Sicherer Dateizugriff durch Dynamic Access Control (DAC)

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/secure-file-access-dynamic-access-control-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Sicherer Dateizugriff durch Dynamic Access Control (DAC) . . . 1
- Informationen zur DAC-Dateizugriffsicherheit für ONTAP SMB-Server . . . 1
  - Ergänzungen zu den CIFS-Anmeldeinformationen . . . 1
  - Zentrale Zugriffsrichtlinien . . . 1
  - Zentrale Bereitstellung von Zugriffsrichtlinien mit erweiterter Protokollierung . . . 1
- Unterstützte DAC-Funktionalität für ONTAP SMB Server . . . 2
  - Unterstützt für Dynamic Access Control . . . 2
  - Nicht unterstützt für Dynamic Access Control . . . 3
- Informationen zur Verwendung von DAC und zentralen Zugriffsrichtlinien mit ONTAP SMB-Servern . . . 3
  - Der NFS-Zugriff kann dem Root-Benutzer verweigert werden, wenn eine Richtlinienregel für den Benutzer „domain\administrator“ gilt. . . . 4
  - Die Gruppe BUILTIN\Administrators des CIFS-Servers hat Zugriff auf Ressourcen, wenn die angewendete zentrale Zugriffsrichtlinie in Active Directory nicht gefunden wird. . . . 4
- DAC für ONTAP SMB-Server aktivieren oder deaktivieren . . . 4
- Verwaltung von ACLs mit DAC-ACEs, wenn DAC auf ONTAP SMB-Servern deaktiviert ist . . . 5
- Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf ONTAP SMB Servern zu schützen . . . 5
- Informationen zur DAC-Sicherheit für ONTAP SMB-Server . . . 8
- Überlegungen zum Zurücksetzen von DAC auf ONTAP SMB-Servern . . . 10

Sicherer Dateizugriff durch Dynamic Access Control (DAC)

Informationen zur DAC-Dateizugriffsicherheit für ONTAP SMB-Server

Sie können den Zugriff sichern, indem Sie die dynamische Zugriffssteuerung nutzen und zentrale Zugriffsrichtlinien in Active Directory erstellen und diese über angewendete Gruppenrichtlinienobjekte (GPOs) auf Dateien und Ordner auf SVMs anwenden. Es besteht die Möglichkeit, die Protokollierung so zu konfigurieren, dass zentrale Zugriffsrichtlinien-Staging-Ereignisse verwendet werden, um die Auswirkungen von Änderungen an zentralen Zugriffsrichtlinien zu sehen, bevor diese angewendet werden.

Ergänzungen zu den CIFS-Anmeldeinformationen

Vor der dynamischen Zugriffssteuerung enthielt eine CIFS-Anmeldeinformation die Identität des Sicherheitsprinzipals (des Benutzers) und die Windows-Gruppenzugehörigkeit. Mit der dynamischen Zugriffssteuerung werden der Anmeldeinformation drei weitere Informationstypen hinzugefügt: Geräteidentität, Geräteansprüche und Benutzeransprüche.

- Geräteidentität

  Das Analogon zu den Identitätsinformationen des Benutzers, nur dass es sich um die Identität und Gruppenzugehörigkeit des Geräts handelt, von dem sich der Benutzer einloggt.

- Geräteansprüche

  Aussagen über einen Gerätesicherheitsprinzipal. Beispielsweise könnte eine Geräteaussage lauten, dass das Gerät Mitglied einer bestimmten Organisationseinheit (OU) ist.

- Benutzeransprüche

  Aussagen über einen Benutzer-Sicherheitsprinzipal. Beispielsweise könnte eine Benutzer-Assertion lauten, dass das AD-Konto Mitglied einer bestimmten OU ist.

Zentrale Zugriffsrichtlinien

Zentrale Zugriffsrichtlinien für Dateien ermöglichen Organisationen, Autorisierungsrichtlinien, die bedingte Ausdrücke mit Benutzergruppen, Benutzeransprüchen, Geräteansprüchen und Ressourceneigenschaften enthalten, zentral bereitzustellen und zu verwalten.

