使用动态访问控制（DAC）确保文件访问安全

ONTAP 9

NetApp
September 12, 2024

目录

使用动态访问控制（DAC）确保文件访问安全

使用动态访问控制（DAC）概述确保文件访问安全

您可以使用动态访问控制来保护访问安全，也可以在 Active Directory 中创建中央访问策略，并通过已应用的组策略对象（GPO）将这些策略应用于 SVM 上的文件和文件夹。您可以配置审核，以便在应用对中央访问策略所做的更改之前，使用中央访问策略暂存事件查看这些更改的影响。

CIFS 凭据的附加项

在动态访问控制之前， CIFS 凭据包括安全主体（用户）的身份和 Windows 组成员资格。通过动态访问控制，凭据中又添加了三种类型的信息：设备标识，设备声明和用户声明：

- 设备标识

  模拟用户的身份信息，但用户登录设备的身份和组成员资格除外。

- 设备声明

  有关设备安全主体的断言。例如，设备声明可能是它是特定 OU 的成员。

- 用户声明

  有关用户安全主体的断言。例如，用户声明可能是其 AD 帐户是特定 OU 的成员。

中央访问策略

通过文件的中央访问策略，组织可以使用用户组，用户声明，设备声明和资源属性集中部署和管理包括条件表达式在内的授权策略。

例如，要访问对业务影响较高的数据，用户必须是全职员工，并且只能从受管设备访问数据。中央访问策略在 Active Directory 中定义，并通过 GPO 机制分发到文件服务器。

具有高级审核功能的中央访问策略暂存

中央访问策略可以是 " `stated` " ，在这种情况下，在文件访问检查期间会以 "`what - if` " 的方式对其进行评估。如果策略有效，会发生什么情况以及这与当前配置有何不同，则会将结果记录为审核事件。通过这种方式，管理员可以使用审核事件日志来研究访问策略更改的影响，然后再实际应用该策略。在评估访问策略更改的影响后，可以通过 GPO 将此策略部署到所需的 SVM 。

相关信息

支持的 GPO

将组策略对象应用于 CIFS 服务器

在 CIFS 服务器上启用或禁用 GPO 支持

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

显示有关中央访问策略规则的信息

配置中央访问策略以保护 CIFS 服务器上的数据安全

显示有关动态访问控制安全性的信息

"SMB 和 NFS 审核和安全跟踪"

支持的动态访问控制功能

如果要在 CIFS 服务器上使用动态访问控制（DAC），则需要了解 ONTAP 如何在 Active Directory 环境中支持动态访问控制功能。

支持动态访问控制

在 CIFS 服务器上启用动态访问控制时， ONTAP 支持以下功能：

功能	注释
声明到文件系统	声明是简单的名称和值对，用于说明有关用户的一些事实。用户凭据包含声明信息、文件上的安全描述符可以执行包括声明检查在内的访问检查。这样，管理员可以更精细地控制谁可以访问文件。
文件访问检查的条件表达式	修改文件的安全参数时、用户可以将任意复杂的条件表达式添加到文件的安全描述符中。条件表达式可以包括对声明的检查。
通过中央访问策略集中控制文件访问	中央访问策略是存储在 Active Directory 中的一种 ACL，可以标记为文件。只有在磁盘上的安全描述符和带标记的中央访问策略的访问检查均允许访问时，才会授予对文件的访问权限。这样，管理员便可以从中央位置（AD）控制对文件的访问，而无需修改磁盘上的安全描述符。
中央访问策略暂存	增加了在不影响实际文件访问的情况下尝试安全更改的功能，方法是 " `staging` " 对中央访问策略的更改，并在审核报告中查看更改的影响。
支持使用 ONTAP 命令行界面显示有关中央访问策略安全性的信息	扩展 `vserver security file-directory show` 命令以显示有关应用的中央访问策略的信息。
包括中央访问策略的安全跟踪	扩展 `vserver security trace` 命令系列、以显示包含应用的中央访问策略相关信息的结果。

