Enable local account access

ONTAP 9

NetApp
November 28, 2022
# Table of Contents

Enable local account access .................................................. 1
   Enable local account access overview ................................ 1
Enable password account access ............................................ 1
Enable SSH public key accounts ............................................. 1
Enable SSH multifactor authentication (MFA) .......................... 3
Enable SSL certificate accounts ............................................. 4
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:

   ```bash
   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.

   ```bash
   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.

**Note:** Host key algorithm support has changed in ONTAP 9.11.1 and later releases.

<table>
<thead>
<tr>
<th>ONTAP release</th>
<th>Supported key types</th>
<th>Unsupported key types</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.11.1 and later</td>
<td>ecdsa-sha2-nistp256</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>ssh-dss</td>
</tr>
<tr>
<td></td>
<td>ssh-ed25519</td>
<td>ssh-rsa</td>
</tr>
</tbody>
</table>

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:

   ```bash
   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:

   ```bash
   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.
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.

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.

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

Before you begin
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.

Associate 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:

   ```bash
   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:

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

   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 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