Manage administrator authentication and RBAC with the CLI

ONTAP 9

NetApp
March 23, 2022

Table of Contents

Manage administrator authentication and RBAC with the CLI

Administrator authentication and RBAC overview with the CLI

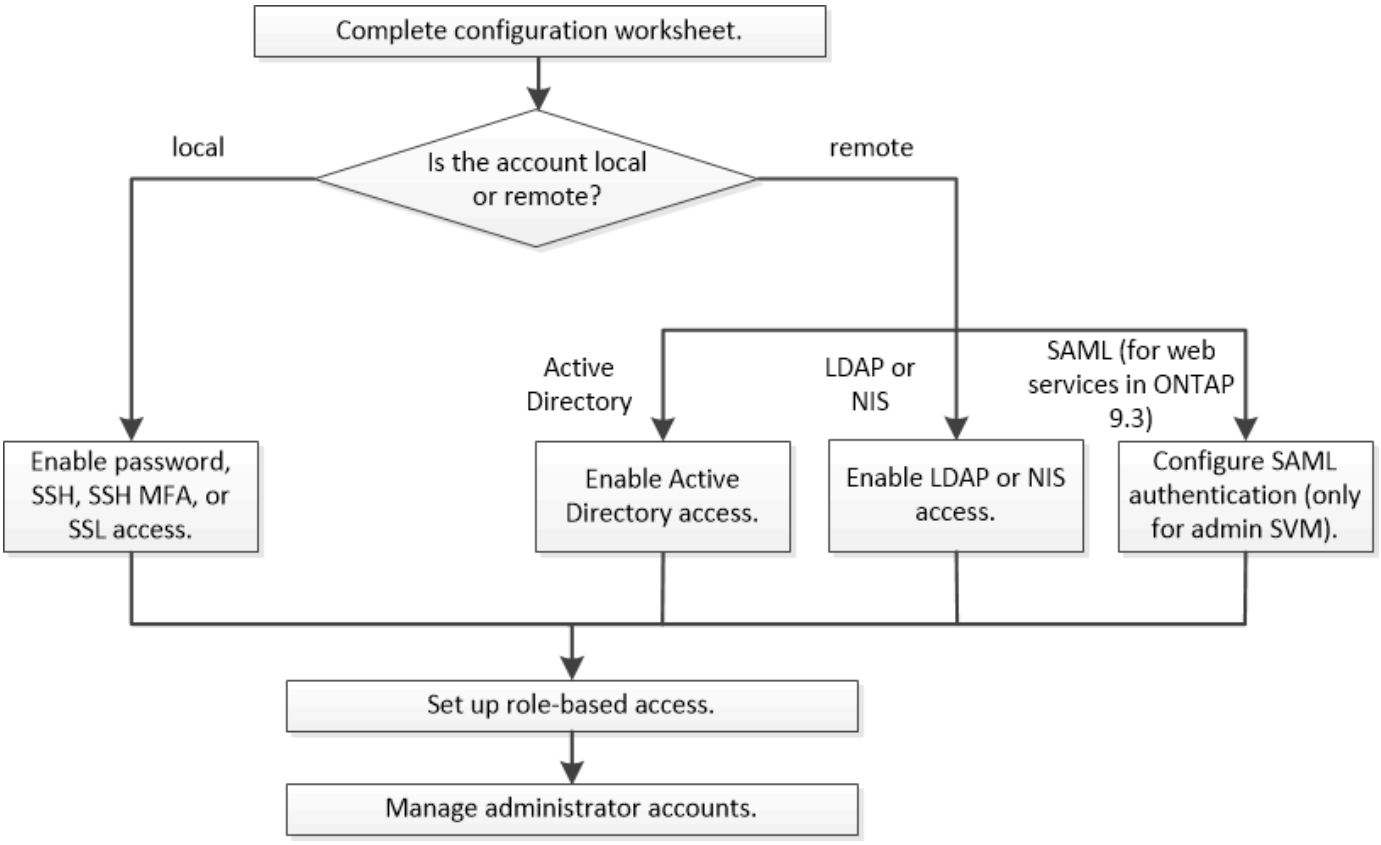
You can enable login accounts for ONTAP cluster administrators and storage virtual machine (SVM) administrators. You can also use role-based access control (RBAC) to define the capabilities of administrators.

You enable login accounts and RBAC in the following ways:

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

Administrator authentication and RBAC workflow

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



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

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

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

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

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

  Beginning with ONTAP 9.3, Security Assertion Markup Language (SAML) authentication can be used for accessing the admin SVM by using any of the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

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

Worksheets for administrator authentication and RBAC configuration

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

Create or modify login accounts

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

Field	Description	Your value
`-vserver`	The name of the SVM that the account accesses. The default value is the name of the admin SVM for the cluster.	
`-user-or-group-name`	The user name or group name of the account. Specifying a group name enables access to each user in the group. You can associate a user name or group name with multiple applications.	

