



Use local users and groups for authentication and authorization

ONTAP 9

NetApp
April 06, 2023

Table of Contents

- Use local users and groups for authentication and authorization 1
 - How ONTAP uses local users and groups 1
 - What local privileges are 5
 - Guidelines for using BUILTIN groups and the local administrator account 6
 - Requirements for local user passwords 6
 - Predefined BUILTIN groups and default privileges 7
 - Enable or disable local users and groups functionality 8
 - Manage local user accounts 11
 - Manage local groups 16
 - Manage local privileges 22

Use local users and groups for authentication and authorization

How ONTAP uses local users and groups

Local users and groups concepts

You should know what local users and groups are, and some basic information about them, before determining whether to configure and use local users and groups in your environment.

- **Local user**

A user account with a unique security identifier (SID) that has visibility only on the storage virtual machine (SVM) on which it is created. Local user accounts have a set of attributes, including user name and SID. A local user account authenticates locally on the CIFS server using NTLM authentication.

User accounts have several uses:

- Used to grant *User Rights Management* privileges to a user.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

- **Local group**

A group with a unique SID has visibility only on the SVM on which it is created. Groups contain a set of members. Members can be local users, domain users, domain groups, and domain machine accounts. Groups can be created, modified, or deleted.

Groups have several uses:

- Used to grant *User Rights Management* privileges to its members.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

- **Local domain**

A domain that has local scope, which is bounded by the SVM. The local domain's name is the CIFS server name. Local users and groups are contained within the local domain.

- **Security identifier (SID)**

A SID is a variable-length numeric value that identifies Windows-style security principals. For example, a typical SID takes the following form: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **NTLM authentication**

A Microsoft Windows security method used to authenticate users on a CIFS server.

- **Cluster replicated database (RDB)**

A replicated database with an instance on each node in a cluster. Local user and group objects are stored in the RDB.

Reasons for creating local users and local groups

There are several reasons for creating local users and local groups on your storage virtual machine (SVM). For example, you can access an SMB server by using a local user account if the domain controllers (DCs) are unavailable, you might want to use local groups to assign privileges, or your SMB server is in a workgroup.

You can create one or more local user accounts for the following reasons:

- Your SMB server is in a workgroup, and domain users are not available.

Local users are required in workgroup configurations.

- You want the ability to authenticate and log in to the SMB server if the domain controllers are unavailable.

Local users can authenticate with the SMB server by using NTLM authentication when the domain controller is down, or when network problems prevent your SMB server from contacting the domain controller.

- You want to assign *User Rights Management* privileges to a local user.

User Rights Management is the ability for an SMB server administrator to control what rights the users and groups have on the SVM. You can assign privileges to a user by assigning the privileges to the user's account, or by making the user a member of a local group that has those privileges.

You can create one or more local groups for the following reasons:

- Your SMB server is in a workgroup, and domain groups are not available.

Local groups are not required in workgroup configurations, but they can be useful for managing access privileges for local workgroup users.

- You want to control access to file and folder resources by using local groups for share and file-access control.
- You want to create local groups with customized *User Rights Management* privileges.

Some built-in user groups have predefined privileges. To assign a customized set of privileges, you can create a local group and assign the necessary privileges to that group. You can then add local users, domain users, and domain groups to the local group.

Related information

[How local user authentication works](#)

[List of supported privileges](#)

How local user authentication works

Before a local user can access data on a CIFS server, the user must create an authenticated session.

Because SMB is session-based, the identity of the user can be determined just once, when the session is first set up. The CIFS server uses NTLM-based authentication when authenticating local users. Both NTLMv1 and

NTLMv2 are supported.

ONTAP uses local authentication under three use cases. Each use case depends on whether the domain portion of the user name (with the DOMAIN\user format) matches the CIFS server's local domain name (the CIFS server name):

- The domain portion matches

Users who provide local user credentials when requesting access to data are authenticated locally on the CIFS server.

- The domain portion does not match

ONTAP attempts to use NTLM authentication with a domain controller in the domain to which the CIFS server belongs. If authentication succeeds, the login is complete. If it does not succeed, what happens next depends on why authentication did not succeed.

