



Secure file access by using Dynamic Access Control (DAC)

ONTAP 9

NetApp
November 19, 2022

This PDF was generated from <https://docs.netapp.com/us-en/ontap/smb-admin/secure-file-access-dynamic-access-control-concept.html> on November 19, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Secure file access by using Dynamic Access Control (DAC)..... 1
 - Secure file access by using Dynamic Access Control (DAC) overview 1
 - Supported Dynamic Access Control functionality..... 2
 - Considerations when using Dynamic Access Control and central access policies with CIFS servers 3
 - Enable or disable Dynamic Access Control overview 4
 - Manage ACLs that contain Dynamic Access Control ACEs when Dynamic Access Control is disabled 4
 - Configure central access policies to secure data on CIFS servers 5
 - Display information about Dynamic Access Control security 8
 - Revert considerations for Dynamic Access Control 10
 - Where to find additional information about configuring and using Dynamic Access Control and central access policies 10

Secure file access by using Dynamic Access Control (DAC)

Secure file access by using Dynamic Access Control (DAC) overview

You can secure access by using Dynamic Access Control and by creating central access policies in Active Directory and applying them to files and folders on SVMs through applied Group Policy Objects (GPOs). You can configure auditing to use central access policy staging events to see the effects of changes to central access policies before you apply them.

Additions to CIFS credentials

Before Dynamic Access Control, a CIFS credential included a security principal's (the user's) identity and Windows group membership. With Dynamic Access Control, three more types of information are added to the credential—device identity, device claims, and user claims:

- Device identity

The analog of the user's identity information, except it is the identity and group membership of the device that the user is logging in from.

- Device claims

Assertions about a device security principal. For example, a device claim might be that it is a member of a specific OU.

- User claims

Assertions about a user security principal. For example, a user claim might be that their AD account is a member of a specific OU.

Central access policies

Central access policies for files enable organizations to centrally deploy and manage authorization policies that include conditional expressions using user groups, user claims, device claims, and resource properties.

For example, for accessing high business impact data, a user needs to be a full time employee and only have access to the data from a managed device. Central access policies are defined in Active Directory and distributed to file servers via the GPO mechanism.

Central access policy staging with advanced auditing

Central access policies can be “staged”, in which case they are evaluated in a “what-if” manner during file access checks. The results of what would have happened if the policy was in effect and how that differs from what is currently configured are logged as an audit event. In this way, administrators can use audit event logs to study the impact of an access policy change before actually putting the policy in play. After evaluating the impact of an access policy change, the policy can be deployed via GPOs to the desired SVMs.

Related information

[Supported GPOs](#)

[Applying Group Policy Objects to CIFS servers](#)

[Enabling or disabling GPO support on a CIFS server](#)

[Displaying information about GPO configurations](#)

[Displaying information about central access policies](#)

[Displaying information about central access policy rules](#)

[Configuring central access policies to secure data on CIFS servers](#)

[Displaying information about Dynamic Access Control security](#)

[SMB and NFS auditing and security tracing](#)

Supported Dynamic Access Control functionality

If you want to use Dynamic Access Control (DAC) on your CIFS server, you need to understand how ONTAP supports Dynamic Access Control functionality in Active Directory environments.

Supported for Dynamic Access Control

ONTAP supports the following functionality when Dynamic Access Control is enabled on the CIFS server:

Functionality	Comments
Claims into the file system	Claims are simple name and value pairs that state some truth about a user. User credentials now contain claim information, and security descriptors on files can perform access checks that include claims checks. This gives administrators a finer level of control over who can access files.
Conditional expressions to file access checks	When modifying the security parameters of a file, users can now add arbitrarily complex conditional expressions to the file's security descriptor. The conditional expression can include checks for claims.
Central control of file access via central access policies	Central access policies are a kind of ACL stored in Active Directory that can be tagged to a file. Access to the file is only granted if the access checks of both the security descriptor on disk and the tagged central access policy allows access. This gives administrators the ability to control access to files from a central location (AD) without having to modify the security descriptor on disk.

Functionality	Comments
Central access policy staging	Adds the ability to try out security changes without affecting actual file access, by “staging” a change to the central access policies, and seeing the effect of the change in an audit report.
Support for displaying information about central access policy security by using the ONTAP CLI	Extends the <code>vserver security file-directory show</code> command to display information about applied central access policies.
Security tracing that includes central access policies	Extends the <code>vserver security trace</code> command family to display results that include information about applied central access policies.