`-application`	The application that is used to access the SVM: • `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 SVM), the default value is `admin`. • For a data SVM, the default value is `vsadmin`.	
`-comment`	(Optional) Descriptive text for the account. You should enclose the text in double quotation marks (").	
`-is-ns-switch-group`	Whether the account is an LDAP group account or NIS group account (`yes` or `no`).	
`-second-authentication -method`	Second authentication method in case of multifactor authentication in **ONTAP 9.3**: • `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 Support for nsswitch is available from **ONTAP 9.4** The order of authentication is always the public key followed by the password.	

Define custom roles

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

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

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

Install a CA-signed server digital certificate

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

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

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

Field	Description	Your value

`-vserver`	The name of the SVM on which the certificate is to be installed.	
`-type`	The certificate type: • `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 SVM and you want to configure the SVM as a gateway or *tunnel* for Active Directory domain controller access to the cluster.

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

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

Field	Description	Your value
`-vserver`	The name of the SVM for which you want to create an Active Directory computer account.	
`-account-name`	The NetBIOS name of the computer account.	
`-domain`	The fully qualified domain name (FQDN).	

`-ou`	The organizational unit in the domain. The default value is `CN=Computers`. ONTAP appends this value to the domain name to produce the Active Directory distinguished name.	

Configure LDAP or NIS server access

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

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

Only the options that are relevant to this guide are shown in the following table:

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

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

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

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

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

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

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

Field	Description	Your value

`-vserver`	The name of the SVM on which the name service look-up order is to be configured.	
`-database`	The name service database: • `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.

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

Create login accounts

Create login accounts overview

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

Cluster and SVM administrators

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

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

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

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

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

Merged roles

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

Enable local account access

Enable local account access overview

A local account is one in which the account information, public key, or security certificate

resides on the storage system. You can use the `security login create` command to enable local accounts to access an admin or data SVM.

Enable password account access

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

Step

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

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

   For complete command syntax, see the worksheet.

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

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

Enable SSH public key accounts

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

  Associating a public key with a user account

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

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

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

- Supported key types: ecdsa-sha2-nistp256, ssh-ed25519
- Unsupported key types: ssh-rsa, ssh-dss

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

For more information, see Configure network security using FIPS.

Step

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

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

   For complete command syntax, see the worksheet.

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

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

After you finish

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

Associating a public key with a user account

Enable SSH multifactor authentication (MFA)

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

  Associating a public key with a user account

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

- If you are unsure of the access control role that you want to assign to the login account, you can use the

`security login modify` command to add the role later.

Modifying the role assigned to an administrator

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

Step

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

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

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

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

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

After you finish

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

Associating a public key with a user account

Enable SSL certificate accounts

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

  Generating and installing a CA-signed server certificate

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

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

  Modifying the role assigned to an administrator

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

Step

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

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

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

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

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

After you finish

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

Generating and installing a CA-signed server certificate

Enable Active Directory account access

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

What you'll need

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

About this task

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

  Configuring Active Directory domain controller access

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

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

  Modifying the role assigned to an administrator

AD group account access is supported only with the `SSH` and `ontapi` applications.

Step

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

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

   For complete command syntax, see the worksheet.

   Creating or modifying login accounts

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

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

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

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

After you finish

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

Configuring Active Directory domain controller access

Enable LDAP or NIS account access

You can use the `security login create` command to enable LDAP or NIS user accounts to access an admin or data SVM. If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

What you'll need

You must be a cluster administrator to perform this task.

About this task

- Group accounts are not supported.
- You must configure LDAP or NIS server access to the SVM before the account can access the SVM.

  Configuring LDAP or NIS server access

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

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

  Modifying the role assigned to an administrator

- Beginning with ONTAP 9.4, multifactor authentication (MFA) is supported for remote users over LDAP or NIS servers.
- Because of a known LDAP issue, you should not use the `':'` (colon) character in any field of LDAP user account information (for example, `gecos`, `userPassword`, and so on). Otherwise, the lookup operation will fail for that user.

Steps

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

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

   For complete command syntax, see the worksheet.

   Creating or modifying login accounts

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

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

2. Enable MFA login for LDAP or NIS users:

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

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

   The following example shows the MFA authentication being enabled:

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

After you finish

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

Configuring LDAP or NIS server access

Configure SAML authentication

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

What you'll need

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

About this task

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

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

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

Steps

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

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

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

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

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

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

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

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

The URL to access the ONTAP host metadata is displayed.