For example, if the user exists in Active Directory but the password is invalid or expired, ONTAP does not attempt to use the corresponding local user account on the CIFS server. Instead, authentication fails. There are other cases where ONTAP uses the corresponding local account on the CIFS server, if it exists, for authentication—even though the NetBIOS domain names do not match. For example, if a matching domain account exists but it is disabled, ONTAP uses the corresponding local account on the CIFS server for authentication.

- The domain portion is not specified

ONTAP first attempts authentication as a local user. If authentication as a local user fails, then ONTAP authenticates the user with a domain controller in the domain to which the CIFS server belongs.

After local or domain user authentication is completed successfully, ONTAP constructs a complete user access token, which takes into account local group membership and privileges.

For more information about NTLM authentication for local users, see the Microsoft Windows documentation.

Related information

[Enabling or disabling local user authentication](#)

How user access tokens are constructed

When a user maps a share, an authenticated SMB session is established and a user access token is constructed that contains information about the user, the user's group membership and cumulative privileges, and the mapped UNIX user.

Unless the functionality is disabled, local user and group information is also added to the user access token. The way access tokens are constructed depends on whether the login is for a local user or an Active Directory domain user:

- Local user login

Although local users can be members of different local groups, local groups cannot be members of other local groups. The local user access token is composed of a union of all privileges assigned to groups to which a particular local user is a member.

- Domain user login

When a domain user logs in, ONTAP obtains a user access token that contains the user SID and SIDs for all the domain groups to which the user is a member. ONTAP uses the union of the domain user access token with the access token provided by local memberships of the user's domain groups (if any), as well as any direct privileges assigned to the domain user or any of its domain group memberships.

For both local and domain user login, the Primary Group RID is also set for the user access token. The default RID is `Domain Users` (RID 513). You cannot change the default.

The Windows-to-UNIX and UNIX-to-Windows name mapping process follows the same rules for both local and domain accounts.



There is no implied, automatic mapping from a UNIX user to a local account. If this is required, an explicit mapping rule must be specified using the existing name mapping commands.

Guidelines for using SnapMirror on SVMs that contain local groups

You should be aware of the guidelines when you configure SnapMirror on volumes owned by SVMs that contain local groups.

You cannot use local groups in ACEs applied to files, directories, or shares that are replicated by SnapMirror to another SVM. If you use the SnapMirror feature to create a DR mirror to a volume on another SVM and the volume has an ACE for a local group, the ACE is not valid on the mirror. If data is replicated to a different SVM, the data is effectively crossing into a different local domain. The permissions granted to local users and groups are valid only within the scope of the SVM on which they were originally created.

What happens to local users and groups when deleting CIFS servers

The default set of local users and groups is created when a CIFS server is created, and they are associated with the storage virtual machine (SVM) hosting the CIFS server. SVM administrators can create local users and groups at any time. You need to be aware of what happens to local users and groups when you delete the CIFS server.

Local users and groups are associated with SVMs; therefore, they are not deleted when CIFS servers are deleted due to security considerations. Although local users and groups are not deleted when the CIFS server is deleted, they are hidden. You cannot view or manage local users and groups until you re-create a CIFS server on the SVM.



The CIFS server administrative status does not affect visibility of local users or groups.

How you can use Microsoft Management Console with local users and groups

You can view information about local users and groups from the Microsoft Management Console. With this release of ONTAP, you cannot perform other management tasks for local users and groups from the Microsoft Management Console.

Guidelines for reverting

If you plan to revert the cluster to an ONTAP release that does not support local users and groups and local users and groups are being used to manage file access or user

rights, you must be aware of certain considerations.

- Due to security reasons, information about configured local users, groups, and privileges are not deleted when ONTAP is reverted to a version that does not support local users and groups functionality.
- Upon a revert to a prior major version of ONTAP, ONTAP does not use local users and groups during authentication and credential creation.
- Local users and groups are not removed from file and folder ACLs.
- File access requests that depend on access being granted because of permissions granted to local users or groups are denied.

