key-id 0x0`

The value of `-data-key-id` should be set to 0x0 whether you are returning a SAS or NVMe drive to unprotected mode.

You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Confirm the operation succeeded with the command:

`storage encryption disk show-status`

Repeat the show-status command until the numbers are the same. The operation is complete when the numbers in "disks begun" and "disks done" are the same.

**Maintenance mode**

Beginning with ONTAP 9.7, you can rekey a FIPS drive from maintenance mode. You should only use maintenance mode if you cannot use the ONTAP CLI instructions in the earlier section.

**Steps**

1. Set the FIPS authentication key ID for the node back to the default MSID 0x0:

   `disk encrypt rekey_fips 0x0 disklist`

2. Set the data authentication key ID for the node back to the default MSID 0x0:

   `disk encrypt rekey 0x0 disklist`

3. Confirm the FIPS authentication key was successfully rekeyed:

   `disk encrypt show_fips`

4. Confirm data authentication key was successfully rekeyed with:

   `disk encrypt show`

   Your output will likely display either the default MSID 0x0 key ID or the 64-character value held by the key server. The `Locked?` field refers to data-locking.

```
Disk        FIPS Key ID                     Locked?
----------  ---------------------------     -------
0a.01.0     0x0                                 Yes
```

**Remove an external key manager connection**

You can disconnect a KMIP server from a node when you no longer need the server. For example, you might disconnect a KMIP server when you are transitioning to volume encryption.

**What you'll need**

You must be a cluster or SVM administrator to perform this task.

**About this task**

When you disconnect a KMIP server from one node in an HA pair, the system automatically disconnects the server from all cluster nodes.

> (i) If you plan to continue using external key management after disconnecting a KMIP server, make sure another KMIP server is available to serve authentication keys.

**Step**

1. Disconnect a KMIP server from the current node:

| For this ONTAP version… | Use this command… |
|---|---|
| ONTAP 9.6 and later | `security key-manager external remove-servers -vserver SVM -key-servers host_name|IP_address:port,…` |
| ONTAP 9.5 and earlier | `security key-manager delete -address key_management_server_ipaddress` |

In a MetroCluster environment, you must repeat these commands on both clusters for the admin SVM.

For complete command syntax, see the man pages.

The following ONTAP 9.6 command disables the connections to two external key management servers for `cluster1`, the first named `ks1`, listening on the default port 5696, the second with the IP address 10.0.0.20, listening on port 24482:

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

**Modify external key management server properties**

Beginning with ONTAP 9.6, you can use the `security key-manager external modify-server` command to change the I/O timeout and user name of an external key management server.

**Before you begin**
- You must be a cluster or SVM administrator to perform this task.
- Advanced privileges are required for this task.
- In a MetroCluster environment, you must repeat these steps on both clusters for the admin SVM.

**Steps**
1. On the storage system, change to advanced privilege level:

   `set -privilege advanced`

2. Modify external key manager server properties for the cluster:

   `security key-manager external modify-server -vserver admin_SVM -key-server host_name|IP_address:port,… -timeout 1…60 -username user_name`

   > The timeout value is expressed in seconds. If you modify the user name, you are prompted to enter a new password. If you run the command at the cluster login prompt, *admin_SVM* defaults to the admin SVM of the current cluster. You must be the cluster administrator to modify external key manager server properties.

The following command changes the timeout value to 45 seconds for the `cluster1` external key management server listening on the default port 5696:

```
clusterl::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

3. Modify external key manager server properties for an SVM (NVE only):

```
security key-manager external modify-server -vserver SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> (i) The timeout value is expressed in seconds. If you modify the user name, you are prompted to enter a new password. If you run the command at the SVM login prompt, *SVM* defaults to the current SVM. You must be the cluster or SVM administrator to modify external key manager server properties.

