vserver security commands

ONTAP 9.10.1 commands

NetApp
September 27, 2022

Table of Contents

vserver security commands

vserver security file-directory apply

Apply security descriptors on files and directories defined in a policy to a Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory apply` command applies security settings to files and directories defined in a security policy of a Vserver.

Applying a security policy to a Vserver is the last step to creating and applying NTFS ACLs to files or folders. A security policy contains definitions for the security configuration of a file (or folder) or set of files (or, folders). The policy is a container for tasks. A task associates a file/folder path name to the security descriptor that needs to be set on the file/folder. Every task in a policy is uniquely identified by the file/folder path. A policy cannot have duplicate task entries. There can be only one task per path.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLs and SACLs to the NTFS security descriptor.

> If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding the SACL to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.
* Create policy tasks.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.
* Apply a policy to the associated Vserver.

Parameters

`-vserver <vserver name>` - Vserver

Specifies the Vserver that contains the path to which the security policy is applied.

`-policy-name <Security policy name>` - Policy Name

Specifies the security policy to apply.

`[-ignore-broken-symlinks {true|false}]` - Skip Broken Symlinks

If you specify this parameter as *`true`* , the file-directory apply job will skip all the symlinks that are broken instead of failing the job.

Examples

The following example applies a security policy named “p1” to Vserver vs0.

```
cluster1::> vserver security file-directory apply -vserver vs0 -policy
-name p1
```

vserver security file-directory remove-slag

Removes Storage-Level Access Guard

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory remove-slag` command removes Storage-Level Access Guard (SLAG) security from the specified volume or qtree path.

Parameters

`-vserver <vserver>` - Vserver

Specifies the name of the Vserver that is associated with the volume or qtree path from where you want to remove SLAG.

`-path <text>` - Path

Specifies the volume or qtree mounted junction path from which you want to remove SLAG security.

Examples

The following example removes SLAG security from the volume path "/vol1" on Vserver vs1.

```
cluster1::>vserver security file-directory show -vserver vs1 -path /vol1
Vserver: vs1
                    File Path: /vol1
            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
DACL (Applies to Directories):
                                ALLOW-CIFS1\Administrator-0x1200a9
                             DACL (Applies to Files):
                                ALLOW-CIFS1\Administrator-0x1200a9
cluster1::>vserver security file-directory remove-slag -path /vol1
-vserver vs1
cluster1::>vserver security file-directory show -vserver vs1 -path /vol1
                     Vserver: vs1
                    File Path: /vol1
            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: -
```

The following example removes SLAG security from the qtree path "/vol1/q1" on Vserver vs1.

```
cluster1::>vserver security file-directory show -vserver vs1 -path
/vol1/q1
Vserver: vs1
                     File Path: /vol1/q1
                 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
DACL (Applies to Directories):
                                    ALLOW-CIFS1\Administrator-0x1200a9
                                 DACL (Applies to Files):
                                    ALLOW-CIFS1\Administrator-0x1200a9
cluster1::>vserver security file-directory remove-slag -path /vol1/q1
-vserver vs1
cluster1::>vserver security file-directory show -vserver vs1 -path
/vol1/q1
                       Vserver: vs1
                     File Path: /vol1/q1
                 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: -
```

vserver security file-directory show-effective-permissions

Display effective file or folder permissions

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory show-effective-permissions ` command displays the effective permission granted to a Windows or UNIX user on the specified file or folder path. The command output depends on the parameter or parameters specified with the command.

The `-vserver` , `-win-user-name` or `-unix-user-name` and `-path` parameters are required for this command. If the optional parameter `-share-name` is specified, it will display the effective share permission.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

-vserver <vserver> - Vserver

Use this required parameter to specify the Vserver that contains the path to the file or folder specified with the required `-path` parameter. Query characters, such as "*", are not supported.

{ -win-user-name <text> - Windows User Name

Use this parameter to specify the Windows user for which effective permission needs to be displayed on the given file or folder.

| -unix-user-name <text> - Unix User Name }

Use this parameter to specify the UNIX user for which effective permission needs to be displayed on the given file or folder.

-path <text> - File Path

Use this mandatory parameter to specify the path of the file or the folder for which you want to display effective permissions. The path is relative to the Vserver root volume. If `-share-name` is specified then the path will be relative to the share path. Query characters,such as "*", are not supported.

[-share-name <Share>] - CIFS Share Name

If you specify this optional parameter, the command displays the file or directory effective permission for the mentioned user, only for files and directories con-tained where the specified path is relative to the root of the specified share. If this parameter is not specified, the Vserver root volume is taken as the default. If this optional parameter is specified, then it will also display the effective share permission of the user. Wildcard query characters are not supported.

[-client-ip-address <IP Address>] - Client IP Address

If you specify this optional parameter, the command displays the effective permission for the user with the specified client ip address.

[-expand-mask {true|false}] - Expand Bit Masks

If you specify this optional parameter, the command displays effective permission for files and directories where the hexadecimal bit mask entries are in expanded bit form. If set to default (false), the command displays effective permission for file or directory in collapsed (textual) form.

[-share-path <text>] - CIFS Share Path

If you specify this parameter, the command displays information only about the CIFS share that match the specified path. Query characters, such as "*", are not supported.

[-permission <Security acl>,…] - Effective Permissions

If you specify this parameter, the command displays effective permission only if specified permission matches. Wildcard query characters are not supported.

vserver security file-directory show

Display file/folder security information

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory show` command displays file/folder security information. The command output depends on the parameter or parameters specified with the command.

The `-vserver` and `-path` parameters are required for this command. If you do not specify any of the optional parameters, the command displays all security information in list format for the specified path.

You can specify the `-fields` parameter to specify which fields of information to display about files and folders security.

You can specify the `-instance` parameter to display all the security information in list format.

Parameters

{ [-fields <fieldname>,…]

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| [-instance] }

If you specify the -instance parameter, the command displays detailed information about all entries.

-vserver <vserver> - Vserver

Use this required parameter to specify the Vserver that contains the path to the file or folder specified with the required `-path` parameter.

{ [-path <text>] - File Path

Use this field to specify the path of the file or folder for which you want to display security information. If the volume name is not specified in the path, the path is relative to the Vserver root volume. If the path's last subcomponent has a wildcard ("*"), the output will display information for all files and directories below the parent path.

If you want to display information of a file or directory which contains wildcard ("*") as its last sub-component, then provide the complete path inside "<path>".

For instance, vserver security file-directory show -vserver vs1 -path "/vol1/**" will show ACL information for the directory named ""**, only.

| [-inode <integer>] - File Inode Number }

Use this field to specify the inode number of the file or folder for which you want to display security information. If the volume name is not specified, inode is searched in the Vserver root volume.

{ [-volume-name <volume name>] - Volume Name

If you specify this parameter, the command displays information about file and directory security only for files and directories where the specified path is relative to the specified volume. If this parameter is not specified, the Vserver root volume is taken as default.

| [-share-name <Share>] - Share Name }

If you specify this parameter, the command displays information about file and directory security only for files and directories contained where the specified path is relative to the root of the specified share. If this parameter is not specified, the Vserver root volume is taken as default.

[-lookup-names {true|false}] - SID to Name Lookups

If you specify this parameter, the command displays information about file and directory security for files and directories where the information about owner and group are stored as names. If set to false, the command displays information about file and directory security for files and directories where the information for owner and group are stored as SIDs.

{ [-expand-mask {true|false}] - Expand Bit Masks

If you specify this parameter, the command displays information about file and directory security for files and directories where the hexadecimal bit mask entries are in expanded bit form. If set to false, the command displays information about file and directory security for files and directories where the hexadecimal bit mask entries are in collapsed form.

| [-textual-mask {true|false}] - Show Textual Mask

If you specify this parameter as *true* , the command displays information about file and directory security for files and directories where the hexadecimal bit mask is translated to texual format.

| [-sddl {true|false}] - Display ACLs in SDDL Format }

If you specify this parameter, the command displays the ACL information for files and directories in Security Descriptor Definition Language (SDDL) format. If the file has `effective-style` as "unix" then this flag has no effect.

[-security-style <security style>] - Security Style

If you specify this parameter, the command displays information about file and directory security only for files and directories with paths in volumes of the specified security style.

[-effective-style <security style>] - Effective Style

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified effective security style on the path.

[-dos-attributes <Hex Integer>] - DOS Attributes

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified DOS attributes.

[-text-dos-attr <TextNoCase>] - DOS Attributes in Text

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified text DOS attributes.

[-expanded-dos-attr <TextNoCase>] - Expanded Dos Attributes

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified extended DOS attributes. This parameter is useful only for files or directories where the `-expand-mask` is set to true.

[-user-id <user name>] - UNIX User Id

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified UNIX user ID.

[-group-id <group name>] - UNIX Group Id

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified UNIX group ID.

[-mode-bits <Octal Permission>] - UNIX Mode Bits

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified UNIX mode bits in Octal form.

[-text-mode-bits <text>] - UNIX Mode Bits in Text

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified UNIX mode bits in text form.

