



Manage administrator authentication and RBAC with the CLI

ONTAP 9

NetApp
July 11, 2023

Table of Contents

- Manage administrator authentication and RBAC with the CLI 1
 - Administrator authentication and RBAC overview with the CLI 1
 - Administrator authentication and RBAC workflow 1
 - Worksheets for administrator authentication and RBAC configuration 2
 - Create login accounts 13
 - Manage access-control roles 28
 - Manage administrator accounts 34
 - Manage multi-admin verification 49

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
<code>-vserver</code>	The name of the SVM that the account accesses. The default value is the name of the admin SVM for the cluster.	
<code>-user-or-group-name</code>	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.	

<code>-application</code>	<p>The application that is used to access the SVM:</p> <ul style="list-style-type: none"> • <code>http</code> • <code>ontapi</code> • <code>snmp</code> • <code>ssh</code> 	
<code>-authmethod</code>	<p>The method that is used to authenticate the account:</p> <ul style="list-style-type: none"> • <code>cert</code> for SSL certificate authentication • <code>domain</code> for Active Directory authentication • <code>nsswitch</code> for LDAP or NIS authentication • <code>password</code> for user password authentication • <code>publickey</code> for public key authentication • <code>community</code> for SNMP community strings • <code>usm</code> for SNMP user security model • <code>saml</code> for Security Assertion Markup Language (SAML) authentication 	
<code>-remote-switch-ipaddress</code>	<p>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 <code>snmp</code> and the authentication method is <code>usm</code>.</p>	

-role	<p>The access control role that is assigned to the account:</p> <ul style="list-style-type: none"> • For the cluster (the admin SVM), the default value is <code>admin</code>. • For a data SVM, the default value is <code>vsadmin</code>. 	
-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 (<code>yes</code> or <code>no</code>).	
-second-authentication-method	<p>Second authentication method in case of multifactor authentication in ONTAP 9.3:</p> <ul style="list-style-type: none"> • <code>none</code> if not using multifactor authentication, default value • <code>publickey</code> for public key authentication when the <code>authmethod</code> is <code>password</code> or <code>nsswitch</code> • <code>password</code> for user password authentication when the <code>authmethod</code> is <code>public key</code> • <code>nsswitch</code> for user password authentication when the <code>authmethod</code> is <code>publickey</code> <div>  <p>Beginning with ONTAP 9.4, support for <code>nsswitch</code> is available.</p> </div> <p>The order of authentication is always the public key followed by the password.</p>	

-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 <code>DEFAULT</code> to specify all command directories.	

-access	<p>(Optional) The access level for the role. For command directories:</p> <ul style="list-style-type: none"> • <code>none</code> (the default value for custom roles) denies access to commands in the command directory • <code>readonly</code> grants access to the <code>show</code> commands in the command directory and its subdirectories • <code>all</code> grants access to all of the commands in the command directory and its subdirectories <p>For <i>nonintrinsic commands</i> (commands that do not end in <code>create</code>, <code>modify</code>, <code>delete</code>, or <code>show</code>):</p> <ul style="list-style-type: none"> • <code>none</code> (the default value for custom roles) denies access to the command • <code>readonly</code> is not applicable • <code>all</code> grants access to the command <p>To grant or deny access to intrinsic commands, you must specify the command directory.</p>	
-query	<p>(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 (<code>"</code>). For example, if the command directory is <code>volume</code>, the query object <code>"-aggr aggr0"</code> would enable access for the <code>aggr0</code> aggregate only.</p>	

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, <code>admin</code> , 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 ("").	

<code>-x509-certificate</code>	<p>(Optional) Beginning with ONTAP 9.13.1, enables you to manage X.509 certificate association with the SSH public key.</p> <p>When you associate an X.509 certificate with the SSH public key, ONTAP checks upon SSH login to see if this certificate is valid. If it has expired or been revoked, login is disallowed and the associated SSH public key is disabled.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <code>install</code>: Install the specified PEM-encoded X.509 certificate and associate it with the SSH public key. Include the full text for the certificate you want to install. • <code>modify</code>: Update the existing PEM-encoded X.509 certificate with the specified certificate and associate it with the SSH public key. Include the full text for the new certificate. • <code>delete</code>: Remove the existing X.509 certificate association with the SSH public key. 	
--------------------------------	--	--

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
<code>-common-name</code>	The name of the certificate, which is either a fully qualified domain name (FQDN) or a custom common name.	
<code>-size</code>	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	<p>The certificate type:</p> <ul style="list-style-type: none"> • <code>server</code> for server certificates and intermediate certificates • <code>client-ca</code> for the public key certificate of the root CA of the SSL client • <code>server-ca</code> for the public key certificate of the root CA of the SSL server of which ONTAP is a client • <code>client</code> 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
<code>-vserver</code>	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
<code>-vserver</code>	The name of the SVM for which you want to create an Active Directory computer account.	
<code>-account-name</code>	The NetBIOS name of the computer account.	
<code>-domain</code>	The fully qualified domain name (FQDN).	
<code>-ou</code>	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
<code>-vserver</code>	The name of the SVM for the client configuration.	