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

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

3. Enable SAML configuration:

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

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

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

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

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

   b. Verify that the user entry is created:
      `security login show`

```
cluster_12::> security login show

Vserver: cluster_12

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

Related information

ONTAP 9 commands

Manage access-control roles

Manage access-control roles overview

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

Modify the role assigned to an administrator

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

What you'll need

You must be a cluster administrator to perform this task.

Step

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

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

For complete command syntax, see the worksheet.

Creating or modifying login accounts

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

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

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

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

Define custom roles

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

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

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

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

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

Step

1. Define a custom role:

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

   For complete command syntax, see the worksheet.

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

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

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

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

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

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

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

Predefined roles for cluster administrators

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

The following table lists the predefined roles for cluster administrators:

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

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` • `set`
	none	`security`
	readonly	All other command directories (`DEFAULT`)
none	none	All command directories (`DEFAULT`)

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

Predefined roles for SVM administrators

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

The following table lists the predefined roles for SVM administrators:

Role name	Capabilities

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

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

Manage administrator accounts

Manage administrator accounts overview

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

Associate a public key with an administrator account

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

administrator account.

What you'll need

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

About this task

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

Step

1. Associate a public key with an administrator account:

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

   For complete command syntax, see the worksheet.

   Associating a public key with a user account

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

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

Generate and install a CA-signed server certificate

Generate and install a CA-signed server certificate overview

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

Generate a certificate signing request

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

What you'll need

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

Steps

1. Generate a CSR:

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

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

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

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


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

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

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

third-party CA for signing.

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

Install a CA-signed server certificate

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

What you'll need

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

Step

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

   For complete command syntax, see the worksheet.

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

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

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


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
```

```
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

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

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


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

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


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

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

Configure Active Directory domain controller access

Configure Active Directory domain controller access overview

You must configure AD domain controller access to the cluster or SVM before an AD account can access the SVM. If you have already configured a SMB server for a data

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

ONTAP supports the following domain controller authentication services:

- Kerberos
- LDAP
- Netlogon
- Local Security Authority (LSA)

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

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

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

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

The default is `false`.

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

Configure an authentication tunnel

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

What you'll need

- You must have configured a SMB server for a data SVM.
- You must have enabled an AD domain user account to access the admin SVM for the cluster.
- You must be a cluster administrator to perform this task.

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

NOTE

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

Step

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

   `security login domain-tunnel create -vserver SVM_name`

   For complete command syntax, see the worksheet.

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

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

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

Create an SVM computer account on the domain

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

What you'll need

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

About this task

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

Step

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

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

   For complete command syntax, see the worksheet.

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

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

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

Enter the user name: Administrator

Enter the password:
```

Configure LDAP or NIS server access

Configure LDAP or NIS server access overview

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

Configure LDAP server access

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

What you'll need

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

About this task

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

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

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

- NFS configuration

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

Steps

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

   > Start TLS is supported for access to data SVMs only. It is not supported for access to admin SVMs.

   For complete command syntax, see the worksheet.

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

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

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

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

   For complete command syntax, see the worksheet.

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

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

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

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

   The following command validates LDAP servers on the SVM vs0.

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

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

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

Configure NIS server access

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

What you'll need

- All configured servers must be available and accessible before you configure the NIS domain on the SVM.
- You must be a cluster or SVM administrator to perform this task.

About this task

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

Step

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

   For complete command syntax, see the worksheet.

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

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

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

Create a name service switch

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

What you'll need

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

Step

1. Specify the lookup order for name service sources:

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

   For complete command syntax, see the worksheet.

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

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

Change an administrator password

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

What you'll need

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

About this task

The new password must observe the following rules:

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

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

Step

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

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

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

Lock and unlock an administrator account

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

What you'll need

You must be a cluster administrator to perform these tasks.

Steps

1. Lock an administrator account:

   `security login lock -vserver SVM_name -username user_name`

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

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

2. Unlock an administrator account:

   `security login unlock -vserver SVM_name -username user_name`

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

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

Manage failed login attempts

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

How you will know that login attempts have failed

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

What to do if repeated login attempts fail

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

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

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

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

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

Enforce SHA-2 on administrator account passwords

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

About this task

The password hash functionality enables you to do the following:

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

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

Manageability enhancements

Steps

1. Migrate the MD5 administrator accounts to the SHA-512 password hash function:
   a. Expire all MD5 administrator accounts: `security login expire-password -vserver * -username * -hash-function md5`

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

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

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

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

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

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

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

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