



Create login accounts

ONTAP 9

NetApp
February 28, 2023

Table of Contents

- Create login accounts 1
 - Create login accounts overview 1
 - Enable local account access 1
 - Enable Active Directory account access 5
 - Enable LDAP or NIS account access 6
 - Configure SAML authentication 8

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.

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

ONTAP release	Supported key types	Unsupported key types
---------------	---------------------	-----------------------

9.11.1 and later	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa

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 `svmin1` 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
svmin1 -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.

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:

```
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 `SVMengData1` 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 `svmin2` with the default `vsadmin` role to access the `SVMengData2` using an SSL digital certificate.

```
cluster1::>security login create -vserver engData2 -user-or-group-name  
svmin2 -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.

- 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` 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 [-is-  
ldap-fastbind true]
```

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 `SVMengCluster`.

```
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 `SVMengData`.

```
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.
- 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.

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 SVMengCluster.

```
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**					

Copyright information

Copyright © 2023 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.