不支持动态访问控制

在 CIFS 服务器上启用动态访问控制时， ONTAP 不支持以下功能：

功能	注释
NTFS 文件系统对象的自动分类	这是 ONTAP 不支持的 Windows 文件分类基础架构的扩展。
除中央访问策略暂存之外的高级审核	高级审核仅支持中央访问策略暂存。

对 **CIFS** 服务器使用动态访问控制和中央访问策略时的注意事项

在使用动态访问控制（ DAC ）和中央访问策略保护 CIFS 服务器上的文件和文件夹时，必须牢记一些注意事项。

如果策略规则为适用场景 **domain\administrator user** ，则可以拒绝对 **root** 的 **NFS** 访问

在某些情况下，如果对 root 用户尝试访问的数据应用中央访问策略安全性，则可能会拒绝 NFS 对 root 的访问。如果中央访问策略包含应用于域 \ 管理员且根帐户映射到域 \ 管理员帐户的规则，则会发生问题描述。

您应将规则应用于具有管理权限的组，例如 domain\administrator 组，而不是将规则应用于 domain\administrator 用户。通过这种方式，您可以将 root 映射到域 \ 管理员帐户，而不会使 root 受到此问题描述的影响。

如果在**Active Directory**中找不到应用的中央访问策略、则**CIFS**服务器的**BUILTIN\Administrators**组可以访问资源

CIFS 服务器中包含的资源可能已应用中央访问策略，但当 CIFS 服务器使用中央访问策略的 SID 尝试从 Active Directory 检索信息时， SID 与 Active Directory 中的任何现有中央访问策略 SID 不匹配。在这些情况下， CIFS 服务器会对该资源应用本地默认恢复策略。

本地默认恢复策略允许 CIFS 服务器的 BUILTIN\Administrators 组访问该资源。

启用或禁用动态访问控制概述

默认情况下，用于使用动态访问控制（ DAC ）保护 CIFS 服务器上的对象的选项处于禁用状态。如果要在 CIFS 服务器上使用动态访问控制，则必须启用此选项。如果您稍后决定不使用动态访问控制来保护存储在 CIFS 服务器上的对象，则可以禁用此选项。

关于此任务

启用动态访问控制后，文件系统可以包含具有与动态访问控制相关的条目的 ACL 。如果禁用了动态访问控制，则会忽略当前的动态访问控制条目，并且不允许输入新条目。

此选项仅在高级权限级别可用。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

动态访问控制的目标位置	输入命令 ...
enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. 返回到管理员权限级别： `set -privilege admin`

相关信息

配置中央访问策略以保护 CIFS 服务器上的数据安全

禁用动态访问控制时，管理包含动态访问控制 ACE 的 ACL

如果您的资源使用动态访问控制 ACE 应用 ACL ，并且您在 Storage Virtual Machine （ SVM ）上禁用了动态访问控制，则必须先删除动态访问控制 ACE ，然后才能管理该资源上的非动态访问控制 ACE 。

关于此任务

禁用动态访问控制后，在删除现有动态访问控制 ACE 之前，您无法删除现有的非动态访问控制 ACE 或添加新的非动态访问控制 ACE 。

您可以使用通常用于管理 ACL 的任何工具来执行这些步骤。

步骤

1. 确定对资源应用了哪些动态访问控制 ACE 。
2. 从资源中删除动态访问控制 ACE 。
3. 根据需要在资源中添加或删除非动态访问控制 ACE 。

配置中央访问策略以保护 CIFS 服务器上的数据安全

要使用中央访问策略保护对 CIFS 服务器上数据的访问，您必须执行几个步骤，包括在 CIFS 服务器上启用动态访问控制（ DAC ），在 Active Directory 中配置中央访问策略，将中央访问策略应用于具有 GPO 的 Active Directory 容器， 并在 CIFS 服务器上启用 GPO 。

开始之前

- 必须将 Active Directory 配置为使用中央访问策略。
- 您必须对 Active Directory 域控制器具有足够的访问权限，才能创建中央访问策略，并创建 GPO 并将其应用于包含 CIFS 服务器的容器。

- 您必须对 Storage Virtual Machine （ SVM ）具有足够的管理访问权限才能执行必要的命令。

关于此任务

中央访问策略已定义并应用于 Active Directory 上的组策略对象（ GPO ）。有关配置中央访问策略和 GPO 的说明，请参见 Microsoft TechNet 库。

