Authentication and access control

ONTAP 9

NetApp
February 20, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap/concept_authentication_access_control_overview.html on February 20, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Authentication and access control . . . 1
- Authentication and access control overview . . . 1
  - Client authentication and authorization . . . 1
  - Administrator authentication and RBAC . . . 1
- Manage administrator authentication and RBAC . . . 1
  - Learn about administrator authentication and RBAC in ONTAP . . . 1
  - ONTAP administrator authentication and RBAC workflow . . . 2
  - Worksheets for ONTAP administrator authentication and RBAC setup . . . 3
  - Create login accounts . . . 18
  - Manage access-control roles . . . 33
  - Manage administrator accounts . . . 46
  - Manage multi-admin verification . . . 71
  - Manage dynamic authorization . . . 106
- Authentication and authorization using OAuth 2.0 . . . 115
  - Overview of the ONTAP OAuth 2.0 implementation . . . 115
  - Concepts . . . 119
  - Configure and deploy . . . 133
- Configure SAML authentication for remote ONTAP users . . . 140
  - Enable SAML authentication . . . 140
  - Disable SAML authentication . . . 146
  - Configure third-party IdP . . . 146
  - Troubleshoot issues with SAML configuration . . . 148
- Working with OAuth 2.0 or SAML IdP groups in ONTAP . . . 150
  - How groups are identified . . . 150
  - Manage groups with names . . . 151
  - Manage groups with UUIDs . . . 152
- Authentication and authorization using WebAuthn MFA . . . 154
  - Learn about WebAuthn multi-factor authentication for ONTAP System Manager users . . . 154
  - Enable WebAuthn MFA for ONTAP System Manager users or groups . . . 154
  - Disable WebAuthn MFA for ONTAP System Manager users . . . 156
  - View ONTAP WebAuthn MFA settings and manage credentials . . . 157
- Manage web services . . . 159
  - Manage web services overview . . . 159
  - Manage access to ONTAP web services . . . 160
  - Manage the web protocol engine in ONTAP . . . 162
  - ONTAP commands for managing the web protocol engine . . . 163
  - Configure access to ONTAP web services . . . 164
  - ONTAP commands for managing web services . . . 165
  - Commands for managing mount points on ONTAP nodes . . . 165
  - Manage SSL in ONTAP . . . 166
  - Use HSTS for ONTAP web services . . . 167
  - Troubleshoot ONTAP web service access problems . . . 168
- Verify the identity of remote servers using certificates . . . 172

Learn about verifying the identity of remote servers using certificates in ONTAP 172
Verify digital certificates are valid using OCSP in ONTAP 172
View default certificates for TLS-based applications in ONTAP 174
Mutually authenticate the cluster and a KMIP server 175
Mutually authenticating the ONTAP cluster and a KMIP server overview 175
Generate a certificate signing request for the cluster in ONTAP 175
Install a CA-signed server certificate for the ONTAP cluster 176
Install a CA-signed client certificate for the KMIP server in ONTAP 177

Authentication and access control

Authentication and access control overview

You can manage ONTAP cluster authentication and access control to ONTAP web services.

Using System Manager or the CLI, you can control and secure client and administrator access to the cluster and storage.

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

Client authentication and authorization

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

Administrator authentication and RBAC

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

Manage administrator authentication and RBAC

Learn about administrator authentication and RBAC in ONTAP

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 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

  Beginning with ONTAP 9.13.1, you can use an SSH public key as either your primary or secondary authentication method for an Active Directory user.

- 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.

- LDAP or NIS

  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.

ONTAP 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.

1 **Complete configuration worksheet**

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

2 **Determine if the administrator account is local or remote**

- **If local:** Enable password, SSH, SSH MFA, or SSL access.
- **If remote:** Determine the type of remote access. Depending on the access type, enable Active Directory access, enable LDAP or NIS access, or configure SAML authentication (only for admin SVM).

3 **Set up role-based access**

The role assigned to an administrator determines the commands to which the administrator has access. The role is assigned when you create the administrator account and can be modified later. You can use predefined roles for cluster and SVM administrators, or define custom roles as needed.

4 **Manage administrator accounts**

Depending on how you have enabled account access, you may need to associate a public key with a local account, manage public keys and X.509 certificates, configure Cisco Duo 2FA for SSH logins, install a CA-signed server digital certificate, or configure Active Directory, LDAP, or NIS access. You can perform any of these tasks before or after enabling account access.

5 **Configure additional security features**

- Manage multi-admin verification if you want to ensure that certain operations require approval from designated administrators.
- Manage dynamic authorization if you want to dynamically apply additional authorization checks based on a

user's trust level.

- Configure just-in-time (JIT) privilege elevation if you want to allow users to temporarily access elevated privileges to perform certain tasks.

Worksheets for ONTAP administrator authentication and RBAC setup

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

Learn more about the commands described in this procedure in the ONTAP command reference.

Create or modify login accounts

You provide these values with the `security login create` command when you enable login accounts to access a storage VM. Learn more about `security login create` in the ONTAP command reference.

You provide the same values with the `security login modify` command when you modify how an account accesses a storage VM. Learn more about `security login modify` in the ONTAP command reference.

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

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

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

Configure Cisco Duo security information

You provide these values with the `security login duo create` command when you enable Cisco Duo two-factor authentication with SSH logins for a storage VM. Learn more about `security login duo create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The storage VM (referred to as a vserver in the ONTAP CLI) to which the Duo authentication settings apply.	

`-integration-key`	Your integration key, obtained when registering your SSH application with Duo.	
`-secret-key`	Your secret key, obtained when registering your SSH application with Duo.	
`-api-host`	The API hostname, obtained when registering your SSH application with Duo. For example: `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	On service or configuration errors that prevent Duo authentication, fail `safe` (allow access) or `secure` (deny access). The default is `safe`, which means that Duo authentication is bypassed if it fails due to errors such as the Duo API server being inaccessible.	
`-http-proxy`	Use the specified HTTP proxy. If the HTTP proxy requires authentication, include the credentials in the proxy URL. For example: `http-proxy=http://username:password@proxy.example.org:8080`	

`-autopush`	Either `true` or `false`. Default is `false`. If `true`, Duo automatically sends a push login request to the user's phone, reverting to a phone call if push is unavailable. Note that this effectively disables passcode authentication. If `false`, the user is prompted to choose an authentication method. When configured with `autopush = true`, we recommend setting `max-prompts = 1`.	
`-max-prompts`	If a user fails to authenticate with a second factor, Duo prompts the user to authenticate again. This option sets the maximum number of prompts that Duo displays before denying access. Must be `1`, `2`, or `3`. The default value is `1`. For example, when `max-prompts = 1`, the user needs to successfully authenticate on the first prompt, whereas if `max-prompts = 2`, if the user enters incorrect information at the initial prompt, he/she will be prompted to authenticate again. When configured with `autopush = true`, we recommend setting `max-prompts = 1`. For the best experience, a user with only publickey authentication will always have `max-prompts` set to `1`.	
`-enabled`	Enable Duo two-factor authentication. Set to `true` by default. When enabled, Duo two-factor authentication is enforced during SSH login according to the configured parameters. When Duo is disabled (set to `false`), Duo authentication is ignored.	

`-pushinfo`	This option provides additional information in the push notification, such as the name of the application or service being accessed. This helps users verify that they are logging in to the correct service and provides an additional layer of security.	

Define custom roles

You provide these values with the `security login role create` command when you define a custom role. Learn more about `security login role create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	(Optional) The name of the storage VM (referred to as a vserver in the ONTAP CLI) that is associated with the role.	
`-role`	The name of the role.	
`-cmddirname`	The command or command directory to which the role gives access. You should enclose command subdirectory names in double quotation marks (`"`). For example, `"volume snapshot"`. You must enter `DEFAULT` to specify all command directories.	

`-access`	(Optional) The access level for the role. For command directories: • `none` (the default value for custom roles) denies access to commands in the command directory • `readonly` grants access to the `show` commands in the command directory and its subdirectories • `all` grants access to all of the commands in the command directory and its subdirectories For *nonintrinsic commands* (commands that do not end in `create`, `modify`, `delete`, or `show`): • `none` (the default value for custom roles) denies access to the command • `readonly` is not applicable • `all` grants access to the command To grant or deny access to intrinsic commands, you must specify the command directory.	
`-query`	(Optional) The query object that is used to filter the access level, which is specified in the form of a valid option for the command or for a command in the command directory. You should enclose the query object in double quotation marks (`"`). For example, if the command directory is `volume`, the query object `"-aggr aggr0"` would enable access for the `aggr0` aggregate only.	

Associate a public key with a user account

You provide these values with the `security login publickey create` command when you associate an SSH public key with a user account. Learn more about `security login publickey create` in the ONTAP command reference.

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

`-x509-certificate`	(Optional) Beginning with ONTAP 9.13.1, enables you to manage X.509 certificate association with the SSH public key. 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. Possible values: • `install`: 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. • `modify`: 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. • `delete`: Remove the existing X.509 certificate association with the SSH public key.	

Configure dynamic authorization global settings

Beginning with ONTAP 9.15.1, you provide these values with the `security dynamic-authorization modify` command. Learn more about `security dynamic-authorization modify` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM for which the trust score setting should be modified. If you omit this parameter, the cluster-level setting is used.	

`-state`	The dynamic authorization mode. Possible values: • `disabled`: (Default) Dynamic authorization is disabled. • `visibility`: This mode is useful for testing dynamic authorization. In this mode, the trust score is checked with every restricted activity, but not enforced. However, any activity that would have been denied or subject to additional authentication challenges is logged. • `enforced`: Intended for use after you have completed testing with `visibility` mode. In this mode, the trust score is checked with every restricted activity, and activity restrictions are enforced if the restriction conditions are met. The suppression interval is also enforced, preventing additional authentication challenges within the specified interval.	
`-suppression-interval`	Prevents additional authentication challenges within the specified interval. The interval is in ISO-8601 format and accepts values from 1 minute to 1 hour inclusive. If set to 0, the suppression interval is disabled and the user is always prompted for an authentication challenge if one is needed.	
`-lower-challenge-boundary`	The lower multi-factor authentication (MFA) challenge percentage boundary. The valid range is from 0 to 99. The value 100 is invalid, because this causes all requests to be denied. The default value is 0.	

`-upper-challenge-boundary`	The upper MFA challenge percentage boundary. The valid range is from 0 to 100. This must be equal to or greater than the value of the lower boundary. A value of 100 means that every request will either be denied or subject to an additional authentication challenge; there are no requests that are allowed without a challenge. The default value is 90.	

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 storage VM as an SSL server. Learn more about `security certificate generate-csr` in the ONTAP command reference.

Field	Description	Your value
`-common-name`	The name of the certificate, which is either a fully qualified domain name (FQDN) or a custom common name.	
`-size`	The number of bits in the private key. The higher the value, the more secure the key. The default value is `2048`. Possible values are `512`, `1024`, `1536`, and `2048`.	
`-country`	The country of the storage VM, in a two-letter code. The default value is `US`. For a list of codes, see the ONTAP command reference.	
`-state`	The state or province of the storage VM.	
`-locality`	The locality of the storage VM.	
`-organization`	The organization of the storage VM.	
`-unit`	The unit in the organization of the storage VM.	

`-email-addr`	The email address of the contact administrator for the storage VM.	
`-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 storage VM as an SSL server. Only the options that are relevant to account configuration are shown in the following table. Learn more about `security certificate install` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM on which the certificate is to be installed.	
`-type`	The certificate type: • `server` for server certificates and intermediate certificates • `client-ca` for the public key certificate of the root CA of the SSL client • `server-ca` for the public key certificate of the root CA of the SSL server of which ONTAP is a client • `client` for a self-signed or CA-signed digital certificate and private key for ONTAP as an SSL client	

Configure Active Directory domain controller access

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

Field	Description	Your value
`-vserver`	The name of the storage VM 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 storage VM computer account on the Active Directory domain. Learn more about `vserver active-directory create` in the ONTAP command reference.

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

Configure LDAP or NIS server access

You provide these values with the `vserver services name-service ldap client create` command when you create an LDAP client configuration for the storage VM. Learn more about `vserver services name-service ldap client create` in the ONTAP command reference.

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

Field	Description	Your value
`-vserver`	The name of the storage VM for the client configuration.	
`-client-config`	The name of the client configuration.	
`-ldap-servers`	A comma-separated list of IP addresses and host names for the LDAP servers to which the client connects.	
`-schema`	The schema that the client uses to make LDAP queries.	

`-use-start-tls`	Whether the client uses Start TLS to encrypt communication with the LDAP server (`true` or `false`). Start TLS is supported for access to data storage VMs only. It is not supported for access to admin storage VMs.	

You provide these values with the `vserver services name-service ldap create` command when you associate an LDAP client configuration with the storage VM. Learn more about `vserver services name-service ldap create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM with which the client configuration is to be associated.	
`-client-config`	The name of the client configuration.	
`-client-enabled`	Whether the storage VM can use the LDAP client configuration (`true` or `false`).	

You provide these values with the `vserver services name-service nis-domain create` command when you create an NIS domain configuration on an storage VM. Learn more about `vserver services name-service nis-domain create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM on which the domain configuration is to be created.	
`-domain`	The name of the domain.	
`-nis-servers`	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. Learn more about `vserver services name-`

`service ns-switch create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM on which the name service look-up order is to be configured.	
`-database`	The name service database: • `hosts` for files and DNS name services • `group` for files, LDAP, and NIS name services • `passwd` for files, LDAP, and NIS name services • `netgroup` for files, LDAP, and NIS name services • `namemap` for files and LDAP name services	
`-sources`	The order in which to look up name service sources (in a comma-separated list): • `files` • `dns` • `ldap` • `nis`	

Configure SAML access

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

Field	Description	Your value
`-idp-uri`	The FTP address or HTTP address of the Identity Provider (IdP) host from where the IdP metadata can be downloaded.	

`-sp-host`	The host name or IP address of the SAML service provider host (ONTAP system). By default, the IP address of the cluster-management LIF is used.	
`-cert-ca` and `-cert-serial`, or `-cert-common-name`	The server certificate details of the service provider host (ONTAP system). You can enter either the service provider's certificate issuing certification authority (CA) and the certificate's serial number, or the Server Certificate Common Name.	
`-verify-metadata-server`	Whether the identity of the IdP metadata server must be validated (`true` or `false`). The best practice is to always set this value to `true`.	

Create login accounts

Learn about creating ONTAP login accounts

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.

Naming conventions

The following generic names cannot be used for remote cluster and SVM administrator accounts:

- "adm"
- "bin"
- "cli"

- "daemon"
- "ftp"
- "games"
- "halt"
- "lp"
- "mail"
- "man"
- "naroot"
- "netapp"
- "news"
- "nobody"
- "operator"
- "root"
- "shutdown"
- "sshd"
- "sync"
- "sys"
- "uucp"
- "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

Learn about enabling local ONTAP account access

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.

Related information

- security login create

Enable ONTAP account password 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.

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.

Learn more about `security login modify` in the ONTAP command reference.

Before you begin

You must be a cluster administrator to perform this task.

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`*

   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
   ```

   Learn more about `security login create` in the ONTAP command reference.

Enable ONTAP account SSH public key access

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

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.

  Learn more about `security login modify` in the ONTAP command reference.

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

Support for the ssh-ed25519 host key algorithm is removed beginning with ONTAP 9.11.1.

For more information, see Configure network security using FIPS.

Before you begin

You must be a cluster administrator to perform this task.

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`*

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

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

   Learn more about `security login create` in the ONTAP command reference.

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

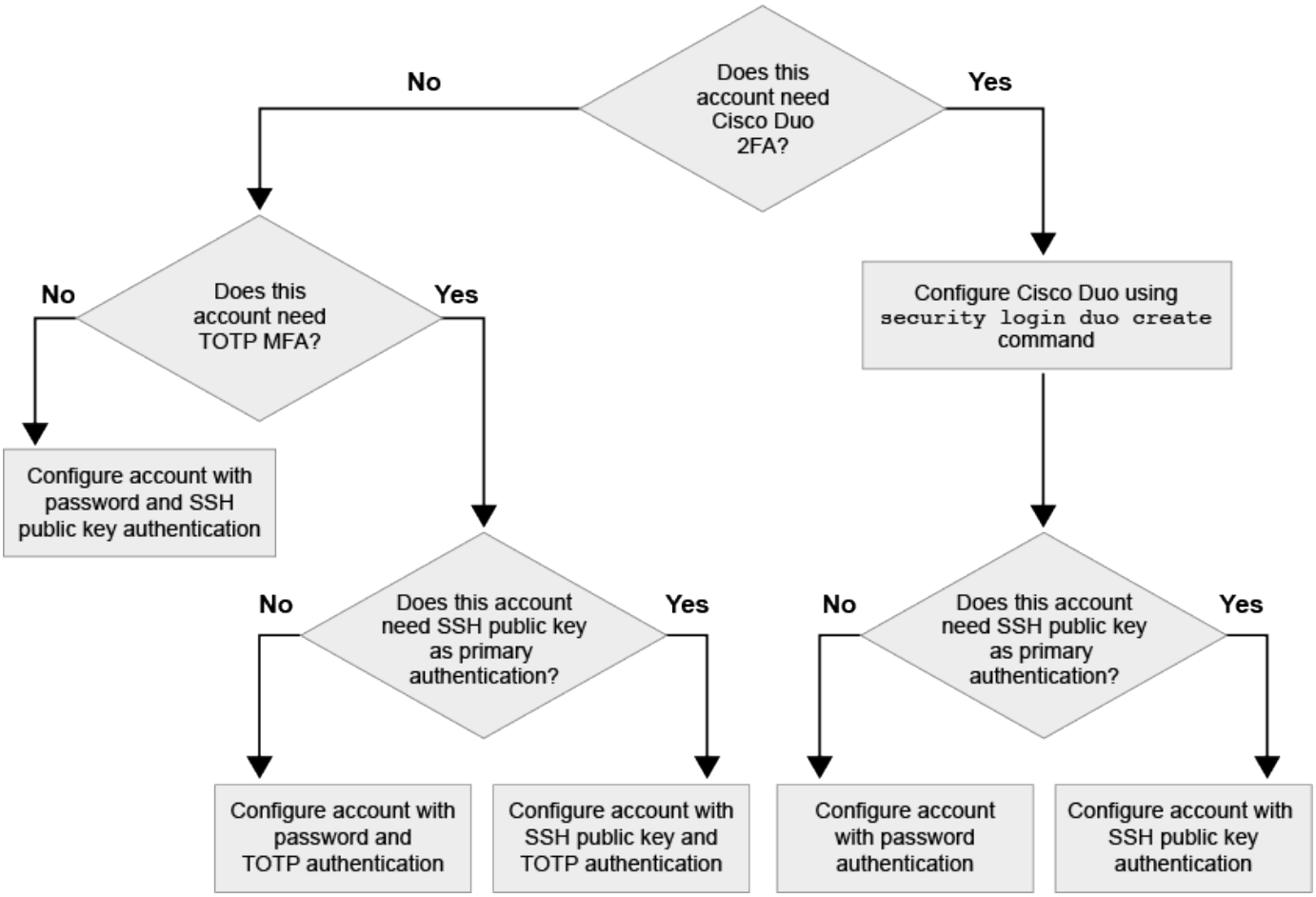
Learn about ONTAP multifactor authentication

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

Depending upon your version of ONTAP, you can use a combination of an SSH public key, a user password, and a time-based one-time password (TOTP) for multifactor authentication. When you enable and configure Cisco Duo (ONTAP 9.14.1 and later), it serves as an additional authentication method, supplementing the existing methods for all users.

Available beginning with…	First authentication method	Second authentication method
ONTAP 9.14.1	SSH public key	TOTP
	User Password	TOTP
	SSH public key	Cisco Duo
	User password	Cisco Duo
ONTAP 9.13.1	SSH public key	TOTP
	User password	TOTP
ONTAP 9.3	SSH public key	User password

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



Enable ONTAP multifactor authentication with SSH and TOTP

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.

  Learn more about `security login modify` in the ONTAP command reference.

  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 SVM`engData1` with both an SSH public key and a user password:

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

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

   Learn more about `security login create` in the ONTAP command reference.

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>
   ```

   Learn more about `security login modify` in the ONTAP command reference.

