Enable or disable local users and groups functionality

ONTAP 9

NetApp
April 15, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/smb-admin/enable-disable-local-users-groups-concept.html on April 15, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Enable or disable local users and groups functionality 1
Enable or disable local users and groups functionality overview 1
Enable or disable local users and groups 1
Enable or disable local user authentication 2

Enable or disable local users and groups functionality

Enable or disable local users and groups functionality overview

Before you can use local users and groups for access control of NTFS security-style data, local user and group functionality must be enabled. Additionally, if you want to use local users for SMB authentication, the local user authentication functionality must be enabled.

Local users and groups functionality and local user authentication are enabled by default. If they are not enabled, you must enable them before you can configure and use local users and groups. You can disable local users and groups functionality at any time.

In addition to explicitly disabling local user and group functionality, ONTAP disables local user and group functionality if any node in the cluster is reverted to an ONTAP release that does not support the functionality. Local user and group functionality is not enabled until all nodes in the cluster are running a version of ONTAP that supports it.

Related information

Managing local user accounts

Managing local groups

Managing local privileges

Enable or disable local users and groups

You can enable or disable local users and groups for SMB access on storage virtual machines (SVMs). Local users and groups functionality is enabled by default.

About this task

You can use local users and groups when configuring SMB share and NTFS file permissions and can optionally use local users for authentication when creating an SMB connection. To use local users for authentication, you must also enable the local users and groups authentication option.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want local users and groups to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`

If you want local users and groups to be…	Enter the command…
Disabled	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables local users and groups functionality on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Related information

Enabling or disabling local user authentication

Enabling or disabling local user accounts

Enable or disable local user authentication

You can enable or disable local user authentication for SMB access on storage virtual machines (SVMs). The default is to allow local user authentication, which is useful when the SVM cannot contact a domain controller or if you choose not to use domain-level access controls.

Before you begin

Local users and groups functionality must be enabled on the CIFS server.

About this task

You can enable or disable local user authentication at any time. If you want to use local users for authentication when creating an SMB connection, you must also enable the CIFS server's local users and groups option.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want local authentication to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables local user authentication on SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Related information

How local user authentication works

Enabling or disabling local users and groups

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.