To allow access, you must reconfigure file permissions to allow access based on domain objects instead of local user and group objects.

What local privileges are

List of supported privileges

ONTAP has a predefined set of supported privileges. Certain predefined local groups have some of these privileges added to them by default. You can also add or remove privileges from the predefined groups or create new local users or groups and add privileges to the groups that you created or to existing domain users and groups.

The following table lists the supported privileges on the storage virtual machine (SVM) and provides a list of BUILTIN groups with assigned privileges:

Privilege name	Default security setting	Description
SeTcbPrivilege	None	Act as part of the operating system
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Back up files and directories, overriding any ACLs
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Restore files and directories, overriding any ACLs Set any valid user or group SID as the file owner
SeTakeOwnershipPrivilege	BUILTIN\Administrators	Take ownership of files or other objects
SeSecurityPrivilege	BUILTIN\Administrators	Manage auditingThis includes viewing, dumping, and clearing the security log.
SeChangeNotifyPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators, BUILTIN\Power Users, BUILTIN\Users, Everyone	Bypass traverse checkingUsers with this privilege are not required to have traverse (x) permissions to traverse folders, symlinks, or junctions.

Related information

- [Assign local privileges](#)
- [Configuring bypass traverse checking](#)

Assign privileges

You can assign privileges directly to local users or domain users. Alternatively, you can assign users to local groups whose assigned privileges match the capabilities that you want those users to have.

- You can assign a set of privileges to a group that you create.

You then add a user to the group that has the privileges that you want that user to have.

- You can also assign local users and domain users to predefined groups whose default privileges match the privileges that you want to grant to those users.

Related information

- [Adding privileges to local or domain users or groups](#)
- [Removing privileges from local or domain users or groups](#)
- [Resetting privileges for local or domain users and groups](#)
- [Configuring bypass traverse checking](#)

Guidelines for using BUILTIN groups and the local administrator account

There are certain guidelines you should keep in mind when you use BUILTIN groups and the local administrator account. For example, you can rename the local administrator account, but you cannot delete this account.

- The Administrator account can be renamed but cannot be deleted.
- The Administrator account cannot be removed from the BUILTIN\Administrators group.
- BUILTIN groups can be renamed but cannot be deleted.

After the BUILTIN group is renamed, another local object can be created with the well-known name; however, the object is assigned a new RID.

- There is no local Guest account.

Related information

[Predefined BUILTIN groups and default privileges](#)

Requirements for local user passwords

By default, local user passwords must meet complexity requirements. The password complexity requirements are similar to the requirements defined in the Microsoft Windows *Local security policy*.

The password must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Special characters:

~ ! @ # \$ % ^ & * _ - + = ` \ | () [] : ; " ' < > , . ? /

Related information

[Enabling or disabling required password complexity for local SMB users](#)

[Displaying information about CIFS server security settings](#)

[Changing local user account passwords](#)

Predefined BUILTIN groups and default privileges

You can assign membership of a local user or domain user to a predefined set of BUILTIN groups provided by ONTAP. Predefined groups have predefined privileges assigned.

The following table describes the predefined groups:

Predefined BUILTIN group	Default privileges
<p>BUILTIN\AdministratorsRID 544</p> <p>When first created, the local Administrator account, with a RID of 500, is automatically made a member of this group. When the storage virtual machine (SVM) is joined to a domain, the domain\Domain Admins group is added to the group. If the SVM leaves the domain, the domain\Domain Admins group is removed from the group.</p>	<ul style="list-style-type: none">• SeBackupPrivilege• SeRestorePrivilege• SeSecurityPrivilege• SeTakeOwnershipPrivilege• SeChangeNotifyPrivilege