Beispielsweise muss ein Benutzer, um auf geschäftskritische Daten zuzugreifen, Vollzeitbeschäftigter sein und darf nur von einem verwalteten Gerät aus auf die Daten zugreifen. Zentrale Zugriffsrichtlinien werden in Active Directory definiert und über den GPO-Mechanismus an Dateiserver verteilt.

Zentrale Bereitstellung von Zugriffsrichtlinien mit erweiterter Protokollierung

Zentrale Zugriffsrichtlinien können „staged“ werden, wobei sie bei Dateizugriffsprüfungen in einer „what-if“-Manier ausgewertet werden. Die Ergebnisse dessen, was passiert wäre, wenn die Richtlinie wirksam gewesen wäre, und wie sich das von der aktuellen Konfiguration unterscheidet, werden als Protokollierungsereignis

erfasst. Auf diese Weise können Administratoren Protokollierungsereignisse nutzen, um die Auswirkungen einer Änderung der Zugriffsrichtlinie zu untersuchen, bevor die Richtlinie tatsächlich angewendet wird. Nach der Bewertung der Auswirkungen einer Änderung der Zugriffsrichtlinie kann die Richtlinie über GPOs auf die gewünschten SVMs bereitgestellt werden.

Verwandte Informationen

- Informationen zu unterstützten Gruppenrichtlinienobjekten (GPOs)
- Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- GPO-Unterstützung auf Servern aktivieren oder deaktivieren
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln
- Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf Servern zu sichern.
- Informationen zur Serversicherheit
- "SMB und NFS Auditierung und Sicherheitsverfolgung"

Unterstützte DAC-Funktionalität für ONTAP SMB Server

Wenn Sie Dynamic Access Control (DAC) auf Ihrem CIFS-Server verwenden möchten, ist es wichtig zu verstehen, wie ONTAP die Dynamic Access Control Funktionalität in Active Directory-Umgebungen unterstützt.

Unterstützt für Dynamic Access Control

ONTAP unterstützt die folgende Funktionalität, wenn die Dynamic Access Control auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Ansprüche im Dateisystem	Ansprüche sind einfache Namens-Wert-Paare, die eine bestimmte Wahrheit über einen Benutzer aussagen. Benutzeranmeldeinformationen enthalten Anspruchsinformationen, und Sicherheitsdeskriptoren von Dateien können Zugriffsprüfungen durchführen, die auch Anspruchsprüfungen umfassen. Dies gibt Administratoren eine feinere Kontrolle darüber, wer auf Dateien zugreifen kann.
Bedingte Ausdrücke für Dateizugriffsprüfungen	Beim Ändern der Sicherheitsparameter einer Datei können Benutzer dem Sicherheitsdeskriptor der Datei beliebig komplexe bedingte Ausdrücke hinzufügen. Der bedingte Ausdruck kann Prüfungen auf Claims enthalten.

Funktionalität	Kommentare
Zentrale Steuerung des Dateizugriffs über zentrale Zugriffsrichtlinien	Zentrale Zugriffsrichtlinien sind eine Art Zugriffskontrollliste (ACL), die in Active Directory gespeichert und einer Datei zugeordnet werden kann. Der Zugriff auf die Datei wird nur gewährt, wenn sowohl die Zugriffsprüfungen des Sicherheitsdeskriptors auf dem Datenträger als auch die zugeordnete zentrale Zugriffsrichtlinie den Zugriff erlauben. Dies ermöglicht Administratoren, den Zugriff auf Dateien zentral (in Active Directory) zu steuern, ohne den Sicherheitsdeskriptor auf dem Datenträger ändern zu müssen.
Staging der zentralen Zugriffsrichtlinie	Fügt die Möglichkeit hinzu, Sicherheitsänderungen auszuprobieren, ohne den tatsächlichen Dateizugriff zu beeinflussen, indem eine Änderung an den zentralen Zugriffsrichtlinien „gestagt“ wird und die Auswirkung der Änderung in einem Prüfbericht angezeigt wird.
Unterstützung für die Anzeige von Informationen zur zentralen Zugriffsrichtliniensicherheit mithilfe der ONTAP CLI	Erweitert den `vserver security file-directory show` Befehl, um Informationen über angewendete zentrale Zugriffsrichtlinien anzuzeigen.
Sicherheitsverfolgung einschließlich zentraler Zugriffsrichtlinien	Erweitert die `vserver security trace`Befehlsfamilie und zeigt Ergebnisse an, die Informationen über angewendete zentrale Zugriffsrichtlinien enthalten.