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

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

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: <ul style="list-style-type: none"> • <code>hosts</code> for files and DNS name services • <code>group</code> for files, LDAP, and NIS name services • <code>passwd</code> for files, LDAP, and NIS name services • <code>netgroup</code> for files, LDAP, and NIS name services • <code>namemap</code> for files and LDAP name services 	

<code>-sources</code>	<p>The order in which to look up name service sources (in a comma-separated list):</p> <ul style="list-style-type: none"> • <code>files</code> • <code>dns</code> • <code>ldap</code> • <code>nis</code> 	
-----------------------	--	--

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
<code>-idp-uri</code>	The FTP address or HTTP address of the Identity Provider (IdP) host from where the IdP metadata can be downloaded.	
<code>-sp-host</code>	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.	
<code>-cert-ca</code> and <code>-cert-serial</code> , or <code>-cert-common-name</code>	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.	
<code>-verify-metadata-server</code>	Whether the identity of the IdP metadata server must be validated (<code>true</code> or <code>false</code>). The best practice is to always set this value to <code>true</code> .	

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", "ssh", "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 FIPS mode on your cluster, existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type. The accounts should be reconfigured before you enable FIPs or the administrator authentication will fail.

The following table indicates host key type algorithms that are supported for ONTAP SSH connections. These key types do not apply to configuring SSH public authentication.

ONTAP release	Key types supported in FIPS mode	Key types supported in non-FIPS mode
9.11.1 and later	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa

9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa
--------------------	------------------------------------	--



ssh-ed25519 host key algorithm support is removed in 9.11.1

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 `svmin1` with the predefined `vsadmin-volume` role to access the `SVMengData1` using an SSH public key:

```
cluster1::>security login create -vserver engData1 -user-or-group-name
svmin1 -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 multifactor authentication (MFA) accounts

Multifactor authentication overview

Multifactor authentication (MFA) allows you to enhance security by requiring users to provide two authentication methods to log in to an admin or data SVM.

Depending upon your version of ONTAP, you can use a combination of an SSH public key, user password, and time-based one-time password (TOTP) to set up multifactor authentication.

ONTAP version	First authentication method	Second authentication method
9.13.1 and later	SSH public key	TOTP
	User password	TOTP
9.3 and later	SSH public key	User password

If MFA is configured with TOTP, the cluster administrator must first enable the local user account, then the account must be configured by the local user.



Enable multifactor authentication

Multifactor authentication (MFA) allows you to enhance security by requiring users to provide two authentication methods to log in to an admin or data SVM.

About this task

- You must be a cluster administrator to perform 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.

Modifying the role assigned to an administrator

- If you are using a public key for authentication, 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.

- 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.

Enable MFA with SSH public key and user password

Beginning with ONTAP 9.3, a cluster administrator can set up local user accounts to log in with MFA using an SSH public key and a user password.

1. Enable MFA on local user account with SSH public key and user password:

```
security login create -vserver <svm_name> -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 `SVMengData1` 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".

Enable MFA with TOTP

Beginning with ONTAP 9.13.1, you can enhance security by requiring local users to log in to an admin or data SVM with both an SSH public key or user password and a time-based one-time password (TOTP). After the account is enabled for MFA with TOTP, the local user must log in to [complete the configuration](#).

TOTP is a computer algorithm that uses the current time to generate a one-time password. If TOTP is used, it is always the second form of authentication after the SSH public key or the user password.

Before you begin

You must be a storage administrator to perform these tasks.

Steps

You can set up MFA to with a user password or an SSH public key as the first authentication method and TOTP as the second authentication method.

Enable MFA with user password and TOTP

1. Enable a user account for multifactor authentication with a user password and TOTP.

For new user accounts

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

For existing user accounts

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Verify that MFA with TOTP is enabled:

```
security login show
```

Enable MFA with SSH public key and TOTP

1. Enable a user account for multifactor authentication with an SSH public key and TOTP.

For new user accounts

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

For existing user accounts

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Verify that MFA with TOTP is enabled:

```
security login show
```

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](#)

- The local user must log in to complete MFA configuration with TOTP.

[Configure local user account for MFA with TOTP](#)

Related information

Learn more about [Multifactor Authentication in ONTAP 9 \(TR-4647\)](#).

Configure local user account for MFA with TOTP

Beginning in ONTAP 9.13.1, user accounts can be configured with multifactor authentication (MFA) using a time-based one-time password (TOTP).

