



Secure file access by using Storage-Level Access Guard

ONTAP 9

NetApp
June 12, 2023

Table of Contents

- Secure file access by using Storage-Level Access Guard 1
 - Secure file access by using Storage-Level Access Guard 1
 - Use cases for using Storage-Level Access Guard 2
 - Workflow to configure Storage-Level Access Guard 2
 - Configure Storage-Level Access Guard 4
 - Effective SLAG matrix 10
 - Display information about Storage-Level Access Guard 10
 - Remove Storage-Level Access Guard 13

Secure file access by using Storage-Level Access Guard

Secure file access by using Storage-Level Access Guard

In addition to securing access by using native file-level and export and share security, you can configure Storage-Level Access Guard, a third layer of security applied by ONTAP at the volume level. Storage-Level Access Guard applies to access from all NAS protocols to the storage object to which it is applied.

Only NTFS access permissions are supported. For ONTAP to perform security checks on UNIX users for access to data on volumes for which Storage-Level Access Guard has been applied, the UNIX user must map to a Windows user on the SVM that owns the volume.

Storage-Level Access Guard behavior

- Storage-Level Access Guard applies to all the files or all the directories in a storage object.

Because all files or directories in a volume are subject to Storage-Level Access Guard settings, inheritance through propagation is not required.

- You can configure Storage-Level Access Guard to apply to files only, to directories only, or to both files and directories within a volume.

- File and directory security

Applies to every directory and file within the storage object. This is the default setting.

- File security

Applies to every file within the storage object. Applying this security does not affect access to, or auditing of, directories.

- Directory security

Applies to every directory within the storage object. Applying this security does not affect access to, or auditing of, files.

- Storage-Level Access Guard is used to restrict permissions.

It will never give extra access permissions.

- If you view the security settings on a file or directory from an NFS or SMB client, you do not see the Storage-Level Access Guard security.

It's applied at the storage object level and stored in the metadata used to determine the effective permissions.

- Storage-level security cannot be revoked from a client, even by a system (Windows or UNIX) administrator.

It is designed to be modified by storage administrators only.

- You can apply Storage-Level Access Guard to volumes with NTFS or mixed security style.
- You can apply Storage-Level Access Guard to volumes with UNIX security style as long as the SVM containing the volume has a CIFS server configured.
- When volumes are mounted under a volume junction path and if Storage-Level Access Guard is present on that path, it will not be propagated to volumes mounted under it.
- The Storage-Level Access Guard security descriptor is replicated with SnapMirror data replication and with SVM replication.
- There is special dispensation for virus scanners.

Exceptional access is allowed to these servers to screen files and directories, even if Storage-Level Access Guard denies access to the object.

- FPolicy notifications are not sent if access is denied because of Storage-Level Access Guard.

Order of access checks

Access to a file or directory is determined by the combined effect of the export or share permissions, the Storage-Level Access Guard permissions set on volumes, and the native file permissions applied to files and/or directories. All levels of security are evaluated to determine what the effective permissions a file or directory has. The security access checks are performed in the following order:

1. SMB share or NFS export-level permissions
2. Storage-Level Access Guard
3. NTFS file/folder access control lists (ACLs), NFSv4 ACLs, or UNIX mode bits

Use cases for using Storage-Level Access Guard

Storage-Level Access Guard provides additional security at the storage level, which is not visible from a client side; therefore, it cannot be revoked by any of the users or administrators from their desktops. There are certain use cases where the ability to control access at the storage level is beneficial.

Typical use cases for this feature include the following scenarios:

- Intellectual property protection by auditing and controlling all users' access at the storage level
- Storage for financial services companies, including banking and trading groups
- Government services with separate file storage for individual departments
- Universities protecting all student files

Workflow to configure Storage-Level Access Guard

The workflow to configure Storage-Level Access Guard (SLAG) uses the same ONTAP CLI commands that you use to configure NTFS file permissions and auditing policies. Instead of configuring file and directory access on a designated target, you configure SLAG on the designated storage virtual machine (SVM) volume.



Related information

[Configuring Storage-Level Access Guard](#)

Configure Storage-Level Access Guard

There are a number of steps you need to follow to configure Storage-Level Access Guard on a volume or qtree. Storage-Level Access Guard provides a level of access security that is set at the storage level. It provides security that applies to all accesses from all NAS protocols to the storage object to which it has been applied.

Steps

1. Create a security descriptor by using the `vserver security file-directory ntfs create` command.

```
vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver
security file-directory ntfs show -vserver vs1
```

Vserver: vs1

NTFS Security Descriptor Name	Owner Name
-----	-----
sd1	-

A security descriptor is created with the following four default DACL access control entries (ACEs):

Vserver: vs1

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
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

If you do not want to use the default entries when configuring Storage-Level Access Guard, you can remove them prior to creating and adding your own ACEs to the security descriptor.

2. Remove any of the default DACL ACEs from the security descriptor that you do not want configured with Storage-Level Access Guard security:

- a. Remove any unwanted DACL ACEs by using the `vserver security file-directory ntfs dacl remove` command.

In this example, three default DACL ACEs are removed from the security descriptor:
`BUILTIN\Administrators`, `BUILTIN\Users`, and `CREATOR OWNER`.

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. Verify that the DACL ACEs you do not want to use for Storage-Level Access Guard security are removed from the security descriptor by using the `vserver security file-directory ntfs dacl show` command.