Predefined BUILTIN group	Default privileges
<p>BUILTIN\Power UsersRID 547</p> <p>When first created, this group does not have any members. Members of this group have the following characteristics:</p> <ul style="list-style-type: none"> • Can create and manage local users and groups. • Cannot add themselves or any other object to the BUILTIN\Administrators group. 	SeChangeNotifyPrivilege
<p>BUILTIN\Backup OperatorsRID 551</p> <p>When first created, this group does not have any members. Members of this group can override read and write permissions on files or folders if they are opened with backup intent.</p>	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeChangeNotifyPrivilege
<p>BUILTIN\UsersRID 545</p> <p>When first created, this group does not have any members (besides the implied Authenticated Users special group). When the SVM is joined to a domain, the domain\Domain Users group is added to this group. If the SVM leaves the domain, the domain\Domain Users group is removed from this group.</p>	SeChangeNotifyPrivilege
<p>EveryoneSID S-1-1-0</p> <p>This group includes all users, including guests (but not anonymous users). This is an implied group with an implied membership.</p>	SeChangeNotifyPrivilege

Related information

[Guidelines for using BUILTIN groups and the local administrator account](#)

[List of supported privileges](#)

[Configuring bypass traverse checking](#)

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

[Modify local user accounts](#)

[Modify local groups](#)

[Add privileges to local or domain users or groups](#)

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	<code>vserver cifs options modify -vserver <i>vserver_name</i> -is-local-users-and -groups-enabled true</code>
Disabled	<code>vserver cifs options modify -vserver <i>vserver_name</i> -is-local-users-and -groups-enabled false</code>

- 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

[Enable or disable local user authentication](#)

[Enable or disable 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	<code>vserver cifs options modify -vserver <i>vserver_name</i> -is-local-auth-enabled true</code>
Disabled	<code>vserver cifs options modify -vserver <i>vserver_name</i> -is-local-auth-enabled false</code>

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

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

Related information

[How local user authentication works](#)

[Enabling or disabling local users and groups](#)

Manage local user accounts

Modify local user accounts

You can modify a local user account if you want to change an existing user's full name or description, and if you want to enable or disable the user account. You can also rename a local user account if the user's name is compromised or if a name change is needed for administrative purposes.

If you want to...	Enter the command...
Modify the local user's full name	<code>vsserver cifs users-and-groups local-user modify -vsserver vsserver_name -user -name user_name -full-name text</code> If the full name contains a space, then it must be enclosed within double quotation marks.
Modify the local user's description	<code>vsserver cifs users-and-groups local-user modify -vsserver vsserver_name -user -name user_name -description text</code> If the description contains a space, then it must be enclosed within double quotation marks.
Enable or disable the local user account	<code>vsserver cifs users-and-groups local-user modify -vsserver vsserver_name -user -name user_name -is-account-disabled {true false}</code>

If you want to...	Enter the command...
Rename the local user account	<code>vserver cifs users-and-groups local-user rename -vserver vserver_name -user-name user_name -new-user-name new_user_name</code> When renaming a local user, the new user name must remain associated with the same CIFS server as the old user name.

Example

The following example renames the local user “CIFS_SERVER\sue” to “CIFS_SERVER\sue_new” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Enable or disable local user accounts

You enable a local user account if you want the user to be able to access data contained in the storage virtual machine (SVM) over an SMB connection. You can also disable a local user account if you do not want that user to access SVM data over SMB.

About this task

You enable a local user by modifying the user account.

Step

1. Perform the appropriate action:

If you want to...	Enter the command...
Enable the user account	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled false</code>
Disable the user account	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled true</code>

Change local user account passwords

You can change a local user’s account password. This can be useful if the user’s password is compromised or if the user has forgotten the password.

Step

1. Change the password by performing the appropriate action: `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

Example

The following example sets the password for the local user “CIFS_SERVER\sue” associated with storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user  
-name CIFS_SERVER\sue -vserver vs1
```

Enter the new password:

Confirm the new password:

Related information

[Enabling or disabling required password complexity for local SMB users](#)

[Displaying information about CIFS server security settings](#)

Display information about local users

You can display a list of all local users in a summary form. If you want to determine which account settings are configured for a specific user, you can display detailed account information for that user as well as the account information for multiple users. This information can help you determine if you need to modify a user’s settings, and also to troubleshoot authentication or file access issues.

About this task

Information about a user’s password is never displayed.

Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Display information about all users on the storage virtual machine (SVM)	<code>vserver cifs users-and-groups local-user show -vserver <i>vserver_name</i></code>
Display detailed account information for a user	<code>vserver cifs users-and-groups local-user show -instance -vserver <i>vserver_name</i> -user-name <i>user_name</i></code>

There are other optional parameters that you can choose when you run the command. See the man page for more information.

Example

The following example displays information about all local users on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----  -
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue    Jones
```

Display information about group memberships for local users

You can display information about which local groups that a local user belongs to. You can use this information to determine what access the user should have to files and folders. This information can be useful in determining what access rights the user should have to files and folders or when troubleshooting file access issues.