Nicht unterstützt für Dynamic Access Control

ONTAP unterstützt die folgende Funktionalität nicht, wenn die Dynamic Access Control auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Automatische Klassifizierung von NTFS-Dateisystemobjekten	Dies ist eine Erweiterung der Windows-Dateiklassifizierungsinfrastruktur, die in ONTAP nicht unterstützt wird.
Erweiterte Überwachung mit Ausnahme des Stagings von zentralen Zugriffsrichtlinien	Nur das zentrale Staging von Zugriffsrichtlinien wird für erweiterte Prüfverfahren unterstützt.

Informationen zur Verwendung von DAC und zentralen Zugriffsrichtlinien mit ONTAP SMB-Servern

Bei der Verwendung von Dynamic Access Control (DAC) und zentralen Zugriffsrichtlinien zum Schutz von Dateien und Ordnern auf CIFS-Servern sind bestimmte Aspekte zu berücksichtigen.

Der NFS-Zugriff kann dem Root-Benutzer verweigert werden, wenn eine Richtlinienregel für den Benutzer „domain\administrator“ gilt.

Unter bestimmten Umständen kann der NFS-Zugriff auf Root verweigert werden, wenn auf die Daten, auf die der Root-Benutzer zugreifen möchte, eine zentrale Zugriffsrichtlinie angewendet wird. Das Problem tritt auf, wenn die zentrale Zugriffsrichtlinie eine Regel enthält, die auf domain\administrator angewendet wird und das Root-Konto dem domain\administrator-Konto zugeordnet ist.

Anstatt die Regel auf den Benutzer domain\administrator anzuwenden, sollte die Regel auf eine Gruppe mit administrativen Rechten angewendet werden, wie zum Beispiel die domain\administrators Gruppe. Auf diese Weise kann root dem domain\administrator Konto zugeordnet werden, ohne dass root von diesem Problem betroffen ist.

Die Gruppe BUILTIN\Administrators des CIFS-Servers hat Zugriff auf Ressourcen, wenn die angewendete zentrale Zugriffsrichtlinie in Active Directory nicht gefunden wird.

Es ist möglich, dass auf Ressourcen innerhalb des CIFS-Servers zentrale Zugriffsrichtlinien angewendet werden. Wenn der CIFS-Server versucht, mithilfe der SID der zentralen Zugriffsrichtlinie Informationen aus Active Directory abzurufen, stimmt die SID mit keiner vorhandenen SID einer zentralen Zugriffsrichtlinie in Active Directory überein. Unter diesen Umständen wendet der CIFS-Server die lokale Standardwiederherstellungsrichtlinie für diese Ressource an.

Die lokale Standardwiederherstellungsrichtlinie gewährt der Gruppe BUILTIN\Administrators des CIFS-Servers Zugriff auf diese Ressource.

DAC für ONTAP SMB-Server aktivieren oder deaktivieren

Die Option, mit der Sie Dynamic Access Control (DAC) zum Schutz von Objekten auf Ihrem CIFS-Server verwenden können, ist standardmäßig deaktiviert. Die Option muss aktiviert werden, wenn Dynamic Access Control auf dem CIFS-Server verwendet werden soll. Falls später entschieden wird, Dynamic Access Control nicht mehr zum Schutz von auf dem CIFS-Server gespeicherten Objekten zu verwenden, kann die Option deaktiviert werden.

Informationen darüber, wie die dynamische Zugriffssteuerung in Active Directory konfiguriert wird, sind in der Microsoft TechNet Library zu finden.

"Microsoft TechNet: Übersicht über Szenarien zur dynamischen Zugriffskontrolle"

Über diese Aufgabe

Sobald die dynamische Zugriffskontrolle aktiviert ist, kann das Dateisystem ACLs mit Einträgen zur dynamischen Zugriffskontrolle enthalten. Wenn die dynamische Zugriffskontrolle deaktiviert ist, werden die aktuellen Einträge zur dynamischen Zugriffskontrolle ignoriert und neue werden nicht zugelassen.

