

Manage administrator accounts ONTAP 9

NetApp September 18, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap/authentication/manage-user-accounts-concept.html on September 18, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Μ	anage administrator accounts	1
	Manage administrator accounts overview	1
	Associate a public key with an administrator account	1
	Manage SSH public keys and X.509 certificates for an administrator account	2
	Configure Cisco Duo 2FA for SSH logins	4
	Generate and install a CA-signed server certificate overview	8
	Manage certificates with System Manager	. 13
	Configure Active Directory domain controller access overview	. 17
	Configure LDAP or NIS server access overview	. 20
	Change an administrator password	. 23
	Lock and unlock an administrator account.	. 24
	Manage failed login attempts	. 24
	Enforce SHA-2 on administrator account passwords	. 25
	Diagnose and correct file access issues	. 26

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.

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
```

For complete command syntax, see the worksheet reference for Associating a public key with a user account.

2. Verify the change by viewing the public key:

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

Example

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

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

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

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

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

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

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:
 - $\,\circ\,$ You must have received the certificate from a certificate authority (CA).
 - You must install the certificate chain (intermediate and root CA certificates) using security certificate install commands.
 - You need to enable OCSP for SSH. Refer to Verify digital certificates are valid using OCSP for instructions.

Steps

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

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

For complete command syntax, see the worksheet reference for Associating a public key with a user account.

2. Verify the change by viewing the public key:

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

Example

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

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

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

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

Before you begin

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

Steps

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

```
security login publickey modify -vserver SVM_name -username user_name -index
index -x509-certificate delete
```

2. Verify the change by viewing the public key:

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

Example

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

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

Remove the public key and certificate association from an administrator account

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

Before you begin

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

Steps

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

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

2. Verify the change by viewing the public key:

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

Example

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

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

Configure Cisco Duo 2FA for 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.

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.

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>
```

For more information on the required and optional parameters for this command, refer to Worksheets for administrator authentication and RBAC configuration.

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.

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 \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-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.

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.

Steps

- 1. Log in to your ONTAP account using SSH.
- 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:
b79ffa4blc50blc747fbacdb34g671d4814
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.

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> -exclude-users <USER1, USER2>
```

The name of the Duo group must match an Active Directory, LDAP, or local group. Users you specify with the optional -exclude-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.

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> -exclude-users <USER1, USER2>
```

The name of the Duo group must match an Active Directory, LDAP, or local group. Users you specify with the optional -exclude-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.

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 -vserver <STORAGE_VM_NAME> -is-duo-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 group modify -group-name <GROUP_NAME> -exclude-users
<USER1, USER2>
```

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

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 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.

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.

```
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----
MIIBGjCBxQIBADBqMRQwEqYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBqNVBAqTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBqNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EaqLfso5+4q+ejiRKKTUPQ0
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
----END CERTIFICATE REQUEST----
Private Key :
----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
qQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsK0077itF+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.

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
```

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 SVM "engData2".

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
----BEGIN CERTIFICATE----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBqNV
BAOTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFqAwHhcNMTAwNDI2MTk00TI4
WhcNMTAwNTI2MTk00TI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBqNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFqAwXDANBqkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
----END CERTIFICATE-----
Please enter Private Key: Press <Enter> when done
----BEGIN RSA PRIVATE KEY----
MIIBPAIBAAJBAM16ytrK8nQj82UsWeHOeT8qk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsqPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3qOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfqTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Juqckrbosd/lSd7nQIq
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
Yy4xNTAzBqNVBAsTLFZhbGlDZXJ0IENsYXNzIDIqUG9saWN5IFZhbGlkYXRpb24q
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEW1uZm9AdmFsaWN1cnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwqSW5jLjExMC8GA1UECxMoR28qRGFkZHkqQ2xhc3MqMiBDZXJ0
----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----

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUN1cnQsIEluYy4xNTAz
BgNVBAsTLFZhbG1DZXJ0IENsYXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRw0i8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWN1cnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUN1cnQsIEluYy4xNTAzBgNVBAsTLFZhbG1DZXJ0IENs
YXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----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.
```

Manage certificates with System Manager

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

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

View certificate information

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

Steps

- 1. In System Manager, select Cluster > Settings.
- 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 i 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 inext 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.
 - $\circ\,$ 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 inext 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 inext 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 inext 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 inext 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 **i** next to the name, then click **Renew**.

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 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)	ONTAP 9.10.1
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.	
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 domaintunnel create command to configure the SVM as a gateway, or *tunnel*, for AD access to the cluster.

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.

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.

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.

Before you begin

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

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 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 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.

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.

For complete command syntax, see the worksheet.

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
```



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.

 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 Idap 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.

About this task

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

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 -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 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.

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
```

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 SVM "engData".

```
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.

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 command reference.

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 SVMvs1.example.com. You are prompted to enter the current password, then enter and reenter the new password.

```
vsl.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.

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

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-logincreate 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.

Diagnose and correct file access issues

Steps

- 1. In System Manager, select Storage > Storage VMs.
- 2. Select the storage VM on which you want to perform a trace.
- 3. Click **More**.
- 4. Click Trace File Access.
- 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 \checkmark in the left column of the results table to view the file access permissions.

Copyright information

Copyright © 2024 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.