2. Verify that MFA with TOTP is enabled:

```
security login show
```

Learn more about `security login show` in the ONTAP command reference.

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

- Multifactor Authentication in ONTAP 9 (TR-4647)
- ONTAP command reference

Configure local ONTAP user accounts for MFA with TOTP

Beginning with 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.

  Microsoft Authenticator, Google Authenticator, Authy and any other TOTP-compatible authenticator is supported.

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>"
```

Related information

- security login totp create
- security login totp show

Reset the TOTP secret key for an ONTAP user account

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>
```

Related information

- security login totp create
- security login totp delete
- security login totp show

Disable the TOTP secret key for an ONTAP user 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 modify -vserver <svm_name> -username
<account_username> -enabled false
```

Learn more about `security login totp modify` in the ONTAP command reference.

Enable SSL certificate ONTAP account access

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

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 with the `http`, `ontapi`, and `rest` applications. For SVM administrator accounts, certificate authentication is supported only with the `ontapi` and `rest` applications.

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
   ```

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

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

   Learn more about `security login create` in the ONTAP command reference.

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

Learn more about the commands described in this procedure in the ONTAP command reference.

Enable Active Directory ONTAP 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.

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.

If you choose to use an SSH public key as your primary authentication, no AD authentication takes place.

- Beginning with ONTAP 9.11.1, you can use Use LDAP fast bind for nsswitch authentication for ONTAP NFS SVMs 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.

  Learn more about `security login modify` in the ONTAP command reference.

  Modifying the role assigned to an administrator

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

Before you begin

- 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.

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	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

ONTAP Version	Primary authentication	Secondary authentication	Command

9.13.1 and later	Domain	Public key	**For a new user**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			For an existing user
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 and later	Domain	None	`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]`

For AD groups:

ONTAP version	Primary authentication	Secondary authentication	Command
9.0 and later	Domain	None	`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]`

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

Related information

- security login create

Enable LDAP or NIS ONTAP 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.

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.

  Learn more about `security login modify` in the ONTAP command reference.

  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 Use LDAP fast bind for nsswitch authentication for ONTAP NFS SVMs 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.

Before you begin

You must be a cluster administrator to perform this task.

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]
   ```

   Creating or modifying login accounts

   The following command enables the LDAP or NIS cluster administrator account `guest2` with the

predefined `backup` role to access the admin SVM`engCluster`.

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

Learn more about `security login create` in the ONTAP command reference.

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

Related information

- security login

Manage access-control roles

Learn about managing ONTAP access-control roles

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 ONTAP 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.

Before you begin

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`

   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
   ```

   Learn more about `security login modify` in the ONTAP command reference.

Define custom roles for ONTAP administrators

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.

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.

Before you begin

You must be a cluster administrator to perform this task.

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
   ```

   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
   ```

   Learn more about `security login role create` in the ONTAP command reference.

Related information

- security login role create
- storage aggregate plex offline
- storage encryption

Predefined roles for ONTAP cluster administrators

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

The following table lists the predefined roles for cluster administrators:

This role…	Has this level of access…	To the following commands or command directories
admin	all	All command directories (`DEFAULT`)
admin-no-fsa (available beginning with ONTAP 9.12.1)	Read/Write	• All command directories (`DEFAULT`) • `security login rest-role` • `security login role`
	Read only	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`
	None	`volume file show-disk-usage`
autosupport	all	• `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	• `security login password` For managing own user account local password and key information only • `set`
	• Beginning with ONTAP 9.8, readonly • Prior to ONTAP 9.8, none	`security`
	readonly	All other command directories (`DEFAULT`)
snaplock	all	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`
	none	• `volume move governor` • `volume move recommend`
	none	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.

Related information

- security login
- set
- volume
- vserver services ndmp

Predefined roles for ONTAP SVM administrators

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

The following table lists the predefined roles for SVM administrators:

Role name	Capabilities
vsadmin	• Managing own user account local password and key information • Managing volumes, except volume moves • Managing quotas, qtrees, snapshots, and files • Managing LUNs • Performing SnapLock operations, except privileged delete • Configuring protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configuring services: DNS, LDAP, and NIS • Monitoring jobs • Monitoring network connections and network interface • Monitoring the health of the SVM
vsadmin-volume	• Managing own user account local password and key information • Managing volumes, except volume moves • Managing quotas, qtrees, snapshots, and files • Managing LUNs • Configuring protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configuring services: DNS, LDAP, and NIS • Monitoring network interface • Monitoring the health of the SVM

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

Manage ONTAP administrator access with System Manager

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

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

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

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

Assigning a role to an administrator

Assign a role to an administrator, as follows:

Steps

1. Select **Cluster > Settings**.
2. Select → next to **Users and Roles**.
3. Select + Add under **Users**.
4. Specify a user name, and select a role in the drop-down menu for **Role**.
5. Specify a login method and password for the user.

Changing an administrator's role

Change the role for an administrator, as follows:

Steps

1. Click **Cluster > Settings**.
2. Select the name of user whose role you want to change, then click the ⋮ that appears next to the user name.
3. Click **Edit**.
4. Select a role in the drop-down menu for **Role**.

Access JIT privilege elevation in ONTAP

Beginning with ONTAP 9.17.1, cluster administrators can configure just-in-time (JIT) privilege elevation to allow ONTAP users to temporarily elevate their privileges to perform certain tasks. When JIT is configured for a user, they can temporarily elevate their privilege to a role that has the necessary permissions to perform a task. After the session expires, the user returns to their original access level.

Cluster administrators can configure the duration for which a user can access JIT elevation. For example, cluster administrators can configure user access to JIT elevation with a 30 minute per-session limit (the *session validity period*) for a 30-day period (the *JIT validity period*). During the 30-day period, the user can elevate their privilege as many times as needed, but each session is limited to 30 minutes.

About this task

- JIT privilege elevation is only available to users accessing ONTAP with SSH. Elevated privilege is only available within the current SSH session, but you can elevate privileges within as many concurrent SSH sessions as needed.
- JIT privilege elevation is only supported for users using password, nsswitch, or domain authentication to

log in. Multi-factor authentication (MFA) is not supported for JIT privilege elevation.

- A user's JIT session will be terminated if the configured session or JIT validity period expires, or if a cluster administrator revokes JIT access for the user.

Before you begin

- To access JIT privilege elevation, a cluster administrator must configure JIT access for your account. The cluster administrator determines the role to which you can elevate your privileges, and the duration for which you can access elevated privileges.

Steps

1. Temporarily elevate your privileges to the configured role:

   ```
   security jit-privilege elevate
   ```

   After entering this command, you are prompted to enter your login password. If JIT access is configured for your account, you will be granted elevated access for the configured session duration. After the session duration expires, you will return to your original access level. You can elevate your privileges as many times as needed within the configured JIT validity period.

2. View the remaining time in your JIT session:

   ```
   security jit-privilege show-remaining-time
   ```

   If you are currently in a JIT session, this command displays the remaining time.

3. If needed, end your JIT session early:

   ```
   security jit-privilege reset
   ```

   If you are currently in a JIT session, this command ends the JIT session and restores your original access level.

Configure JIT privilege elevation in ONTAP

Beginning with ONTAP 9.17.1, cluster administrators can configure just-in-time (JIT) privilege elevation to allow ONTAP users to temporarily elevate their privileges to perform certain tasks. When JIT is configured for a user, they can temporarily elevate their privilege to a role that has the necessary permissions to perform a task. After the session duration expires, the user returns to their original access level.

Cluster administrators can configure the duration for which a user can access JIT elevation. For example, you can configure user access to JIT elevation with a 30 minute per-session limit (the *session validity period*) for a 30-day period (the *JIT validity period*). During the 30-day period, the user can elevate their privilege as many times as needed, but each session is limited to 30 minutes.

JIT privilege elevation supports the principle of least privilege, allowing users to perform tasks that require elevated privileges without permanently granting them those privileges. This helps reduce the risk of

unauthorized access or accidental changes to the system. The following examples describe some common use cases for JIT privilege elevation:

- Allow temporary access to the `security login create` and `security login delete` commands to enable onboarding and offboarding of users.
- Allow temporary access to `system node image update` and `system node upgrade-revert` during an update window. After the update is complete, command access is revoked.
- Allow temporary access to `cluster add-node`, `cluster remove-node`, and `cluster modify` to enable cluster expansion or reconfiguration. Once the cluster changes are complete, command access is revoked.
- Allow temporary access to `volume snapshot restore` to enable restore operations and backup target management. Once the restore or configuration is complete, command access is revoked.
- Allow temporary access to `security audit log show` to enable audit log review and export during a compliance check.

For a more expansive list of common JIT use cases, refer to Common JIT use cases.

Cluster administrators can set up JIT access for ONTAP users, and configure the default JIT validity periods either globally across the cluster or for specific SVMs.

About this task

- JIT privilege elevation is only available to users accessing ONTAP with SSH. Elevated privileges are only available within the user's current SSH session, but they can elevate privileges within as many concurrent SSH sessions as needed.
- JIT privilege elevation is only supported for users using password, nsswitch, or domain authentication to log in. Multi-factor authentication (MFA) is not supported for JIT privilege elevation.

Before you begin

- You must be an ONTAP cluster administrator at the `admin` privilege level to perform the following tasks.

Modify global JIT settings

You can modify the default JIT settings globally across the ONTAP cluster or for a specific SVM. These settings determine the default session validity period and the maximum JIT validity period for users who are configured for JIT access.

About this task

- The default `default-session-validity-period` value is one hour. This setting determines how long a user can access elevated privileges in a JIT session before needing to re-elevate.
- The default `max-jit-validity-period` value is 90 days. This setting determines the maximum period during which a user can access JIT elevation after the configured start date. You can configure the JIT validity period for individual users, but it cannot exceed the maximum JIT validity period.

Steps

1. Check the current JIT settings:

   ```
   security jit-privilege show -vserver <svm_name>
   ```

   `-vserver` is optional. If you don't specify a SVM, the command shows the global JIT settings.

2. Modify the JIT settings globally or for an SVM:

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

If you don't specify a SVM, the command modifies the global JIT settings. The following example will set the default JIT session duration to 45 minutes and the maximum JIT duration to 30-days for SVM `svm1`: `security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

In this example, users will be able to access JIT elevation for 45 minutes at a time and can initiate JIT sessions for a maximum of 30-days after their configured start date.

Configure JIT privilege elevation access for a user

You can assign JIT privilege elevation access to ONTAP users.

Steps

1. Check the current JIT access for a user:

```
security jit-privilege user show -username <username>
```

`-username` is optional. If you don't specify a username, the command shows the JIT access for all users.

2. Assign new JIT access for a user:

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- If `-vserver` is not specified, JIT access is assigned at the cluster level.
- `-role` is the RBAC role that the user will be elevated to. If not specified, `-role` defaults to `admin`.
- `-session-validity-period` is the duration for which the user can access the elevated role before needing to start a new JIT session. If not specified, the global or SVM `default-session-validity-period` is used.
- `-jit-validity-period` is the maximum duration for which a user can initiate JIT sessions after the configured start date. If not specified, the `session-validity-period` is used. This parameter cannot exceed the global or SVM `max-jit-validity-period`.
- `-start-time` is the date and time after which the user can initiate JIT sessions. If not specified, the current date and time is used.

  The following example will allow `ontap_user` to access the `admin` role for 1 hour before needing to start a new JIT session. `ontap_user` will be able to initiate JIT sessions for a 60-day period starting at 1PM on July 1, 2025:
  `security jit-privilege user create -username ontap_user -role admin -session`

```
-validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"
```

3. If needed, revoke a user's JIT access:

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

This command will revoke a user's JIT access, even if their access has not expired. If `-vserver` is not specified, the JIT access is revoked at the cluster level. If the user is in an active JIT session, the session will be terminated.

Common JIT use cases

The following table contains common use cases for JIT privilege elevation. For each use case, an RBAC role would need to be configured to provide access to the relevant commands. Each command links to the ONTAP command reference, with more information about the command and its parameters.

Use case	Commands	Details
User and role management	• `security login create` • `security login delete`	Temporarily elevate to add/remove users or change roles during onboarding or offboarding.
Certificate management	• `security certificate create` • `security certificate install`	Grant short-term access for certificate installation or renewal.
SSH/CLI access control	• `security login create -application ssh`	Temporarily grant SSH access for troubleshooting or vendor support.
License management	• `system license add` • `system license delete`	Grant rights to add or remove licenses during feature activation or deactivation.
System upgrades and patching	• `system node image update` • `system node upgrade-revert`	Elevate for the upgrade window, then revoke.
Network security settings	• `security login role create` • `security login role modify`	Allow temporary changes to network-related security roles.

Use case	Commands	Details
Cluster management	• `cluster add-node` • `cluster remove-node` • `cluster modify`	Elevate for cluster expansion or reconfiguration.
SVM management	• `vserver create` • `vserver delete` • `vserver modify`	Temporarily grant an SVM admin rights for provisioning or decommissioning.
Volume management	• `volume create` • `volume delete` • `volume modify`	Elevate for volume provisioning, resizing, or removal.
Snapshot management	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	Elevate for snapshot deletion or restore during recovery.
Network configuration	• `network interface create` • `network port vlan create`	Grant rights for network changes during maintenance windows.
Disk/aggregate management	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	Elevate for adding or removing disks or managing aggregates.
Data protection	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	Temporarily elevate for configuring or restoring SnapMirror relationships.
Performance tuning	• `qos policy-group create` • `qos policy-group modify`	Elevate for performance troubleshooting or tuning.
Audit log access	• `security audit log show`	Temporarily elevate for audit log review or export during compliance checks.

Use case	Commands	Details
Event and alert management	• `event notification create` • `event notification modify`	Elevate for configuring or testing event notifications or SNMP traps.
Compliance-driven data access	• `volume show` • `security audit log show`	Grant temporary read-only access for auditors to review sensitive data or logs.
Privileged access reviews	• `security login show` • `security login role show`	Temporarily elevate to review and report on privileged access. Grant read-only elevated access for a limited time.

Related information

- cluster
- event notification
- network
- qos policy-group
- security
- snapmirror
- storage
- system
- volume
- vserver

Manage administrator accounts

Learn about managing ONTAP administrator accounts

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 ONTAP 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.

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.

Before you begin

- You must have generated the SSH key.
- You must be a cluster or SVM administrator to perform this task.

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`*

   Learn more about `security login publickey create` in the ONTAP command reference.

2. Verify the change by viewing the public key:

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

   Learn more about `security login publickey show` in the ONTAP command reference.

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 ONTAP administrators

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.

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.

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. Learn more about `security certificate install` in the ONTAP command reference.
  - You need to enable OCSP for SSH. Refer to Verify digital certificates are valid using OCSP for instructions.

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`

   Learn more about `security login publickey create` in the ONTAP command reference.

2. Verify the change by viewing the public key:

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

   Learn more about `security login publickey show` in the ONTAP command reference.

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`

Learn more about `security login publickey modify` in the ONTAP command reference.

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`*

   Learn more about `security login publickey delete` in the ONTAP command reference.

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
```

Related information

- security login publickey

Configure Cisco Duo 2FA for ONTAP SSH logins

Beginning with ONTAP 9.14.1, you can configure ONTAP to use Cisco Duo for two-factor authentication (2FA) during SSH logins. You configure Duo at the cluster level, and it applies to all user accounts by default. Alternatively, you can configure Duo at the level of the storage VM (previously referred to as vserver), in which case it applies only to users for that storage VM. If you enable and configure Duo, it serves as an additional authentication method, supplementing the existing methods for all users.

If you enable Duo authentication for SSH logins, users will need to enroll a device the next time they log in using SSH. For enrollment information, refer to the Cisco Duo enrollment documentation.

You can use the ONTAP command line interface to perform the following tasks with Cisco Duo:

- Configure Cisco Duo
- Change Cisco Duo configuration
- Remove Cisco Duo configuration
- View Cisco Duo configuration
- Remove a Duo group
- View Duo groups
- Bypass Duo authentication for users

Configure Cisco Duo

You can create a Cisco Duo configuration for either the entire cluster or for a specific storage VM (referred to as a vserver in the ONTAP CLI) using the `security login duo create` command. When you do this, Cisco Duo is enabled for SSH logins for this cluster or storage VM. Learn more about `security login duo create` in the ONTAP command reference.

Steps

1. Log in to the Cisco Duo Admin Panel.
2. Go to **Applications > UNIX Application**.
3. Record your integration key, secret key, and API hostname.
4. Log in to your ONTAP account using SSH.
5. Enable Cisco Duo authentication for this storage VM, substituting information from your environment for the values in brackets:

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

Change Cisco Duo configuration

You can change the way Cisco Duo authenticates users (for example, how many authentication prompts are given, or what HTTP proxy is used). If you need to change the Cisco Duo configuration for a storage VM (referred to as a vserver in the ONTAP CLI), you can use the `security login duo modify` command. Learn more about `security login duo modify` in the ONTAP command reference.

Steps

1. Log in to the Cisco Duo Admin Panel.
2. Go to **Applications > UNIX Application**.
3. Record your integration key, secret key, and API hostname.
4. Log in to your ONTAP account using SSH.
5. Change the Cisco Duo configuration for this storage VM, substituting updated information from your environment for the values in brackets:

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-max-prompts 1|2|3 \
-is-enabled true|false \
-fail-mode safe|secure
```

Remove Cisco Duo configuration

You can remove the Cisco Duo configuration, which will remove the need for SSH users to authenticate using Duo upon login. To remove the Cisco Duo configuration for a storage VM (referred to as a vserver in the ONTAP CLI), you can use the `security login duo delete` command. Learn more about `security login duo delete` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Remove the Cisco Duo configuration for this storage VM, substituting your storage VM name for `<STORAGE_VM_NAME>`:

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

This permanently deletes the Cisco Duo configuration for this storage VM.