Diese Option ist nur auf der Stufe „Erweitert“ verfügbar.

Schritt

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die Dynamic Access Control…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver vserver_name -is-dac-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -is-dac-enabled false`

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Verwandte Informationen

Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf Servern zu sichern.

Verwaltung von ACLs mit DAC-ACEs, wenn DAC auf ONTAP SMB-Servern deaktiviert ist

Wenn Sie Ressourcen haben, auf die ACLs mit Dynamic Access Control ACEs angewendet wurden, und Sie Dynamic Access Control auf der Storage Virtual Machine (SVM) deaktivieren, müssen Sie die Dynamic Access Control ACEs entfernen, bevor Sie die nicht-Dynamic Access Control ACEs auf dieser Ressource verwalten können.

Über diese Aufgabe

Nachdem die dynamische Zugriffskontrolle deaktiviert ist, können bestehende nicht-dynamische Zugriffskontroll-ACEs weder entfernt noch neue nicht-dynamische Zugriffskontroll-ACEs hinzugefügt werden, bis die bestehenden dynamischen Zugriffskontroll-ACEs entfernt wurden.

Sie können das Tool, das Sie normalerweise zur Verwaltung von ACLs verwenden, für diese Schritte einsetzen.

Schritte

1. Ermitteln, welche Dynamic Access Control ACEs auf die Ressource angewendet sind.
2. Die ACEs der dynamischen Zugriffssteuerung aus der Ressource entfernen.
3. Nicht-dynamische Zugriffskontroll-ACEs können nach Bedarf zur Ressource hinzugefügt oder daraus entfernt werden.

Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf ONTAP SMB Servern zu schützen

Es sind mehrere Schritte erforderlich, um den Zugriff auf Daten auf dem CIFS-Server mithilfe zentraler Zugriffsrichtlinien zu sichern, darunter das Aktivieren der Dynamic Access Control (DAC) auf dem CIFS-Server, das Konfigurieren zentraler Zugriffsrichtlinien in Active Directory, das Anwenden der zentralen Zugriffsrichtlinien auf Active Directory Container mit Gruppenrichtlinienobjekten (GPOs) und das Aktivieren von GPOs auf dem CIFS-Server.

Bevor Sie beginnen

- Das Active Directory muss so konfiguriert sein, dass zentrale Zugriffsrichtlinien verwendet werden.

- Sie benötigen ausreichende Zugriffsrechte auf den Active Directory Domänencontrollern, um zentrale Zugriffsrichtlinien zu erstellen und GPOs auf die Container zu erstellen und anzuwenden, die die CIFS-Server enthalten.
- Sie benötigen ausreichende administrative Zugriffsrechte auf der Storage Virtual Machine (SVM), um die erforderlichen Befehle auszuführen.

Über diese Aufgabe

Zentrale Zugriffsrichtlinien werden definiert und auf Gruppenrichtlinienobjekte (GPOs) in Active Directory angewendet. Informationen zur Konfiguration zentraler Zugriffsrichtlinien in Active Directory sind in der Microsoft TechNet Library verfügbar.

"Microsoft TechNet: Szenario für zentrale Zugriffsrichtlinie"

Schritte

1. Die dynamische Zugriffskontrolle auf der SVM kann aktiviert werden, falls sie noch nicht aktiviert ist, indem der `vserver cifs options modify` Befehl verwendet wird.

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

2. Gruppenrichtlinienobjekte (GPOs) auf dem CIFS-Server können aktiviert werden, falls sie noch nicht aktiviert sind, indem der `vserver cifs group-policy modify` Befehl verwendet wird.

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

3. Zentrale Zugriffsregeln und zentrale Zugriffsrichtlinien in Active Directory erstellen.
4. Ein Gruppenrichtlinienobjekt (GPO) wird erstellt, um die zentralen Zugriffsrichtlinien auf Active Directory bereitzustellen.
5. Die Gruppenrichtlinie wird auf den Container angewendet, in dem sich das Computerkonto des CIFS-Servers befindet.
6. Die auf den CIFS-Server angewendeten GPOs werden mit dem `vserver cifs group-policy update` Befehl manuell aktualisiert.

