



Display information about file security and audit policies

ONTAP 9

NetApp
February 12, 2026

Table of Contents

Display information about file security and audit policies	1
Learn about viewing ONTAP SMB file security and audit policies	1
Displaying information about file security	1
Displaying information about audit policies	1
Displaying information about Storage-Level Access Guard (SLAG) security	1
Displaying information about Dynamic Access Control (DAC) security	1
Display information about ONTAP SMB file security on NTFS security-style volumes	2
Display information about ONTAP SMB file security on mixed security-style volumes	8
Display information about ONTAP SMB file security on UNIX security-style volumes	11
ONTAP commands to display information about NTFS audit policies on SMB FlexVol volumes	14
ONTAP commands to display information about NFSv4 audit policies on SMB FlexVol volumes	17
Learn how to display ONTAP SMB file security and audit policies information	18

Display information about file security and audit policies

Learn about viewing ONTAP SMB file security and audit policies

You can display information about file security on files and directories contained within volumes on storage virtual machines (SVMs). You can display information about audit policies on FlexVol volumes. If configured, you can display information about Storage-Level Access Guard and Dynamic Access Control security settings on FlexVol volumes.

Displaying information about file security

You can display information about file security applied to data contained within volumes and qtrees (for FlexVol volumes) with the following security styles:

- NTFS
- UNIX
- Mixed

Displaying information about audit policies

You can display information about audit policies for auditing access events on FlexVol volumes over the following NAS protocols:

- SMB (all versions)
- NFSv4.x

Displaying information about Storage-Level Access Guard (SLAG) security

Storage-Level Access Guard security can be applied on FlexVol volumes and qtree objects with the following security styles:

- NTFS
- Mixed
- UNIX (if a CIFS server is configured on the SVM that contains the volume)

Displaying information about Dynamic Access Control (DAC) security

Dynamic Access Control security can be applied on an object within a FlexVol volume with the following security styles:

- NTFS
- Mixed (if the object has NTFS effective security)

Related information

- [Learn about secure file access by using Storage-Level Access Guard](#)

- [Display information about Storage-Level Access Guard on servers](#)

Display information about ONTAP SMB file security on NTFS security-style volumes

You can display information about file and directory security on NTFS security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about DOS attributes. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

- Because NTFS security-style volumes and qtrees use only NTFS file permissions and Windows users and groups when determining file access rights, UNIX-related output fields contain display-only UNIX file permission information.
- ACL output is displayed for file and folders with NTFS security.
- Because Storage-Level Access Guard security can be configured on the volume root or qtree, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file ACLs and Storage-Level Access Guard ACLs.
- The output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<code>vserver security file-directory show -vserver vserver_name -path path</code>
With expanded detail	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Examples

The following example displays the security information about the path `/vol4` in SVM `vs1`:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

          Vserver: vs1
          File Path: /vol4
          File Inode Number: 64
          Security Style: ntfs
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
              Unix User Id: 0
              Unix Group Id: 0
              Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner:BUILTIN\Administrators
          Group:BUILTIN\Administrators
          DACL - ACES
          ALLOW-Everyone-0x1f01ff
          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

The following example displays the security information with expanded masks about the path /data/engineering in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
          /data/engineering -expand-mask true

          Vserver: vs1
          File Path: /data/engineering
          File Inode Number: 5544
          Security Style: ntfs
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: 0x10
          ...0 ..... .... = Offline
          .... ..0. .... .... = Sparse
          .... .... 0.... .... = Normal
          .... .... .... 0.... = Archive
          .... .... .... .... 1.... = Directory
          .... .... .... .... 0... = System
          .... .... .... .... 0.. = Hidden
          .... .... .... .... 0 = Read Only
```