View Cisco Duo configuration

You can view the existing Cisco Duo configuration for a storage VM (referred to as a vserver in the ONTAP CLI) by using the `security login duo show` command. Learn more about `security login duo show` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Show the Cisco Duo configuration for this storage VM. Optionally, you can use the `vserver` parameter to specify a storage VM, substituting the storage VM name for `<STORAGE_VM_NAME>`:

   ```
   security login duo show -vserver <STORAGE_VM_NAME>
   ```

   You should see output similar to the following:

   ```
   Vserver: testcluster
   Enabled: true

   Status: ok
   INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
   SKEY SHA Fingerprint:
   b79ffa4b1c50b1c747fbacdb34g671d4814
   API Host: api-host.duosecurity.com
   Autopush: true
   Push info: true
   Failmode: safe
   Http-proxy: 192.168.0.1:3128
   Prompts: 1
   Comments: -
   ```

Create a Duo group

You can instruct Cisco Duo to include only the users in a certain Active Directory, LDAP, or local user group in the Duo authentication process. If you create a Duo group, only the users in that group are prompted for Duo authentication. You can create a Duo group by using the `security login duo group create` command. When you create a group, you can optionally exclude specific users in that group from the Duo authentication process. Learn more about `security login duo group create` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Create the Duo group, substituting information from your environment for the values in brackets. If you omit the `-vserver` parameter, the group is created at the cluster level:

   ```
   security login duo group create -vserver <STORAGE_VM_NAME> -group-name
   <GROUP_NAME> -excluded-users <USER1, USER2>
   ```

The name of the Duo group must match an Active Directory, LDAP, or local group. Users you specify with the optional `-excluded-users` parameter will not be included in the Duo authentication process.

View Duo groups

You can view existing Cisco Duo group entries by using the `security login duo group show` command. Learn more about `security login duo group show` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Show the Duo group entries, substituting information from your environment for the values in brackets. If you omit the `-vserver` parameter, the group is shown at the cluster level:

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

The name of the Duo group must match an Active Directory, LDAP, or local group. Users you specify with the optional `-excluded-users` parameter will not be displayed.

Remove a Duo group

You can remove a Duo group entry using the `security login duo group delete` command. If you remove a group, the users in that group are no longer included in the Duo authentication process. Learn more about `security login duo group delete` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Remove the Duo group entry, substituting information from your environment for the values in brackets. If you omit the `-vserver` parameter, the group is removed at the cluster level:

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

The name of the Duo group must match an Active Directory, LDAP, or local group.

Bypass Duo authentication for users

You can exclude all users or specific users from the Duo SSH authentication process.

Exclude all Duo users

You can disable Cisco Duo SSH authentication for all users.

Steps

1. Log in to your ONTAP account using SSH.
2. Disable Cisco Duo authentication for SSH users, substituting the Vserver name for `<STORAGE_VM_NAME>`:

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

Exclude Duo group users

You can exclude certain users that are part of a Duo group from the Duo SSH authentication process.

Steps

1. Log in to your ONTAP account using SSH.
2. Disable Cisco Duo authentication for specific users in a group. Substitute the group name and list of users to exclude for the values in brackets:

   ```
   security login duo group modify -group-name <GROUP_NAME> -excluded-users
   <USER1, USER2>
   ```

   The name of the Duo group must match an Active Directory, LDAP, or local group. Users you specify with the `-excluded-users` parameter will not be included in the Duo authentication process.

   Learn more about `security login duo group modify` in the ONTAP command reference.

Exclude local Duo users

You can exclude specific local users from using Duo authentication by using the Cisco Duo Admin Panel. For instructions, refer to the Cisco Duo documentation.

Generate and install a CA-signed server certificate in ONTAP

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. Learn more about `security certificate generate-csr` and `security certificate install` in the ONTAP command reference.

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.

Before you begin

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.

Example of creating a CSR

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

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

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

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

Install a CA-signed server certificate

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

Before you begin

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

Step

1. Install a CA-signed server certificate:

```
security certificate install -vserver SVM_name -type certificate_type
```

> 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 SVM `engData2`.

Example of installing a CA-signed server certificate intermediate certificates

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----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-----
<certificate_value>
-----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-----
<certificate_value>
-----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.
```

Related information

- security certificate generate-csr

Manage ONTAP certificates with System Manager

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

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

View certificate information

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

Steps

1. In System Manager, select **Cluster > Settings**.
2. Scroll to the **Security** area.
   In the **Certificates** section, the following details are displayed:
   - The number of stored trusted certificate authorities.
   - The number of stored client/server certificates.
   - The number of stored local certificate authorities.
3. Select any number to view details about a category of certificates, or select → to open the **Certificates** page, which contains information about all categories.
   The list displays the information for the entire cluster. If you want to display information for only a specific storage VM, perform the following steps:
   a. Select **Storage > Storage VMs**.
   b. Select the storage VM.
   c. Switch to the **Settings** tab.
   d. Select a number shown in the **Certificate** section.

What to do next

- From the **Certificates** page, you can Generate a certificate signing request.
- The certificate information is separated into three tabs, one for each category. You can perform the following tasks from each tab:

On this tab…	You can perform these procedures…
Trusted certificate authorities	• Install (add) a trusted certificate authority • Delete a trusted certificate authority • Renew a trusted certificate authority
Client/server certificates	• Install (add) a client/server certificate • Generate (add) a self-signed client/server certificate • Delete a client/server certificate • Renew a client/server certificate

Local certificate authorities	• Create a new local certificate authority • Sign a certificate using a local certificate authority • Delete a local certificate authority • Renew a local certificate authority

Generate a certificate signing request

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

Steps

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

Install (add) a trusted certificate authority

You can install additional trusted certificate authorities in System Manager.

Steps

1. View the **Trusted Certificate Authorities** tab. See View certificate information.
2. Select + Add .
3. On the **Add Trusted Certificate Authority** panel, perform the following:
   - Enter a **name**.
   - For the **scope**, select a storage VM.
   - Enter a **common name**.
   - Select a **type**.
   - Enter or import **certificate details**.

Delete a trusted certificate authority

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

> You cannot delete trusted certificate authorities preinstalled with ONTAP.

Steps

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

2. Select the name of the trusted certificate authority.
3. Select ⋮ next to the name, then select **Delete**.

Renew a trusted certificate authority

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

Steps

1. View the **Trusted Certificate Authorities** tab. See View certificate information.
2. Select the name of the trusted certificate authority.
3. Select ⋮ next to the certificate name then **Renew**.

Install (add) a client/server certificate

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

Steps

1. View the **Client/Server Certificates** tab. See View certificate information.
2. Select + Add .
3. On the **Add Client/Server Certificate** panel, perform the following:
   - Enter a **certificate name**.
   - For the **scope**, select a storage VM.
   - Enter a **common name**.
   - Select a **type**.
   - Enter or import **certificate details**.
     You can either write in or copy and paste in the certificate details from a text file or you can import the text from a certificate file by clicking **Import**.
   - Enter the **private key**.
     You can either write in or copy and paste in the private key from a text file or you can import the text from a private key file by clicking **Import**.

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

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

Steps

1. View the **Client/Server Certificates** tab. See View certificate information.
2. Select **+Generate Self-signed Certificate**.
3. On the **Generate Self-Signed Certificate** panel, perform the following:
   - Enter a **certificate name**.
   - For the **scope**, select a storage VM.
   - Enter a **common name**.
   - Select a **type**.
   - Select a **hash function**.

- Select a **key size**.
- Select a **storage VM**.

Delete a client/server certificate

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

Steps

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

Renew a client/server certificate

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

Steps

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

Create a new local certificate authority

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

Steps

1. View the **Local Certificate Authorities** tab. See View certificate information.
2. Select + Add .
3. On the **Add Local Certificate Authority** panel, perform the following:
   - Enter a **name**.
   - For the **scope**, select a storage VM.
   - Enter a **common name**.
4. If you want to override defaults, select **More Options** and provide additional information.

Sign a certificate using a local certificate authority

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

Steps

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

Delete a local certificate authority

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

Steps

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

Renew a local certificate authority

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

Steps

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

Configure Active Directory domain controller access in ONTAP

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 an 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 beginning with…
HMAC-SHA256, based on the Advanced Encryption Standard (AES) If your cluster is running ONTAP 9.9.1 or earlier and your domain controller enforces AES for secure Netlogon services, the connection fails. In this case, you need to reconfigure your domain controller to instead accept strong key connections with ONTAP.	ONTAP 9.10.1
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, you need to verify that AES is enabled on your SVM.

- Beginning with ONTAP 9.14.1, AES is enabled by default when you create an SVM, and you don't need to modify the security settings of your SVM to use AES session keys during Netlogon secure channel establishment.
- In ONTAP 9.10.1 through 9.13.1, AES is disabled by default when you create an SVM. You need to enable AES using the following command:

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

> When you upgrade to ONTAP 9.14.1 or later, the AES setting for existing SVMs that were created with older ONTAP releases will not automatically change. You still need to update the value for this setting to enable AES on these SVMs.

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.

Prior to ONTAP 9.16.1, you must use an authentication tunnel to manage cluster administrator accounts with AD.

Before you begin

- 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.

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

Steps

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>
   ```

   Learn more about `security login domain-tunnel create` in the ONTAP command reference.

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

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

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

Create an SVM computer account on the domain

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

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.

Beginning with ONTAP 9.16.1, you can use this procedure to manage cluster administrator accounts with AD.

Before you begin

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

Steps

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>
   ```

   Beginning with ONTAP 9.16.1, the `-vserver` parameter accepts the admin SVM. Learn more about `vserver active-directory create` in the ONTAP command reference.

   The following command creates a computer account named `ADSERVER1` on the domain `example.com` for 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 in ONTAP

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.

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 2016 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:

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

Before you begin

- 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.

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.

   Learn more about `vserver services name-service ldap client create` in the ONTAP command reference.

   The following command creates an LDAP client configuration named `corp` on 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
   ```

> The `-ldap-servers` field replaces the `-servers` field. You can use the `-ldap-servers` field to specify 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>`

   Learn more about `vserver services name-service ldap create` in the ONTAP command reference.

   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
   ```

   > 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".                                              |
   ```

   You can use the `name service check` command to validate the status of the name servers.

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.

Before you begin

- 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.

Step

1. Create an NIS domain configuration on an SVM:

```
vserver services name-service nis-domain create -vserver <SVM_name> -domain
<client_configuration> -nis-servers <NIS_server_IPs>
```

Learn more about `vserver services name-service nis-domain create` in the ONTAP command reference.

> The `-nis-servers` field replaces the `-servers` field. You can use the `-nis-servers` field to specify either a hostname or an IP address for the NIS server.

The following command creates an NIS domain configuration on SVM `engData`. The NIS domain `nisdomain` 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 -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.

Before you begin

- 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>
   ```

   Learn more about `vserver services name-service ns-switch modify` in the ONTAP command reference.

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

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

Change an ONTAP 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.

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.

Before you begin

- 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.

Step

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

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

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

Related information

- security login role config modify
- security login password

Lock and unlock an ONTAP 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.

Before you begin

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
```

Learn more about `security login lock` in the ONTAP command reference.

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
```

Learn more about `security login unlock` in the ONTAP command reference.

Related information

- security login

Manage failed login attempts in ONTAP

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. Learn more about `security login role config modify` in the ONTAP command reference.

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. Learn more about `security ssh modify` in the ONTAP command reference.
- Migrate existing MD5-algorithm accounts to the more secure SHA-512 algorithm by requiring users to change their passwords.

Enforce SHA-2 on ONTAP 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`).

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` *`svm_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.

Related information

- security login expire-password
- security login unlock

Diagnose and correct ONTAP file access issues with System Manager

Beginning with ONTAP 9.8, you can trace and view file access concerns.

Steps

1. In System Manager, select **Storage > Storage VMs**.
2. Select the storage VM on which you want to perform a trace.
3. Click ⋮ **More**.
4. Click **Trace File Access**.
5. Provide the user name and client IP address, then click **Start Tracing**.

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

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

Manage multi-admin verification

Learn about ONTAP multi-admin verification

Beginning with ONTAP 9.11.1, you can use multi-admin verification (MAV) to ensure that certain operations, such as deleting volumes or snapshots, 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 these steps:

1. When a user initiates the operation, a request is generated.
2. Before the operation can be executed, at least one MAV administrator must approve.
3. Upon approval, the user is prompted and completes the operation.

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

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 that you 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.

> Multi-admin verification is not available with Cloud Volumes ONTAP.

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.

System-defined rules

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` operation `*`

  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.

Rule-protected commands

In addition to system-defined operations, 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

Each ONTAP version provides more commands you can choose to protect with multi-admin verification rules. Choose your ONTAP release for the full list of commands available for protection.

9.17.1

- `cluster date modify` [3]
- `cluster log-forwarding create` [3]
- `cluster log-forwarding delete` [3]
- `cluster log-forwarding modify` [3]
- `cluster peer delete`
- `cluster time-service ntp server create` [3]
- `cluster time-service ntp server delete` [3]
- `cluster time-service ntp key create` [3]
- `cluster time-service ntp key delete` [3]
- `cluster time-service ntp key modify` [3]
- `cluster time-service ntp server modify` [3]
- `event config modify`
- `event config set-mail-server-password` [3]
- `lun delete` [3]
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` [2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` [2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` [3]
- `security saml-sp create` [3]

- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]

- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume rename [5]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]

- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.16.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]

- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]

- system health policy definition modify[3]
- system node autosupport modify[3]
- system node autosupport trigger modify[3]
- system node coredump delete[3]
- system node coredump delete-all[3]
- system node hardware nvram-encryption modify[3]
- system node run
- system node systemshell
- system script delete[3]
- system service-processor ssh add-allowed-addresses[3]
- system service-processor ssh remove-allowed-addresses[3]
- system smtape restore[3]
- system switch ethernet log disable-collection[3]
- system switch ethernet log modify[3]
- timezone[3]
- volume create[3]
- volume delete
- volume encryption conversion start[4]
- volume encryption rekey start[4]
- volume file privileged-delete[3]
- volume flexcache delete
- volume modify[3]
- volume recovery-queue modify[2]
- volume recovery-queue purge[2]
- volume recovery-queue purge-all[2]
- volume snaplock modify[1]
- volume snapshot autodelete modify
- volume snapshot create[3]
- volume snapshot delete
- volume snapshot modify[3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]

- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.15.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete

- security login publickey modify
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume file privileged-delete [3]

- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]

- vserver security file-directory remove-slag [3]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete

- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create [2]
- vserver modify [2]
- vserver peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume pause [1]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify

- `volume snapshot policy modify-schedule`
- `volume snapshot policy remove-schedule`
- `volume snapshot restore`
- `vserver peer delete`

9.12.1/9.11.1

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

1. New rule-protected command for 9.13.1
2. New rule-protected command for 9.14.1
3. New rule-protected command for 9.15.1
4. New rule-protected command for 9.16.1
5. New rule-protected command for 9.17.1

*This command is only available with CLI and is unavailable for System Manager in some releases.

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 initiate protected operations; regular administrators must initiate protected operations, 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.

> A requestor can’t approve their own requests even if they are in the approval group (although they can get email notifications for their own requests). 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.

MAV rules are evaluated before the protected operation is executed. This means that rules are enforced based on the current state of the system. For example, if a MAV rule is created for `volume modify` with a query of `-size 5GB`, using `volume modify` to resize a 5GB volume to 2GB will require MAV approval, but resizing a 2GB volume to 5GB will not.

Related information

- cluster
- lun
- security
- snaplock legal-hold end
- storage aggregate
- storage encryption
- system

Manage ONTAP administrator approval groups for MAV

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.

Beginning with ONTAP 9.15.1, you can configure Active Directory (AD) users as MAV administrators. The AD user must be configured as an ONTAP administrator.

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`*

   Learn more about `event config show` and `event config modify` in the ONTAP command reference.

2. Identify administrators to receive multi-admin verification

If you want to…	Enter this command
Display current administrators	`security login show`

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

Learn more about `security login show`, `security login modify`, and `security login create` in the ONTAP command reference.

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. For AD users, use the format `domain\user`. For example, `mydomain\pavan`.
   - `-email` - One or more email addresses that are notified when a request is created, approved, vetoed, or executed.

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

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

4. Verify group creation and membership:

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

   Example:

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

Use these commands to modify your initial MAV group configuration.

Note: All require MAV administrator approval before execution.

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

Related information

- security multi-admin-verify

Enable or disable multi-admin verification in ONTAP

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 NetApp Knowledge Base: 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: 1hour)
      - Mail server*
      - From email address*

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

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

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

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

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

To disable multi-admin verification:

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

   MAV approval is required to complete this operation.

CLI procedure

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

If you want to…	Enter this command

Enable MAV functionality	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`
	
	Example : the following command enables MAV with 1 approval group, 2 required approvers, and default expiry periods.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Complete initial configuration by adding at least one operation rule.

If you want to…	Enter this command
Modify a MAV configuration (requires MAV approval)	`security multi-admin-verify approval-group modify [-approval-groups group1 [,group2…]] [-required-approvers nn ] [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`

Verify MAV functionality	`security multi-admin-verify show`
	
	Example:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

Disable MAV functionality (requires MAV approval)	`security multi-admin-verify modify -enabled false`

Related information

- security multi-admin-verify

Manage multi-admin verification rules for protected operations in ONTAP

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.

Only one MAV rule can be created per operation; for example, you cannot make multiple `volume-snapshot-delete` rules. Any desired rule constraints must be contained within one rule.

You can create rules to protect these commands. You can protect each command beginning with the ONTAP version in which protection capability for the command first became available.

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

In addition to system-defined operations, 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

Rule constraints

When you create a rule, you can optionally specify the `-query` option to limit the request to a subset of the command functionality. The `-query` option can also be used to limit configuration elements, such as the SVM, the volume, and snapshot names.

For example, in the `volume snapshot delete` command, `-query` can be set to `-snapshot !hourly*,!daily*,!weekly*`, meaning that volume snapshots prefixed with hourly, daily, or weekly attributes are excluded from MAV protections.

```
smci-vsim20::> security multi-admin-verify rule show
                                                Required  Approval
Vserver Operation                               Approvers Groups
------- ------------------------------------- --------- -------------
vs01    volume snapshot delete                  -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

> Any excluded configuration elements would not be protected by MAV, and any administrator could delete or rename them.

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 separately.

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. Select **Cluster > Settings**.
2. Select ⚙ next to **Multi-Admin Approval** in the **Security** section.
3. Select + Add to add at least one rule; you can also modify or delete existing rules.
    - Operation – Select a supported command from the list.

- Query – Enter any desired command options and values.
- Optional parameters – Leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
  - Required number of approvers
  - Approval groups

CLI procedure

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

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

Modify credentials of current administrators	`security login modify <parameters>`
	
	Example: the following rule requires approval to delete the root volume.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

Modify a rule	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Delete a rule	`security multi-admin-verify rule delete -operation "protected_operation"`
Show rules	`security multi-admin-verify rule show`

Related information

- security multi-admin-verify rule
- security login modify

Request execution of MAV protected operations in ONTAP

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

If approved, you must then respond to the query to complete the operation within the request expiry period. If

vetoed, or if the request or expiry periods are exceeded, you must delete the request and resubmit.

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

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

System Manager procedure

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

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

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

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

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

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

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

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

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

CLI procedure

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

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

   - `volume delete`

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

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

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

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

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

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

2. Check the status of the request and respond to the MAV notice.
   a. If the request is approved, respond to the CLI message to complete the operation.

      Example:

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

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

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

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

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

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

   Example:

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

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

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

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

Related information

- security multi-admin-verify

Manage MAV protected operation requests in ONTAP

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 (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.

> `multi-admin-verify` requests in a terminal state may be overwritten or removed automatically. Use the audit log to review previous requests.