[-acls <Security acl>,…] - ACLs

If you specify this parameter, the command displays information about file and directory security only for files and directories with the specified ACLs. If the specified path is a volume or qtree path and Storage-Level Access Guard (SLAG) is configured on the volume or qtree, this parameter displays the SLAG information. It also displays the Dynamic Access Control (DAC) policies if DAC is configured for the given file or directory path. The following ACL information can be entered:

- Type of ACL - NTFS or NFSV4
- Control bits in the security descriptors
- Owner - only in case of NTFS security descriptors
- Group - only in case of NTFS security descriptors
- Access Control Entries - discretionary access control list (DACL) and system access control list (SACL) access control entries (ACEs) in the ACL

Examples

The following example displays the security information about the path "/vol4" in Vserver vs1.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol4
              (vserver security file-directory show)
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 about the path "/a/b/file.txt" in Vserver vs1.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/a/b/file.txt -volume-name vol1
                  (vserver security file-directory show)
Vserver: vs1
                                File Path: /vol1/a/b/file.txt
                      File Inode Number: 101
                         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 of the volume path "/vol1" containing SLAG.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                 File Inode Number: 64
                    Security Style: mixed
                   Effective Style: ntfs
                    DOS Attributes: 10
            DOS Attributes in Text: ----D---
            Expanded Dos Attribute: -
                      Unix User Id: 0
                     Unix Group Id: 1
                    Unix Mode Bits: 777
            Unix Mode Bits in Text: rwxrwxrwx
                              ACLs: NTFS Security Descriptor
                                    Control:0xbf14
                                    Owner:CIFS1\Administrator
                                    Group:CIFS1\Domain Admins
                                    SACL - ACEs
                                       ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                       RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                       POLICY ID-All resources - No Write-
0x0-OI|CI
                                    DACL - ACEs
                                       ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                       ALLOW-Everyone-0x1f01ff-OI|CI
                                       ALLOW CALLBACK-DAC\skanyal-
0x1200a9-OI|CI

((@User.department==@Resource.Department_MS@Resource.Impact_MS>1000)@Devic
e.department==@Resource.Department_MS)
Storage-Level Access Guard security
                                    SACL (Applies to Directories):
                                       AUDIT-R1\user1-0x001f01ff-FA
                                    DACL (Applies to Directories):
                                       ALLOW-R1\user1-0x001f01ff
                                       ALLOW-R1\user2-0x001200a9
                                    SACL (Applies to Files):
                                       AUDIT-R1\user1-0x001f01ff-FA
                                    DACL (Applies to Files):
                                       ALLOW-R1\user1-0x001f01ff
                                       ALLOW-R1\user2-0x001200a9
```

The following example displays the security information of the qtree path "/vol1/q1" containing SLAG.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/vol1/q1
                           Vserver: vs1
                         File Path: /vol1/q1
                 File Inode Number: 105
                    Security Style: mixed
                   Effective Style: ntfs
                    DOS Attributes: 10
            DOS Attributes in Text: ----D---
            Expanded Dos Attribute: -
                      Unix User Id: 0
                     Unix Group Id: 1
                    Unix Mode Bits: 777
            Unix Mode Bits in Text: rwxrwxrwx
                              ACLs: NTFS Security Descriptor
                                    Control:0xbf14
                                    Owner:CIFS1\Administrator
                                    Group:CIFS1\Domain Admins
                                    SACL - ACEs
                                       ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                    DACL - ACEs
                                       ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                       ALLOW-Everyone-0x1f01ff-OI|CI
Storage-Level Access Guard security
                                    SACL (Applies to Directories):
                                       AUDIT-R1\user1-0x001f01ff-FA
                                    DACL (Applies to Directories):
                                       ALLOW-R1\user1-0x001f01ff
                                       ALLOW-R1\user2-0x001200a9
                                    SACL (Applies to Files):
                                       AUDIT-R1\user1-0x001f01ff-FA
                                    DACL (Applies to Files):
                                       ALLOW-R1\user1-0x001f01ff
                                       ALLOW-R1\user2-0x001200a9
```

vserver security file-directory job show

Display a list of file security jobs

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory job show` command displays information about security file-directory jobs.

To display detailed information about a specific job, run the command with the `-id` parameter.

You can specify additional parameters to select information that matches the values you specify for those parameters. For example, to display information only about security file-directory jobs running on a specific node, run the command with the `-node` parameter.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-inprogress]

Displays the job ID, the job name, the owning Vserver, and the progress of the security file-directory job.

| [-jobstate]

Displays information about each job's state, including the queue state, whether the job was restarted and when the job has completely timed out.

| [-sched]

Displays the job ID, the job name, the owning Vserver, and the schedule on which the security file-directory job runs.

| [-times]

Displays the job ID, the job name, the owning Vserver, the time when the job was last queued, the time when the job was last started, and the time when the job most recently ended.

| [-type]

Displays the job ID, the job name, the job type, and the job category.

| [-jobuuid]

Displays the job ID, the job name, the owning Vserver, and the job UUID.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-id <integer>] - Job ID

Selects the jobs that match the ID or range of IDs that you specify.

[-vserver <vserver name>] - Owning Vserver

Selects jobs that are owned by the specified Vserver.

[-name <text>] - Name

Selects the jobs that match this parameter value.

[-description <text>] - Description

Selects the jobs that match this parameter value.

[-priority {Low|Medium|High|Exclusive}] - Priority

Selects the jobs that match this parameter value.

[-node <nodename>] - Node

Selects the jobs that match this parameter value.

[-affinity {Cluster|Node}] - Affinity

Selects the jobs that match this parameter value.

[-schedule <job_schedule>] - Schedule

Selects the jobs that match this parameter value.

[-queuetime <MM/DD HH:MM:SS>] - Queue Time

Selects the jobs that match this parameter value.

[-starttime <MM/DD HH:MM:SS>] - Start Time

Selects the jobs that match this parameter value.

[-endtime <MM/DD HH:MM:SS>] - End Time

Selects the jobs that match this parameter value.

[-dropdeadtime <MM/DD HH:MM:SS>] - Drop-dead Time

Selects the jobs that match this parameter value.

[-restarted {true|false}] - Restarted?

Selects the jobs that match this parameter value.

[-state {Initial|Queued|Running|Waiting|Pausing|Paused|Quitting|Success|Failure|Reschedule|Error|Quit|Dead|Unknown|Restart|Dormant}] - State

Selects the jobs that match this parameter value.

[-code <integer>] - Status Code

Selects the jobs that match this parameter value.

[-completion <text>] - Completion String

Selects the jobs that match this parameter value.

[-jobtype <text>] - Job Type

Selects the jobs that match this parameter value.

[-category <text>] - Job Category

Selects the jobs that match this parameter value.

[-uuid <UUID>] - UUID

Selects the jobs that match this parameter value.

[-progress <text>] - Execution Progress

Selects the jobs that match this parameter value.

[-username <text>] - User Name

Selects the jobs that match this parameter value.

[-process <text>] - Process

Selects jobs with the specified process number.

Examples

The following example displays information abthe file-directory security job.

```
cluster1::> vserver security file-directory apply -policy-name pol
-vserver vs1
cluster1::> vserver security file-directory job show
                            Owning
            Job ID Name                 Vserver    Node           State
            ------ -------------------- ---------- --------------
----------
            25     Fsecurity Apply      vsim2.3    vsim2.3-01     Success
               Description: File Directory Security Apply Job
```

vserver security file-directory ntfs create

Create an NTFS security descriptor

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs create` command creates an NTFS security descriptor to which you can add access control entries (ACEs) to the discretionary access control list (DACL) and the system access control list (SACL).

Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within a namespace. Later, you will associate the security descriptor to a policy task.

You can create NTFS security descriptors for files and folders residing within FlexVol volumes with NTFS security-style or on NTFS security descriptors on mixed security-style volumes.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLs and SACLs to the NTFS security descriptor.

If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding a SACL to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.
* Create a policy task.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.
* Apply a policy to the associated Vserver.

Parameters

-vserver <vserver name> - Vserver

Specifies the name of the Vserver on which to create the security descriptor.

-ntfs-sd <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor you want to create. After you create a security descriptor, you can add SACL and DACL access control entries (ACEs) to it.

Every newly created security descriptor contains the 4 default DACL ACEs as mentioned below:

```
Vserver: vserver1
                         NTFS Security Descriptor Name: sd1
Account Name     Access   Access             Apply To
                                            Type     Rights
                           --------------   -------  -------
-----------
                           BUILTIN\Administrators
                                            allow    full-control
this-folder, sub-folders, files
                           BUILTIN\Users    allow    full-control
this-folder, sub-folders, files
                           CREATOR OWNER    allow    full-control
this-folder, sub-folders, files
                           NT AUTHORITY\SYSTEM
                                            allow    full-control
this-folder, sub-folders, files
```

+

[-owner <name or sid>] - Owner

Specifies the owner of the security descriptor. You can specify the owner using either a user name or SID.

The owner of the security descriptor can modify the permissions on the file (or folder) or files (or folders) to which the security descriptor is applied and can give other users the right to take ownership of the object or

objects to which the security descriptor is applied. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

> If you specify any of the three user name formats for the value of `-owner` , keep in mind that the value for the user name is case insensitive. The value for the user name is ignored for Storage-Level Access Guard (SLAG).

`[-group <name or sid>]` - Primary Group

Specifies the owner group of the security descriptor. You can specify the owner group using either a group name or SID. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

> If you specify any of the three user name formats for the value of `-group` , keep in mind that the value for the user name is case insensitive. The value for the user name is ignored for SLAG.

`[-control-flags-raw <Hex Integer>]` - Raw Control Flags

Specifies the control flags in the security descriptor.

> The value for the control flag is ignored for SLAG.

Examples

The following example creates an NTFS security descriptor named “sd1” on Vserver "vs1" and assigns “DOMAIN\Administrator” as the security descriptor owner.

```
cluster1::> vserver security file-directory ntfs create -ntfs-sd sd1
-vserver vs1 -owner DOMAIN\Administrator
cluster1::> vserver security file-directory ntfs show -vserver vs1 -ntfs
-sd sd1
                                        Vserver: vs1
                      Security Descriptor Name: sd2
              Owner of the Security Descriptor: DOMAIN\Administrator
```

vserver security file-directory ntfs delete

Delete an NTFS security descriptor

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs delete` command deletes an NTFS security descriptor. Deleting a security descriptor also deletes all the contained DACL and SACL access control entries (ACEs).

Parameters

`-vserver <vserver name>` - Vserver

Specifies the name of the Vserver that is associated with the security descriptor that you want to delete.

`-ntfs-sd <ntfs sd name>` - NTFS Security Descriptor Name

Specifies the name of the security descriptor to delete.

Examples

The following example deletes an NTFS security descriptor named "sd1" on Vserver vs1.

```
cluster1::> vserver security file-directory ntfs delete -ntfs-sd sd1
-vserver vs1
```

vserver security file-directory ntfs modify

Modify an NTFS security descriptor

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs modify` command modifies an NTFS security descriptor. You can change the `-owner` , `-group` and `-control-flags-raw ` of the security descriptor with this command.