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

7. Es sollte überprüft werden, ob die zentrale Zugriffsrichtlinie des Gruppenrichtlinienobjekts (GPO) auf die Ressourcen auf dem CIFS-Server angewendet wird, indem der `vserver cifs group-policy show-applied` Befehl verwendet wird.

   Das folgende Beispiel zeigt, dass die Default Domain Policy zwei zentrale Zugriffsrichtlinien enthält, die auf den CIFS-Server angewendet werden:

   ```
   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.
```

Verwandte Informationen

- Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln
- DAC für Server aktivieren oder deaktivieren

Informationen zur DAC-Sicherheit für ONTAP SMB-Server

Sie können Informationen zur dynamischen Zugriffssteuerung (DAC) auf NTFS-Volumes und zu Daten mit effektiver NTFS-Sicherheit auf Volumes mit gemischtem Sicherheitsstil

anzeigen. Dies umfasst Informationen zu bedingten ACEs, Ressourcen-ACEs und zentralen Zugriffsrichtlinien-ACEs. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Ordnersicherheitsinformationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Mit erweiterten Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Wo die Ausgabe mit Gruppen- und Benutzer-SIDs angezeigt wird	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Informationen zur Datei- und Verzeichnissicherheit für Dateien und Verzeichnisse, bei denen die hexadezimale Bitmaske in ein Textformat übersetzt wird	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Beispiele

Das folgende Beispiel zeigt Sicherheitsinformationen zur Dynamic Access Control über den Pfad `/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)
```

Verwandte Informationen

- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln

Überlegungen zum Zurücksetzen von DAC auf ONTAP SMB-Servern

Sie sollten sich darüber im Klaren sein, was passiert, wenn auf eine Version von ONTAP zurückgesetzt wird, die Dynamic Access Control (DAC) nicht unterstützt, und was vor und nach dem Zurücksetzen zu tun ist.

Wenn der Cluster auf eine Version von ONTAP zurückgesetzt werden soll, die Dynamic Access Control nicht unterstützt, und Dynamic Access Control auf einer oder mehreren Storage Virtual Machines (SVMs) aktiviert ist, sind vor dem Zurücksetzen die folgenden Schritte erforderlich:

- Die dynamische Zugriffskontrolle muss auf allen SVMs deaktiviert werden, auf denen sie im Cluster aktiviert ist.
- Sie müssen alle Überwachungskonfigurationen auf dem Cluster, die den `cap-staging` Ereignistyp enthalten, so ändern, dass nur der `file-op` Ereignistyp verwendet wird.

Einige wichtige Überlegungen zum Zurücksetzen von Dateien und Ordnern mit Dynamic Access Control-ACEs sollten verstanden und berücksichtigt werden:

- Wenn der Cluster zurückgesetzt wird, werden bestehende Dynamic Access Control ACEs nicht entfernt; sie werden jedoch bei Dateizugriff-Prüfungen ignoriert.
- Da Dynamic Access Control-ACEs nach der Rücksetzung ignoriert werden, ändert sich der Zugriff auf

Dateien mit Dynamic Access Control-ACEs.

Dies könnte dazu führen, dass Benutzer auf Dateien zugreifen können, auf die sie zuvor keinen Zugriff hatten, oder umgekehrt, dass sie auf Dateien nicht mehr zugreifen können, auf die sie zuvor Zugriff hatten.

- Nicht-dynamische Zugriffskontroll-ACEs sollten auf die betroffenen Dateien angewendet werden, um deren vorheriges Sicherheitsniveau wiederherzustellen.

  Dies kann entweder vor dem Zurücksetzen oder unmittelbar nach Abschluss der Rücksetzung erfolgen.

> Da Dynamic Access Control-ACEs nach dem Zurücksetzen ignoriert werden, ist es nicht erforderlich, sie zu entfernen, wenn nicht-Dynamic Access Control-ACEs auf die betroffenen Dateien angewendet werden. Falls gewünscht, können sie manuell entfernt werden.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.