Unsupported for Dynamic Access Control

ONTAP does not support the following functionality when Dynamic Access Control is enabled on the CIFS server:

Functionality	Comments
Automatic classification of NTFS file system objects	This is an extension to the Windows File Classification Infrastructure that is not supported in ONTAP.
Advanced auditing other than central access policy staging	Only central access policy staging is supported for advanced auditing.

Considerations when using Dynamic Access Control and central access policies with CIFS servers

There are certain considerations you must keep in mind when using Dynamic Access Control (DAC) and central access policies to secure files and folders on CIFS servers.

NFS access can be denied to root if policy rule applies to domain\administrator user

Under certain circumstances, NFS access to root might be denied when central access policy security is applied to the data that the root user is attempting to access. The issue occurs when the central access policy contains a rule that is applied to the domain\administrator and the root account is mapped to the domain\administrator account.

Instead of applying a rule to the domain\administrator user, you should apply the rule to a group with administrative privileges, such as the domain\administrators group. In this way, you can map root to the domain\administrator account without root being impacted by this issue.

CIFS server’s BUILTIN\Administrators group has access to resources when the applied central access policy is not found in Active Directory

It is possible that resources contained within the CIFS server have central access policies applied to them, but when the CIFS server uses the central access policy’s SID to attempt to retrieve information from Active Directory, the SID does not match any existing central access policy SIDs in Active Directory. Under these circumstances, the CIFS server applies the local default recovery policy for that resource.

The local default recovery policy allows the CIFS server’s BUILTIN\Administrators group access to that resource.

Enable or disable Dynamic Access Control overview

The option that enables you to use Dynamic Access Control (DAC) to secure objects on your CIFS server is disabled by default. You must enable the option if you want to use Dynamic Access Control on your CIFS server. If you later decide that you do not want to use Dynamic Access Control to secure objects stored on the CIFS server, you can disable the option.

About this task

Once Dynamic Access Control is enabled, the file system can contain ACLs with Dynamic Access Control-related entries. If Dynamic Access Control is disabled, the current Dynamic Access Control entries will be ignored, and new ones will not be allowed.

This option is available only at the advanced privilege level.

Step

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

If you want Dynamic Access Control to be...	Enter the command...
Enabled	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</code>
Disabled	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</code>

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

Related information

[Configuring central access policies to secure data on CIFS servers](#)

Manage ACLs that contain Dynamic Access Control ACEs when Dynamic Access Control is disabled

If you have resources that have ACLs applied with Dynamic Access Control ACEs and you disable Dynamic Access Control on the storage virtual machine (SVM), you must

remove the Dynamic Access Control ACEs before you can manage the non-Dynamic Access Control ACEs on that resource.

About this task

After Dynamic Access Control is disabled, you cannot remove existing non-Dynamic Access Control ACEs or add new non-Dynamic Access Control ACEs until you have removed the existing Dynamic Access Control ACEs.

You can use whichever tool you normally use to manage ACLs to perform these steps.

Steps

1. Determine what Dynamic Access Control ACEs are applied to the resource.
2. Remove the Dynamic Access Control ACEs from the resource.
3. Add or remove non-Dynamic Access Control ACEs as desired from the resource.

Configure central access policies to secure data on CIFS servers

There are several steps that you must take to secure access to data on the CIFS server using central access policies, including enabling Dynamic Access Control (DAC) on the CIFS server, configuring central access policies in Active Directory, applying the central access policies to Active Directory containers with GPOs, and enabling GPOs on the CIFS server.

Before you begin

- The Active Directory must be configured to use central access policies.
- You must have sufficient access on the Active Directory domain controllers to create central access policies and to create and apply GPOs to the containers that contain the CIFS servers.
- You must have sufficient administrative access on the storage virtual machine (SVM) to execute the necessary commands.

About this task

Central access policies are defined and applied to group policy objects (GPOs) on Active Directory. You can consult the Microsoft TechNet Library for instructions about configuring central access policies and GPOs.