Parameters

`-vserver <vserver name>` - Vserver

Specifies the name of the Vserver associated with the security descriptor that you want to modify.

`-ntfs-sd <ntfs sd name>` - NTFS Security Descriptor Name

Specifies the name of the security descriptor that you want to modify.

`[-owner <name or sid>]` - Owner

Specifies the owner of the security descriptor. You can specify the owner using either the user name or SID.

The owner of the security descriptor can modify the permissions on the file (or folder) or files (or folders) to which the security descriptor is applied and can give other users the right to take ownership of the object or objects to which the security descriptor is applied. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

> If you specify any of the three user name formats for the value of `-owner` , keep in mind that the value for the user name is case insensitive. The value for the user name is ignored for Storage-Level Access Guard (SLAG).

`[-group <name or sid>]` - Primary Group

Specifies the owner group of the security descriptor. You can specify the owner group using either a group name or SID. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

> If you specify any of the three user name formats for the value of `-group` , keep in mind that the value for the user name is case insensitive. The value for the user name is ignored for SLAG.

`[-control-flags-raw <Hex Integer>]` - Raw Control Flags

Specifies the control flags in the security descriptor to be modified.

> The value for the control flag is ignored for SLAG.

Examples

The following example modifies the owner of an NTFS security descriptor named "sd2" on Vserver vs1.

```
cluster1::> vserver security file-directory ntfs modify -ntfs-sd sd2
-vserver vs1 -owner domain\administrator
cluster1::> vserver security file-directory ntfs show -vserver vs1 -ntfs
-sd sd2
Vserver: vs1
                    Security Descriptor Name: sd2
            Owner of the Security Descriptor: DOMAIN\Administrator
```

vserver security file-directory ntfs show

Display an NTFS security descriptors

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs show` command displays information about the security descriptor. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays all information about all security descriptors defined on the cluster.

You can specify the `-fields` parameter to specify which fields of information to display about security descriptors.

You can specify the `-instance` parameter to display all the information about security descriptors in list format.

Parameters

{ [-fields <fieldname>,…]

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| [-instance] }

If you specify the -instance parameter, the command displays detailed information about all entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the security descriptors associated with the Vserver that you specify.

[-ntfs-sd <ntfs sd name>] - NTFS Security Descriptor Name

If you specify this parameter, the command displays information only about the security descriptors that you specify.

[-owner <name or sid>] - Owner

If you specify this parameter, the command displays information only about the security descriptors owned by the specified user name or SID.

[-group <name or sid>] - Primary Group

If you specify this parameter, the command displays information only about the security descriptors associated with the owner group.

[-control-flags-raw <Hex Integer>] - Raw Control Flags

If you specify this parameter, the command displays information only about the security descriptors associated with the control flags.

Examples

The following example displays information about an NTFS security descriptor named “sd2” on Vserver vs1.

```
cluster1::> vserver security file-directory ntfs show -vserver vs1 -ntfs
-sd sd2
Vserver: vs1
                    Security Descriptor Name: sd2
             Owner of the Security Descriptor: DOMAIN\Administrator
```

vserver security file-directory ntfs dacl add

Add a DACL entry to NTFS security descriptor

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs dacl add` command adds access control entries (ACEs) into a security descriptor's discretionary access control list (DACL).

If the security descriptor contains a DACL that has existing ACEs, the command adds the new ACE to the DACL. If the security descriptor does not contain a DACL, the command creates the DACL and adds the new ACE to it.

Adding a DACL entry to the security descriptor is the second step in configuring and applying ACLs to a file or folder. Before you can add a DACL entry to a security descriptor, you must first create the security descriptor.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLs and SACLs to the NTFS security descriptor.

> If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding the SACL to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.
* Create policy tasks.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.
* Apply a policy to the associated Vserver.

Parameters

`-vserver <vserver name>` - Vserver

Specifies the name of the Vserver associated with the security descriptor to which you want to add a discretionary access control entry (discretionary ACE).

-ntfs-sd <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor to which you want to add a discretionary access control entry.

-access-type {deny|allow} - Allow or Deny

Specifies whether the discretionary access control entry is an *allow* or *deny* type of access control.

-account <name or sid> - Account Name or SID

Specifies the account on which to apply the discretionary access control entry. You can specify the account by using a user name or SID. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

If you specify any of the three user name formats for the value of -account, keep in mind that the value for the user name is case insensitive.

{ [-rights {no-access|full-control|modify|read-and-execute|read|write}] - DACL ACE's Access Rights

Specifies the right that you want to add for the account specified in the `-account` parameter. The `-rights` parameter is mutually exclusive with the `-advanced-rights` and `-rights-raw` parameter. If you specify the `-rights` parameter, you can only specify one value.

You can specify one of the following rights values:

- no-access
- full-control
- modify
- read-and-execute
- read
- write

| [-advanced-rights <Advanced access right>,…] - DACL ACE's Advanced Access Rights }

Specifies the advanced rights that you want to add for the account specified in the `-account` parameter. The `-advanced-rights` parameter is mutually exclusive with the `-rights` and `-rights-raw` parameter. You can specify more than one advanced-rights value by using a comma-delimited list.

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data
- read-ea
- write-ea

- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

| [-rights-raw <Hex Integer>] - DACL ACE's Raw Access Rights }

Specifies the raw rights that you want to add for the account specified in the `-account` parameter. The `rights-raw` parameter is mutually exclusive with the `-advanced-rights` and `-rights` parameter. Specify the value as a hexadecimal integer, for example: *`0xA10F`* or *`0xb3ff`* etc.

[-apply-to {this-folder|sub-folders|files}] - Apply DACL Entry

Specifies where to apply the discretionary access control entry. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

Select one of the following combinations of values for the `-apply-to` parameter for Storage-Level Access Guard (SLAG):

- this-folder, sub-folder, files
- this-folder, sub-folder
- files

If you specify an invalid `-apply-to` value, this security descriptor is removed from the associated Storage-Level Access Guard (SLAG) `security file-directory policy task .`

Examples

The following example adds a DACL entry to the security descriptor named “sd1” on Vserver "vs1" for the "DOMAIN\Administrator" account.

```
cluster1::> vserver security file-directory ntfs dacl add -ntfs-sd sd1
-access-type deny -account DOMAIN\Administrator -rights full-control
-apply-to this-folder -vserver vs1
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
-ntfs-sd sd1 -access-type deny -account domain\administrator
Vserver: vs1
              Security Descriptor Name: sd1
                        Allow or Deny: deny
                   Account Name or SID: DOMAIN\Administrator
                        Access Rights: full-control
                Advanced Access Rights: -
                             Apply To: this-folder
                        Access Rights: full-control
```

vserver security file-directory ntfs dacl modify

Modify an NTFS security descriptor DACL entry

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs dacl modify` command modifies parameters in an existing discretionary access control (DACL) entry.

You can unambiguously define which DACL entry to modify by specifying the following four parameters in the modify command:

- Vserver associated with the security descriptor that contains the DACL entry
- Name of the security descriptor that contains the DACL entry
- Whether the DACL is an allow or deny type of DACL entry
- The account name or SID to which the DACL is applied

You can modify the following parameters:

- -right,-advanced-rights ,-rights-raw
- -apply-to

Parameters

`-vserver <vserver name>` - Vserver

Specifies the name of the Vserver associated with the security descriptor containing the discretionary access control entry whose parameters you want to modify.

`-ntfs-sd <ntfs sd name>` - NTFS Security Descriptor Name

Specifies the name of the security descriptor that contains the discretionary access control entry that you want to modify.

-access-type {deny|allow} - Allow or Deny

Specifies whether the discretionary access control entry that you want to modify is an *allow* or *deny* type of access control.

-account <name or sid> - Account Name or SID

Specifies the account associated with the discretionary access control entry you want to modify. You can specify the account by using a user name or SID. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

If you specify any of the three user name formats for the value of -account, keep in mind that the value for the user name is case insensitive.

{ [-rights {no-access|full-control|modify|read-and-execute|read|write}] - Access Rights

Specifies the right that you want to add for the account specified in the `-account` parameter. The `-rights` parameter is mutually exclusive with the `-advanced-rights` and `-rights-raw` parameter. If you specify the `-rights` parameter, you can only specify one value.

You can specify one of the following rights values:

- no-access
- full-control
- modify
- read-and-execute
- read
- write

| [-rights-raw <Hex Integer>] - Raw Access Rights

Specifies the raw rights that you want to add for the account specified in the `-account` parameter. The `-rights-raw` parameter is mutually exclusive with the `-advanced-rights` and `-rights` parameter. Specify the value as a hexadecimal integer, for example: *0xA10F* or *0xb3ff* etc.

| [-advanced-rights <Advanced access right>,…] - Advanced Access Rights }

Specifies the advanced rights that you want to add for the account specified in the `-account` parameter. The `-advanced-rights` parameter is mutually exclusive with the `-rights` and `-rights-raw` parameter. You can specify more than one advanced-rights value by using a comma-delimited list.

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data

- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

[-apply-to {this-folder|sub-folders|files}] - Apply DACL Entry

Specifies where to apply the discretionary access control entry. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

Select one of the following combinations of values for the `-apply-to` parameter for Storage-Level Access Guard (SLAG):

- this-folder, sub-folder, files
- this-folder, sub-folder
- files

If you specify an invalid `-apply-to` value, this security descriptor is removed from the associated Storage-Level Access Guard (SLAG) `security file-directory policy task`.

Examples

The following example modifies the `-right` and `-apply-to` parameters in the DACL entry associated to the security descriptor named “sd2” on Vserver vs1 for the "BUILTIN\Administrators" account.

```
cluster1::> vserver security file-directory ntfs dacl modify -ntfs-sd sd2
-access-type allow -account BUILTIN\Administrators -vserver vs1 -rights
modify -apply-to this-folder,sub-folders
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
-ntfs-sd sd2 -account BUILTIN\Administrators -instance
Vserver: vs1
            Security Descriptor Name: sd2
                      Allow or Deny: allow
                 Account Name or SID: BUILTIN\Administrators
                       Access Rights: modify
              Advanced Access Rights: -
                            Apply To: this-folder, sub-folders
                       Access Rights: modify
```

vserver security file-directory ntfs dacl remove

Remove a DACL entry from NTFS security descriptor.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs dacl remove` command removes a discretionary access control entry from a security descriptor.