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.

System Manager

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

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

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

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

Example:

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

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


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

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

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

Example:

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

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


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

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

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

Related information

- security multi-admin-verify

Manage dynamic authorization

Learn about ONTAP dynamic authorization

Beginning with ONTAP 9.15.1, administrators can configure and enable dynamic authorization to increase security of remote access to ONTAP while also mitigating potential damage that could be caused by a malicious actor. With ONTAP 9.15.1, dynamic authorization provides an initial framework for assigning a security score to users and, if their activity looks suspicious, challenging them with additional authorization checks or denying an operation completely. Administrators can create rules, assign trust scores, and restrict commands to determine when certain activity is allowed or denied for a user. Administrators can enable dynamic authorization cluster-wide or for individual storage VMs.

How dynamic authorization works

Dynamic authorization uses a trust scoring system to assign users a different level of trust depending on the authorization policies. Based on the user's trust level, an activity they perform can be allowed or denied, or the user can be prompted for further authentication.

Refer to Customize dynamic authorization to learn more about how to configure criteria score weights and other dynamic authorization attributes.

Trusted devices

When dynamic authorization is in use, the definition of a trusted device is a device used by a user to log in to ONTAP using public key authentication as one of the authentication methods. The device is trusted because only that user has possession of the corresponding private key.

Dynamic authorization example

Take the example of three different users attempting to delete a volume. When they try to perform the operation, the risk rating for each user is examined:

- The first user logs in from a trusted device with very few previous authentication failures, which makes her risk rating low; the operation is allowed without additional authentication.
- The second user logs in from a trusted device with a moderate percentage of previous authentication failures, which makes the risk rating moderate; she is prompted for additional authentication before the operation is allowed.
- The third user logs in from an untrusted device with a high percentage of previous authentication failures, which makes the risk rating high; the operation is not allowed.

What's next

- Enable or disable dynamic authorization
- Customize dynamic authorization

Enable or disable dynamic authorization in ONTAP

Beginning with ONTAP 9.15.1, administrators can configure and enable dynamic authorization either in `visibility` mode to test the configuration, or in `enforced` mode to activate the configuration for CLI users connecting over SSH. If you no longer need dynamic authorization, you can disable it. When you disable dynamic authorization, the configuration settings remain available and you can use them later if you decide to re-enable it.

Learn more about `security dynamic-authorization modify` in the ONTAP command reference.

Enable dynamic authorization for testing

You can enable dynamic authorization in visibility mode, which enables you to test the feature and ensure that users will not be accidentally locked out. In this mode, the trust score is checked with every restricted activity, but not enforced. However, any activity that would have been denied or subject to additional authentication challenges is logged. As a best practice, you should test your intended settings in this mode before enforcing them.

> You can follow this step to enable dynamic authorization for the first time even if you haven't yet configured any other dynamic authorization settings. Refer to Customize dynamic authorization for steps to configure other dynamic authorization settings to customize it to your environment.

Steps

1. Enable dynamic authorization in visibility mode by configuring global settings and changing the feature state to `visibility`. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment. Parameters in bold are required:

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Check the result by using the `show` command to display the global configuration:

```
security dynamic-authorization show
```

Enable dynamic authorization in enforced mode

You can enable dynamic authorization in enforced mode. Typically, you use this mode after you have completed testing with visibility mode. In this mode, the trust score is checked with every restricted activity, and activity restrictions are enforced if the restriction conditions are met. The suppression interval is also enforced, preventing additional authentication challenges within the specified interval.

> This step assumes that you have previously configured and enabled dynamic authorization in `visibility` mode, which is strongly recommended.

Steps

1. Enable dynamic authorization in `enforced` mode by changing its state to `enforced`. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment. Parameters in bold are required:

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. Check the result by using the `show` command to display the global configuration:

```
security dynamic-authorization show
```

Disable dynamic authorization

You can disable dynamic authorization if you no longer need the added authentication security.

Steps

1. Disable dynamic authorization by changing its state to `disabled`. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment. Parameters in bold are required:

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Check the result by using the `show` command to display the global configuration:

```
security dynamic-authorization show
```

   Learn more about `security dynamic-authorization show` in the ONTAP command reference.

What's next

(Optional) Depending on your environment, refer to Customize dynamic authorization to configure other dynamic authorization settings.

Customize dynamic authorization in ONTAP

As an administrator, you can customize different aspects of your dynamic authorization configuration to increase the security of remote administrator SSH connections to your ONTAP cluster.

You can customize the following dynamic authorization settings depending on your security needs:

- Configure dynamic authorization global settings
- Configure dynamic authorization trust score components
- Configure a custom trust score provider
- Configure restricted commands
- Configure dynamic authorization groups

Configure dynamic authorization global settings

You can configure global settings for dynamic authorization, including the storage VM to secure, the suppression interval for authentication challenges, and the trust score settings.

Learn more about `security login domain-tunnel create` in the ONTAP command reference.

Steps

1. Configure global settings for dynamic authorization. If you don't use the `-vserver` parameter, the

command is run at the cluster level. Update the values in brackets <> to match your environment:

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. View the resulting configuration:

```
security dynamic-authorization show
```

Configure restricted commands

When you enable dynamic authorization, the feature includes a default set of restricted commands. You can modify this list to suit your needs. Refer to the multi-admin verification (MAV) documentation for information on the default list of restricted commands.

Add a restricted command

You can add a command to the list of commands that are restricted with dynamic authorization.

Learn more about `security dynamic-authorization rule create` in the ONTAP command reference.

Steps

1. Add the command. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. View the resulting list of restricted commands:

```
security dynamic-authorization rule show
```

Remove a restricted command

You can remove a command from the list of commands that are restricted with dynamic authorization.

Learn more about `security dynamic-authorization rule delete` in the ONTAP command reference.

Steps

1. Remove the command. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. View the resulting list of restricted commands:

```
security dynamic-authorization rule show
```

Configure dynamic authorization groups

By default, dynamic authorization applies to all users and groups as soon as you enable it. However, you can create groups using the `security dynamic-authorization group create` command, so that dynamic authorization only applies to those specific users.

Add a dynamic authorization group

You can add a dynamic authorization group.

Learn more about `security dynamic-authorization group create` in the ONTAP command reference.

Steps

1. Create the group. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. View the resulting dynamic authorization groups:

```
security dynamic-authorization group show
```

Remove a dynamic authorization group

You can remove a dynamic authorization group.

Learn more about `security dynamic-authorization group delete` in the ONTAP command reference.

Steps

1. Delete the group. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. View the resulting dynamic authorization groups:

```
security dynamic-authorization group show
```

Configure dynamic authorization trust score components

You can configure the maximum score weight to change priority of scoring criteria or to remove certain criteria from risk scoring.

> As a best practice, you should leave the default score weight values in place, and only adjust them if needed.

Learn more about `security dynamic-authorization trust-score-component modify` in the ONTAP command reference.

The following are the components that you can modify, along with their default score and percentage weights:

Criteria	Component name	Default raw score weight	Default percentage weight
Trusted device	`trusted-device`	20	50
User login authentication history	`authentication-history`	20	50

Steps

1. Modify trust score components. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. View the resulting trust score component settings:

```
security dynamic-authorization trust-score-component show
```

Reset the trust score for a user

If a user is denied access due to system policies and is able to prove their identity, the administrator can reset the user's trust score.

Learn more about `security dynamic-authorization user-trust-score reset` in the ONTAP command reference.

Steps

1. Add the command. Refer to Configure dynamic authorization trust score components for a list of trust score components that you can reset. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Display your trust score

A user can display their own trust score for a login session.

Steps

1. Display your trust score:

```
security login whoami
```

You should see output similar to the following:

```
User: admin
Role: admin
Trust Score: 50
```

Learn more about `security login whoami` in the ONTAP command reference.

Configure a custom trust score provider

If you already receive scoring methods from an external trust score provider, you can add the custom provider to the dynamic authorization configuration.

Before you begin

- The custom trust score provider must return a JSON response. The following syntax requirements must be met:
  - The field that returns the trust score must be a scalar field and not an element of an array.
  - The field that returns the trust score can be a nested field, such as `trust_score.value`.

    - There must be a field within the JSON response that returns a numeric trust score. If this is not natively available, you can write a wrapper script to return this value.
- The value provided can be either a trust score or a risk score. The difference is that the trust score is in ascending order with a higher score denoting a higher trust level, while the risk score is in descending order. For example, a trust score of 90 for a score range of 0 to 100 indicates that the score is very trustworthy and likely to result in an "allow" without additional challenge, while a risk score of 90 for a score range of 0 to 100 indicates high risk and likely to result in a "deny" without an additional challenge.
- The custom trust score provider must be accessible via the ONTAP REST API.
- The custom trust score provider must be configurable using one of the supported parameters. Custom trust score providers that require configuration that is not in the supported parameter list are not supported.

  Learn more about `security dynamic-authorization trust-score-component create` in the ONTAP command reference.

Steps

1. Add a custom trust score provider. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. View the resulting trust score provider settings:

```
security dynamic-authorization trust-score-component show
```

Configure custom trust score provider tags

You can communicate with external trust score providers using tags. This enables you to send information in the URL to the trust score provider without exposing sensitive information.

Learn more about `security dynamic-authorization trust-score-component create` in the ONTAP command reference.

Steps

1. Enable trust score provider tags. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

For example:

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

Authentication and authorization using OAuth 2.0

Overview of the ONTAP OAuth 2.0 implementation

Beginning with ONTAP 9.14, you have the option to control access to your ONTAP clusters using the Open Authorization (OAuth 2.0) framework. You can configure this feature using any of the ONTAP administrative interfaces, including the ONTAP CLI, System Manager, and REST API. However, the OAuth 2.0 authorization and access control decisions can only be applied when a client accesses ONTAP using the REST API.

> OAuth 2.0 support was first introduced with ONTAP 9.14.0 and so its availability depends on the ONTAP release you are using. See the ONTAP release notes for more information.

Features and benefits

The major features and benefits of using OAuth 2.0 with ONTAP are described below.

Support for the OAuth 2.0 standard

OAuth 2.0 is the industry standard authorization framework. It is used to restrict and control access to protected resources using signed access tokens. There are several benefits to using OAuth 2.0:

- Many options for the authorization configuration
- Never reveal the client credentials including passwords
- Tokens can be set to expire based on your configuration
- Ideally suited for use with REST APIs

Tested with popular authorization servers

The ONTAP OAuth 2.0 implementation has been tested with several popular servers or services based on the

ONTAP release as follows:

- ONTAP 9.16.1 (support for group UUID to name mapping and external roles):
  - Microsoft Entra ID
- ONTAP 9.14.1 (support for standard OAuth 2.0 features)
  - Auth0
  - Active Directory Federation Service (ADFS)
  - Keycloak

See Authorization servers and access tokens for more details about the features and capabilities available with each ONTAP release.

Support for multiple concurrent authorization servers

You can define up to eight authorization servers for a single ONTAP cluster. This gives you the flexibility to meet the needs of your diverse security environment.

Integration with the REST roles

The ONTAP authorization decisions are ultimately based on the REST roles assigned to users or groups. These roles are either carried in the access token as self-contained scopes or based on local ONTAP definitions along with Active Directory or LDAP groups.

Option to use sender-constrained access tokens

You can configure ONTAP and the authorization servers to use Mutual Transport Layer Security (mTLS) which strengthens client authentication. It guarantees the OAuth 2.0 access tokens are only used by the clients to which they were originally issued. This feature supports and aligns with several popular security recommendations, including those established by FAPI and MITRE.

Implementation and configuration

At a high level, there are several aspects of an OAuth 2.0 implementation and configuration you should consider when getting started.

OAuth 2.0 entities within ONTAP

The OAuth 2.0 authorization framework defines several entities that can be mapped to real or virtual elements within your data center or network. The OAuth 2.0 entities and their adaptation to ONTAP are presented in the table below.

OAuth 2.0 Entity	Description
Resource	The REST API endpoints that provide access to the ONTAP resources through internal ONTAP commands.
Resource owner	The ONTAP cluster user that created the protected resource or owns it by default.
Resource server	The host for the protected resources which is the ONTAP cluster.
Client	An application requesting access to a REST API endpoint on behalf of or with permission from the resource owner.
Authorization server	Typically a dedicated server responsible for issuing access tokens and enforcing administrative policy.

Core ONTAP configuration

You need to configure the ONTAP cluster to enable and use OAuth 2.0. This includes establishing a connection to the authorization server and defining the required ONTAP authorization configuration. You can perform this configuration using any of the administrative interfaces, including:

- ONTAP command line interface
- System Manager
- ONTAP REST API

Environment and supporting services

In addition to the ONTAP definitions, you also need to configure the authorization servers. If you're using group-to-role mapping, you need also to configure the Active Directory groups or LDAP equivalent.

Supported ONTAP clients

Beginning with ONTAP 9.14, a REST API client can access ONTAP using OAuth 2.0. Before issuing a REST API call, you need to obtain an access token from the authorization server. The client then passes this token to the ONTAP cluster as a *bearer token* using the HTTP authorization request header. Depending on the level of security needed, you can also create and install a certificate at the client to use sender-constrained tokens based on mTLS.

Selected terminology

As you begin exploring an OAuth 2.0 deployment with ONTAP, it is helpful to become familiar with some of the terminology. See Additional resources for links to more information about OAuth 2.0.

Access token

A token issued by an authorization server and used by an OAuth 2.0 client application to make requests to access the protected resources.

JSON Web Token

The standard used to format the access tokens. JSON is used to represent the OAuth 2.0 claims in a compact format with the claims arranged in three main sections.

Sender-constrained access token

An optional feature based on the Mutual Transport Layer Security (mTLS) protocol. By using an additional confirmation claim in the token, this ensures the access token is only used by the client to which it was originally issued.

JSON Web Key Set

A JWKS is a collection of public keys used by ONTAP to verify the JWT tokens presented by the clients. The key sets are typically available at the authorization server through a dedicated URI.

Scope

Scopes provide a way to limit or control an application's access to protected resources such as the ONTAP REST API. They are represented as strings in the access token.

ONTAP REST role

REST roles were introduced with ONTAP 9.6 and are a core part of the ONTAP RBAC framework. These roles are different than the earlier traditional roles which are still supported by ONTAP. The OAuth 2.0 implementation in ONTAP only supports REST roles.

HTTP authorization header

A header included in the HTTP request to identify the client and associated permissions as part of making a REST API call. There are several flavors or implementations available depending on how authentication and authorization is performed. When presenting an OAuth 2.0 access token to ONTAP, the token is identified as a *bearer token*.

HTTP basic authentication

An early HTTP authentication technique still supported by ONTAP. The plaintext credentials (username and password) are concatenated with a colon and encoded in base64. The string is placed in the authorization request header and sent to the server.

FAPI

A working group at the OpenID Foundation providing protocols, data schemas, and security recommendations for the financial industry. The API was originally known as the Financial Grade API.

MITRE

A private not-for-profit company providing technical and security guidance to the United States Air Force and US government.

Additional resources

Several additional resources are provided below. You should review these sites to get more information about OAuth 2.0 and the related standards.

Protocols and standards

- RFC 6749: The OAuth 2.0 Authorization Framework
- RFC 7519: JSON Web Tokens (JWT)
- RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
- RFC 7662: OAuth 2.0 Token Introspection
- RFC 7800: Proof-of-Possession Key for JWTs
- RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

Organizations

- OpenID Foundation
- FAPI Working Group
- MITRE
- IANA - JWT

Products and services

- Auth0
- Entra ID
- ADFS overview
- Keycloak

Additional tools and utilities

- JWT by Auth0
- OpenSSL

NetApp documentation and resources

- ONTAP automation documentation

Concepts

OAuth 2.0 authorization servers and access tokens in ONTAP

Authorization servers perform several important functions as a central component within the OAuth 2.0 Authorization framework.

OAuth 2.0 authorization servers

Authorization servers are primarily responsible for creating and signing access tokens. These tokens contain identity and authorization information enabling a client application to selectively access protected resources. The servers are generally isolated from one another and can be implemented in several different ways, including as a standalone dedicated server or as part of a larger identity and access management product.

> Different terminology can sometimes be used for an authorization server, especially when the OAuth 2.0 functionality is packaged within a larger identity and access management product or solution. For example, the term **identity provider (IdP)** is frequently used interchangeably with **authorization server**.

Administration

In addition to issuing access tokens, authorization servers also provide related administrative services, typically through a web user interface. For example, you can define and administer:

- Users and user authentication
- Scopes
- Administrative segregation through tenants and realms
- Policy enforcement
- Connection to various external services
- Support for other identity protocols (such as SAML)

ONTAP is compatible with authorization servers that are compliant with the OAuth 2.0 standard.

Defining to ONTAP

You need to define one or more authorization servers to ONTAP. ONTAP securely communicates with each server to verify tokens and perform other related tasks in support of the client applications.

The major aspects of ONTAP configuration are presented below. Also see OAuth 2.0 deployment scenarios for more information.

How and where the access tokens are validated

There are two options for validating access tokens.

- Local validation

  ONTAP can validate access tokens locally based on information provided by the authorization server that issued the token. The information retrieved from the authorization server is cached by ONTAP and

refreshed at regular intervals.

- Remote introspection

  You can also use remote introspection to validate tokens at the authorization server. Introspection is a protocol allowing authorized parties to query an authorization server about an access token. It provides ONTAP a way to extract certain metadata from an access token and validate the token. ONTAP caches some of the data for performance reasons.

Network location

ONTAP may be behind a firewall. In this case, you need to identify a proxy as part of the configuration.

How the authorization servers are defined

You can define an authorization server to ONTAP using any of the administrative interfaces, including the CLI, System Manager, or REST API. For example, with the CLI you use the command `security oauth2 client create`.

Learn more about `security oauth2 client create` in the ONTAP command reference.

Number of authorization servers

You can define up to eight authorization servers to a single ONTAP cluster. The same authorization server can be defined more than once to the same ONTAP cluster as long as the issuer or issuer/audience claims are unique. For example, with Keycloak this will always be the case when using different realms.

OAuth 2.0 features supported in ONTAP

Support for OAuth 2.0 was initially available with ONTAP 9.14.1 and continues to be enhanced with subsequent releases. The OAuth 2.0 features supported by ONTAP are described below.

> Features introduced with a specific ONTAP release are carried forward to future releases.

ONTAP 9.16.1

ONTAP 9.16.1 expands the standard OAuth 2.0 features to include Entra ID specific extensions for native Entra ID groups. This involves the use of GUIDs in the access token instead of names. In addition, the release adds support for external role mapping to map the native identity provider roles to ONTAP roles using the "roles" field in the access token.

ONTAP 9.14.1

Beginning with ONTAP 9.14.1, authorization servers are supported through the following standard OAuth 2.0 features for applications using:

- OAuth 2.0 with the standard fields including "iss", "aud", and "exp" as described in RFC6749: The OAuth 2.0 Authorization Framework and RFC 7519: JSON Web Token (JWT). This also includes support for uniquely identifying users through fields in the access token such as "upn", "appid", "sub", "username" or "preferred_username".
- ADFS vendor-specific extensions for group names with the "group" field.
- Azure vendor-specific extensions for group UUIDs with the "group" field.
- ONTAP extensions for authorization support using self-contained and named roles within the OAuth 2.0 access token scope. This includes the "scope" and "scp" fields as well as group names within the scope.