[Microsoft TechNet Library](#)

Steps

1. Enable Dynamic Access Control on the SVM if it is not already enabled by using the `vserver cifs options modify` command.

```
vserver cifs options modify -vserver vs1 -is-dac-enabled true
```

2. Enable group policy objects (GPOs) on the CIFS server if they are not already enabled by using the `vserver cifs group-policy modify` command.

```
vserver cifs group-policy modify -vserver vs1 -status enabled
```

3. Create central access rules and central access policies on Active Directory.
4. Create a group policy object (GPO) to deploy the central access policies on Active Directory.
5. Apply the GPO to the container where the CIFS server computer account is located.
6. Manually update the GPOs applied to the CIFS server by using the `vserver cifs group-policy update` command.

```
vserver cifs group-policy update -vserver vs1
```

7. Verify that the GPO central access policy is applied to the resources on the CIFS server by using the `vserver cifs group-policy show-applied` command.

The following example shows that the Default Domain Policy has two central access policies that are applied to the CIFS server:

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
-----
GPO Name: Default Domain Policy
  Level: Domain
  Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
```


Registry Values:
 Signing Required: false
Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2

GPO Name: Resultant Set of Policy
 Level: RSOP
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: all-versions
Security Settings:
 Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
File Security:
 /vol1/home
 /vol1/dir1
Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
Registry Values:
 Signing Required: false
Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false

```
Restrict anonymous access to shares and named pipes: true
Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2
2 entries were displayed.
```

Related information

[Displaying information about GPO configurations](#)

[Displaying information about central access policies](#)

[Displaying information about central access policy rules](#)

[Enabling or disabling Dynamic Access Control](#)

Display information about Dynamic Access Control security

You can display information about Dynamic Access Control (DAC) security on NTFS volumes and on data with NTFS effective security on mixed security-style volumes. This includes information about conditional ACEs, resource ACEs, and central access policy ACEs. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

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

Step

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

If you want to display information...	Enter the following command...
In summary form	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
With expanded detail	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>
Where output is displayed with group and user SIDs	<pre>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</pre>

If you want to display information...	Enter the following command...
About file and directory security for files and directories where the hexadecimal bit mask is translated to textual format	<code>vserver security file-directory show -vserver vserver_name -path path -textual-mask true</code>

Examples

The following example displays Dynamic Access Control security information about the path `/vol1` in SVM `vs1`:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
      Vserver: vs1
      File Path: /vol1
      File Inode Number: 112
      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\user1-0x1200a9-
      OI|CI

      ((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
      evice.department==@Resource.Department_MS)
```

Related information

[Displaying information about GPO configurations](#)

[Displaying information about central access policies](#)

[Displaying information about central access policy rules](#)

Revert considerations for Dynamic Access Control

You should be aware of what happens when reverting to a version of ONTAP that does not support Dynamic Access Control (DAC) and what you must do before and after reverting.

If you want to revert the cluster to a version of ONTAP that does not support Dynamic Access Control and Dynamic Access Control is enabled on one or more the storage virtual machines (SVMs), you must do the following before reverting:

- You must disable Dynamic Access Control on all SVMs that have it enabled on the cluster.
- You must modify any auditing configurations on the cluster that contain the `cap-staging` event type to use only the `file-op` event type.

You must understand and act on some important revert considerations for files and folders with Dynamic Access Control ACEs:

- If the cluster is reverted, existing Dynamic Access Control ACEs are not removed; however, they will be ignored in file access checks.
- Since Dynamic Access Control ACEs are ignored after reversion, access to files will change on files with Dynamic Access Control ACEs.

This could allow users to access files they previously could not, or not be able to access files that they previously could.

- You should apply non-Dynamic Access Control ACEs to the affected files to restore their previous level of security.

This can be done either before reverting or immediately after reversion completes.



Since Dynamic Access Control ACEs are ignored after reversion, it is not required that you remove them when applying non-Dynamic Access Control ACEs to the affected files. However, if desired, you can manually remove them.

Where to find additional information about configuring and using Dynamic Access Control and central access policies

Additional resources are available to help you configure and use Dynamic Access Control and central access policies.

You can find information about how to configure Dynamic Access Control and central access policies on Active Directory in the Microsoft TechNet Library.

[Microsoft TechNet: Dynamic Access Control Scenario Overview](#)

The following references can help you configure the SMB server to use and support Dynamic Access Control and central access policies:

- **Using GPOs on the SMB server**

[Applying Group Policy Objects to SMB servers](#)

- **Configuring NAS auditing on the SMB server**

[SMB and NFS auditing and security tracing](#)

Copyright information

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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.