You can unambiguously define which DACL entry to remove by specifying the following four parameters in the command:

- Vserver associated with the security descriptor that contains the DACL entry
- Name of the security descriptor that contains the DACL entry
- Whether the DACL is an allow or deny type of DACL entry
- The account name or SID to which the DACL is applied

Parameters

`-vserver <vserver name>` - Vserver

Specifies the name of the Vserver associated with the security descriptor from which you want to remove a discretionary access control entry.

`-ntfs-sd <ntfs sd name>` - NTFS Security Descriptor Name

Specifies the name of the security descriptor that contains the discretionary access control entry that you want to remove.

`-access-type {deny|allow}` - Allow or Deny

Specifies whether the discretionary access control entry you want to remove is an *`allow`* or *`deny`* of access control.

-account <name or sid> - Account Name or SID

Specifies the account name or SID associated with the discretionary access control entry that you want to remove.

Examples

The following example removes a DACL entry from the security descriptor named “sd2” with “allow” access type for the "BUILTIN\Administrators" account on Vserver vs1.

```
cluster1::> vserver security file-directory ntfs dacl remove -ntfs-sd sd2
-access-type allow -account BUILTIN\Administrators -vserver vs1
```

vserver security file-directory ntfs dacl show

Display NTFS security descriptor DACL entries

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs dacl show` command displays information about all the discretionary access control entries in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all DACL entries:

- Vserver name
- Security descriptor
- List of DACL entries

You can specify the `-fields` parameter to specify which fields of information to display about DACL entries.

You can specify the `-instance` parameter to display all information about DACL entries in a list format.

Parameters

{ [-fields <fieldname>,…]

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| [-instance] }

If you specify the -instance parameter, the command displays detailed information about all entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about discretionary access control entries associated with the specified Vserver.

[-ntfs-sd <ntfs sd name>] - NTFS Security Descriptor Name

If you specify this parameter, the command displays information only about the discretionary access control entries for the security descriptor that you specify.

[-access-type {deny|allow}] - Allow or Deny

If you specify this parameter, the command displays information only about the discretionary access control entries with the access type that you specify.

[-account <name or sid>] - Account Name or SID

If you specify this parameter, the command displays information only about the discretionary access control entries associated with the account name or SID that you specify. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

If you specify any of the three user name formats for the value of -account, keep in mind that the value for the user name is case insensitive.

[-rights {no-access|full-control|modify|read-and-execute|read|write}] - Access Rights

If you specify this parameter, the command displays information only about the discretionary access control entries with the user right that you specify. Only one value can be specified.

You can specify one of the following rights values:

- no-access
- full-control
- modify
- read-and-execute
- read
- write

[-rights-raw <Hex Integer>] - Raw Access Rights

If you specify this parameter, the command displays information only about the discretionary access control entries with the advanced user rights that you specify. This value for this parameter is mutually exclusive with any other rights values. Specify the value as a hexadecimal integer, for example: *0xA10F* or *0xb3ff* etc.

[-advanced-rights <Advanced access right>,…] - Advanced Access Rights

If you specify this parameter, the command displays information only about the discretionary access control entries with the advanced user rights that you specify. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data

- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

[-apply-to {this-folder|sub-folders|files}] - Apply DACL Entry

If you specify this parameter, the command displays information only about the discretionary access control entries with the -applied-to value or values that you specify. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

[-readable-access-rights <TextNoCase>] - Access Rights

If you specify this parameter, the command displays information only the discretionary access control entries with the readable access rights that you specify.

Examples

The following example shows information about a DACL entry.

```
cluster1::> vserver security file-directory ntfs dacl show
Vserver: vs1
                NTFS Security Descriptor Name: sd2
Account Name     Access   Access             Apply To
                                  Type     Rights
                  --------------   -------  -------            -----------
                  BUILTIN\Users    allow    full-control      this-folder,
sub-folders, files
                  CREATOR OWNER    allow    full-control      this-folder,
sub-folders, files
                  NT AUTHORITY\SYSTEM
                                   allow    full-control      this-folder,
sub-folders, files
              3 entries were displayed.
```

vserver security file-directory ntfs sacl add

Add a SACL entry to NTFS security descriptor

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs sacl add` command adds system access control list entries (ACEs) into a security descriptor's system access control list (SACL).

If the security descriptor contains a SACL that has existing security ACEs, the command adds the new security ACE to the SACL. If the security descriptor does not contain a SACL, the command creates the SACL and adds the new security ACE to it.

Adding a SACL entry to the security descriptor is the second step in configuring and applying security ACLs to a file or folder. Before you can add a SACL entry to a security descriptor, you must first create the security descriptor.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACL and SACL entries to the NTFS security descriptor.

If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding the SACL to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.
* Create policy tasks.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst

other things, the task defines which security descriptor to apply to a path.
* Apply a policy to the associated Vserver.

Parameters

-vserver <vserver name> - Vserver

Specifies the name of the Vserver associated with the security descriptor to which you want to add a system access control list entry.

-ntfs-sd <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor to which you want to add a system access control list entry.

-access-type {failure|success} - Success or Failure

Specifies whether the system access control list entry that you want to add is a *failure* or *success* access audit type.

-account <name or sid> - Account Name or SID

Specifies the account on which to apply the system access control list entry. You can specify the account by using a user name or SID. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

If you specify any of the three user name formats for the value of `-account` , keep in mind that the value for the user name is case insensitive.

{ [-rights {no-access|full-control|modify|read-and-execute|read|write}] - Access Rights

Specifies the rights that you want to get audited for the account specified in the `-account` parameter. The `-rights` parameter is mutually exclusive with the `-advanced-rights` and `-rights-raw` parameter. If you specify the `-rights` parameter, you can only specify one value.

You can specify one of the following rights values:

- no-access
- full-control
- modify
- read-and-execute
- read
- write

| [-advanced-rights <Advanced access right>,…] - Advanced Access Rights }

Specifies the advanced rights that you want to get audited for the account specified in the `-account` parameter. The `-advanced-rights` parameter is mutually exclusive with the `-rights` and `-rights -raw` parameter. You can specify more than one advanced-rights value by using a comma-delimited list.

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data
- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

| [-rights-raw <Hex Integer>] - Raw Access Rights }

Specifies the raw rights that you want to get audited for the account specified in the `-account` parameter. The `-rights-raw` parameter is mutually exclusive with the `-advanced-rights` and `-rights` parameter. Specify the value as a hexadecimal integer, for example: *`0xA10F`* or *`0xb3ff`* etc.

[-apply-to {this-folder|sub-folders|files}] - Apply SACL To

Specifies where to apply the system access control list entry. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

Select one of the following combinations of values for the `-apply-to` parameter for Storage-Level Access Guard (SLAG):

- this-folder, sub-folder, files
- this-folder, sub-folder
- files

If you specify an invalid `-apply-to` value, this security descriptor is removed from the associated Storage-Level Access Guard (SLAG) `security file-directory policy task .`

Examples

The following example adds a SACL entry to the security descriptor named “sd1” on Vserver vs1.

```
cluster1::> vserver security file-directory ntfs sacl add -ntfs-sd sd1
-access-type failure -account DOMAIN\Administrator -rights full-control
-apply-to this-folder -vserver vs1
cluster1::> vserver security file-directory ntfs sacl show -vserver vs1
-ntfs-sd sd1 -access-type deny -account DOMAIN\Administrator
Vserver: vs1
                                Security Descriptor Name: sd1
                Access type for Specified Access Rights: failure
                                    Account Name or SID:
DOMAIN\Administrator
                                           Access Rights: full-control
                                  Advanced Access Rights: -
                                               Apply To: this-folder
                                           Access Rights: full-control
```

vserver security file-directory ntfs sacl modify

Modify an NTFS security descriptor SACL entry

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs sacl modify` command modifies parameters in an existing system access control list entry.

You can unambiguously define which SACL entry to modify by specifying the following four parameters in the modify command:

- Vserver associated with the security descriptor that contains the SACL entry
- Name of the security descriptor that contains the SACL entry
- Whether the SACL is a success or failure type of SACL entry
- The account name or SID to which the SACL is applied

You can modify the following parameters:

- -rights,-advanced-rights,-rights-raw
- -apply-to

Parameters

-vserver <vserver name> - Vserver

Specifies the name of the Vserver associated with the security descriptor containing the system access control list entry whose fields you want to modify.

-ntfs-sd <ntfs sd name> - NTFS Security Descriptor Name

Specifies the name of the security descriptor that contains the system access control list entry that you want to modify.

-access-type {failure|success} - Success or Failure

Specifies whether the system access control list entry that you want to modify is a *failure* or *success* access audit type.

-account <name or sid> - Account Name or SID

Specifies the account on which to apply the system access control list entry. You can specify the account by using a user name or SID. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

If you specify any of the three user name formats for the value of `-account` , keep in mind that the value for the user name is case insensitive.

{ [-rights {no-access|full-control|modify|read-and-execute|read|write}] - Access Rights

Specifies the rights that you want to get audited for the account specified in the `-account` parameter. The `-rights` parameter is mutually exclusive with the `-advanced-rights` and `-rights-raw` parameter. If you specify the `-rights` parameter, you can only specify one value.

You can specify one of the following rights values:

- no-access
- full-control
- modify
- read-and-execute
- read
- write

| [-rights-raw <Hex Integer>] - Raw Access Rights

Specifies the raw rights that you want to get audited for the account specified in the `-account` parameter. The `-rights-raw` parameter is mutually exclusive with the `-advanced-rights` and `-rights` parameter. Specify the value as a hexadecimal integer, for example: *0xA10F* or *0xb3ff* etc.

| [-advanced-rights <Advanced access right>,…] - Advanced Access Rights }

Specifies the advanced rights that you want to get audited for the account specified in the `-account` parameter. The `-advanced-rights` parameter is mutually exclusive with the `-rights` and `-rights`

`-raw` parameter. You can specify more than one advanced-rights value by using a comma-delimited list.