Using OAuth 2.0 access tokens

The OAuth 2.0 access tokens issued by the authorization servers are verified by ONTAP and used to make role-based access decisions for the REST API client requests.

Acquiring an access token

You need to acquire an access token from an authorization server defined to the ONTAP cluster where you use the REST API. To acquire a token, you must contact the authorization server directly.

> ONTAP does not issue access tokens or redirect requests from clients to the authorization servers.

How you request a token depends on several factors, including:

- Authorization server and its configuration options
- OAuth 2.0 grant type
- Client or software tool used to issue the request

Grant types

A *grant* is a well-defined process, including a set of network flows, used to request and receive an OAuth 2.0 access token. Several different grant types can be used depending on the client, environment, and security requirements. A list of the popular grant types is presented in the table below.

Grant type	Description
Client credentials	A popular grant type based on using only credentials (such as an ID and shared secret). The client is assumed to have a close trust relationship with the resource owner.
Password	The resource owner password credentials grant type can be used in cases where the resource owner has an established trust relation with the client. It can also be useful when migrating legacy HTTP clients to OAuth 2.0.
Authorization code	This is an ideal grant type for confidential clients and is based on a redirection-based flow. It can be used to obtain both an access token and refresh token.

JWT contents

An OAuth 2.0 access token is formatted as a JWT. The content is created by the authorization server based on your configuration. However, the tokens are opaque to the client applications. A client has no reason to inspect a token or to be aware of the contents.

Each JWT access token contains a set of claims. The claims describe characteristics of the issuer and the authorization based on administrative definitions at the authorization server. Some of the claims registered with the standard are described in the table below. All the strings are case sensitive.

Claim	Keyword	Description
Issuer	iss	Identifies the principal that issued the token. The claim processing is application specific.

Claim	Keyword	Description
Subject	sub	The subject or user of the token. The name is scoped to be globally or locally unique.
Audience	aud	The recipients the token is intended for. Implemented as an array of strings.
Expiration	exp	The time after which the token expires and must be rejected.

See RFC 7519: JSON Web Tokens for more information.

Client authorization

Overview and options for ONTAP client authorization

The ONTAP OAuth 2.0 implementation is designed to be flexible and robust, providing the features you need to secure your ONTAP environment. There are several mutually exclusive configuration options available. The authorization decisions are ultimately based on the ONTAP REST roles either contained in or derived from the OAuth 2.0 access tokens.

> You can only use ONTAP REST roles when configuring authorization for OAuth 2.0. The earlier ONTAP traditional roles are not supported.

ONTAP applies the single most appropriate authorization option based on your configuration. See How ONTAP determines access for more about how ONTAP makes client access decisions.

OAuth 2.0 self-contained scopes

These scopes contain one or more custom REST roles, each encapsulated within a single string in the access token. They are independent of the ONTAP role definitions. You need to configure the scope strings at your authorization server. See Self-contained OAuth 2.0 scopes for more information.

Local ONTAP REST roles

A single named REST role, either builtin or custom, can be used. The scope syntax for a named role is **ontap-role-**<URL-encoded-ONTAP-role-name>. For example, if the ONTAP role is `admin` the scope string will be `ontap-role-admin`.

Users

The username in the access token defined with access to the application "http" can be used. A user is tested in the following order based on the defined authentication method: password, domain (Active Directory), nsswitch (LDAP).

Groups

The authorization servers can be configured to use ONTAP groups for authorization. If the local ONTAP definitions are examined but no access decision can be made, the Active Directory ("domain") or LDAP ("nsswitch") groups are used. Group information can be specified in one of two ways:

- OAuth 2.0 scope string

  Supports confidential applications using the client credentials flow where there is no user with a group membership. The scope should be named **ontap-group-**<URL-encoded-ONTAP-group-name>. For example, if the group is "development" the scope string will be "ontap-group-development".

- In the "group" claim

  This is intended for access tokens issued by ADFS using the resource owner (password grant) flow.

See Working with OAuth 2.0 or SAML IdP groups in ONTAP for more information.

Self-contained OAuth 2.0 scopes in ONTAP

Self-contained scopes are strings carried in the access token. Each is a complete custom role definition and includes everything ONTAP needs to make an access decision. The scope is separate and distinct from any of the REST roles defined within ONTAP itself.

Format of the scope string

At a base level, the scope is represented as a contiguous string and composed of six colon-separated values. The parameters used in the scope string are described below.

ONTAP literal

The scope must begin with the literal value `ontap` in lowercase. This identifies the scope as specific to ONTAP.

Cluster

This defines which ONTAP cluster the scope applies to. The values can include:

- Cluster UUID

  Identifies a single cluster.

- Asterisk (*)

  Indicates the scope applies to all clusters.

You can use the ONTAP CLI command `cluster identity show` to display the UUID of your cluster. If not specified, the scope applies to all clusters. Learn more about `cluster identity show` in the ONTAP command reference.

Role

The name of the REST role contained in the self-contained scope. This value is not examined by ONTAP or matched to any existing REST roles defined to ONTAP. The name is used for logging.

Access level

This value indicates the access level applied to the client application when using the API endpoint in the scope. There are six possible values as described in the table below.

Access level	Description
none	Denies all access to the specified endpoint.
readonly	Allows only read access using GET.

Access level	Description
read_create	Allows read access as well as the creation of new resource instances using POST.
read_modify	Allows read access as well as the ability to update existing resources using PATCH.
read_create_modify	Allows all access except delete. The allowed operations include GET (read), POST (create), and PATCH (update).
all	Allows full access.

SVM

The name of the SVM within the cluster the scope applies to. Use the * value (asterisk) to indicate all SVMs.

> This feature is not fully supported with ONTAP 9.14.1. You can ignore the SVM parameter and use an asterisk as a placeholder. Review the ONTAP release notes to check for future SVM support.

REST API URI

The complete or partial path to a resource or set of related resources. The string must begin with `/api`. If you don't specify a value, the scope applies to all API endpoints at the ONTAP cluster.

Scope examples

A few examples of self-contained scopes are presented below.

ontap:*:joes-role:read_create_modify:*:/api/cluster

Provides the user assigned this role read, create, and modify access to the `/cluster` endpoint.

CLI administrative tool

To make the administration of the self-contained scopes easier and less error-prone, ONTAP provides the CLI command `security oauth2 scope` to generate scope strings based on your input parameters.

The command `security oauth2 scope` has two use cases based on your input:

- CLI parameters to scope string

  You can use this version of the command to generate a scope string based on the input parameters.

- Scope string to CLI parameters

  You can use this version of the command to generate the command parameters based on the input scope string.

Example

The following example generates a scope string with the output included after the command example below. The definition applies to all clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

`ontap:*:joes-role:readonly:*:/api/cluster`

Learn more about `security oauth2 scope` in the ONTAP command reference.

OAuth 2.0 external role mapping in ONTAP

An external role is defined at an identify provider configured for use by ONTAP. You can create and administer mapping relationships between these external roles and the ONTAP roles using the ONTAP CLI.

> You can also configure the external role mapping feature using the ONTAP REST API. Learn more in the ONTAP automation documentation.

External roles in an access token

Here's a fragment of a JSON access token containing two external roles.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configuration

You can use the ONTAP command line interface to administer the external role mapping feature.

Create

You can define a role mapping configuration with the `security login external-role-mapping create` command. You need to be at the ONTAP **admin** privilege level to issue this command as well as the related options.

Parameters

The parameters used to create a group mapping are described below.

Parameter	Description
`external-role`	The name of the role defined at the external identity provider.
`provider`	The name of the identity provider. This should be the identifier for the system.
`ontap-role`	Indicates the existing ONTAP role the external role is mapped to.

Example

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Learn more about `security login external-role-mapping create` in the ONTAP command reference.

Additional CLI operations

The command supports several additional operations, including:

- Show
- Modify
- Delete

Related information

- ONTAP command reference

How ONTAP determines client access

To properly design and implement OAuth 2.0, you need to understand how your authorization configuration is used by ONTAP to make access decisions for the clients. The major steps used to determine access are presented below based on the ONTAP release.

> There were no significant OAuth 2.0 updates with ONTAP 9.15.1. If you are using the 9.15.1 release, refer to the description for ONTAP 9.14.1.

Related information

- OAuth 2.0 features supported in ONTAP

ONTAP 9.16.1

ONTAP 9.16.1 expands the standard OAuth 2.0 support to include Microsoft Entra ID specific extensions for native Entra ID groups as well as external role mapping.

Determine client access for ONTAP 9.16.1

Step 1: Self-contained scopes

If the access token contains any self-contained scopes, ONTAP examines these scopes first. If there are no self-contained scopes, go to step 2.

With one or more self-contained scopes present, ONTAP applies each scope until an explicit **ALLOW** or **DENY** decision can be made. If an explicit decision is made, processing ends.

If ONTAP can't make an explicit access decision, continue to step 2.

Step 2: Check the local roles flag

ONTAP examines the boolean parameter `use-local-roles-if-present`. The value of this flag is set separately for each authorization server defined to ONTAP.

- If the value is `true` continue to step 3.
- If the value is `false` processing ends and access is denied.

Step 3: Named ONTAP REST role

If the access token contains a named REST role in the `scope` or `scp` field, or as a claim, ONTAP uses the role to make the access decision. This always results in an **ALLOW** or **DENY** decision and processing ends.

If there is no named REST role or the role is not found, continue to step 4.

Step 4: Users

Extract the username from the access token and attempt to match it to users that have access to the application "http". The users are examined based on the authentication method in the following order:

- password
- domain (Active Directory)
- nsswitch (LDAP)

If a matching user is found, ONTAP uses the role defined for the user to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends.

If a user is not matched or if there's no username in the access token, continue to step 5.

Step 5: Groups

If one or more groups are included, the format is examined. If the groups are represented as UUIDs, an internal group mapping table is searched. If there's a group match and an associated role, ONTAP uses the role defined for the group to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends. For more information see Working with OAuth 2.0 or SAML IdP groups in ONTAP.

If groups are represented as names and configured with domain or nsswitch authorization, ONTAP attempts to match them to an Active Directory or LDAP group, respectively. If there's a group match, ONTAP uses the role defined for the group to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends.

If there's no group match or if there's no group in the access token, access is denied and processing ends.

ONTAP 9.14.1

Initial OAuth 2.0 supported is introduced with ONTAP 9.14.1 based on the standard OAuth 2.0 features.

Determine client access for ONTAP 9.14.1

Step 1: Self-contained scopes

If the access token contains any self-contained scopes, ONTAP examines these scopes first. If there are no self-contained scopes, go to step 2.

With one or more self-contained scopes present, ONTAP applies each scope until an explicit **ALLOW** or **DENY** decision can be made. If an explicit decision is made, processing ends.

If ONTAP can't make an explicit access decision, continue to step 2.

Step 2: Check the local roles flag

ONTAP examines the boolean parameter `use-local-roles-if-present`. The value of this flag is set separately for each authorization server defined to ONTAP.

- If the value is `true` continue to step 3.
- If the value is `false` processing ends and access is denied.

Step 3: Named ONTAP REST role

If the access token contains a named REST role in the `scope` or `scp` field, ONTAP uses the role to make the access decision. This always results in an **ALLOW** or **DENY** decision and processing ends.

If there is no named REST role or the role is not found, continue to step 4.

Step 4: Users

Extract the username from the access token and attempt to match it to users that have access to the application "http". The users are examined based on the authentication method in the following order:

- password
- domain (Active Directory)
- nsswitch (LDAP)

If a matching user is found, ONTAP uses the role defined for the user to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends.

If a user is not matched or if there's no username in the access token, continue to step 5.

Step 5: Groups

If one or more groups are included and configured with domain or nsswitch authorization, ONTAP attempts to match them to an Active Directory or LDAP group, respectively.

If there's a group match, ONTAP uses the role defined for the group to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends.

If there's no group match or if there's no group in the access token, access is denied and processing ends.

OAuth 2.0 deployment scenarios with ONTAP

There are several configuration options available when defining an authorization server to ONTAP. Based on these options, you can define an authorization server appropriate for your environment using one of several deployment scenarios.

Summary of the configuration parameters

There are several configuration parameters available when defining an authorization server to ONTAP. These parameters are generally supported in all the administrative interfaces.

> The name used for an individual parameter or field can vary depending on the ONTAP administrative interface. To accommodate the differences in the administrative interfaces, a single generic name is used for each parameter in the table. The exact name used with a specific interface should be obvious based on the context.

Parameter	Description
Name	The name of the authorization server as it is known to ONTAP.
Application	The ONTAP internal application the definition applies to. This must be **http**.
Issuer URI	The FQDN with path identifying the site or organization that issues the tokens.
Provider JWKS URI	The FQDN with path and file name where ONTAP obtains the JSON Web Key Sets used to validate the access tokens.
JWKS refresh interval	The time interval determining how often ONTAP refreshes certificate information from the provider JWKS URI. The value is specified in ISO-8601 format.
Introspection endpoint	The FQDN with path that ONTAP uses to perform remote token validation through introspection.
Client ID	The name of the client as defined at the authorization server. When this value is included, you also need to provide the associated client secret based on the interface.
Outgoing proxy	This is to provide access to the authorization server when ONTAP is behind a firewall. The URI must be in curl format.
Use local roles if present	A boolean flag determining if the local ONTAP definitions are used, including a named REST role and local users.
Remote user claim	An alternative name that ONTAP uses to match local users. Use the `sub` field in the access token to match the local username.
Audience	This field defines the endpoints where the access token can be used.

Deployment scenarios

Several common deployment scenarios are presented below. They are organized based on whether token validation is performed locally by ONTAP or remotely by the authorization server. Each scenario includes a list of the required configuration options. See Deploy OAuth 2.0 in ONTAP for examples of the configuration commands.

After defining an authorization server, you can display its configuration through the ONTAP administrative interface. For example, use the command `security oauth2 client show` with the ONTAP CLI.

Local validation

The following deployment scenarios are based on ONTAP performing token validation locally.

Use self-contained scopes without a proxy

This is the simplest deployment using only OAuth 2.0 self-contained scopes. None of the local ONTAP identity definitions are used. You need to include the following parameters:

- Name
- Application (http)
- Provider JWKS URI
- Issuer URI

You also need to add the scopes at the authorization server.

Use self-contained scopes with a proxy

This deployment scenario uses the OAuth 2.0 self-contained scopes. None of the local ONTAP identity definitions are used. But the authorization server is behind a firewall and so you need to configure a proxy. You need to include the following parameters:

- Name
- Application (http)
- Provider JWKS URI
- Outgoing proxy
- Issuer URI
- Audience

You also need to add the scopes at the authorization server.

Use local user roles and default username mapping with a proxy

This deployment scenario uses local user roles with default name mapping. The remote user claim uses the default value of `sub` and so this field in the access token is used to match the local username. The username must be 40 characters or less. The authorization server is behind a firewall so you also need to configure a proxy. You need to include the following parameters:

- Name
- Application (http)
- Provider JWKS URI
- Use local roles if present (`true`)
- Outgoing proxy
- Issuer

You need to make sure the local user is defined to ONTAP.

Use local user roles and alternate username mapping with a proxy

This deployment scenario uses local user roles with an alternate username which is used to match a local ONTAP user. The authorization server is behind a firewall, so you need to configure a proxy. You need to include the following parameters:

- Name
- Application (http)
- Provider JWKS URI
- Use local roles if present (`true`)
- Remote user claim
- Outgoing proxy
- Issuer URI
- Audience

You need to make sure the local user is defined to ONTAP.

Remote introspection

The following deployment configurations are based on ONTAP performing token validation remotely through introspection.

Use self-contained scopes with no proxy

This is a simple deployment based on using the OAuth 2.0 self-contained scopes. None of the ONTAP identity definitions are used. You must include the following parameters:

- Name
- Application (http)
- Introspection endpoint
- Client ID
- Issuer URI

You need to define the scopes as well as the client and client secret at the authorization server.

Related information

- security oauth2 client show

ONTAP client authentication using OAuth 2.0 Mutual TLS

Depending on your security needs, you can optionally configure Mutual TLS (mTLS) to implement strong client authentication. When used with ONTAP as part of an OAuth 2.0 deployment, mTLS guarantees the access tokens are only used by the clients to which they were originally issued.

Mutual TLS with OAuth 2.0

Transport Layer Security (TLS) is used to establish a secure communication channel between two applications, typically a client browser and web server. Mutual TLS extends this by providing strong identification of the client through a client certificate. When used in an ONTAP cluster with OAuth 2.0, the base mTLS functionality

is extended by creating and using sender-constrained access tokens.

A sender-constrained access token can only be used by the client to which it was originally issued. To support this feature, a new confirmation claim (`cnf`) is inserted into the token. The field contains property `x5t#S256` which holds a digest of the client certificate used when requesting the access token. This value is verified by ONTAP as part of validating the token. Access tokens issued by authorization servers that are not sender-constrained do not include the additional confirmation claim.

You need to configure ONTAP to use mTLS separately for each authorization server. For example, the CLI command `security oauth2 client` includes the parameter `use-mutual-tls` to control mTLS processing based on three values as shown in the table below.

> In each configuration, the outcome and action taken by ONTAP is dependent on the configuration parameter value as well as the contents of the access token and the client certificate. The parameters in the table are organized from the least to the most restrictive.

Parameter	Description
none	OAuth 2.0 mutual TLS authentication is completely disabled for the authorization server. ONTAP will not perform mTLS client certificate authentication even if the confirmation claim is present in the token or a client certificate is supplied with the TLS connection.
request	OAuth 2.0 mutual TLS authentication is enforced if a sender-constrained access token is presented by the client. That is, mTLS is enforced only if the confirmation claim (with property `x5t#S256`) is present in the access token. This is the default setting.
required	OAuth 2.0 mutual TLS authentication is enforced for all access tokens issued by the authorization server. Therefore, all access tokens must be sender-constrained. Authentication and the REST API request fail if the confirmation claim is not present in the access token or there is an invalid client certificate.

High-level implementation flow

The typical steps involved when using mTLS with OAuth 2.0 in an ONTAP environment are presented below. See RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens for more details.

Step 1: Create and install a client certificate

Establishing client identity is based on proving knowledge of a client private key. The corresponding public key is placed in a signed X.509 certificate presented by the client. At a high level, the steps involved in creating the client certificate include:

1. Generate a public and private key pair
2. Create a certificate signing request
3. Send the CSR file to a well-known CA
4. CA verifies the request and issues the signed certificate

You can normally install the client certificate in your local operating system or use it directly with a common utility such as curl.

Step 2: Configure ONTAP to use mTLS

You need to configure ONTAP to use mTLS. This configuration is done separately for each authorization server. For example, with the CLI the command `security oauth2 client` is used with the optional parameter `use-mutual-tls`. See Deploy OAuth 2.0 in ONTAP for more information.

Step 3: Client requests an access token

The client needs to request an access token from the authorization server configured to ONTAP. The client application must use mTLS with the certificate created and installed in step 1.

Step 4: Authorization server generates the access token

The authorization server verifies the client request and generates an access token. As part of this, it creates a message digest of the client certificate which is included in the token as a confirmation claim (field `cnf`).

