



Configure Active Directory domain controller access

ONTAP 9

NetApp
December 01, 2021

This PDF was generated from <https://docs.netapp.com/us-en/ontap/authentication/enable-ad-users-groups-access-cluster-svm-task.html> on December 01, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Configure Active Directory domain controller access..... 1
 - Configure Active Directory domain controller access overview 1
 - Configure an authentication tunnel 1
 - Create an SVM computer account on the domain 1

Configure Active Directory domain controller access

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 CIFS 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 a CIFS server, you can create a computer account for the SVM on the AD domain.

Configure an authentication tunnel

If you have already configured a CIFS server for a data SVM, you can use the `security login domain-tunnel create` command to configure the SVM as a gateway, or *tunnel*, for AD access to the cluster.

What you'll need

- You must have configured a CIFS 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.

Step

1. Configure a CIFS-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 CIFS-enabled data SVMengData 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 a CIFS 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.

What you'll need

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

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.

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 the 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:

Copyright Information

Copyright © 2021 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.