You can specify one or more of the following advanced rights:

- read-data
- write-data
- append-data
- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

`[-apply-to {this-folder|sub-folders|files}]` - Apply SACL To

Specifies where to apply the system access control list entry. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

Select one of the following combinations of values for the `-apply-to` parameter for Storage-Level Access Guard (SLAG):

- this-folder, sub-folder, files
- this-folder, sub-folder
- files

If you specify an invalid `-apply-to` value, this security descriptor is removed from the associated Storage-Level Access Guard (SLAG) `security file-directory policy task`.

Examples

The following example modifies the rights and -apply-to fields in the SACL entry.

```
cluster1::> vserver security file-directory ntfs sacl modify -ntfs-sd sd2
-access-type success -account BUILTIN\Administrators -vserver vs1 -rights
modify -apply-to this-folder,sub-folders
cluster1::> vserver security file-directory ntfs sacl show -vserver vs1
-ntfs-sd sd2 -account BUILTIN\Administrators -instance
Vserver: vs1
                            Security Descriptor Name: sd2
            Access type for Specified Access Rights: success
                                Account Name or SID:
BUILTIN\Administrators
                                      Access Rights: modify
                              Advanced Access Rights: -
                                           Apply To: this-folder, sub-
folders
                                      Access Rights: modify
```

vserver security file-directory ntfs sacl remove

Remove a SACL entry from NTFS security descriptor

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs sacl remove` command removes a system access control list entry from a security descriptor.

You can unambiguously define which SACL entry to remove by specifying the following four parameters in the command:

- Vserver associated with the security descriptor that contains the SACL entry
- Name of the security descriptor that contains the SACL entry
- Whether the SACL is a success or failure type of SACL entry
- The account name or SID to which the SACL is applied

Parameters

`-vserver <vserver name>` - Vserver

Specifies the name of the Vserver associated with the security descriptor from which you want to remove the system access control list entry.

`-ntfs-sd <ntfs sd name>` - NTFS Security Descriptor Name

Specifies the name of the security descriptor that contains the system access control list entry that you want to remove.

-access-type {failure|success} - Success or Failure

Specifies whether the system access control list entry that you want to remove is a *failure* or *success* access audit type.

-account <name or sid> - Account Name or SID

Specifies the account name or SID associated with the system access control list entry that you want to remove.

Examples

The following example removes a SACL entry named “sd2” on Vserver vs1 with an access type of “success” associated with the "BUILTIN\Administrators" account.

```
cluster1::> vserver security file-directory ntfs sacl remove -ntfs-sd sd2
-access-type success -account BUILTIN\Administrators -vserver vs1
```

vserver security file-directory ntfs sacl show

Display NTFS security descriptor SACL entries

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory ntfs sacl show` command displays information about all the system access control list entries in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all SACL entries:

- Vserver name
- Security descriptor
- List of SACL entries

You can specify the `-fields` parameter to specify which fields of information to display about SACL entries.

You can specify the `-instance` parameter to display all information about SACL entries in a list format.

Parameters

{ [-fields <fieldname>,…]

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| [-instance] }

If you specify the -instance parameter, the command displays detailed information about all entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about system access control list entries associated with the specified Vserver.

[-ntfs-sd <ntfs sd name>] - NTFS Security Descriptor Name

If you specify this parameter, the command displays information only about the system access control list entries for the security descriptor that you specify.

[-access-type {failure|success}] - Success or Failure

If you specify this parameter, the command displays information only about the system access control list entries with the access type that you specify.

[-account <name or sid>] - Account Name or SID

If you specify this parameter, the command displays information only about the system access control list entries associated with the account name or SID that you specify. You can use any of the following formats when specifying the value for this parameter:

+
* SID
* Domain\user-name
* user-name@Domain
* user-name@FQDN

If you specify any of the three user name formats for the value of -account, keep in mind that the value for the user name is case insensitive.

[-rights {no-access|full-control|modify|read-and-execute|read|write}] - Access Rights

If you specify this parameter, the command displays information only about the system access control list entries with the user right that you specify. The value for this parameter is mutually exclusive with any other rights values. Only one value can be specified.

You can specify one of the following rights values:

- no-access
- full-control
- modify
- read-and-execute
- read
- write

[-rights-raw <Hex Integer>] - Raw Access Rights

If you specify this parameter, the command displays information only about the system access control list entries with the advanced user rights that you specify. This value for this parameter is mutually exclusive with any other rights values. Specify the value as a hexadecimal integer, for example: *0xA10F* or *0xb3ff* etc.

[-advanced-rights <Advanced access right>,…] - Advanced Access Rights

If you specify this parameter, the command displays information only about the system access control list entries with the advanced user rights that you specify. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following advanced rights values:

- read-data
- write-data
- append-data
- read-ea
- write-ea
- execute-file
- delete-child
- read-attr
- write-attr
- delete
- read-perm
- write-perm
- write-owner
- full-control

[-apply-to {this-folder|sub-folders|files}] - Apply SACL To

If you specify this parameter, the command displays information only about the system access control list entries with the -applied-to value or values that you specify. You can specify more than one value by using a comma-delimited list.

You can specify one or more of the following values:

- this-folder
- sub-folder
- files

[-readable-access-rights <TextNoCase>] - Access Rights

If you specify this parameter, the command displays information only about the system access control list entries with the readable access rights that you specify.

Examples

The following example shows a SACL entry.

```
cluster1::> vserver security file-directory sacl show
               (vserver security file-directory ntfs sacl show)
Vserver: vs1
                 NTFS Security Descriptor Name: sd1
Account Name     Access   Access             Apply To
                                Type     Rights
                --------------   -------  -------            -----------
                domain\user      success  full-control      this-folder,
sub-folders, files
```

vserver security file-directory policy create

Create a file security policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory policy create` command creates a security policy for a Vserver. A policy acts as a container for various tasks where each task is a single entry that can be applied to a file/folder.

Creating a security policy is the third step in configuring and applying security ACLs to a file or folder. You will later add tasks to the security policy.

> You cannot modify a security policy. If you want to apply a policy with the same settings to a different Vserver, you must create a new policy with the same configuration and apply it to the desired Vserver.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLS and SACLS to the NTFS security descriptor.

> If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding SACLs to the security descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.
* Create policy tasks.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.
* Apply a policy to the associated Vserver.

Parameters

`-vserver <vserver name>` - Vserver

Specifies the name of the Vserver on which to create the security policy.

`-policy-name <Security policy name>` - Policy Name

Specifies the name of the security policy.

Examples

The following example creates a security policy named “policy1” on Vserver vs1.

```
cluster1::> vserver security file-directory policy create -policy-name
policy1 -vserver vs1
            cluster1::> vserver security file-directory policy show
Vserver          Policy Name
               ------------     --------------
               vs1              policy1
```

vserver security file-directory policy delete

Delete a file security policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

```
The `vserver security file-directory policy delete` command deletes a
security policy from a Vserver.
```

Deleting a policy fails if a job is currently running for the specified policy.

Parameters

-vserver <vserver name> - Vserver

Specifies the name of the Vserver associated with the security policy that you want to delete.

-policy-name <Security policy name> - Policy Name

Specifies the name of the security policy you want to delete.

Examples

The following example deletes a security policy named “policy1” from Vserver vs1.

```
cluster1::> vserver security file-directory policy delete -policy-name
policy1 -vserver vs1
```

vserver security file-directory policy show

Display file security policies

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory policy show` command displays information about all security policies in the Vserver. The command output depends on the parameter or parameters specified with the command.

You can specify the `-fields` parameter to specify which fields of information to display about security policies.

You can specify the `-instance` parameter to display information for all security policies in a list format.

Parameters

{ [-fields <fieldname>,…]

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| [-instance] }

If you specify the -instance parameter, the command displays detailed information about all entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about security policies associated with the specified Vserver.

[-policy-name <Security policy name>] - Policy Name

If you specify this parameter, the command displays information only about the security policy you specify.

Examples

The following example displays information about the security policies on the cluster.

```
cluster1::> vserver security file-directory policy show
               Vserver          Policy Name
               ------------     --------------
               vs1              policy1
               vs1              policy2
             2 entries were displayed.
```

vserver security file-directory policy task add

Add a policy task

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory policy task add` command adds a single task entry to a security policy. A task refers to a single operation that can be done by a security policy to a file/folder.

Before you create a security policy task, you must first create a security policy and a security descriptor. You

should also add DACL entries and SACL entries (if desired) to the security descriptor before you create the security policy task.

> You can add DACL and SACL entries to the security descriptor after you have associated it to a security policy task.

Creating a policy task is the fourth step in configuring and applying ACLs to a file or folder. When you create the policy task, you associate a security descriptor to it. You also associate the task to a security policy.

The steps to creating and applying NTFS ACLs are the following:

- Create an NTFS security descriptor.
- Add DACLS and SACLS to the NTFS security descriptor.

> If you want to audit file and directory events, you must configure auditing on the Vserver in addition to adding SACLs to the Security Descriptor.

- Create a file/directory security policy.

This step associates the policy with a Vserver.
* Create policy tasks.

A policy task refers to a single operation to apply to a file (or folder) or to a set of files (or folders). Amongst other things, the task defines which security descriptor to apply to a path.

> Adding a policy task fails if a job is currently running for the specified policy to which a task is being added.

- Apply a policy to the associated Vserver.

Parameters

`-vserver <vserver name>` - Vserver

Specifies the Vserver associated with the security policy to which you want to add a task.

`-policy-name <Security policy name>` - Policy Name

Specifies the name of the security policy into which you want to add the task.

`-path <text>` - Path

Specifies the path of the file/folder on which to apply the security descriptor associated with this task.

