Create login accounts
ONTAP 9
NetApp
March 08, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap/authentication/create-svm-user-accounts-task.html on March 08, 2024. Always check docs.netapp.com for the latest.
# Table of Contents

Create login accounts .................................................................................................................. 1
  Create login accounts overview ............................................................................................... 1
Enable local account access .......................................................................................................... 2
Enable Active Directory account access ..................................................................................... 11
Enable LDAP or NIS account access ........................................................................................... 13
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.

Naming conventions

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

- "adm"
- "bin"
- "cli"
- "daemon"
- "ftp"
- "games"
- "halt"
- "lp"
- "mail"
- "man"
- "naroot"
- "netapp"
- "news"
- "nobody"
- "operator"
- "root"
- "shutdown"
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.

**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.

**Before you begin**

You must be a cluster administrator to perform this task.

**Step**

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

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

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`MengCluster` using a password. You are prompted for the password after you enter the command.
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.

About this task

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

  **Associating a public key with a user account**

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

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

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

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

<table>
<thead>
<tr>
<th>ONTAP release</th>
<th>Key types supported in FIPS mode</th>
<th>Key types supported in non-FIPS mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.11.1 and later</td>
<td>ecdsa-sha2-nistp256</td>
<td>ecdsa-sha2-nistp256</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rsa-sha2-512</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rsa-sha2-256</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ssh-ed25519</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ssh-dss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ssh-rsa</td>
</tr>
<tr>
<td>9.10.1 and earlier</td>
<td>ecdsa-sha2-nistp256</td>
<td>ecdsa-sha2-nistp256</td>
</tr>
<tr>
<td></td>
<td>ssh-ed25519</td>
<td>ssh-ed25519</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ssh-dss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ssh-rsa</td>
</tr>
</tbody>
</table>

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

For more information, see [Configure network security using FIPS](#).

Before you begin

You must be a cluster administrator to perform this task.

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

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

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 SVMengData1 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 multifactor authentication (MFA) accounts**

**Multifactor authentication overview**

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

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

<table>
<thead>
<tr>
<th>Available beginning with...</th>
<th>First authentication method</th>
<th>Second authentication method</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP 9.14.1</td>
<td>SSH public key</td>
<td>TOTP</td>
</tr>
<tr>
<td></td>
<td>User Password</td>
<td>TOTP</td>
</tr>
<tr>
<td></td>
<td>SSH public key</td>
<td>Cisco Duo</td>
</tr>
<tr>
<td></td>
<td>User password</td>
<td>Cisco Duo</td>
</tr>
<tr>
<td>ONTAP 9.13.1</td>
<td>SSH public key</td>
<td>TOTP</td>
</tr>
<tr>
<td></td>
<td>User password</td>
<td>TOTP</td>
</tr>
<tr>
<td>ONTAP 9.3</td>
<td>SSH public key</td>
<td>User password</td>
</tr>
</tbody>
</table>

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

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

About this task

- You must be a cluster administrator to perform this task.
- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

Modifying the role assigned to an administrator

- If you are using a public key for authentication, you must associate the public key with the account before the account can access the SVM.

Associate a public key with a user account

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

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

Enable MFA with SSH public key and user password

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

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

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

The following command requires the SVM administrator account admin2 with the predefined admin role to log in to the 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".

---

Enable MFA with TOTP

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

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

**Before you begin**
You must be a storage administrator to perform these tasks.

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

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

For new user accounts

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

For existing user accounts

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

2. Verify that MFA with TOTP is enabled:

```
security login show
```

Enable MFA with SSH public key and TOTP

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

For new user accounts

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

For existing user accounts

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

2. Verify that MFA with TOTP is enabled:
After you finish

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

Associating a public key with a user account

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

Configure local user account for MFA with TOTP

Related information

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

Configure local user account for MFA with TOTP

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

Before you begin

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

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

Steps

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

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

2. Create the TOTP configuration on your account:

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

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

   ```
   security login totp show -vserver "<svm_name>" -username "<account_username>
   ```
Reset TOTP secret key

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

Reset TOTP if your key is compromised

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

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

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

3. Create a new TOTP secret key:

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

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

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

Reset TOTP if your key is lost

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

Before you begin

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

Steps

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

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

3. Verify that the TOTP configuration is enabled on your account:
security login totp show -vserver <svm_name> -username <account_username>

### Disable TOTP secret key for local account

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

**About this task**

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

**Step**

1. Disable the TOTP secret key:

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

### Enable SSL certificate accounts

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

**About this task**

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

  **Generating and installing a CA-signed server certificate**

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

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

  **Modifying the role assigned to an administrator**

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

**Step**

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

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment
   ```
For complete command syntax, see the ONTAP man pages by release.

The following command enables the SVM administrator account svmadmin2 with the default vsadmin role to access the SVMengData2 using an SSL digital certificate.

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

**After you finish**

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

**Generating and installing a CA-signed server certificate**

**Enable Active Directory account access**

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

**About this task**

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

**Configuring Active Directory domain controller access**

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

- Beginning with ONTAP 9.13.1, you can use an SSH public key as either your primary or secondary authentication method with an AD user password.
  
  If you choose to use an SSH public key as your primary authentication, no AD authentication takes place.

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

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

**Modifying the role assigned to an administrator**

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

**Before you begin**

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

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

For AD users:

<table>
<thead>
<tr>
<th>ONTAP Version</th>
<th>Primary authentication</th>
<th>Secondary authentication</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.13.1 and later</td>
<td>Public key</td>
<td>None</td>
<td>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application ssh -authentication-method publickey -role &lt;role&gt;</td>
</tr>
</tbody>
</table>
| 9.13.1 and later | Domain | Public key | For a new user

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

For an existing user

security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role> |

| 9.0 and later | Domain | None | security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true] |

For AD groups:
<table>
<thead>
<tr>
<th>ONTAP version</th>
<th>Primary authentication</th>
<th>Secondary authentication</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0 and later</td>
<td>Domain</td>
<td>None</td>
<td>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application &lt;application&gt; -authentication-method domain -role &lt;role&gt; -comment &lt;comment&gt; [-is-ldap-fastbind true]</td>
</tr>
</tbody>
</table>

For complete command syntax, see worksheets for administrator authentication and RBAC configuration

After you finish

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

Configuring Active Directory domain controller access

Enable LDAP or NIS account access

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

About this task

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

Configuring LDAP or NIS server access

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

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

Modifying the role assigned to an administrator

- Beginning with ONTAP 9.4, multifactor authentication (MFA) is supported for remote users over LDAP or NIS servers.
- Beginning with ONTAP 9.11.1, you can use LDAP fast bind for nsswitch authentication if it is supported by the LDAP server.
- Because of a known LDAP issue, you should not use the `:` (colon) character in any field of LDAP user account information (for example, `gecos`, `userPassword`, and so on). Otherwise, the lookup operation will fail for that user.

Before you begin
You must be a cluster administrator to perform this task.

Steps

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

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

   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