```
.....0.... =  
Execute  
.....0.... =  
Write EA  
.....0.... =  
Read EA  
.....0.... =  
Append  
.....0.... =  
Write  
.....0.... =  
Read
```

The following example displays security information, including Storage-Level Access Guard security information, for the volume with the path /datavol1 in SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

          Vserver: vs1
          File Path: /datavol1
          File Inode Number: 77
          Security Style: ntfs
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
              Unix User Id: 0
              Unix Group Id: 0
              Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
              ACLs: NTFS Security Descriptor
              Control:0x8004
              Owner:BUILTIN\Administrators
              Group:BUILTIN\Administrators
              DACL - ACES
                  ALLOW-Everyone-0x1f01ff
                  ALLOW-Everyone-0x10000000-OI|CI|IO

```

Storage-Level Access Guard security

SACL (Applies to Directories):

- AUDIT-EXAMPLE\Domain Users-0x120089-FA
- AUDIT-EXAMPLE\engineering-0x1f01ff-SA

DACL (Applies to Directories):

- ALLOW-EXAMPLE\Domain Users-0x120089
- ALLOW-EXAMPLE\engineering-0x1f01ff
- ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

SACL (Applies to Files):

- AUDIT-EXAMPLE\Domain Users-0x120089-FA
- AUDIT-EXAMPLE\engineering-0x1f01ff-SA

DACL (Applies to Files):

- ALLOW-EXAMPLE\Domain Users-0x120089
- ALLOW-EXAMPLE\engineering-0x1f01ff
- ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

Related information

- [Display information about file security on mixed security-style volumes](#)
- [Display information about file security on UNIX security-style volumes](#)

Display information about ONTAP SMB file security on mixed security-style volumes

You can display information about file and directory security on mixed security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

- Mixed security-style volumes and qtrees can contain some files and folders that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.
- The top level of a mixed security-style volume can have either UNIX or NTFS effective security.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security.

This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both UNIX file permissions and Storage-Level Access Guard ACLs.
- If the path entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<code>vserver security file-directory show -vserver vserver_name -path path</code>
With expanded detail	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Examples

The following example displays the security information about the path `/projects` in SVM `vs1` in expanded-mask form. This mixed security-style path has UNIX effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

        Vserver: vs1
        File Path: /projects
        File Inode Number: 78
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: 0x10
        ....0 ..... .... .... = Offline
        .... .0. ..... .... = Sparse
        .... .... 0... .... = Normal
        .... .... ...0. .... = Archive
        .... .... ....1 .... = Directory
        .... .... .... .0.. = System
        .... .... .... ..0. = Hidden
        .... .... .... ....0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
        Unix Mode Bits in Text: rwx-----
        ACLs: -
```

The following example displays the security information about the path /data in SVM vs1. This mixed security-style path has an NTFS effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

          Vserver: vs1
          File Path: /data
          File Inode Number: 544
          Security Style: mixed
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
          Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner:BUILTIN\Administrators
          Group:BUILTIN\Administrators
          DACL - ACES
          ALLOW-Everyone-0x1f01ff
          ALLOW-Everyone-0x10000000-
```