`[-index-num <integer>]` - Position

Specifies the index number of a task. Tasks are applied in order. A task with a larger index value is applied after a task with a lower index number. If you do not specify this optional parameter, new tasks are applied to the end of the index list.

The range of supported values is 1 through 9999. If there is a gap between the highest existing index number and the value entered for this parameter, the task with this number is considered to be the last task in the policy and is treated as having an index number of the previous highest index plus one.

If you specify an index number that is already assigned to an existing task, index number will be auto arranged to highest index number in the table.

[-security-type {ntfs|nfsv4}] - Security Type of the File

Specifies whether the security descriptor associated with this task is an NTFS or a NFSv4 security descriptor type. If you do not specify a value for this optional parameter, the default is “ntfs”.

The nfsv4 security descriptor type is not supported in this release. If you specify this optional parameter, you must enter ntfs for the -security-type value.

[-ntfs-mode {propagate|ignore|replace}] - Propagation Mode

Specifies how to propagate security settings to child subfolders and files. This setting determines how child files and/or folders contained within a parent folder inherit access control and audit information from the parent folder.

You can specify one of the three parameter values that correspond to three types of propagation modes:

- propagate - propagate inheritable permissions to all subfolders and files
- replace - replace existing permissions on all subfolders and files with inheritable permissions
- ignore - do not allow permissions on this file or folder to be replaced

The ntfs-mode value is ignored for Storage-Level Access Guard (SLAG).

[-ntfs-sd <ntfs sd name>,…] - NTFS Security Descriptor Name

Specifies the list of security descriptor names to apply to the path specified in the `-path` parameter.

[-access-control {file-directory|slag}] - Access Control Level

Specifies the access control of the task to be applied. Valid values are *`file-directory`* or *`slag`*. Use the value *`slag`* to apply the specified security descriptors with the task for the volume or qtree. Otherwise, the security descriptors are applied on files and directories at the specified path. The value *`slag`* is not supported on FlexGroups. The default value is *`file-directory`*.

Examples

The following example adds a security policy task entry to the policy named “policy1” on Vserver vs1.

```
cluster1::> vserver security file-directory policy task add -vserver vs1
-policy-name policy1 -path / -access-control slag -security-type ntfs
-ntfs-mode propagate -ntfs-sd sd -index-num 1
cluster1::> vserver security file-directory policy task add -vserver vs1
-policy-name policy2 -path /1 -security-type ntfs -ntfs-mode propagate
-ntfs-sd sd1,sd2
              cluster1::> vserver security file-directory policy task show
Vserver: vs1
                Policy: policy1
Index  File/Folder  Access           Security  NTFS       NTFS Security
                         Path         Control          Type      Mode
Descriptor Name
                   -----  -----------  ---------------  --------
---------- ---------------
                   1      /            slag             ntfs
propagate  sd
Vserver: vs1
                Policy: policy2
Index  File/Folder  Access           Security  NTFS       NTFS Security
                         Path         Control          Type      Mode
Descriptor Name
                   -----  -----------  ---------------  --------
---------- ---------------
                   1      /1           file-directory   ntfs
propagate  sd1, sd2
```

vserver security file-directory policy task modify

Modify policy tasks

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory policy task modify` command modifies a task entry in a security policy.

> Modifying a policy task fails if a job is currently running for the specified policy in which a task is being modified.

You can unambiguously define which task to modify by specifying the following three parameters in the modify command:

- Vserver associated with the task
- Name of the security policy that contains the task

- Name of the path to which the task is applied

You can modify the following parameters:

- -ntfs-mode
- -ntfs-sd
- -index-num

> The only security type supported in this Data ONTAP release is *"ntfs"*; therefore, you cannot modify the `-security-type` parameter.

Parameters

`-vserver <vserver name>` - Vserver

Specifies the Vserver associated with the security policy that contains the task you want to modify.

`-policy-name <Security policy name>` - Policy Name

Specifies the name of the security policy that contains the task you want to modify.

`-path <text>` - Path

Specifies the path of the file/folder associated with the task that you want to modify.

`[-index-num <integer>]` - Position

Specifies the index number of a task. Tasks are applied in order. A task with a larger index value is applied after a task with a lower index number. If you do not specify this optional parameter, new tasks are applied to the end of the index list.

The range of supported values is 1 through 9999. If there is a gap between the highest existing index number and the value entered for this parameter, the task with this number is considered to be the last task in the policy and is treated as having an index number of the previous highest index plus one.

> If you specify an index number that is already assigned to an existing task, the command fails when you attempt to create a duplicate entry.

`[-security-type {ntfs|nfsv4}]` - Security Type

Specifies whether the security descriptor in the task that you want to modify should be an NTFS security descriptor type or an NFSv4 security descriptor type. Default value is *ntfs*.

> The nfsv4 security descriptor type is not supported in this release. If you specify this optional parameter, you must enter ntfs for the -security-type value.

`[-ntfs-mode {propagate|ignore|replace}]` - NTFS Propagation Mode

Specifies how to propagate security settings to child subfolders and files. This setting determines how child files and/or folders contained within a parent folder inherit access control and audit information from the parent folder.

You can specify one of the three parameter values that correspond to three types of propagation modes:

- propagate - propagate inheritable permissions to all subfolders and files

- replace - replace existing permissions on all subfolders and files with inheritable permissions
- ignore - do not allow permissions on this file or folder to be replaced

[-ntfs-sd <ntfs sd name>,…] - NTFS Security Descriptor Name

Specifies the list of security descriptor names to apply to the path specified in the `-path` parameter.

Examples

The following example modifies the ntfs mode, index, and ntfs-sd parameters in the security policy task entry.

```
cluster1::> vserver security file-directory policy task modify -vserver
vs1 -policy-name policy1 -path / -security-type ntfs -ntfs-mode propagate
-ntfs-sd sd -index-num 1
cluster1::> vserver security file-directory policy task modify -vserver
vs1 -policy-name policy1 -path /1 -security-type ntfs -ntfs-mode propagate
-ntfs-sd sd1, sd2 -index-num 2
cluster1::> vserver security file-directory policy task show -vserver vs1
-policy-name policy1
Vserver: vs1
                Policy: policy1
                 Index    File/Folder  Access          Security   NTFS
NTFS Security
                          Path         Control         Type       Mode
Descriptor Name
                 -----    --------     --------------  ------     -----
-----------------
                 1        /            file-directory  ntfs
propagate  sd
                 2        /1           file-directory  ntfs
propagate  sd1, sd2
```

vserver security file-directory policy task remove

Remove a policy task

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory policy task remove` command removes a task entry from a security policy.

Removing a policy task fails if a job is currently running for the specified policy from which a task is being removed.

Parameters

-vserver <vserver name> - Vserver

Specifies the Vserver associated with the security policy that contains the task you want to remove.

-policy-name <Security policy name> - Policy Name

Specifies the name of the security policy that contains the task you want to remove.

-path <text> - Path

Specifies the path of the file/folder associated with the task that you want to remove.

Examples

The following example removes a security policy task entry.

```
cluster1::> vserver security file-directory policy task remove -vserver
vs1 -policy-name policy1 -path /
```

vserver security file-directory policy task show

Display policy tasks

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security file-directory policy task show` command displays information about all the task entries in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all task entries:

- Vserver name
- Policy name
- Task entries

Parameters

{ [-fields <fieldname>,…]

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| [-instance] }

If you specify the -instance parameter, the command displays detailed information about all entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only tasks associated with the specified Vserver.

[-policy-name <Security policy name>] - Policy Name

If you specify this parameter, the command displays information only about tasks associated with the specified security policy.

[-index-num <integer>] - Position

If you specify this parameter, the command displays information only about tasks assigned the index number that you specify.

[-path <text>] - Path

If you specify this parameter, the command displays information only about tasks applied to the specified path.

[-security-type {ntfs|nfsv4}] - Security Type

If you specify this parameter, the command displays information only about tasks associated with the specified security type.

The nfsv4 security descriptor type is not supported in this release.

[-ntfs-mode {propagate|ignore|replace}] - NTFS Propagation Mode

If you specify this parameter, the command displays information only about tasks configured with the NTFS propagation mode that you specify.

[-ntfs-sd <ntfs sd name>,…] - NTFS Security Descriptor Name

If you specify this parameter, the command displays information only about the policy tasks associated with the NTFS security descriptor that you specify.

[-access-control {file-directory|slag}] - Access Control Level

If you specify this parameter, the command displays information only about tasks associated to the access control.

Examples

The following example displays policy task entries for a policy named “policy1” on Vserver vs1.

```
cluster1::> vserver security file-directory policy task show -vserver vs1
-policy-name policy1
Vserver: vs1
                  Policy: policy1
Index  File/Folder  Access           Security  NTFS       NTFS Security
                         Path         Control          Type      Mode
Descriptor Name
                  -----  -----------  ---------------  --------
---------- ---------------
                  1      /1           file-directory   ntfs      propagate
sd1, sd2
                  2      /2           file-directory   ntfs      ignore
-
2 entries were displayed.
```

vserver security trace filter create

Create a security trace entry

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security trace filter create` command creates a security trace filter entry. Prior to Data ONTAP 9.3, this feature was only supported for CIFS. In Data ONTAP 9.3 and later, this feature is supported for both NFS and CIFS.

NFS security trace filters are not supported for FlexGroup volumes, and will only be applied to the FlexVol volumes within the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which the permission trace is applied.

`-index <integer>` - Filter Index

This parameter specifies the index number you want to assign to the trace filter. A maximum of 10 entries can be created. The allowed values for this parameter are 1 through 10.

`[-protocols {cifs|nfs}]` - Protocols

This parameter specifies the protocols for which the permission trace is created. If the `-protocols` parameter is not specified, the filter will only apply to the CIFS protocol.

`[-client-ip <IP Address>]` - Client IP Address to Match

This parameter specifies the IP Address from which the user is accessing the Vserver.

[-path <TextNoCase>] - Path

This parameter specifies the path to which permission tracing is applied. The value can be the complete path, starting from the root of the share (for a CIFS filter) or the root of the junction path (for an NFS filter) that the client is accessing, or the value can be a part of the path that the client is accessing. Use NFS style directory separators in the path value.