Step 5: Client application presents the access token to ONTAP

The client application makes a REST API call to the ONTAP cluster and includes the access token in the authorization request header as a **bearer token**. The client must use mTLS with the same certificate used to request the access token.

Step 6: ONTAP verifies client and token.

ONTAP receives the access token in an HTTP request as well as the client certificate used as part of mTLS processing. ONTAP first validates the signature in the access token. Based on the configuration, ONTAP generates a message digest of the client certificate and compares it to the confirmation claim **cnf** in the token. If the two values match, ONTAP has confirmed the client making the API request is the same client the access token was originally issued to.

Related information

- security oauth2 client

Configure and deploy

Prepare to deploy OAuth 2.0 with ONTAP

Before configuring OAuth 2.0 in an ONTAP environment, you should prepare for the deployment. A summary of the major tasks and decisions is included below. The arrangement of the sections is generally aligned with the order you should follow. But while it's applicable for most deployments, you should adapt it to your environment as needed. You should also consider creating a formal deployment plan.

> Based on your environment, you can select the configuration for the authorization servers defined to ONTAP. This includes the parameter values you need to specific for each type of deployment. See OAuth 2.0 deployment scenarios for more information.

Protected resources and client applications

OAuth 2.0 is an authorization framework for controlling access to protected resources. Given this, an important first step with any deployment is to determine what the available resources are and which clients need access to them.

Identify client applications

You need to decide which clients will use OAuth 2.0 when issuing REST API calls and what API endpoints they need access to.

Review existing ONTAP REST roles and local users

You should review the existing ONTAP identity definitions, including the REST roles and local users. Depending on how you configure OAuth 2.0, these definitions can be used for making access decisions.

Global transition to OAuth 2.0

While you might implement OAuth 2.0 authorization gradually, you can also move all the REST API clients to OAuth 2.0 immediately by setting a global flag for each authorization server. This allows access decisions to be made based on your existing ONTAP configuration without the need for creating self-contained scopes.

Authorization servers

The authorization servers play an important role in your OAuth 2.0 deployment by issuing access tokens and enforcing administrative policy.

Select and install the authorization server

You need to select and install one or more authorization servers. It's important to become familiar with the configuration options and procedures of your identity providers, including how to define scopes. Note that some authorization servers, including Microsoft Entra ID, represent groups using UUIDs instead of names.

Determine if the authorization root CA certificate needs to be installed

ONTAP uses the authorization server's certificate to validate the signed access tokens presented by the clients. To do this, ONTAP needs the root CA certificate and any intermediate certificates. These might be pre-installed with ONTAP. If not, you need to install them.

Assess network location and configuration

If the authorization server is behind a firewall, ONTAP needs to be configured to use a proxy server.

Client authentication and authorization

There are several aspects of client authentication and authorization you need to consider.

Self-contained scopes or local ONTAP identity definitions

At a high level, you can either define self-contained scopes defined at the authorization server or rely on the existing local ONTAP identity definitions including roles and users.

Options with local ONTAP processing

If you use the ONTAP identity definitions, you must decide which to apply, including:

- Named REST role
- Match local users
- Active Directory or LDAP groups

Local validation or remote introspection

You need to decide if the access tokens will be validated locally by ONTAP or at the authorization server through introspection. There are also several related values to consider, such as the refresh interval.

Sender-constrained access tokens

For environments requiring a high level of security, you can use send-constrained access tokens based on mTLS. This requires a certificate for each client.

Groups as UUIDs and identity mapping

If you are using an authorization server that represents groups using UUIDs, you need to plan how to map

these to group names and possibly to associated roles.

Administrative interface

You can perform administration of OAuth 2.0 through any of the ONTAP interfaces, including:

- Command line interface
- System Manager
- REST API

How clients request access tokens

The client applications must request access tokens directly from the authorization server. You need to decide how this will be done, including the grant type.

Configure ONTAP

There are several ONTAP configuration tasks you need to perform.

Define REST roles and local users

Based on your authorization configuration, local ONTAP identify processing can be used. In this case, you need to review and define the REST roles and user definitions. And depending on your authorization server, this might also include administering groups based on UUID values.

Core configuration

There are three major steps needed to perform the core ONTAP configuration, including:

- Optionally install the root certificate (and any intermediate certificates) for the CA that signed the authorization server's certificate.
- Define the authorization server.
- Enable OAuth 2.0 processing for the cluster.

Deploy OAuth 2.0 in ONTAP

Deploying the core OAuth 2.0 functionality involves three primary steps.

Before you begin

You must prepare for the OAuth 2.0 deployment before configuring ONTAP. For example, you need to assess the authorization server, including how its certificate was signed and if it's behind a firewall. See Prepare to deploy OAuth 2.0 with ONTAP for more information.

Step 1: Install the authorization server root CA certificates

ONTAP includes a large number of pre-installed root CA certificates. So in many cases, the certificate for your authorization server will be immediately recognized by ONTAP without additional configuration. But depending on how the authorization server certificate was signed, you may need to install a root CA certificate and any intermediate certificates.

Follow the instructions provided below to install the certificate if it's needed. You should install all the required certificates at the cluster level.

Choose the correct procedure based on how you access ONTAP.

Example 1. Steps

System Manager

1. In System Manager, select **Cluster** > **Settings**.
2. Scroll down to the **Security** section.
3. Click → next to **Certificates**.
4. Under the **Trusted certificate authorities** tab click **Add**.
5. Click **Import** and select the certificate file.
6. Complete the configuration parameters for your environment.
7. Click **Add**.

CLI

1. Begin the installation:

   ```
   security certificate install -type server-ca
   ```

2. Look for the following console message:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Open the certificate file with a text editor.
4. Copy the entire certificate including the following lines:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. Paste the certificate into the terminal after the command prompt.
6. Press **Enter** to complete the installation.
7. Confirm the certificate is installed using one of the following:

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

Step 2: Configure the authorization server

You need to define at least one authorization server to ONTAP. You should choose the parameter values based on your configuration and deployment plan. Review OAuth2 deployment scenarios to determine the exact parameters needed for your configuration.

> To modify an authorization server definition, you can delete the existing definition and create a new one.

The example provided below is based on the first simple deployment scenario at Local validation. Self-

contained scopes are used without a proxy.

Choose the correct procedure based on how you access ONTAP. The CLI procedure uses symbolic variables that you need to replace before issuing the command.

Example 2. Steps

System Manager

1. In System Manager, select **Cluster** > **Settings**.
2. Scroll down to the **Security** section.
3. Click **+** next to **OAuth 2.0 authorization**.
4. Select **More options**.
5. Provide the required values for your deployment, such as:
   - Name
   - Application (http)
   - Provider JWKS URI
   - Issuer URI
6. Click **Add**.

CLI

1. Create the definition again:

   ```
   security oauth2 client create -config-name <NAME> -provider-jwks-uri
   <URI_JWKS> -application http -issuer <URI_ISSUER>
   ```

   For example:

   ```
   security oauth2 client create \
   -config-name auth0 \
   -provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
   realm/protocol/openid-connect/certs \
   -application http \
   -issuer https://superzap.dev.netapp.com:8443/realms/my-realm
   ```

   Learn more about `security oauth2 client create` in the ONTAP command reference.

Step 3: Enable OAuth 2.0

The final step is to enable OAuth 2.0. This is a global setting for the ONTAP cluster.

> Don’t enable OAuth 2.0 processing until you confirm that ONTAP, the authorization servers, and any supporting services have all been properly configured.

Choose the correct procedure based on how you access ONTAP.

Example 3. Steps

System Manager

1. In System Manager, select **Cluster** > **Settings**.
2. Scroll down to the **Security section**.
3. Click → next to **OAuth 2.0 authorization**.
4. Enable **OAuth 2.0 authorization**.

CLI

1. Enable OAuth 2.0:

   ```
   security oauth2 modify -enabled true
   ```

2. Confirm OAuth 2.0 is enabled:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Related information

- security certificate install
- security certificate show
- security oauth2 modify
- security oauth2 show

Issue an ONTAP REST API call using OAuth 2.0

The OAuth 2.0 implementation in ONTAP supports REST API client applications. You can issue a simple REST API call using curl to get started using OAuth 2.0. The example presented below retrieves the ONTAP cluster version.

Before you begin

You must configure and enable the OAuth 2.0 feature for your ONTAP cluster. This includes defining an authorization server.

Step 1: Acquire an access token

You need to acquire an access token to use with the REST API call. The token request is performed outside of ONTAP and the exact procedure depends on the authorization server and its configuration. You might request the token through a web browser, with a curl command, or using a programming language.

For illustration purposes, an example of how an access token can be requested from Keycloak using curl is presented below.

Keycloak example

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

You should copy and save the returned token.

Step 2: Issue the REST API call

After you have a valid access token, you can use a curl command with the access token to issue a REST API call.

Parameters and variables

The two variables in the curl example are described in the table below.

Variable	Description
$FQDN_IP	The fully qualified domain name or IP address of the ONTAP management LIF.
$ACCESS_TOKEN	The OAuth 2.0 access token issued by the authorization server.

You should first set these variables in the Bash shell environment before issuing the curl example. For example, in the Linux CLI type the following command to set and display the FQDN variable:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

After both variables are defined in your local Bash shell, you can copy the curl command and paste it into the CLI. Press **Enter** to substitute the variables and issue the command.

Curl example

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

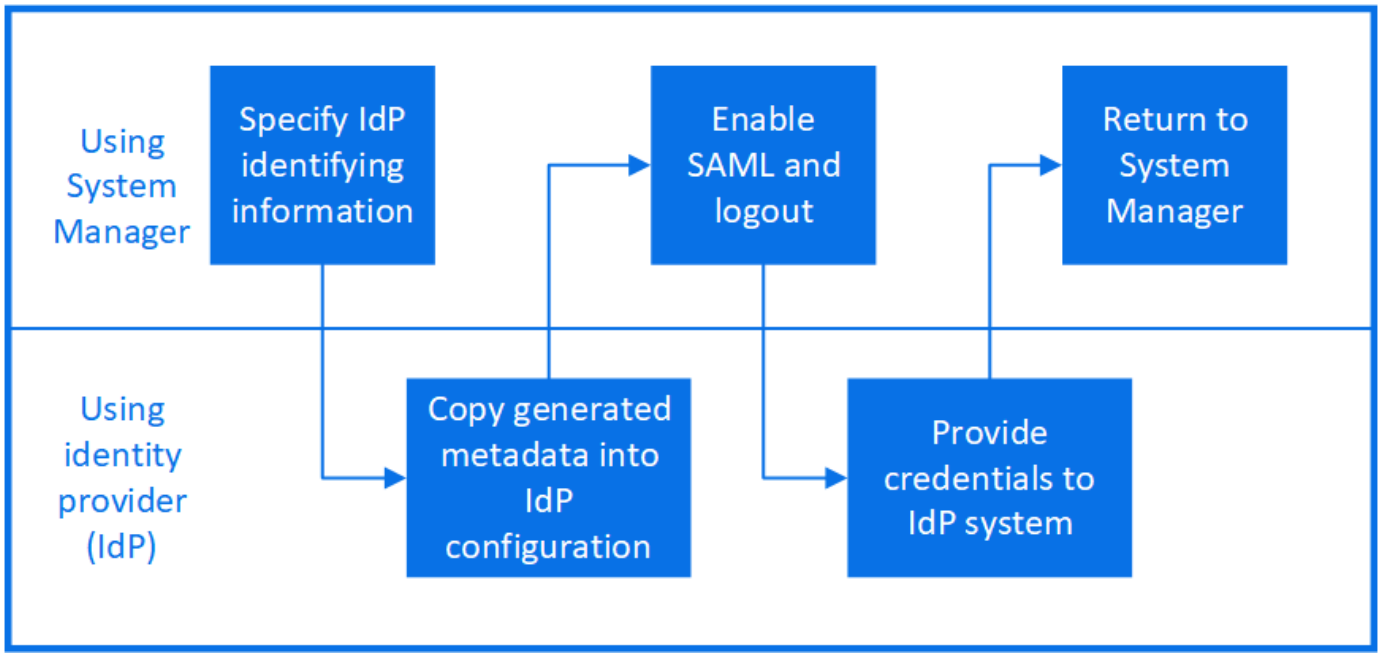
Configure SAML authentication for remote ONTAP users

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. When SAML authentication is disabled, the configured directory service providers such as Active Directory and LDAP are used for authentication.

Enable SAML authentication

To enable SAML authentication with System Manager or with the CLI, perform the following steps. If your cluster is running ONTAP 9.7 or earlier, the System Manager steps you need to follow are different. Refer to the System Manager online help available on your system.

> After you enable SAML authentication, only remote users configured for SAML authentication can access the System Manager GUI. Local users cannot access the System Manager GUI after SAML authentication is enabled.



About this task

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

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

- SAML authentication is applicable only for accessing the admin SVM.
- Beginning with ONTAP 9.17.1, IdP-provided group information can be mapped to ONTAP roles. This allows you to assign roles to users based on groups that are defined in the IdP. For more information, see Working with OAuth 2.0 or SAML IdP groups in ONTAP.

The following IdPs have been validated with System Manager:

- Microsoft Entra ID (validated with ONTAP 9.17.1 and later)
- Active Directory Federation Services
- Cisco Duo (validated with the following ONTAP versions:)
  - 9.7P21 and later 9.7 releases (refer to the System Manager Classic documentation)
  - 9.8P17 and later 9.8 patch releases
  - 9.9.1P13 and later 9.9.1 patch releases
  - 9.10.1P9 and later 9.10.1 patch releases
  - 9.11.1P4 and later 9.11.1 patch releases
  - 9.12.1 and later releases
- Shibboleth

Before you begin

- The IdP that you plan to use for remote authentication must be configured. You must have the URI of the IdP. The IdP URI is the web address that ONTAP sends authentication requests to and receive responses from.
- Port 443 must be open between the ONTAP cluster and the IdP.
- The ONTAP cluster and the IdP must each be able to ping the other's fully qualified domain name. Ensure DNS is properly configured and the cluster certificate is not expired.
- If needed, add the IdP's trusted certificate authority (CA) to ONTAP. You can manage ONTAP certificates with System Manager. You might need to configure the ONTAP cluster certificate in the IdP.
- You must be able to access the ONTAP cluster's Service Processor (SP) console. If SAML is misconfigured, you will need to disable it from the SP console.
- If you are using Entra ID (validated beginning with ONTAP 9.17.1), you must configure Entra ID with the ONTAP metadata before creating the ONTAP SAML configuration. Entra ID will not provide the IdP URI until it is configured with the ONTAP metadata. The IdP URI is required to create the ONTAP SAML configuration.
  - If you are using System Manager to configure SAML, leave the IdP URI field blank until System Manager provides the ONTAP metadata. Configure Entra ID with the ONTAP metadata, and then copy the IdP URI into System Manager before enabling the SAML configuration.
  - If you are using the ONTAP CLI to configure SAML, you must generate the ONTAP metadata before enabling the ONTAP SAML configuration. You can generate the ONTAP metadata file with the following command:

    ```
    security saml-sp default-metadata create -sp-host <ontap_host_name>
    ```

    `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 cluster-management IP address is used. You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.

    Configure Entra ID with the provided metadata. You must configure Entra ID before creating the ONTAP SAML configuration. After Entra is configured, proceed with the below CLI procedure.

  - You cannot generate the ONTAP metadata for Entra ID until all nodes in the cluster are on version 9.17.1.

Steps

Perform the following steps depending on your environment:

System Manager

1. Click **Cluster > Settings**.
2. Next to **SAML Authentication**, click ⚙.
3. Ensure there is a check in the **Enable SAML Authentication** checkbox.
4. Enter the URL of the IdP URI (including "https://"). If you are using Entra ID, skip this step.
5. Modify the host system address, if needed. This is the address that the IdP will direct to after authentication. The default is the cluster-management IP address.
6. Ensure the correct certificate is being used:
   - If your system was mapped with only one certificate with type "server", then that certificate is considered the default and it isn't displayed.
   - If your system was mapped with multiple certificates as type "server", then one of the certificates is displayed. To select a different certificate, click **Change**.
7. Click **Save**. A confirmation window displays the metadata information, which has been automatically copied to your clipboard.
8. Go to the IdP system you specified and copy the metadata from your clipboard to update the system metadata. If you are using Entra ID, copy the IdP URI into ONTAP after you have configured Entra ID with the system metadata.
9. Return to the confirmation window (in System Manager) and check the checkbox **I have configured the IdP with the host URI or metadata**.
10. Click **Logout** to enable SAML-based authentication. The IdP system will display an authentication screen.
11. In the IdP sign-on page, enter your SAML-based credentials. After your credentials are verified, you will be directed to the System Manager home page.

CLI

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.

   > Some URLs include the question mark (?) character. The question mark activates the ONTAP command line active help. In order to enter a URL with a question mark, you need to first disable active help with the command `set -active-help false`. Active help can later be re-enabled with the command `set -active-help true`. Learn more in the ONTAP command reference.

   `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://example.url.net/idp/shibboleth

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://10.0.0.1/saml-sp/Metadata

Configure the IdP and 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 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. If you are using Entra ID, you have already completed this step.
3. Once the IdP is configured, 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. Prior to ONTAP 9.17.1, a SAML login is automatically created for existing `http` or `ontapi` users when SAML is enabled. New users must be configured for SAML. Beginning with ONTAP 9.17.1, all users created with `password`, `domain`, or `nsswitch` authentication methods are automatically authenticated against the IdP when SAML is enabled.

   a. Create a login method for new users with SAML authentication. The `user_name` must match the username configured in the IdP:

      > The `user_name` value is case-sensitive. Unless you are using Entra ID, include only the user name, and do not include any portion of the domain. If you are using Entra ID, you can create the user name with the domain, for example *user_name@domain.com*.