In this example, the output from the command verifies that three default DACL ACEs have been removed from the security descriptor, leaving only the `NT AUTHORITY\SYSTEM` default DACL ACE entry:

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access      Access      Apply To
                  Type       Rights
-----
NT AUTHORITY\SYSTEM
                  allow      full-control this-folder, sub-
folders, files
```

3. Add one or more DACL entries to a security descriptor by using the `vserver security file-directory ntfs dacl add` command.

In this example, two DACL ACEs are added to the security descriptor:

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. Add one or more SACL entries to a security descriptor by using the `vserver security file-directory ntfs sacl add` command.

In this example, two SACL ACEs are added to the security descriptor:

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
```

```
this-folder,sub-folders,files vserver security file-directory ntfs sac1 add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verify that the DACL and SACL ACEs are configured correctly by using the `vserver security file-directory ntfs dacl show` and `vserver security file-directory ntfs sac1 show` commands, respectively.

In this example, the following command displays information about DACL entries for security descriptor “sd1”:

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

Vserver: vs1

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
EXAMPLE\Domain Users	allow	read	this-folder, sub-folders, files
EXAMPLE\engineering	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

In this example, the following command displays information about SACL entries for security descriptor “sd1”:

```
vserver security file-directory ntfs sac1 show -vserver vs1 -ntfs-sd sd1
```

Vserver: vs1

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
EXAMPLE\Domain Users	failure	read	this-folder, sub-folders, files
EXAMPLE\engineering	success	full-control	this-folder, sub-folders, files

6. Create a security policy by using the `vserver security file-directory policy create` command.

The following example creates a policy named “policy1”:

```
vserver security file-directory policy create -vserver vs1 -policy-name policy1
```

7. Verify that the policy is correctly configured by using the `vserver security file-directory policy show` command.

```
vserver security file-directory policy show
```

Vserver	Policy Name
vs1	policy1

8. Add a task with an associated security descriptor to the security policy by using the `vserver security file-directory policy-task add` command with the `-access-control` parameter set to `slag`.

Even though a policy can contain more than one Storage-Level Access Guard task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

In this example, a task is added to the policy named “policy1”, which is assigned to security descriptor “sd1”. It is assigned to the `/datavol1` path with the access control type set to “slag”.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1
```

9. Verify that the task is configured correctly by using the `vserver security file-directory policy task show` command.

```
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	/datavol1	slag	ntfs	propagate	sd1

10. Apply the Storage-Level Access Guard security policy by using the `vserver security file-directory apply` command.

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

The job to apply the security policy is scheduled.

11. Verify that the applied Storage-Level Access Guard security settings are correct by using the `vserver security file-directory show` command.

In this example, the output from the command shows that Storage-Level Access Guard security has been applied to the NTFS volume `/datavol1`. Even though the default DACL allowing Full Control to Everyone remains, Storage-Level Access Guard security restricts (and audits) access to the groups defined in the Storage-Level Access Guard settings.

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```

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

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

```

Related information

[Managing NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI](#)

[Workflow to configure Storage-Level Access Guard](#)

[Displaying information about Storage-Level Access Guard](#)

[Removing Storage-Level Access Guard](#)

Effective SLAG matrix

You can configure SLAG on a volume or a qtree or both. The SLAG matrix defines on which volume or qtree is the SLAG configuration applicable under various scenarios listed in the table.

	Volume SLAG in an AFS	Volume SLAG in a Snapshot copy	Qtree SLAG in an AFS	Qtree SLAG in a Snapshot copy
Volume access in an Access File System (AFS)	YES	NO	N/A	N/A
Volume access in a Snapshot copy	YES	NO	N/A	N/A
Qtree access in an AFS (when SLAG is present in the qtree)	NO	NO	YES	NO
Qtree access in an AFS (when SLAG is not present in qtree)	YES	NO	NO	NO
Qtree access in Snapshot copy (when SLAG is present in the qtree AFS)	NO	NO	YES	NO
Qtree access in Snapshot copy (when SLAG is not present in the qtree AFS)	YES	NO	NO	NO

Display information about Storage-Level Access Guard

Storage-Level Access Guard is a third layer of security applied on a volume or qtree. Storage-Level Access Guard settings cannot be viewed by using the Windows Properties window. You must use the ONTAP CLI to view information about Storage-Level Access Guard security, which you can use to validate your configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the volume or qtree whose Storage-Level Access Guard security information you want to display. You can display the output in summary form or as a detailed list.

Step

1. Display Storage-Level Access Guard security settings with the desired level of detail:

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

Examples

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

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

```

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

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

The following example displays the Storage-Level Access Guard information about the mixed security-style volume at the path /datavol15 in SVM vs1. The top level of this volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Remove Storage-Level Access Guard

You can remove Storage-Level Access Guard on a volume or qtree if you no longer want set access security at the storage level. Removing Storage-Level Access Guard does not modify or remove regular NTFS file and directory security.

Steps

1. Verify that the volume or qtree has Storage-Level Access Guard configured by using the `vserver security file-directory show` command.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

        Vserver: vs1
        File Path: /datavol2
    File Inode Number: 99
        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:0xbf14
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            SACL - ACEs
                AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
            DACL - ACEs
                ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

        Storage-Level Access Guard security
        DACL (Applies to Directories):
            ALLOW-BUILTIN\Administrators-0x1f01ff
            ALLOW-CREATOR OWNER-0x1f01ff
            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
        DACL (Applies to Files):
            ALLOW-BUILTIN\Administrators-0x1f01ff
            ALLOW-CREATOR OWNER-0x1f01ff
            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. Remove Storage-Level Access Guard by using the `vserver security file-directory remove-slag` command.

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. Verify that Storage-Level Access Guard has been removed from the volume or qtree by using the `vserver security file-directory show` command.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```



```
Vserver: vs1
File Path: /datavol2
File Inode Number: 99
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:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
    AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
    ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
    ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.