About this task

You can customize the command to display only the information that you want to see.

Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Display local user membership information for a specified local user	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>
Display local user membership information for the local group of which this local user is a member	<code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>
Display user membership information for local users that are associated with a specified storage virtual machine (SVM)	<code>vserver cifs users-and-groups local-user show-membership -vserver <i>vserver_name</i></code>
Display detailed information for all local users on a specified SVM	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver <i>vserver_name</i></code>

Example

The following example displays the membership information for all local users on SVM vs1; user “CIFS_SERVER\Administrator” is a member of the “BUILTIN\Administrators” group, and “CIFS_SERVER\sue” is a member of “CIFS_SERVER\g1” group:


```
cluster1::> vsserver cifs users-and-groups local-user show-membership
-vserver vs1
```

Vserver	User Name	Membership
vs1	CIFS_SERVER\Administrator	BUILTIN\Administrators
	CIFS_SERVER\sue	CIFS_SERVER\g1

Delete local user accounts

You can delete local user accounts from your storage virtual machine (SVM) if they are no longer needed for local SMB authentication to the CIFS server or for determining access rights to data contained on your SVM.

About this task

Keep the following in mind when deleting local users:

- The file system is not altered.

Windows Security Descriptors on files and directories that refer to this user are not adjusted.

- All references to local users are removed from the membership and privileges databases.
- Standard, well-known users such as Administrator cannot be deleted.

Steps

1. Determine the name of the local user account that you want to delete: `vsserver cifs users-and-groups local-user show -vserver vsserver_name`
2. Delete the local user: `vsserver cifs users-and-groups local-user delete -vserver vsserver_name -user-name username_name`
3. Verify that the user account is deleted: `vsserver cifs users-and-groups local-user show -vserver vsserver_name`

Example

The following example deletes the local user “CIFS_SERVER\sue” associated with SVM vs1:

```

cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith             Built-in administrator
account
vs1      CIFS_SERVER\sue           Sue    Jones

cluster1::> vsriver cifs users-and-groups local-user delete -vsriver vs1
-user-name CIFS_SERVER\sue

cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith             Built-in administrator
account

```

Manage local groups

Modify local groups

You can modify existing local groups by changing the description for an existing local group or by renaming the group.

If you want to...	Use the command...
Modify the local group description	<code>vsriver cifs users-and-groups local-group modify -vsriver vsriver_name -group-name group_name -description text</code> If the description contains a space, then it must be enclosed within double quotation marks.
Rename the local group	<code>vsriver cifs users-and-groups local-group rename -vsriver vsriver_name -group-name group_name -new-group-name new_group_name</code>

Examples

The following example renames the local group “CIFS_SERVER\engineering” to “CIFS_SERVER\engineering_new”:

```

cluster1::> vsriver cifs users-and-groups local-group rename -vsriver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new

```

The following example modifies the description of the local group “CIFS_SERVER\engineering”:

```
cluster1::> vservers cifs users-and-groups local-group modify -vservers vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Display information about local groups

You can display a list of all local groups configured on the cluster or on a specified storage virtual machine (SVM). This information can be useful when troubleshooting file-access issues to data contained on the SVM or user-rights (privilege) issues on the SVM.

Step

1. Perform one of the following actions:

If you want information about...	Enter the command...
All local groups on the cluster	<code>vservers cifs users-and-groups local-group show</code>
All local groups on the SVM	<code>vservers cifs users-and-groups local-group show -vservers vservers_name</code>

There are other optional parameters that you can choose when you run this command. See the man page for more information.

Example

The following example displays information about all local groups on SVM vs1:

```
cluster1::> vservers cifs users-and-groups local-group show -vservers vs1
Vservers  Group Name                Description
-----  -
vs1       BUILTIN\Administrators      Built-in Administrators group
vs1       BUILTIN\Backup Operators    Backup Operators group
vs1       BUILTIN\Power Users         Restricted administrative privileges
vs1       BUILTIN\Users               All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales
```

Manage local group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group or if you want users to have privileges associated with that group.

About this task

Guidelines for adding members to a local group:

- You cannot add users to the special *Everyone* group.
- The local group must exist before you can add a user to it.
- The user must exist before you can add the user to a local group.
- You cannot add a local group to another local group.
- To add a domain user or group to a local group, Data ONTAP must be able to resolve the name to a SID.

Guidelines for removing members from a local group:

- You cannot remove members from the special *Everyone* group.
- The group from which you want to remove a member must exist.
- ONTAP must be able to resolve the names of members that you want to remove from the group to a corresponding SID.

Step

1. Add or remove a member in a group.

If you want to...	Then use the command...
Add a member to a group	<pre>vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>You can specify a comma-delimited list of local users, domain users, or domain groups to add to the specified local group.</p>
Remove a member from a group	<pre>vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>You can specify a comma-delimited list of local users, domain users, or domain groups to remove from the specified local group.</p>

The following example adds a local user “SMB_SERVER\sue” and a domain group “AD_DOM\dom_eng” to the local group “SMB_SERVER\engineering” on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

The following example removes the local users “SMB_SERVER\sue” and “SMB_SERVER\james” from the local group “SMB_SERVER\engineering” on SVM vs1:

```
cluster1::> vsriver cifs users-and-groups local-group remove-members
-vsriver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Related information

[Displaying information about members of local groups](#)

Display information about members of local groups

You can display a list of all members of local groups configured on the cluster or on a specified storage virtual machine (SVM). This information can be useful when troubleshooting file-access issues or user-rights (privilege) issues.

Step

1. Perform one of the following actions:

If you want to display information about...	Enter the command...
Members of all local groups on the cluster	<code>vsriver cifs users-and-groups local-group show-members</code>
Members of all local groups on the SVM	<code>vsriver cifs users-and-groups local-group show-members -vsriver vsriver_name</code>

Example

The following example displays information about members of all local groups on SVM vs1:

```
cluster1::> vsriver cifs users-and-groups local-group show-members
-vsriver vs1
```

Vsriver	Group Name	Members
vs1	BUILTIN\Administrators	CIFS_SERVER\Administrator AD_DOMAIN\Domain Admins AD_DOMAIN\dom_grpl
	BUILTIN\Users	AD_DOMAIN\Domain Users AD_DOMAIN\dom_usr1
	CIFS_SERVER\engineering	CIFS_SERVER\james

Delete a local group

You can delete a local group from the storage virtual machine (SVM) if it is no longer needed for determining access rights to data associated with that SVM or if it is no longer needed for assigning SVM user rights (privileges) to group members.

About this task

Keep the following in mind when deleting local groups:

- The file system is not altered.

Windows Security Descriptors on files and directories that refer to this group are not adjusted.

- If the group does not exist, an error is returned.
- The special *Everyone* group cannot be deleted.
- Built-in groups such as *BUILTIN\Administrators* *BUILTIN\Users* cannot be deleted.

Steps

1. Determine the name of the local group that you want to delete by displaying the list of local groups on the SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Delete the local group: `vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name`
3. Verify that the group is deleted: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Example