      ```
      security login create -user-or-group-name <user_name> -application [http
      | ontapi] -authentication-method saml -vserver <svm_name>
      ```

      Example:

```
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
```

Example:

```
cluster_12::> security login show

Vserver: cluster_12

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

Learn more about `security login show` in the ONTAP command reference.

Disable SAML authentication

You can disable SAML authentication when you want to stop authenticating remote System Manager users with an external Identity Provider (IdP). When SAML authentication is disabled, local user authentication or the configured directory service providers such as Active Directory and LDAP are used to authenticate users.

Perform the following steps depending on your environment:

Example 4. Steps

System Manager

1. Click **Cluster > Settings**.
2. Under **SAML Authentication**, click the **Enabled** toggle button.
3. *Optional*: You can also click ⚙ next to **SAML Authentication**, and then uncheck the **Enable SAML Authentication** checkbox.

CLI

1. Disable SAML authentication:

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

2. If you no longer want to use SAML authentication or if you want to modify the IdP, delete the SAML configuration:

   ```
   security saml-sp delete
   ```

Configure third-party IdP

About this task

In order to authenticate with ONTAP, you might need to change the settings for your IdP. The following sections provide configuration information for supported IdPs.

Entra ID

When configuring Entra ID, create a new application and configure SAML sign-on with the metadata provided by ONTAP. After the application is created, edit the "Attributes & Claims" section of the application SAML settings to match the following:

Setting	Value
Name	urn:oid:0.9.2342.19200300.100.1.1
Namespace	*Leave blank*
Name format	URI
Source	Attribute
Source attribute	user.userprincipalname

If you want to use groups with Entra ID, add a group claim with the following settings:

Setting	Value
Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Namespace	*Leave blank*
Source attribute	Group ID

Entra ID provides group information in UUID format. For more information on using groups with Entra ID, refer to Manage groups with UUIDs.

The *App Federation Metadata URL* provided in the "SAML certificate" section of the application SAML settings is the IdP URI that you will enter in ONTAP.

For information on configuring Entra ID multifactor authentication, refer to Plan a Microsoft Entra multifactor authentication deployment.

For more information, refer to the Entra ID documentation.

Active Directory Federation Services

When configuring Active Directory Federation Services (AD FS), you must add a new claims-aware Relying Party Trust with the service provider metadata provided by ONTAP. Once the Relying Party Trust is created, add the following claim rules to the Relying Party Trust's Claim Issuance Policy using the "Send LDAP Attributes as Claims" template:

Attribute store	LDAP attribute	Outgoing claim type
Active Directory	SAM-account-name	Name ID
Active Directory	SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Active Directory	Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:uri
Active Directory	Token groups - Qualified by Domain Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Active Directory	sAMAccountName	urn:oid:1.2.840.113556.1.4.221

AD FS provides group information in name format. For more information on using groups with AD FS, refer to Manage groups with names.

For more information, refer to the AD FS documentation.

Cisco Duo

Refer to the Cisco Duo documentation for configuration information.

Shibboleth

Prior to configuring the Shibboleth IdP, you must have configured an LDAP server.

When enabling SAML on ONTAP, save the provided host metadata XML. On the host where Shibboleth is installed, replace the contents of `metadata/sp-metadata.xml` with the host metadata XML within the Shibboleth IdP home directory.

For more information, refer to Shibboleth.

Troubleshoot issues with SAML configuration

If configuring Security Assertion Markup Language (SAML) authentication fails, you can manually repair each node on which the SAML configuration failed and recover from the failure. During the repair process, the web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

About this task

When you configure SAML authentication, ONTAP applies SAML configuration on a per-node basis. When you enable SAML authentication, ONTAP automatically tries to repair each node if there are configuration issues. If there are issues with SAML configuration on any node, you can disable SAML authentication and then reenable SAML authentication. There can be situations when SAML configuration fails to apply on one or more nodes even after you reenable SAML authentication. You can identify the node on which SAML configuration has failed and then manually repair that node.

Steps

1. Log in to the advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Identify the node on which SAML configuration failed:

   ```
   security saml-sp status show -instance
   ```

   Example:

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                 Update Status: config-failed
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Learn more about `security saml-sp status show` in the ONTAP command reference.

3. Repair the SAML configuration on the failed node:

   `security saml-sp repair -node <node_name>`

   Example:

```
cluster_12::*> security saml-sp repair -node node2

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 181] Job is running.
[Job 181] Job success.
```

   The web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

   Learn more about `security saml-sp repair` in the ONTAP command reference.

4. Verify that SAML is successfully configured on all of the nodes:

   `security saml-sp status show -instance`

   Example:

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                 Update Status: config-success
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Learn more about `security saml-sp status show` in the ONTAP command reference.

Related information

- ONTAP command reference
- security saml-sp
- security login create

Working with OAuth 2.0 or SAML IdP groups in ONTAP

ONTAP provides several options for configuring groups based on your OAuth 2.0 authorization server or SAML identity provider (IdP). The groups can then be mapped to roles which are used by ONTAP to determine access.

Beginning with ONTAP 9.17.1, SAML IdP-provided group information can be mapped to ONTAP roles. This allows you to assign roles to users based on the groups that are defined in the IdP. For more information, see Configure SAML authentication. Beginning with ONTAP 9.14.1, ONTAP supports group name authentication for OAuth 2.0. Beginning with ONTAP 9.16.1, ONTAP supports OAuth 2.0 group UUID authentication and role mapping. For more information, see Overview of the ONTAP OAuth 2.0 implementation.

How groups are identified

When you configure a group at an authorization server or SAML IdP, it's identified and carried in an OAuth 2.0 access token or SAML assertion using either a name or UUID. You need to be aware of how your authorization server or SAML IdP handles groups before configuring ONTAP.

> If multiple groups are included in an access token, ONTAP will attempt to use each one until there is a match.

Group names

Many authorization servers and SAML IdPs, like Active Directory Federation Service (ADFS), identify and represent groups using a name. Here's a fragment of a JSON OAuth 2.0 access token generated by ADFS containing several groups. See Manage groups with names for more information.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

Group UUIDs

Some authorization servers and SAML IdPs, like Microsoft Entra ID, identify and represent groups using a UUID. Here's a fragment of an OAuth 2.0 access token generated by Entra ID containing several groups. See Manage groups with UUIDs for more information.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Manage groups with names

If your authorization server or SAML IdP uses names to identify groups, you need to make sure each group is defined for your ONTAP cluster. Depending on your security environment, you might already have the group defined.

Here's an example CLI command defining an ONTAP group. Notice it uses a named group from the sample access token. You need to be at the ONTAP **admin** privilege level to issue the command.

Example

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

Use `-authentication-method domain` or `nsswitch` for SAML IdP and OAuth 2.0 authorization server

groups.

> You can also configure this feature using the ONTAP REST API. Learn more in the ONTAP automation documentation.

Manage groups with UUIDs

If your authorization server or SAML IdP represents groups using UUID values, you need to perform a two-step configuration before using a group. Beginning with ONTAP 9.16.1, two mapping features are available and have been tested with Entra ID. Entra ID for OAuth 2.0 is supported beginning with ONTAP 9.16.1, and Entra ID for SAML is supported beginning with ONTAP 9.17.1. You need to be at the ONTAP **admin** privilege level to issue the CLI commands.

> You can also configure these features using the ONTAP REST API. Learn more in the ONTAP automation documentation.

Map a group UUID to a group name

If you're using an authorization server or SAML IdP that represents groups using UUID values, you need to map the group UUIDs to group names. The primary ONTAP CLI operations are described below.

Create

You can define a new group mapping configuration with the `security login group create` command. The group UUID and name should match the configuration at the authorization server or SAML IdP. Learn more about `security login group create` in the ONTAP command reference.

Parameters

The parameters used to create a group mapping are described below.

Parameter	Description
`vserver`	Optionally specifies the name of the SVM (vserver) the group is associated with. If omitted, the group is associated with the ONTAP cluster.
`name`	The unique name of the group that ONTAP will use.
`type`	This value indicates the identity provider the group originates from.
`uuid`	Specifies the universally unique identifier of the group as provided by the authorization server or SAML IdP.

Here's an example CLI command defining a group for ONTAP. Notice it uses a UUID group from the sample access token.

Example

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

After creating the group, a unique read-only integer identifier is generated for the group.

Additional CLI operations

The command supports several additional operations, including:

- Show
- Modify
- Delete

You can use the `show` option to retrieve the unique group ID generated for a group. Learn more about `show` in the ONTAP command reference.

Map a group UUID to a role

If you're using an authorization server or SAML IdP that represents groups using UUID values, you can map the group to a role. For more information on Role-Based Access Control in ONTAP, refer to Learn about managing ONTAP access-control roles. The primary ONTAP CLI operations are described below. You need to be at the ONTAP **admin** privilege level to issue the commands.

> You need to first map a group UUID to a group name and retrieve the unique integer ID generated for the group. You'll need the ID to map the group to a role.

Create

You can define a new role mapping with the `security login group role-mapping create` command. Learn more about `security login group role-mapping create` in the ONTAP command reference.

Parameters

The parameters used to map a group to a role are described below.

Parameter	Description
`group-id`	Specifies the unique ID generated for the group using the command `security login group create`.
`role`	The name of the ONTAP role the group is mapped to.

Example

```
security login group role-mapping create -group-id 1 -role admin
```

Additional CLI operations

The command supports several additional operations, including:

- Show
- Modify
- Delete

Learn more about the commands described in this procedure in the ONTAP command reference.

Related information

- External role mapping

Authentication and authorization using WebAuthn MFA

Learn about WebAuthn multi-factor authentication for ONTAP System Manager users

Beginning with ONTAP 9.16.1, administrators can enable WebAuthn multi-factor authentication (MFA) for users that log in to System Manager. This enables System Manager logins using a FIDO2 key (such as a YubiKey) as a second form of authentication. By default, WebAuthn MFA is disabled for new and existing ONTAP users.

WebAuthn MFA is supported for users and groups that use the following types of authentication for the first authentication method:

- Users: password, domain, or nsswitch
- Groups: domain or nsswitch

After you enable WebAuthn MFA as the second authentication method for a user, the user is asked to register a hardware authenticator upon logging in to System Manager. After registration, the private key is stored in the authenticator, and the public key is stored in ONTAP.

ONTAP supports one WebAuthn credential per user. If a user loses an authenticator and needs to have it replaced, the ONTAP administrator needs to delete the WebAuthn credential for the user so that the user can register a new authenticator upon the next login.

> Users that have WebAuthn MFA enabled as a second authentication method need to use the FQDN (for example, "https://myontap.example.com") instead of the IP address (for example, "https://192.168.100.200") to access System Manager. For users with WebAuthn MFA enabled, attempts to log in to the System Manager using the IP address are rejected.

Enable WebAuthn MFA for ONTAP System Manager users or groups

As an ONTAP administrator, you can enable WebAuthn MFA for a System Manager user or group by either adding a new user or group with the WebAuthn MFA option enabled or enabling the option for an existing user or group.

> After you enable WebAuthn MFA as the second authentication method for a user or group, the user (or all users in that group) will be asked to register a hardware FIDO2 device upon the next login to System Manager. This registration is handled by the user's local operating system, and usually consists of inserting the security key, creating a passkey, and touching the security key (if supported).

Enable WebAuthn MFA when creating a new user or group

You can create a new user or group with WebAuthn MFA enabled using either System Manager or the ONTAP CLI.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. Select **Add** under **Users**.
4. Specify a user or group name and select a role in the drop-down menu for **Role**.
5. Specify a login method and password for the user or group.

   WebAuthn MFA supports login methods of "password", "domain", or "nsswitch" for users, and "domain" or "nsswitch" for groups.

6. In the **MFA for HTTP** column, select **Enabled**.
7. Select **Save**.

CLI

1. Create a new user or group with WebAuthn MFA enabled.

   In the following example, WebAuthn MFA is enabled by choosing "publickey" for the second authentication method:

   ```
   security login create -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

   Learn more about `security login create` in the ONTAP command reference.

Enable WebAuthn MFA for an existing user or group

You can enable WebAuthn MFA for an existing user or group.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. In the list of users and groups, select the option menu for the user or group you want to edit.

   WebAuthn MFA supports login methods of "password", "domain", or "nsswitch" for users, and "domain" or "nsswitch" for groups.

4. In the **MFA for HTTP** column for that user, select **Enabled**.
5. Select **Save**.

CLI

1. Modify an existing user or group to enable WebAuthn MFA for that user or group.

   In the following example, WebAuthn MFA is enabled by choosing "publickey" for the second authentication method:

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

   Learn more about `security login modify` in the ONTAP command reference.

Disable WebAuthn MFA for ONTAP System Manager users

As an ONTAP administrator, you can disable WebAuthn MFA for a user or group by editing the user or group with System Manager or the ONTAP CLI.

Disable WebAuthn MFA for an existing user or group

You can disable WebAuthn MFA for an existing user or group at any time.

> If you disable registered credentials, the credentials are retained. If you enable the credentials again in the future, the same credentials are used, so the user doesn't need to re-register upon logging in.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. In the list of users and groups, select the user or group you want to edit.
4. In the **MFA for HTTP** column for that user, select **Disabled**.
5. Select **Save**.

CLI

1. Modify an existing user or group to disable WebAuthn MFA for that user or group.

   In the following example, WebAuthn MFA is disabled by choosing "none" for the second authentication method.