"Microsoft TechNet 库"

步骤

1. 如果尚未使用启用动态访问控制、请在SVM上启用它 `vserver cifs options modify` 命令：

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

2. 如果尚未使用启用组策略对象(GPO)、请在CIFS服务器上启用它们 `vserver cifs group-policy modify` 命令：

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

3. 在 Active Directory 上创建中央访问规则和中央访问策略。
4. 创建组策略对象（ GPO ）以在 Active Directory 上部署中央访问策略。
5. 将 GPO 应用于 CIFS 服务器计算机帐户所在的容器。
6. 使用手动更新应用于CIFS服务器的GPO `vserver cifs group-policy update` 命令：

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

7. 使用验证是否已将GPO中央访问策略应用于CIFS服务器上的资源 `vserver cifs group-policy show-applied` 命令：

   以下示例显示默认域策略具有两个应用于 CIFS 服务器的中央访问策略：

   ```
   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.
```

相关信息

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

显示有关中央访问策略规则的信息

启用或禁用动态访问控制

显示有关动态访问控制安全性的信息

您可以显示 NTFS 卷上的动态访问控制（DAC）安全性信息，以及混合安全模式卷上使用 NTFS 有效安全性的数据信息。其中包括有关条件 ACE，资源 ACE 和中央访问策略 ACE 的信息。您可以使用结果验证安全配置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （SVM）的名称以及要显示其文件或文件夹安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

要显示信息的项	输入以下命令 ...
摘要形式	`vserver security file-directory show -vserver vserver_name -path path`
扩展了详细信息	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
其中输出显示有组和用户 SID	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
关于十六进制位掩码转换为文本格式的文件和目录的文件和目录安全性	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

示例

以下示例显示了有关路径的动态访问控制安全信息 `/vol1` 在SVM VS1中：

```
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)
```

相关信息

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

显示有关中央访问策略规则的信息

动态访问控制的还原注意事项

您应了解还原到不支持动态访问控制（DAC）的 ONTAP 版本时会发生什么情况，以及还原前后必须执行哪些操作。

如果要将集群还原到不支持动态访问控制的 ONTAP 版本，并且在一个或多个 Storage Virtual Machine （SVM）上启用了动态访问控制，则必须在还原之前执行以下操作：

- 您必须在集群上启用动态访问控制的所有 SVM 上禁用动态访问控制。
- 您必须修改包含的集群上的任何审核配置 `cap-staging` 仅使用的事件类型 `file-op` 事件类型。

对于具有动态访问控制 ACE 的文件和文件夹，您必须了解一些重要的还原注意事项并采取相应措施：

- 如果还原集群，则不会删除现有动态访问控制 ACE ；但是，在文件访问检查中将忽略这些 ACE 。
- 由于还原后将忽略动态访问控制 ACE ，因此使用动态访问控制 ACE 的文件将更改对文件的访问。

  这样，用户就可以访问以前无法访问的文件，或者无法访问以前可以访问的文件。

- 您应将非动态访问控制 ACE 应用于受影响的文件，以还原其先前的安全级别。

  可以在还原之前或还原完成后立即执行此操作。

> 由于还原后会忽略动态访问控制 ACE ，因此在将非动态访问控制 ACE 应用于受影响的文件时，您无需删除它们。但是，如果需要，您可以手动将其删除。

从何处查找有关配置和使用动态访问控制和中央访问策略的追加信息

我们还提供了其他资源来帮助您配置和使用动态访问控制和中央访问策略。

您可以在 Microsoft TechNet 库中找到有关如何在 Active Directory 上配置动态访问控制和中央访问策略的信息。

"Microsoft TechNet： 动态访问控制场景概述"

"Microsoft TechNet： 中央访问策略场景"

以下参考资料可帮助您将SMB服务器配置为使用和支持动态访问控制和中央访问策略：

- *在SMB服务器上使用GPO *

  将组策略对象应用于SMB服务器

- 在**SMB**服务器上配置**NAS**审核

  "SMB 和 NFS 审核和安全跟踪"