

Enable local account access

ONTAP 9

NetApp May 02, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/authentication/create-local-user-accounts-task.html on May 02, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Enable local account access	
Enable local account access overview	
Enable password account access	
Enable SSH public key accounts	
Enable SSH multifactor authentication (MFA)	
Enable SSL certificate accounts	

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

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

Enable SSH public key accounts

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

Associating a public key with a user account

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

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

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

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

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

For more information, see Configure network security using FIPS.

Step

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

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

For complete command syntax, see the worksheet.

The following command enables the SVM administrator account symadmin1 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 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.

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 symadmin2 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

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.