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method none \
                         -application http \
                         -role admin
   ```

   Learn more about `security login modify` in the ONTAP command reference.

View ONTAP WebAuthn MFA settings and manage credentials

As an ONTAP administrator, you can view cluster-wide WebAuthn MFA settings and manage user and group credentials for WebAuthn MFA.

View cluster settings for WebAuthn MFA

You can view the cluster settings for WebAuthn MFA using the ONTAP CLI.

Steps

1. View the cluster settings for WebAuthn MFA. You can optionally specify a storage VM using the `vserver` argument:

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

   Learn more about `security webauthn show` in the ONTAP command reference.

View supported public key WebAuthn MFA algorithms

You can view the supported public key algorithms for WebAuthn MFA for a storage VM or for a cluster.

Steps

1. List the supported public key WebAuthn MFA algorithms. You can optionally specify a storage VM using the `vserver` argument:

   ```
   security webauthn supported-algorithms show -vserver <storage_vm_name>
   ```

   Learn more about `security webauthn supported-algorithms show` in the ONTAP command reference.

View the registered WebAuthn MFA credentials

As an ONTAP administrator, you can view the registered WebAuthn credentials for all users. Non-administrator users that use this procedure can only view their own registered WebAuthn credentials.

Steps

1. View the registered WebAuthn MFA credentials:

   ```
   security webauthn credentials show
   ```

   Learn more about `security webauthn credentials show` in the ONTAP command reference.

Remove a registered WebAuthn MFA credential

You can remove a registered WebAuthn MFA credential. This is useful when a user's hardware key was lost, stolen, or is no longer in use. You can also remove a registered credential when the user still has the original hardware authenticator, but wants to replace it with a new one. After removing the credential, the user will be prompted to register the replacement authenticator.

> Removing a registered credential for a user doesn't disable WebAuthn MFA for the user. If a user loses a hardware authenticator and needs to log in before replacing it, you need to remove the credential using these steps and also Disable WebAuthn MFA for the user.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. In the list of users and groups, select the option menu for the user or group whose credentials you want to remove.
4. Select **Remove MFA for HTTP credentials**.
5. Select **Remove**.

CLI

1. Delete the registered credentials. Note the following:
   - You can optionally specify a storage VM of the user. If omitted, the credential is removed at the cluster level.
   - You can optionally specify a username of the user for whom you are deleting the credential. If omitted, the credential is removed for the current user.

     ```
     security webauthn credentials delete -vserver <storage_vm_name>
     -username <username>
     ```

     Learn more about `security webauthn credentials delete` in the ONTAP command reference.

Manage web services

Manage web services overview

You can enable or disable a web service for the cluster or a storage virtual machine (SVM), display the settings for web services, and control whether users of a role can access a web service.

You can manage web services for the cluster or an SVM in the following ways:

- Enabling or disabling a specific web service
- Specifying whether access to a web service is restricted to only encrypted HTTP (SSL)
- Displaying the availability of web services
- Allowing or disallowing users of a role to access a web service
- Displaying the roles that are permitted to access a web service

For a user to access a web service, all of the following conditions must be met:

- The user must be authenticated.

  For instance, a web service might prompt for a user name and password. The user's response must match a valid account.

- The user must be set up with the correct access method.

  Authentication only succeeds for users with the correct access method for the given web service. For the ONTAP API web service (`ontapi`), users must have the `ontapi` access method. For all other web services, users must have the `http` access method.

  > You use the `security login` commands to manage users' access methods and authentication methods.

- The web service must be configured to allow the user's access-control role.

  > You use the `vserver services web access` commands to control a role's access to a web service.

If a firewall is enabled, the firewall policy for the LIF to be used for web services must be set up to allow HTTP or HTTPS.

If you use HTTPS for web service access, SSL for the cluster or SVM that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

Manage access to ONTAP web services

A web service is an application that users can access by using HTTP or HTTPS. The cluster administrator can set up the web protocol engine, configure SSL, enable a web service, and enable users of a role to access a web service.

Beginning with ONTAP 9.6, the following web services are supported:

- Service Processor Infrastructure (`spi`)

  This service makes a node's log, core dump, and MIB files available for HTTP or HTTPS access through the cluster management LIF or a node management LIF. The default setting is `enabled`.

  Upon a request to access a node's log files or core dump files, the `spi` web service automatically creates a mount point from a node to another node's root volume where the files reside. You do not need to manually create the mount point.

- ONTAP APIs (`ontapi`)

  This service enables you to run ONTAP APIs to execute administrative functions with a remote program. The default setting is `enabled`.

  This service might be required for some external management tools. For example, if you use System Manager, you should leave this service enabled.

- Data ONTAP Discovery (`disco`)

  This service enables off-box management applications to discover the cluster in the network. The default setting is `enabled`.

- Support Diagnostics (`supdiag`)

This service controls access to a privileged environment on the system to assist problem analysis and resolution. The default setting is `disabled`. You should enable this service only when directed by technical support.

- System Manager (`sysmgr`)

  This service controls the availability of System Manager, which is included with ONTAP. The default setting is `enabled`. This service is supported only on the cluster.

- Firmware Baseboard Management Controller (BMC) Update (`FW_BMC`)

  This service enables you to download BMC firmware files. The default setting is `enabled`.

- ONTAP Documentation (`docs`)

  This service provides access to the ONTAP documentation. The default setting is `enabled`.

- ONTAP RESTful APIs (`docs_api`)

  This service provides access to the ONTAP RESTful API documentation. The default setting is `enabled`.

- File Upload and Download (`fud`)

  This service offers file upload and download. The default setting is `enabled`.

- ONTAP Messaging (`ontapmsg`)

  This service supports a publish and subscribe interface allowing you to subscribe to events. The default setting is `enabled`.

- ONTAP Portal (`portal`)

  This service implements the gateway into a virtual server. The default setting is `enabled`.

- ONTAP Restful Interface (`rest`)

  This service supports a RESTful interface that is used to remotely manage all elements of the cluster infrastructure. The default setting is `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

  This service provides resources to support the SAML service provider. The default setting is `enabled`.

- SAML Service Provider (`saml-sp`)

  This service offers services such as SP metadata and the assertion consumer service to the service provider. The default setting is `enabled`.

Beginning with ONTAP 9.7, the following additional services are supported:

- Configuration Backup Files (`backups`)

This service enables you to download configuration backup files. The default setting is `enabled`.

- ONTAP Security (`security`)

  This service supports CSRF token management for enhanced authentication. The default setting is `enabled`.

Manage the web protocol engine in ONTAP

You can configure the web protocol engine on the cluster to control whether web access is allowed and what SSL versions can be used. You can also display the configuration settings for the web protocol engine.

You can manage the web protocol engine at the cluster level in the following ways:

- You can specify whether remote clients can use HTTP or HTTPS to access web service content by using the `system services web modify` command with the `-external` parameter.
- You can specify whether SSLv3 should be used for secure web access by using the `security config modify` command with the `-supported-protocol` parameter.
  By default, SSLv3 is disabled. Transport Layer Security 1.0 (TLSv1.0) is enabled and it can be disabled if needed.

  Learn more about `security config modify` in the ONTAP command reference.

- You can enable Federal Information Processing Standard (FIPS) 140-2 compliance mode for cluster-wide control plane web service interfaces.

  By default, FIPS 140-2 compliance mode is disabled.

  - **When FIPS 140-2 compliance mode is disabled**
    You can enable FIPS 140-2 compliance mode by setting the `is-fips-enabled` parameter to `true` for the `security config modify` command, and then using the `security config show` command to confirm the online status.
  - **When FIPS 140-2 compliance mode is enabled**
    - Beginning with ONTAP 9.11.1, TLSv1, TLSv1.1 and SSLv3 are disabled, and only TSLv1.2 and TSLv1.3 remain enabled. It affects other systems and communications that are internal and external to ONTAP 9. If you enable FIPS 140-2 compliance mode and then subsequently disable, TLSv1, TLSv1.1, and SSLv3 remain disabled. Either TLSv1.2 or TLSv1.3 will remain enabled depending on the previous configuration.
    - For versions of ONTAP prior to 9.11.1, both TLSv1 and SSLv3 are disabled and only TLSv1.1 and TLSv1.2 remain enabled. ONTAP prevents you from enabling both TLSv1 and SSLv3 when FIPS 140-2 compliance mode is enabled. If you enable FIPS 140-2 compliance mode and then subsequently disable it, TLSv1 and SSLv3 remain disabled, but either TLSv1.2 or both TLSv1.1 and TLSv1.2 are enabled depending on the previous configuration.
- You can display the configuration of cluster-wide security by using the `system security config show` command.

  Learn more about `security config show` in the ONTAP command reference.

If the firewall is enabled, the firewall policy for the logical interface (LIF) to be used for web services must be set up to allow HTTP or HTTPS access.

If you use HTTPS for web service access, SSL for the cluster or storage virtual machine (SVM) that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

In MetroCluster configurations, the setting changes you make for the web protocol engine on a cluster are not replicated on the partner cluster.

ONTAP commands for managing the web protocol engine

You use the `system services web` commands to manage the web protocol engine. You use the `system services firewall policy create` and `network interface modify` commands to allow web access requests to go through the firewall.

If you want to…	Use this command…
Configure the web protocol engine at the cluster level: • Enable or disable the web protocol engine for the cluster • Enable or disable SSLv3 for the cluster • Enable or disable FIPS 140-2 compliance for secure web services (HTTPS)	`system services web modify`
Display the configuration of the web protocol engine at the cluster level, determine whether the web protocols are functional throughout the cluster, and display whether FIPS 140-2 compliance is enabled and online	`system services web show`
Display the configuration of the web protocol engine at the node level and the activity of web service handling for the nodes in the cluster	`system services web node show`
Create a firewall policy or add HTTP or HTTPS protocol service to an existing firewall policy to allow web access requests to go through firewall	`system services firewall policy create` Setting the `-service` parameter to `http` or `https` enables web access requests to go through firewall.
Associate a firewall policy with a LIF	`network interface modify` You can use the `-firewall-policy` parameter to modify the firewall policy of a LIF.

Related information

- network interface modify

Configure access to ONTAP web services

Configuring access to web services allows authorized users to use HTTP or HTTPS to access the service content on the cluster or a storage virtual machine (SVM).

Steps

1. If a firewall is enabled, ensure that HTTP or HTTPS access is set up in the firewall policy for the LIF that will be used for web services:

   > You can check whether a firewall is enabled by using the `system services firewall show` command.

   a. To verify that HTTP or HTTPS is set up in the firewall policy, use the `system services firewall policy show` command.

      You set the `-service` parameter of the `system services firewall policy create` command to `http` or `https` to enable the policy to support web access.

   b. To verify that the firewall policy supporting HTTP or HTTPS is associated with the LIF that provides web services, use the `network interface show` command with the `-firewall-policy` parameter.

      Learn more about `network interface show` in the ONTAP command reference.

      You use the `network interface modify` command with the `-firewall-policy` parameter to put the firewall policy into effect for a LIF.

      Learn more about `network interface modify` in the ONTAP command reference.

2. To configure the cluster-level web protocol engine and make web service content accessible, use the `system services web modify` command.
3. If you plan to use secure web services (HTTPS), enable SSL and provide digital certificate information for the cluster or SVM by using the `security ssl modify` command.

   Learn more about `security ssl modify` in the ONTAP command reference.

4. To enable a web service for the cluster or SVM, use the `vserver services web modify` command.

   You must repeat this step for each service that you want to enable for the cluster or SVM.

5. To authorize a role to access web services on the cluster or SVM, use the `vserver services web access create` command.

   The role that you grant access must already exist. You can display existing roles by using the `security login role show` command or create new roles by using the `security login role create` command.

   Learn more about `security login role show` and `security login role create` in the ONTAP command reference.

6. For a role that has been authorized to access a web service, ensure that its users are also configured with the correct access method by checking the output of the `security login show` command.

To access the ONTAP API web service (`ontapi`), a user must be configured with the `ontapi` access method. To access all other web services, a user must be configured with the `http` access method.

Learn more about `security login show` in the ONTAP command reference.

> You use the `security login create` command to add an access method for a user. Learn more about `security login create` in the ONTAP command reference.

ONTAP commands for managing web services

You use the `vserver services web` commands to manage the availability of web services for the cluster or a storage virtual machine (SVM). You use the `vserver services web access` commands to control a role's access to a web service.

If you want to…	Use this command…
Configure a web service for the cluster or anSVM: • Enable or disable a web service • Specify whether only HTTPS can be used for accessing a web service	`vserver services web modify`
Display the configuration and availability of web services for the cluster or anSVM	`vserver services web show`
Authorize a role to access a web service on the cluster or anSVM	`vserver services web access create`
Display the roles that are authorized to access web services on the cluster or anSVM	`vserver services web access show`
Prevent a role from accessing a web service on the cluster or anSVM	`vserver services web access delete`

Related information

ONTAP command reference

Commands for managing mount points on ONTAP nodes

The `spi` web service automatically creates a mount point from one node to another node's root volume upon a request to access the node's log files or core files. Although you do not need to manually manage mount points, you can do so by using the `system node root-mount` commands.

If you want to…	Use this command…
Manually create a mount point from one node to another node's root volume	`system node root-mount create` Only a single mount point can exist from one node to another.
Display existing mount points on the nodes in the cluster, including the time a mount point was created and its current state	`system node root-mount show`
Delete a mount point from one node to another node's root volume and force connections to the mount point to close	`system node root-mount delete`

Related information

ONTAP command reference

Manage SSL in ONTAP

Use the `security ssl` commands to manage the SSL protocol for the cluster or a storage virtual machine (SVM). SSL protocol improves the security of web access by using a digital certificate to establish an encrypted connection between a web server and a browser.

You can manage SSL for the cluster or a storage virtual machine (SVM) in the following ways:

- Enabling SSL
- Generating and installing a digital certificate and associating it with the cluster or SVM
- Displaying the SSL configuration to see whether SSL has been enabled, and, if available, the SSL certificate name
- Setting up firewall policies for the cluster or SVM, so that web access requests can go through
- Defining which SSL versions can be used
- Restricting access to only HTTPS requests for a web service

Commands for managing SSL

You use the `security ssl` commands to manage the SSL protocol for the cluster or a storage virtual machine (SVM).

If you want to…	Use this command…
Enable SSL for the cluster or an SVM, and associate a digital certificate with it	`security ssl modify`
Display the SSL configuration and certificate name for the cluster or an SVM	`security ssl show`

Learn more about `security ssl modify` and `security ssl show` in the ONTAP command reference.

Use HSTS for ONTAP web services

HTTP Strict Transport Security (HSTS) is a web security policy mechanism that helps protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. By enforcing the use of HTTPS, HSTS ensures that all communications between the user's browser and the server are encrypted. Beginning with ONTAP 9.17.1, ONTAP can enforce HTTPS connections for ONTAP web services.

> HSTS is enforced by the web browser only after an initial secure HTTPS connection is established with ONTAP. If the browser does not establish an initial secure connection, HSTS will not be enforced. Refer to your browser documentation for information on HSTS management.

About this task

- For 9.17.1 and above, HSTS is enabled by default for newly installed ONTAP clusters. When you upgrade to 9.17.1, HSTS is not enabled by default. You must enable HSTS after the upgrade.
- HSTS is supported for all ONTAP web services.

Before you begin

- Advanced privileges are required for the following tasks.

Show HSTS configuration

You can show the current HSTS configuration to check if it is enabled and view the maximum age setting.

Steps

1. Use the `system services web show` command to show the current web services configuration, including HSTS settings:

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                        Per Address Limit: 80
                      Wait Queue Capacity: 192
                             HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                             HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

Enable HSTS and set the maximum age

Beginning with ONTAP 9.17.1, HSTS is enabled by default on new ONTAP cluster. If you upgrade an existing cluster to 9.17.1 or later, you need to manually enable HSTS on your cluster to enforce use of HTTPS. You can enable HSTS and set the maximum age. You can change the maximum age at any time if HSTS is enabled. Once HSTS is enabled, browsers will begin enforcing secure connections only after an initial secure connection is established.

Steps

1. Use the `system services web modify` command to enable HSTS or modify the maximum age:

   ```
   system services web modify -hsts-enabled true -hsts-max-age <seconds>
   ```

   `-hsts-max-age` specifies the duration in seconds for which the browser will remember to enforce HTTPS. The default value is 63072000 seconds (two years).

Disable HSTS

Browsers save the HSTS maximum age setting with each connection, and they continue to enforce HSTS for the entire duration even if HSTS is disabled on ONTAP. It will take up to the configured maximum age duration for the browser to stop enforcing HSTS after it is disabled. If a secure connection becomes impossible during this time, browsers enforcing HSTS will not permit access to ONTAP web services until the issue is resolved or the browser's maximum age expires.

Steps

1. Disable HSTS using the `system services web modify` command:

   ```
   system services web modify -hsts-enabled false
   ```

Related information

RFC 6797 - HTTP Strict Transport Security (HSTS)

Troubleshoot ONTAP web service access problems

Configuration errors cause web service access problems to occur. You can address the errors by ensuring that the LIF, firewall policy, web protocol engine, web services, digital certificates, and user access authorization are all configured correctly.

The following table helps you identify and address web service configuration errors:

This access problem…	Occurs because of this configuration error…	To address the error…
Your web browser returns an `unable to connect` or `failure to establish a connection` error when you try to access a web service.	Your LIF might be configured incorrectly.	Ensure that you can ping the LIF that provides the web service. You use the `network ping` command to ping a LIF.
	Your firewall might be configured incorrectly.	Ensure that a firewall policy is set up to support HTTP or HTTPS and that the policy is assigned to the LIF that provides the web service. You use the `system services firewall policy` commands to manage firewall policies. You use the `network interface modify` command with the `-firewall -policy` parameter to associate a policy with a LIF.
	Your web protocol engine might be disabled.	Ensure that the web protocol engine is enabled so that web services are accessible. You use the `system services web` commands to manage the web protocol engine for the cluster.

This access problem…	Occurs because of this configuration error…	To address the error…
Your web browser returns a `not found` error when you try to access a web service.	The web service might be disabled.	Ensure that each web service that you want to allow access to is enabled individually. You use the `vserver services web modify` command to enable a web service for access.
The web browser fails to log in to a web service with a user's account name and password.	The user cannot be authenticated, the access method is not correct, or the user is not authorized to access the web service.	Ensure that the user account exists and is configured with the correct access method and authentication method. Also, ensure that the user's role is authorized to access the web service. You use the `security login` commands to manage user accounts and their access methods and authentication methods. Accessing the ONTAP API web service requires the `ontapi` access method. Accessing all other web services requires the `http` access method. You use the `vserver services web access` commands to manage a role's access to a web service.

This access problem…	Occurs because of this configuration error…	To address the error…
You connect to your web service with HTTPS, and your web browser indicates that your connection is interrupted.	You might not have SSL enabled on the cluster or storage virtual machine (SVM) that provides the web service.	Ensure that the cluster or SVM has SSL enabled and that the digital certificate is valid. You use the `security ssl` commands to manage SSL configuration for HTTP servers and the `security certificate show` command to display digital certificate information.
You connect to your web service with HTTPS, and your web browser indicates that the connection is untrusted.	You might be using a self-signed digital certificate.	Ensure that the digital certificate associated with the cluster or SVM is signed by a trusted CA. You use the `security certificate generate-csr` command to generate a digital certificate signing request and the `security certificate install` command to install a CA-signed digital certificate. You use the `security ssl` commands to manage the SSL configuration for the cluster or SVM that provides the web service.

Related information

- What are Best Practices for Network Configuration for ONTAP?
- network ping
- network interface modify

- security certificate generate-csr
- security certificate install
- security certificate show
- security ssl

Verify the identity of remote servers using certificates

Learn about verifying the identity of remote servers using certificates in ONTAP

ONTAP supports security certificate features to verify the identity of remote servers.

ONTAP software enables secure connections using these digital certificate features and protocols:

- Online Certificate Status Protocol (OCSP) validates the status of digital certificate requests from ONTAP services using SSL and Transport Layer Security (TLS) connections. This feature is disabled by default.
- A default set of trusted root certificates is included with ONTAP software.
- Key Management Interoperability Protocol (KMIP) certificates enable mutual authentication of a cluster and a KMIP server.

Verify digital certificates are valid using OCSP in ONTAP

Online Certificate Status Protocol (OCSP) enables ONTAP applications that use Transport Layer Security (TLS) communications to receive digital certificate status when OCSP is enabled. You can enable or disable OCSP certificate status checks for specific applications at any time. By default, OCSP certificate status checking is disabled.

Before you begin

You need advanced privilege level access to perform this task.

About this task

OCSP supports the following applications:

- AutoSupport
- Event Management System (EMS)
- LDAP over TLS
- Key Management Interoperability Protocol (KMIP)
- Audit Logging
- FabricPool
- SSH (beginning with ONTAP 9.13.1)

Steps

1. Set the privilege level to advanced: `set -privilege advanced`.
2. To enable or disable OCSP certificate status checks for specific ONTAP applications, use the appropriate command.

If you want OCSP certificate status checks for some applications to be…	Use the command…
Enabled	`security config ocsp enable -app` app name
Disabled	`security config ocsp disable -app` app name

The following command enables OCSP support for AutoSupport and EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

When OCSP is enabled, the application receives one of the following responses:

- Good - the certificate is valid and communication proceeds.
- Revoked - the certificate is permanently deemed as not trustworthy by its issuing Certificate Authority and communication fails to proceed.
- Unknown - the server does not have any status information about the certificate and communication fails to proceed.
- OCSP server information is missing in the certificate - the server acts as if OCSP is disabled and continues with TLS communication, but no status check occurs.
- No response from OCSP server - the application fails to proceed.

3. To enable or disable OCSP certificate status checks for all applications using TLS communications, use the appropriate command.

If you want OCSP certificate status checks for all applications to be…	Use the command…

Enabled	`security config ocsp enable`
	
	`-app all`

Disabled	`security config ocsp disable`
	
	`-app all`

When enabled, all applications receive a signed response signifying that the specified certificate is good, revoked, or unknown. In the case of a revoked certificate, the application will fail to proceed. If the application fails to receive a response from the OCSP server or if the server is unreachable, the application will fail to proceed.

4. Use the `security config ocsp show` command to display all the applications that support OCSP and their support status.

```
cluster::*> security config ocsp show
         Application                        OCSP Enabled?
         --------------------               ---------------------
         autosupport                        false
         audit_log                          false
         fabricpool                         false
         ems                                false
         kmip                               false
         ldap_ad                            true
         ldap_nis_namemap                   true
         ssh                                true

         8 entries were displayed.
```

Related information

- security config ocsp enable
- security config ocsp disable
- security config ocsp show

View default certificates for TLS-based applications in ONTAP

ONTAP provides a default set of trusted root certificates for ONTAP applications using Transport Layer Security (TLS).

Before you begin

The default certificates are installed only on the admin SVM during its creation, or during an upgrade.

About this task

The current applications that act as a client and require certificate validation are AutoSupport, EMS, LDAP, Audit Logging, FabricPool, and KMIP.

When certificates expire, an EMS message is invoked that requests the user to delete the certificates. The default certificates can only be deleted at the advanced privilege level.

> Deleting the default certificates may result in some ONTAP applications not functioning as expected (for example, AutoSupport and Audit Logging).

Step

1. You can view the default certificates that are installed on the admin SVM by using the security certificate show command:

   `security certificate show -vserver -type server-ca`

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- --------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

Learn more about `security certificate show` in the ONTAP command reference.

Mutually authenticate the cluster and a KMIP server

Mutually authenticating the ONTAP cluster and a KMIP server overview

Mutually authenticating the cluster and an external key manager such as a Key Management Interoperability Protocol (KMIP) server enables the key manager to communicate with the cluster by using KMIP over SSL. You do so when an application or certain functionality (for example, the Storage Encryption functionality) requires secure keys to provide secure data access.

Generate a certificate signing request for the cluster in ONTAP

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.

Before you begin

You must be a cluster administrator 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
```

Learn more about `security certificate generate-csr` in the ONTAP command reference.

The following command creates a CSR with a 2,048-bit private key generated by the SHA256 hashing function for use by the Software group in the IT department of a company whose custom common name is

server1.companyname.com, located in Sunnyvale, California, USA. The email address of the SVM contact administrator is web@example.com. The system displays the CSR and the private key in the output.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

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

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

Install a CA-signed server certificate for the ONTAP cluster

To enable an SSL server to authenticate the cluster or storage virtual machine (SVM) as an SSL client, you install a digital certificate with the client type on the cluster or SVM. Then you provide the client-ca certificate to the SSL server administrator for installation on the server.

Before you begin

You must have already installed the root certificate of the SSL server on the cluster or SVM with the `server-ca` certificate type.

Steps

1. To use a self-signed digital certificate for client authentication, use the `security certificate create` command with the `type client` parameter.

   Learn more about `security certificate create` in the ONTAP command reference.

2. To use a CA-signed digital certificate for client authentication, complete the following steps:

   a. Generate a digital certificate signing request (CSR) by using the security certificate `generate-csr` command.

      ONTAP displays the CSR output, which includes a certificate request and private key, and reminds you

to copy the output to a file for future reference.

b. Send the certificate request from the CSR output in an electronic form (such as email) to a trusted CA for signing.

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

   After processing your request, the CA sends you the signed digital certificate.

c. Install the CA-signed certificate by using the `security certificate install` command with the `-type client` parameter.

d. Enter the certificate and the private key when you are prompted, and then press **Enter**.

e. Enter any additional root or intermediate certificates when you are prompted, and then press **Enter**.

   You install an intermediate certificate on the cluster or SVM if a certificate chain that begins at the trusted root CA, and ends with the SSL certificate issued to you, is missing the intermediate certificates. An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, goes through the intermediate certificate, and ends with the SSL certificate issued to you.

3. Provide the `client-ca` certificate of the cluster or SVM to the administrator of the SSL server for installation on the server.

   The security certificate show command with the `-instance` and `-type client-ca` parameters displays the `client-ca` certificate information.

Related information

- security certificate install
- security certificate show

Install a CA-signed client certificate for the KMIP server in ONTAP

The certificate subtype of Key Management Interoperability Protocol (KMIP) (the -subtype kmip-cert parameter), along with the client and server-ca types, specifies that the certificate is used for mutually authenticating the cluster and an external key manager, such as a KMIP server.

About this task

Install a KMIP certificate to authenticate a KMIP server as an SSL server to the cluster.

Steps

1. Use the `security certificate install` command with the `-type server-ca` and `-subtype kmip-cert` parameters to install a KMIP certificate for the KMIP server.
2. When you are prompted, enter the certificate, and then press Enter.

   ONTAP reminds you to keep a copy of the certificate for future reference.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


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

cluster1::>
```

Related information

- security certificate install

Copyright information

Copyright © 2026 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.