The following command changes the username and password of the `svm1` external key management server listening on the default port 5696:

```
svml::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. Repeat the last step for any additional SVMs.

**Transition to external key management from onboard key management**

If you want to switch to external key management from onboard key management, you must delete the onboard key management configuration before you can enable external key management.

**What you'll need**

- For hardware-based encryption, you must reset the data keys of all FIPS drives or SEDs to the default value.

  Returning a FIPS drive or SED to unprotected mode

- For software-based encryption, you must unencrypt all volumes.

  Unencrypting volume data

- You must be a cluster administrator to perform this task.

**Step**

1. Delete the onboard key management configuration for a cluster:

| For this ONTAP version… | Use this command… |
| --- | --- |

| ONTAP 9.6 and later | `security key-manager onboard disable -vserver SVM` |
|---|---|
| ONTAP 9.5 and earlier | `security key-manager delete-key-database` |

For complete command syntax, see the ONTAP manual pages.

**Transition to onboard key management from external key management**

If you want to switch to onboard key management from external key management, you must delete the external key management configuration before you can enable onboard key management.

**Before you begin**

- For hardware-based encryption, you must reset the data keys of all FIPS drives or SEDs to the default value.

  Returning a FIPS drive or SED to unprotected mode

- You must have deleted all external key manager connections.

  Deleting an external key manager connection

- You must be a cluster administrator to perform this task.

**Procedure**

> **ONTAP 9.6 and later**
>
> 1. Change to the advanced privilege level:
>
>    `set -privilege advanced`
>
> 2. Use the command:
>
>    `security key-manager external disable -vserver admin_SVM`
>
>    > ⓘ   In a MetroCluster environment, you must repeat the command on both clusters for the admin SVM.
>
> **ONTAP 9.5 and earlier**
>
> Use the command:
> `security key-manager delete-kmip-config`

**What happens when key management servers are not reachable during the boot process**

ONTAP takes certain precautions to avoid undesired behavior in the event that a storage system configured for NSE cannot reach any of the specified key management servers during the boot process.

If the storage system is configured for NSE, the SEDs are rekeyed and locked, and the SEDs are powered on, the storage system must retrieve the required authentication keys from the key management servers to authenticate itself to the SEDs before it can access the data.

The storage system attempts to contact the specified key management servers for up to three hours. If the storage system cannot reach any of them after that time, the boot process stops and the storage system halts.

If the storage system successfully contacts any specified key management server, it then attempts to establish an SSL connection for up to 15 minutes. If the storage system cannot establish an SSL connection with any specified key management server, the boot process stops and the storage system halts.

While the storage system attempts to contact and connect to key management servers, it displays detailed information about the failed contact attempts at the CLI. You can interrupt the contact attempts at any time by pressing Ctrl-C.

As a security measure, SEDs allow only a limited number of unauthorized access attempts, after which they disable access to the existing data. If the storage system cannot contact any specified key management servers to obtain the proper authentication keys, it can only attempt to authenticate with the default key which leads to a failed attempt and a panic. If the storage system is configured to automatically reboot in case of a panic, it enters a boot loop which results in continuous failed authentication attempts on the SEDs.

Halting the storage system in these scenarios is by design to prevent the storage system from entering a boot loop and possible unintended data loss as a result of the SEDs locked permanently due to exceeding the safety limit of a certain number of consecutive failed authentication attempts. The limit and the type of lockout protection depends on the manufacturing specifications and type of SED:

| SED type | Number of consecutive failed authentication attempts resulting in lockout | Lockout protection type when safety limit is reached |
|---|---|---|
| HDD | 1024 | Permanent. Data cannot be recovered, even when the proper authentication key becomes available again. |
| X440_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01 | 5 | Temporary. Lockout is only in effect until disk is power-cycled. |
| X577_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01 | 5 | Temporary. Lockout is only in effect until disk is power-cycled. |
| X440_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions | 1024 | Permanent. Data cannot be recovered, even when the proper authentication key becomes available again. |
| X577_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions | 1024 | Permanent. Data cannot be recovered, even when the proper authentication key becomes available again. |

| All other SSD models | 1024 | Permanent. Data cannot be recovered, even when the proper authentication key becomes available again. |

For all SED types, a successful authentication resets the try count to zero.

If you encounter this scenario where the storage system is halted due to failure to reach any specified key management servers, you must first identify and correct the cause for the communication failure before you attempt to continue booting the storage system.

**Disable encryption by default with ONTAP 9.7 and later**

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager. You can disable encryption by default for the entire cluster, if required.

**What you'll need**

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

**Step**

1. To disable encryption by default for the entire cluster in ONTAP 9.7 or later, run the following command:

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```