Before you begin

- The storage administrator must [enable MFA with TOTP](#) as a second authentication method for your user account.
- Your primary user account authentication method should be a user password or public SSH key.
- You must configure your TOTP app to work with your smartphone and create your TOTP secret key.

TOTP is supported by various authenticator apps such as Google Authenticator.

Steps

1. Log in to your user account with your current authentication method.

Your current authentication method should be a user password or an SSH public key.

2. Create the TOTP configuration on your account:

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. Verify that the TOTP configuration is enabled on your account:

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

Reset TOTP secret key

To protect your account security, if your TOTP secret key is compromised or lost, you should disable it and create a new one.

Reset TOTP if your key is compromised

If your TOTP secret key is compromised, but you still have access to it, you can remove the compromised key and create a new one.

1. Log in to your user account with your user password or SSH public key and your compromised TOTP secret key.
2. Remove the compromised TOTP secret key:

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. Create a new TOTP secret key:

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. Verify that the TOTP configuration is enabled on your account:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Reset TOTP if your key is lost

If your TOTP secret key is lost, contact your storage administrator to [have the key disabled](#). After your key is disabled, you can use your first authentication method to log in and configure a new TOTP.

Before you begin:

The TOTP secret key must be disabled by a storage administrator. If you do not have a storage administrator account, contact your storage administrator to have the key disabled.

Steps

1. After the TOTP secret is disabled by a storage administrator, use your primary authentication method to log in into your local account.
2. Create a new TOTP secret key:

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

3. Verify that the TOTP configuration is enabled on your account:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Disable TOTP secret key for local account

If a local user's time-based one-time password (TOTP) secret key is lost, the lost key must be disabled by a storage administrator before the user can create a new TOTP secret key.

About this task

This task can only be performed from a cluster administrator account.

Step

1. Disable the TOTP secret key:

```
security login totp delete -vserver "<svm_name>" -username  
"<account_username>"
```

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](#)



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 `SVMengData2` 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 9.13.1, you can use an SSH public key as either your primary or secondary authentication method with an AD user password.
- 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](#)



AD group account access is supported only with the `SSH` and `ontapi` applications. AD groups are not supported with SSH public key authentication which is commonly used for multifactor authentication.

Step

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

For AD users:

ONTAP Version	Primary authentication	Secondary authentication	Command
9.13.1 and later	Public key	None	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre>
9.13.1 and later	Domain	Public key	<p>For a new user</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>For an existing user</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre>
9.0 and later	Domain	None	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

For AD groups:

ONTAP version	Primary authentication	Secondary authentication	Command
9.0 and later	Domain	None	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

For complete command syntax, see [worksheets for administrator authentication and RBAC configuration](#)

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 SVMengCluster.

```
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
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 [worksheet](#).

Creating or modifying login accounts

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
<code>admin</code>	<code>all</code>	All command directories (DEFAULT)
<code>admin-no-fsa</code> (available beginning in ONTAP 9.12.1)	Read/Write	<ul style="list-style-type: none"> • All command directories (DEFAULT) • <code>security login rest-role</code> • <code>security login role</code>
	Read only	<ul style="list-style-type: none"> • <code>security login rest-role create</code> • <code>security login rest-role delete</code> • <code>security login rest-role modify</code> • <code>security login rest-role show</code> • <code>security login role create</code> • <code>security login role create</code> • <code>security login role delete</code> • <code>security login role modify</code> • <code>security login role show</code> • <code>volume activity-tracking</code> • <code>volume analytics</code>
	None	<code>volume file show-disk-usage</code>

autosupport	all	<ul style="list-style-type: none"> • set • 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 style="list-style-type: none"> • security login password <p>For managing own user account local password and key information only</p> <ul style="list-style-type: none"> • set
	none	security
	readonly	All other command directories (DEFAULT)
none	none	All command directories (DEFAULT)



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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

Steps

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 reference for [Associating a public key with a user account](#).

2. Verify the change by viewing the public key:

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

Example

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  
"<key text>"
```

Manage SSH public keys and X.509 certificates for an administrator account

For increased SSH authentication security with administrator accounts, you can use the `security login publickey` set of commands to manage the SSH public key and its association with X.509 certificates.

Associate a public key and X.509 certificate with an administrator account

Beginning with ONTAP 9.13.1, you can associate an X.509 certificate with the public key that you associate with the administrator account. This gives you the added security of certificate expiration or revocation checks upon SSH login for that account.

Before you begin

- You must be a cluster or SVM administrator to perform this task.
- You must have generated the SSH key.
- If you only need the X.509 certificate to be checked for expiration, you can use a self-signed certificate.

- If you need the X.509 certificate to be checked for expiration and revocation:
 - You must have received the certificate from a certificate authority (CA).
 - You must install the certificate chain (intermediate and root CA certificates) using `security certificate install` commands.
 - You need to enable OCSP for SSH. Refer to [Verify digital certificates are valid using OCSP](#) for instructions.