The following example deletes the local group “CIFS_SERVER\sales” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name                Description
-----
vs1          BUILTIN\Administrators    Built-in Administrators group
vs1          BUILTIN\Backup Operators  Backup Operators group
vs1          BUILTIN\Power Users       Restricted administrative
privileges
vs1          BUILTIN\Users             All users
vs1          CIFS_SERVER\engineering
vs1          CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name                Description
-----
vs1          BUILTIN\Administrators    Built-in Administrators group
vs1          BUILTIN\Backup Operators  Backup Operators group
vs1          BUILTIN\Power Users       Restricted administrative
privileges
vs1          BUILTIN\Users             All users
vs1          CIFS_SERVER\engineering
```

Update domain user and group names in local databases

You can add domain users and groups to a CIFS server's local groups. These domain objects are registered in local databases on the cluster. If a domain object is renamed, the local databases must be manually updated.

About this task

You must specify the name of the storage virtual machine (SVM) on which you want to update domain names.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform the appropriate action:

If you want to update domain users and groups and...	Use this command...
Display domain users and groups that successfully updated and that failed to update	<code>vserver cifs users-and-groups update-names -vserver vserver_name</code>
Display domain users and groups that successfully updated	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false</code>
Display only the domain users and groups that fail to update	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true</code>
Suppress all status information about updates	<code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true</code>

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

Example

The following example updates the names of domain users and groups associated with storage virtual machine (SVM, formerly known as Vserver) vs1. For the last update, there is a dependent chain of names that needs to be updated:

```

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::~*> vsserver cifs users-and-groups update-names -vsserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:          EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:          Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:          EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:          Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:          EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:          Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::~*> set -privilege admin

```

Manage local privileges

Add privileges to local or domain users or groups

You can manage user rights for local or domain users or groups by adding privileges. The added privileges override the default privileges assigned to any of these objects. This provides enhanced security by allowing you to customize what privileges a user or group has.

Before you begin

The local or domain user or group to which privileges will be added must already exist.

About this task

Adding a privilege to an object overrides the default privileges for that user or group. Adding a privilege does not remove previously added privileges.

You must keep the following in mind when adding privileges to local or domain users or groups:

- You can add one or more privileges.
- When adding privileges to a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller.

The command might fail if ONTAP is unable to contact the domain controller.

Steps

1. Add one or more privileges to a local or domain user or group: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verify that the desired privileges are applied to the object: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Example

The following example adds the privileges “SeTcbPrivilege” and “SeTakeOwnershipPrivilege” to the user “CIFS_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Remove privileges from local or domain users or groups

You can manage user rights for local or domain users or groups by removing privileges. This provides enhanced security by allowing you to customize the maximum privileges

that users and groups have.

Before you begin

The local or domain user or group from which privileges will be removed must already exist.

About this task

You must keep the following in mind when removing privileges from local or domain users or groups:

- You can remove one or more privileges.
- When removing privileges from a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller.

The command might fail if ONTAP is unable to contact the domain controller.

Steps

1. Remove one or more privileges from a local or domain user or group: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verify that the desired privileges have been removed from the object: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Example

The following example removes the privileges “SeTcbPrivilege” and “SeTakeOwnershipPrivilege” from the user “CIFS_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue      -
```

Reset privileges for local or domain users and groups

You can reset privileges for local or domain users and groups. This can be useful when you have made modifications to privileges for a local or domain user or group and those modifications are no longer wanted or needed.

About this task

Resetting privileges for a local or domain user or group removes any privilege entries for that object.

Steps

1. Reset the privileges on a local or domain user or group: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Verify that the privileges are reset on the object: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Examples

The following example resets the privileges on the user “CIFS_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1. By default, normal users do not have privileges associated with their accounts:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

The following example resets the privileges for the group “BUILTIN\Administrators”, effectively removing the privilege entry:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        BUILTIN\Administrators  SeRestorePrivilege
                                SeSecurityPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Display information about privilege overrides

You can display information about custom privileges assigned to domain or local user accounts or groups. This information helps you determine whether the desired user rights

are applied.

Step

- 1. Perform one of the following actions:

If you want to display information about...	Enter this command...
Custom privileges for all domain and local users and groups on the storage virtual machine (SVM)	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i></code>
Custom privileges for a specific domain or local user and group on the SVM	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i> -user-or-group-name <i>name</i></code>

There are other optional parameters that you can choose when you run this command. See the man page for more information.

Example

The following command displays all privileges explicitly associated with local or domain users and groups for SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1          CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

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.