{ [-windows-name <TextNoCase>] - Windows User Name

This parameter specifies the Windows user name to trace. You can use any of the following formats when specifying the value for this parameter:

- user_name
- domain\user_name

| [-unix-name <TextNoCase>] - UNIX User Name or User ID }

This parameter specifies the UNIX user name to trace. It accepts UNIX user ID only for NFS filters.

[-trace-allow {yes|no}] - Trace Allow Events

Security tracing can trace deny events and allow events. Deny event tracing is always ON by default. Allow events can optionally be traced. If set to yes, this option allows tracing of allow events. If set to no, allow events are not traced.

[-enabled {enabled|disabled}] - Filter Enabled

This parameter specifies whether to enable or disable the filter. Filters are enabled by default.

[-time-enabled <integer>] - Minutes Filter is Enabled

This parameter specifies a timeout for this filter, after which it is deleted.

Examples

The following example creates a security trace filter.

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1
-time-enabled 120 -client-ip 10.72.205.207
```

The following examples create filters that include the -path option, these filters are deleted when the time specified in the time enabled field elapses.The default value for the time-enabled option is 60 min. If the client is accessing a file with the path \\server\sharename\dir1\dir2\dir3\file.txt, for a filter applicable to CIFS, a complete path starting from the root of the share or a partial path can be given as shown:

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1
-path /dir1/dir2/dir3/file.txt
```

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1
-path dir3/file.txt
```

Similarly, while creating a filter for NFS, if -path option is specified and the client is accessing a file with path

/junction_path1/junction_path2/dir1/file.txt, a complete path starting from the last junction path or a partial path can be given as shown:

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1
-protocols nfs -path dir1/file.txt
```

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1
-protocols nfs -path file.txt
```

The following example creates a filter that is applicable to both CIFS and NFS.

```
cluster1::> vserver security trace filter create -vserver vs0 -index 1
-protocols cifs,nfs -unix-user root
```

vserver security trace filter delete

Delete a security trace entry

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security trace filter delete` command deletes a security trace filter entry. Prior to Data ONTAP 9.3, this feature was only supported for CIFS. In Data ONTAP 9.3 and later, this feature is supported for both NFS and CIFS.

NFS security trace filters are not supported for FlexGroup volumes, and will only be applied to the FlexVol volumes within the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which the tracing filter entry that you want to delete is applied.

`-index <integer>` - Filter Index

This parameter specifies the index number for the filter that you want to delete. You can display a list of the filter index numbers by using the vserver security trace filter show command.

Examples

The following example deletes a security trace filter.

```
cluster1::> vserver security trace filter delete -vserver vs0 -index 1
```

Related Links

- vserver security trace filter show

vserver security trace filter modify

Modify a security trace entry

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security trace filter modify` command modifies a security trace filter entry. Prior to Data ONTAP 9.3, this feature was only supported for CIFS. In Data ONTAP 9.3 and later, this feature is supported for both NFS and CIFS.

NFS security trace filters are not supported for FlexGroup volumes, and will only be applied to the FlexVol volumes within the specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which the permission trace is applied.

`-index <integer>` - Filter Index

This parameter specifies the index number for the filter. A maximum of 10 entries can be created. The allowed values for this parameter are 1 through 10.

`[-protocols {cifs|nfs}]` - Protocols

This parameter specifies the protocols for which the permission trace is created.

`[-client-ip <IP Address>]` - Client IP Address to Match

This parameter specifies the IP Address from which the user is accessing the Vserver.

`[-path <TextNoCase>]` - Path

This parameter specifies the path to which permission tracing is applied. The value can be the complete path, starting from the root of the share (for a CIFS filter) or the root of the junction path (for an NFS filter) that the client is accessing, or the value can be a part of the path that the client is accessing. Use NFS style directory separators in the path value.

`{ [-windows-name <TextNoCase>]` - Windows User Name

This parameter specifies the Windows user name to trace. You can use any of the following formats when specifying the value for this parameter:

- user_name
- domain\user_name

`| [-unix-name <TextNoCase>]` - UNIX User Name or User ID `}`

This parameter specifies the UNIX user name to trace. It accepts UNIX user ID only for NFS filters.

[-trace-allow {yes|no}] - Trace Allow Events

Security tracing can trace deny events and allow events. Deny event tracing is always ON by default. Allow events can optionally be traced. If set to yes, this option allows tracing of allow events. If set to no, allow events are not traced.

[-enabled {enabled|disabled}] - Filter Enabled

This parameter specifies whether to enable or disable the filter. Filters are enabled by default.

[-time-enabled <integer>] - Minutes Filter is Enabled

This parameter specifies a timeout for this filter, after which it is deleted.

Examples

The following example modifies a security trace filter.

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1
-time-enabled 120 -client-ip 10.72.205.207
```

The following examples modify filters that include the -path option. If the client is accessing a file with the path \\server\sharename\dir1\dir2\dir3\file.txt, for a filter applicable to CIFS, a complete path starting from the root of the share or a partial path can be given as shown:

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1
-path /dir1/dir2/dir3/file.txt
```

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1
-path dir3/file.txt
```

Similarly, for filters applicable to NFS, if -path option is specified and the client is accessing a file with path /junction_path1/junction_path2/dir1/file.txt, a complete path starting from the last junction path or a partial path can be given as shown:

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1
-protocols nfs -path dir1/file.txt
```

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1
-protocols nfs -path file.txt
```

The following example modifies a filter that is applicable to both CIFS and NFS.

```
cluster1::> vserver security trace filter modify -vserver vs0 -index 1
-protocols cifs,nfs -unix-user root -path file.txt
```

vserver security trace filter show

Display a security trace entry

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security trace filter show` command displays information about security trace filter entries. Prior to Data ONTAP 9.3, this feature was only supported for CIFS. In Data ONTAP 9.3 and later, this feature is supported for both NFS and CIFS.

NFS security trace filters are not supported for FlexGroup volumes, and will only be applied to the FlexVol volumes within the specified Vserver.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified Vserver.

[-index <integer>] - Filter Index

If you specify this parameter, the command displays permission tracing information only for filters with the specified filter index number.

[-protocols {cifs|nfs}] - Protocols

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified protocols.

[-client-ip <IP Address>] - Client IP Address to Match

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified client IP address.

[-path <TextNoCase>] - Path

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified path.

[-windows-name <TextNoCase>] - Windows User Name

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified Windows user name.

[-unix-name <TextNoCase>] - UNIX User Name or User ID

If you specify this parameter, the command displays permission tracing information only for filters applied to the specified UNIX user name or user ID(for NFS specififc filters).

[-trace-allow {yes|no}] - Trace Allow Events

If you specify this parameter, the command displays information only about events that either trace or do not trace allow events, depending on the value provided.

[-enabled {enabled|disabled}] - Filter Enabled

If you specify this parameter, the command displays information only about filters that either are enabled or disabled, depending on the value provided.

[-time-enabled <integer>] - Minutes Filter is Enabled

If you specify this parameter, the command displays information about the time durations configured for filters during creation.

Examples

The following example displays security trace filters for Vserver *vserver1* .

```
cluster1::> vserver security trace filter show
Vserver  Index   Client-IP     Path          Trace-Allow Windows-Name
Protocol
-------- ----- ------------ ---------------- ----------- -------------
--------
vserver1 1     -            -               no          domain\user
cifs
vserver1 2     192.168.2.3  -               yes         -
cifs
vserver1 3     -            /dir1/dir2/file  no          domain\
cifs
                                                        administrator
vserver1 4     -            file            yes         -             nfs
4 entries were displayed.
```

vserver security trace trace-result delete

Delete security trace results

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

```
Delete the specified security tracing event record.
```

Parameters

-node {<nodename>|local} - Node

This parameter specifies the cluster node on which the permission tracing event that you want to delete occurred.

-vserver <vserver name> - Vserver

This parameter specifies the Vserver on which the permission tracing event that you want to delete occurred.

-seqnum <integer> - Sequence Number

This parameter specifies the sequence number of the log entry to be deleted.

Examples

```
The following example deletes the security trace result record for the
Vserver ``_vserver_1_`` on node ``_Node_1_`` whose sequence number is
``_999_`` .
```

```
cluster1::> vserver security trace trace-result delete -vserver vserver_1
-node Node_1 -seqnum 999
```

vserver security trace trace-result show

Display security trace results

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver security trace trace-result show` command displays the list of security trace event records stored on the cluster. These records are generated in response to security trace filters that are created using the vserver security trace filter create command. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all the security trace events generated since the filter was enabled:

- Vserver name
- Cluster node name
- Security trace filter index number
- User name

- Security style
- Path
- Reason

```
You can specify additional parameters to display only information that
match those parameters. For example, to display information about events
that occurred for the user "guest", run the command with `-user-name`
parameter set to ``_guest_`` .
```

Parameters

{ [-fields <fieldname>,…]

If you specify this parameter, the command only displays the fields that you specify.

| [-instance] }

If you specify this parameter, the command displays detailed information about all security trace events.

[-node {<nodename>|local}] - Node

If you specify this parameter, the command displays information only about security trace events on the specified node.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about security trace events on the specified Vserver.

[-seqnum <integer>] - Sequence Number

If you specify this parameter, the command displays information only about the security trace events with this sequence number.

[-keytime <Date>] - Time

If you specify this parameter, the command displays information only about security trace events that occurred at the specified time.

[-index <integer>] - Index of the Filter

If you specify this parameter, the command displays information only about security trace events that occurred as a result of the filter corresponding to the specified filter index number.

[-client-ip <IP Address>] - Client IP Address

If you specify this parameter, the command displays information only about security trace events that occurred as a result of file access from the specified client IP address.

[-path <TextNoCase>] - Path of the File Being Accessed

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file accesses to the specified path.

[-win-user <TextNoCase>] - Windows User Name

If you specify this parameter, the command displays information only about the security trace events that

occurred as a result of file access by the specified Windows user.