OI|CI|IO

The following example displays the security information about the volume at the path /datavol5 in SVM vs1. The top level of this mixed security-style volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
          Vserver: vs1
          File Path: /datavol5
          File Inode Number: 3374
          Security Style: mixed
          Effective Style: unix
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
              Unix User Id: 0
              Unix Group Id: 0
              Unix Mode Bits: 755
          Unix Mode Bits in Text: rwxr-xr-x
              ACLs: Storage-Level Access Guard security
              SACL (Applies to Directories):
                  AUDIT-EXAMPLE\Domain Users-0x120089-FA
                  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                  AUDIT-EXAMPLE\market-0x1f01ff-SA
              DACL (Applies to Directories):
                  ALLOW-BUILTIN\Administrators-0x1f01ff
                  ALLOW-Creator OWNER-0x1f01ff
                  ALLOW-EXAMPLE\Domain Users-0x120089
                  ALLOW-EXAMPLE\engineering-0x1f01ff
                  ALLOW-EXAMPLE\market-0x1f01ff
              SACL (Applies to Files):
                  AUDIT-EXAMPLE\Domain Users-0x120089-FA
                  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                  AUDIT-EXAMPLE\market-0x1f01ff-SA
              DACL (Applies to Files):
                  ALLOW-BUILTIN\Administrators-0x1f01ff
                  ALLOW-Creator OWNER-0x1f01ff
                  ALLOW-EXAMPLE\Domain Users-0x120089
                  ALLOW-EXAMPLE\engineering-0x1f01ff
                  ALLOW-EXAMPLE\market-0x1f01ff
```

Related information

- [Display information about file security on NTFS security-style volumes](#)
- [Display information about file security on UNIX security-style volumes](#)

Display information about ONTAP SMB file security on UNIX security-style volumes

You can display information about file and directory security on UNIX security-style

volumes, including what the security styles and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or directory security information you want to display. You can display the output in summary form or as a detailed list.

- UNIX security-style volumes and qtrees use only UNIX file permissions, either mode bits or NFSv4 ACLs when determining file access rights.
- ACL output is displayed only for file and folders with NFSv4 security.

This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output does not apply in the case of NFSv4 security descriptors.

They are only meaningful for NTFS security descriptors.

- Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the `-path` parameter.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<code>vserver security file-directory show -vserver vserver_name -path path</code>
With expanded detail	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Examples

The following example displays the security information about the path `/home` in SVM `vs1`:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

          Vserver: vs1
          File Path: /home
          File Inode Number: 9590
          Security Style: unix
          Effective Style: unix
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
              Unix User Id: 0
              Unix Group Id: 1
              Unix Mode Bits: 700
          Unix Mode Bits in Text: rwx-----
          ACLs: -
```

The following example displays the security information about the path /home in SVM vs1 in expanded-mask form:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

          Vserver: vs1
          File Path: /home
          File Inode Number: 9590
          Security Style: unix
          Effective Style: unix
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: 0x10
              ...0 ..... .... .... = Offline
              .... ..0. .... .... = Sparse
              .... .... 0... .... = Normal
              .... .... ...0. .... = Archive
              .... .... ....1 .... = Directory
              .... .... .... .0.. = System
              .... .... .... ..0. = Hidden
              .... .... .... ....0 = Read Only
              Unix User Id: 0
              Unix Group Id: 1
              Unix Mode Bits: 700
          Unix Mode Bits in Text: rwx-----
          ACLs: -
```

Related information

- [Display information about file security on security-style volumes](#)
- [Display information about file security on mixed security-style volumes](#)

ONTAP commands to display information about NTFS audit policies on SMB FlexVol volumes

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must provide the name of the storage virtual machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

- NTFS security-style volumes and qtrees use only NTFS system access control lists (SACLs) for audit policies.
- Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.

Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, the output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4 SACLs and Storage-Level Access Guard NTFS SACLs.
- If the path that is entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.
- When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information.

NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.

- ACL output is displayed only for files and folders with NTFS or NFSv4 security.

This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

Step

1. Display file and directory audit policy settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	vserver security file-directory show -vserver <u>vserver_name</u> -path <u>path</u>
As a detailed list	vserver security file-directory show -vserver <u>vserver_name</u> -path <u>path</u> -expand-mask true

Examples

The following example displays the audit policy information for the path `/corp` in SVM `vs1`. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
          Vserver: vs1
          File Path: /corp
          File Inode Number: 357
          Security Style: ntfs
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
              Unix User Id: 0
              Unix Group Id: 0
              Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
              ACLs: NTFS Security Descriptor
              Control:0x8014
              Owner:DOMAIN\Administrator
              Group:BUILTIN\Administrators
              SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
              DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

The following example displays the audit policy information for the path `/datavol1` in SVM `vs1`. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1

          Vserver: vs1
          File Path: /datavol1
          File Inode Number: 77
          Security Style: ntfs
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
              Unix User Id: 0
              Unix Group Id: 0
              Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
              ACLs: NTFS Security Descriptor
              Control:0xaal4
              Owner:BUILTIN\Administrators
              Group:BUILTIN\Administrators
              SACL - ACEs
                  AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
              DACL - ACEs
                  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                  ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

          Storage-Level Access Guard security
          SACL (Applies to Directories):
              AUDIT-EXAMPLE\Domain Users-0x120089-FA
              AUDIT-EXAMPLE\engineering-0x1f01ff-SA
          DACL (Applies to Directories):
              ALLOW-EXAMPLE\Domain Users-0x120089
              ALLOW-EXAMPLE\engineering-0x1f01ff
              ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
          SACL (Applies to Files):
              AUDIT-EXAMPLE\Domain Users-0x120089-FA
              AUDIT-EXAMPLE\engineering-0x1f01ff-SA
          DACL (Applies to Files):
              ALLOW-EXAMPLE\Domain Users-0x120089
              ALLOW-EXAMPLE\engineering-0x1f01ff
              ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ONTAP commands to display information about NFSv4 audit policies on SMB FlexVol volumes

You can display information about NFSv4 audit policies on FlexVol volumes using the ONTAP CLI, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists (SACLs). You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the files or directories whose audit information you want to display. You can display the output in summary form or as a detailed list.

- UNIX security-style volumes and qtrees use only NFSv4 SACLs for audit policies.
- Files and directories in a mixed security-style volume that are of UNIX security style can have NFSv4 audit policies applied to them.

Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NFSv4 SACLs.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security.

This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular NFSv4 file and directory SACLs and Storage-Level Access Guard NTFS SACLs.
- Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the `-path` parameter.

Steps

1. Display file and directory security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<code>vserver security file-directory show -vserver vserver_name -path path</code>
With expanded detail	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Examples

The following example displays the security information about the path `/lab` in SVM vs1. This UNIX security-style path has an NFSv4 SACL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

          Vserver: vs1
          File Path: /lab
          File Inode Number: 288
          Security Style: unix
          Effective Style: unix
          DOS Attributes: 11
          DOS Attributes in Text: ----D--R
          Expanded Dos Attributes: -
              Unix User Id: 0
              Unix Group Id: 0
              Unix Mode Bits: 0
          Unix Mode Bits in Text: -----
              ACLs: NFSV4 Security Descriptor
              Control:0x8014
              SACL - ACEs
                  SUCCESSFUL-S-1-520-0-0xf01ff-SA
                  FAILED-S-1-520-0-0xf01ff-FA
              DACL - ACEs
                  ALLOW-S-1-520-1-0xf01ff
```