About this task

If you authenticate an account over SSH with both an SSH public key and an X.509 certificate, ONTAP checks the validity of the X.509 certificate before authenticating with the SSH public key. SSH login will be refused if that certificate is expired or revoked, and the public key will be automatically disabled.

Steps

1. Associate a public key and an X.509 certificate with an administrator account:

```
security login publickey create -vserver SVM_name -username user_name -index
index -publickey certificate -x509-certificate install
```

For complete command syntax, see the worksheet reference for [Associating a public key with a user account](#).

2. Verify the change by viewing the public key:

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

Example

The following command associates a public key and X.509 certificate with the SVM administrator account `svmadmin2` for the SVM `engData2`. The public key is assigned index number 6.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Remove the certificate association from the SSH public key for an administrator account

You can remove the current certificate association from the account's SSH public key, while retaining the public key.

Before you begin

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

Steps

1. Remove the X.509 certificate association from an administrator account, and retain the existing SSH public key:

```
security login publickey modify -vserver SVM_name -username user_name -index
```

```
index -x509-certificate delete
```

2. Verify the change by viewing the public key:

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

Example

The following command removes the X.509 certificate association from the SVM administrator account `svmadmin2` for the SVM `engData2` at index number 6.

```
cluster1::> security login publickey modify -vserver engData2 -username  
svmadmin2 -index 6 -x509-certificate delete
```

Remove the public key and certificate association from an administrator account

You can remove the current public key and certificate configuration from an account.

Before you begin

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

Steps

1. Remove the public key and an X.509 certificate association from an administrator account:

```
security login publickey delete -vserver SVM_name -username user_name -index  
index
```

2. Verify the change by viewing the public key:

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

Example

The following command removes a public key and X.509 certificate from the SVM administrator account `svmadmin3` for the SVM `engData3` at index number 7.

```
cluster1::> security login publickey delete -vserver engData3 -username  
svmadmin3 -index 7
```

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.


```
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBGMRQwEgYDVQQDEwtleGFtcGx1LmNvbTELMakGA1UEBhMCVVMx
CTAHBGNVBAgTADEJMACGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBGNVBAStADEPMAOG
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejirKKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

```
Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTtM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

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.

Install a CA-signed server certificate

What you'll need

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 SVMengData2.

```
cluster1::>security certificate install -vserver engData2 -type server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCA ZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMACGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADBJMACGA1UECzMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMACGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADBJMACGA1UECzMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAYxRk2sry
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrFYC8KwE9k7A0ylRzBLdUwK9
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+zCCBGsgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwwbsxJDAiBgNVBACGTG1Zh
bG1DZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
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-----
```

```
MIIC5zCCA1ACAQEwDQYJKoZIhvcNAQEFBQAwbG90BCQEWEluYy4xNTAzBgNVBAsTLFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQDExodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG9w0BCQEWEluYy4xNTAzBgNVBAsTLFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQDExodHRw
```

```
-----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 SVMengData 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`



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 SVM `engData`. 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](#).



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



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 `SVMvs1.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 vservice_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.



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.

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

The following command can be protected beginning with ONTAP 9.13.1:

- `volume snaplock modify`

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	<code>security login show</code>
Modify credentials of current administrators	<code>security login modify <parameters></code>
Create new administrator accounts	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

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	<code>security multi-admin-verify approval-group modify [parameters]</code>
Add or remove members	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2...]] [-approvers-to-remove approver1[,approver2...]]</code>
Delete a group	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

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.



If you are using MAV with Autonomous Ransomware Protection (ARP), define a new or existing approval group that is responsible for approving ARP pause, disable, and clear suspect requests.

Required approvers

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



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

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 beginning with ONTAP 9.11.1.

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

You can create rules for the following command beginning with ONTAP 9.13.1:

- `volume snaplock modify`

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-vs1m20::> security multi-admin-verify rule show
```

Vserver	Operation	Required Approvers	Approval 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	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>

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

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 voll -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 voll
        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 voll -vserver vs0
```

```
Info: Volume "voll" 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 voll_*" 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 "voll" 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 voll
    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 voll -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	<code>security multi-admin-verify request approve nn</code>
Veto a request	<code>security multi-admin-verify request veto nn</code>

If you want to...	Enter this command
Show all requests, pending requests, or a single request	<pre>security multi-admin-verify request { show show-pending } [nn] { -fields field1[,field2...] [-instance] }</pre> <p>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 <code>-fields</code> parameter) or about all fields (by using the <code>-instance</code> parameter).</p>
Delete a request	<pre>security multi-admin-verify request delete nn</pre>

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
```

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: -
```

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.