[-security-style <security style>] - Effective Security Style On File

If you specify this parameter, the command displays information only about the security trace events that occurred on file systems with the specified security style. The allowed values for security style are the following:

- SECURITY_NONE - Security not Set
- SECURITY_UNIX_MODEBITS - UNIX and UNIX permissions
- SECURITY_UNIX_ACL - UNIX and NFSv4 ACL
- SECURITY_UNIX_SD - UNIX and NT ACL
- SECURITY_MIXED_MODEBITS - MIXED and UNIX permissions
- SECURITY_MIXED_ACL - MIXED and NFSv4 ACL
- SECURITY_MIXED_SD - MIXED and NT ACL
- SECURITY_NTFS_MODEBITS - NTFS and UNIX permissions
- SECURITY_NTFS_ACL - NTFS and NT ACL
- SECURITY_NTFS_SD - NTFS and NT ACL
- SECURITY_UNIX - UNIX
- SECURITY_MIXED - MIXED
- SECURITY_NTFS - NTFS
- SECURITY_MODEBITS - UNIX permissions
- SECURITY_ACL - ACL
- SECURITY_SD - SD

[-result <TextNoCase>] - Result of Security Checks

If you specify this parameter, the command displays information about the security trace events that have the specified result. Access to a file or a directory can be 'allowed' or 'denied'. Output from this command displays the result as a combination of the reason for allowing or denying access, the location where access is either allowed or denied, and the access right for which the file operation is allowed or denied.

The following are the reasons why an access can be allowed:

+
* Access is allowed because the operation is trusted and no security is configured
* Access is allowed because the user has UNIX root privileges
* Access is allowed because the user has UNIX owner privileges
* Access is allowed because UNIX implicit permission grants requested access
* Access is allowed because the CIFS user is owner
* Access is allowed because the user has take ownership privilege
* Access is allowed because there is no CIFS ACL
* Access is allowed because CIFS implicit permission grants requested access
* Access is allowed because the security descriptor is corrupted and the user is a member of the Administrators group
* Access is allowed because the ACL is corrupted and the user is a member of the Administrators group
* Access is allowed because the user has UNIX permissions
* Access is allowed because explicit ACE grants requested access
* Access is allowed because the user has audit privileges

* Access is allowed because the user has superuser credentials
* Access is allowed because inherited ACE grants requested access
* Access is allowed because storage-level access guard (SLAG) grants requested access
* Access is allowed because no central access policies applied
* Access is allowed because no central access policies could be applied from the corrupt SACL
* Access is allowed because matching central access policy could not be located
* Access is allowed because no central access rules apply to the object
* Access is allowed because skipped one or more corrupt central access rules
* Access is allowed because all evaluated central access rules grant access

+
The following are the reasons why an access can be denied:

+

- Access is denied by UNIX permissions
- Access is denied by an explicit ACE
- Access is denied. The requested permissions are not granted by the ACE
- Access is denied. The security descriptor is corrupted
- Access is denied. The ACL is corrupted
- Access is denied. The sticky bit is set on the parent directory and the user is not the owner of file or parent directory
- Access is denied. The owner can be changed only by root
- Access is denied. The UNIX permissions/uid/gid/NFSv4 ACL can be changed only by owner or root
- Access is denied. The GID can be set by owner to a member of its legal group list only if 'Owner can chown' is not set
- Access is denied. The file or the directory has readonly bit set
- Access is denied. There is no audit privilege
- Access is denied. Enforce DOS bits blocks the access
- Access is denied. Hidden attribute is set
- Access is denied by an inherited ACE
- Access is denied as the volume is readonly or directory is a snapshot
- Access is denied. System attribute is not set in the request
- Access is denied by the storage-level access guard (SLAG)
- Access is denied, file is infected
- Access is denied. Central access policy DB not ready
- Access is denied. Central access rule is corrupt
- Access is denied. Central access rule explicitly denied access
- Access is denied. Matching central access policy not found
- Access is denied because the user does not have UNIX root privileges
- Access is denied because the UNIX user could not be mapped to a valid NT user
- Access is denied because the UNIX permissions/uid/gid/NFSv4 ACL cannot be set in an NTFS qtree

The command or the location at which access was denied or allowed are as follows:

- while traversing the directory.
- while truncating the file.
- while creating the directory.
- while creating the file.
- while checking parent’s mode bits during delete.
- while deleting the child.
- while checking for child-delete access on the parent.
- while reading security descriptor.
- while accessing the link.
- while creating the directory.
- while creating or writing the file.
- while opening existing file or directory.
- while setting the attributes.
- while traversing the directory.
- while reading the file.
- while reading the directory.
- while deleting the target during rename.
- while deleting the child during rename.
- while writing data in the parent during rename.
- while adding a directory during rename.
- while adding a file during rename.
- while updating the target directory during rename.
- while setting attributes.
- while writing to the file.
- while extending the coral file.
- while creating the vdisk file.
- while checking for stale locks before open.
- while deleting a file or a directory.
- while truncating a hidden file.
- while truncating a file.
- while truncating a system file.
- while appending to a file or setting a file attribute.
- while opening a file or directory for delete.
- while checking for permission on parent directory during create.
- while appending to the file.
- while creating the device file.

- while reading the user's access rights on an object.

The access rights for which the file operation is allowed or denied are as follows:

+

- Append.
- Delete.
- Delete Child.
- Execute.
- Generic All.
- Generic Execute.
- Generic Read.
- Generic Write.
- Maximum Allowed.
- Read.
- Read Attributes.
- Read Control.
- Read EA.
- System Security.
- Synchronize.
- Write.
- Write Attributes.
- Write DAC.
- Write EA.
- Write Owner.
- None.

[-unix-user <TextNoCase>] - UNIX User Name

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file access by the specified UNIX user.

[-session-id <integer>] - CIFS Session ID

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file access by the specified CIFS session ID.

[-share-name <TextNoCase>] - Accessed CIFS Share Name

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file access by the specified CIFS share name.

[-protocol {cifs|nfs}] - Protocol

If you specify this parameter, the command displays information only about the security trace events that occurred for the specified protocol.

[-volume-name <TextNoCase>] - Accessed Volume Name

If you specify this parameter, the command displays information only about the security trace events that occurred as a result of file access by the specified volume name.

Examples

The following example displays information about security trace records:

```
cluster1::> vserver security trace trace-result show
Vserver: vserver_1

Node                    Index     Filter Details      Reason
----------------------- -------- ---------------------
-------------------------
cluster1-01             1        Security Style: MIXED Access is allowed
because
                                 and NT ACL            CIFS implicit
permission
                                                       grants requested
access
                                                       while opening
existing
                                                       file or directory.
                                                       Access is granted
for:
                                                       "Read Attributes"
                                 Protocol: cifs
                                 Share: sh1
                                 Path: /stk/bit
                                 Win-User: cifs1\
                                 administrator
                                 Unix-User: root
                                 Session-ID: 58455810

1 entries were displayed.
```

The following example displays information about security trace records for path /stk/bit/set:

```
cluster1::> vserver security trace trace-result show -path /stk/bit/set

Vserver: vserver_1

Node                    Index     Filter Details      Reason
----------------------- -------- ---------------------
-------------------------
```

```
cluster1-01             1       Security Style: MIXED Access is allowed
because
                                and UNIX permissions  the user has UNIX
root
                                                      privileges while
opening
                                                      existing file or
                                                      directory.
                                                      Access is granted
for: "Read"
                                Protocol: cifs
                                Share: sh1
                                Path: /stk/bit/set
                                Win-User: cifs1\
                                administrator
                                UNIX-User: root
                                Session-ID: 75435293758455810
cluster1-01             1       Security Style: MIXED Access is denied.
The
                                and NT ACL            requested
permissions
                                                      are not granted by
the
                                                      ACE while checking
for
                                                      child-delete access
on
                                                      the parent. Access
is not
                                                      granted for:
"Delete Child"
                                Protocol: cifs
                                Share: sh1
                                Path: /stk/bit/set
                                Win-User: cifs1\
                                administrator
                                UNIX-User: root
                                Session-ID: 75435293758455324
cluster1-01             1       Security Style: MIXED Access is allowed
because
                                and NT ACL            the CIFS user is
owner.
                                                      Access is denied by
an
                                                      explicit ACE while
                                                      setting the
```

```
attributes.
                                                              Access is not
granted for:
                                                              "Read Attributes"
Protocol: cifs
                                  Share: sh1
                                  Path: /stk/bit/set
                                  Win-User: cifs1\
                                  administrator
                                  UNIX-User: root
                                  Session-ID: 75435293758455324
3 entries were displayed.
```

The following example displays information about security trace records for the protocol nfs:

```
cluster1::> vserver security trace trace-result show -protocol nfs
Vserver: vserver_1

Node            Index Filter Details             Reason
--------------- ----- -------------------------
------------------------------
cluster1-01     2     Security Style: UNIX       Access is allowed because
the
                      permissions                user has UNIX root
privileges
                                                 while setting attributes.
                      Protocol: nfs
                      Volume: testvol_flex
                      Share: -
                      Path: /f1
                      Win-User: -
                      UNIX-User: root
                      Session-ID: -
cluster1-01     2     Security Style: UNIX       Access is allowed because
the
                      permissions                user has UNIX root
privileges
                                                 while writing to the
file.
                                                 Access is granted for:
"Write"
                      Protocol: nfs
                      Volume: testvol_flex
                      Share: -
                      Path: /f1
```

```
                     Win-User: -
                     UNIX-User: root
                     Session-ID: -
cluster1-01     3    Security Style: UNIX       Access is denied by UNIX
                     permissions                permissions while
creating
                                                the file. Access is not
                                                granted for:
"Synchronize",
                                                "Read Control", "Read
                                                Attributes", "Execute",
                                                "Write"
                     Protocol: nfs
                     Volume: testvol_flex
                     Share: -
                     Path: /d1/file
                     Win-User: -
                     UNIX-User: 1029
                     Session-ID: -
3 entries were displayed.
```

Related Links

- vserver security trace filter create