Learn how to display ONTAP SMB file security and audit policies information

You can use the wildcard character (*) to display information about file security and audit policies of all files and directories under a given path or a root volume.

The wildcard character (*) **can be used as the last subcomponent of a given directory path below which you want to display information of all files and directories. If you want to display information of a particular file or directory named as “”, then you need to provide the complete path inside double quotes ("")**.

Example

The following command with the wildcard character displays the information about all files and directories below the path `/1/` of SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*
          Vserver: vs1
          File Path: /1/1
          Security Style: mixed
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
              Unix User Id: 0
              Unix Group Id: 0
              Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
              ACLs: NTFS Security Descriptor
                  Control:0x8514
                  Owner:BUILTIN\Administrators
                  Group:BUILTIN\Administrators
                  DACL - ACES
                  ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
          Vserver: vs1
          File Path: /1/1/abc
          Security Style: mixed
          Effective Style: ntfs
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
              Unix User Id: 0
              Unix Group Id: 0
              Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
              ACLs: NTFS Security Descriptor
                  Control:0x8404
                  Owner:BUILTIN\Administrators
                  Group:BUILTIN\Administrators
                  DACL - ACES
                  ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

The following command displays the information of a file named as "*" under the path /vol1/a of SVM vs1. The path is enclosed within double quotes ("").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

        Vserver: vs1
        File Path: "/vol1/a/*"
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 1002
        Unix Group Id: 65533
        Unix Mode Bits: 755
        Unix Mode Bits in Text: rwxr-xr-x
        ACLs: NFSV4 Security Descriptor
        Control:0x8014
        SACL - ACEs
        AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
        DACL - ACEs
        ALLOW-EVERYONE@-0x1f00a9-FI|DI
        ALLOW-OWNER@-0x1f01ff-FI|DI
        ALLOW-GROUP@-0x1200a9-IG
```

Copyright information

Copyright © 2026 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.