Management der Verifizierung von mehreren Administratoren

ONTAP 9

NetApp
March 21, 2023

Inhaltsverzeichnis

Management der Verifizierung von mehreren Administratoren

Übersicht über die Verifizierung mit mehreren Administratoren

Ab ONTAP 9.11.1 können Sie die Überprüfung durch mehrere Administratoren (Multi-Admin Verification, MAV) verwenden, um sicherzustellen, dass bestimmte Vorgänge, wie das Löschen von Volumes oder Snapshot Kopien, nur nach Genehmigung von zugewiesenen Administratoren ausgeführt werden können. So werden gefährdete, böswillige oder unerfahrene Administratoren daran gehindert, unerwünschte Änderungen vorzunehmen oder Daten zu löschen.

Die Konfiguration der Prüfung für mehrere Administratoren umfasst:

- "Erstellen einer oder mehrerer Genehmigungsgruppen für Administratoren"
- "Aktivieren der Überprüfungsfunktion für mehrere Administratoren"
- "Hinzufügen oder Ändern von Regeln"

Nach der Erstkonfiguration können diese Elemente nur von Administratoren in einer MAV-Genehmigungsgruppe (MAV-Administratoren) geändert werden.

Wenn die Überprüfung durch mehrere Administratoren aktiviert ist, sind für jeden geschützten Vorgang drei Schritte erforderlich:

- Wenn ein Benutzer den Vorgang initiiert, A "Die Anforderung wird generiert."
- Bevor es ausgeführt werden kann, mindestens eine "MAV-Administrator muss genehmigen."
- Nach der Genehmigung schließt der Benutzer den Vorgang ab.

Die Überprüfung durch mehrere Administratoren ist nicht für Volumes oder Workflows gedacht, die mit hoher Automatisierung arbeiten, da jede automatisierte Aufgabe vor Abschluss des Vorgangs eine Genehmigung erfordert. Wenn Sie Automation und MAV gemeinsam nutzen möchten, empfiehlt es sich, Abfragen für bestimmte MAV-Operationen zu verwenden. So können Sie sich beispielsweise bewerben `volume delete` MAV regiert nur zu Volumes, in denen keine Automatisierung beteiligt ist, und Sie können die Volumes mit einem bestimmten Benennungsschema benennen.

> Wenn Sie die Verifizierungsfunktion mehrerer Administratoren ohne Genehmigung eines MAV-Administrators deaktivieren müssen, wenden Sie sich an den NetApp Support und erwähnen Sie den folgenden Knowledge Base-Artikel: "So deaktivieren Sie die Multi-Admin-Überprüfung, wenn MAV-Admin nicht verfügbar ist".

Funktionsweise der Multiadmin-Überprüfung

Die Überprüfung durch mehrere Administratoren umfasst:

- Eine Gruppe von einem oder mehreren Administratoren mit Genehmigung und Veto-Befugnissen.
- Eine Reihe von geschützten Operationen oder Befehlen in einer Tabelle *rules*.

- Eine *rules Engine* zur Identifizierung und Steuerung der Ausführung geschützter Vorgänge.

MAV-Regeln werden nach rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) evaluiert. Daher müssen Administratoren, die einen geschützten Betrieb ausführen oder genehmigen, bereits die minimalen RBAC-Rechte für diese Vorgänge besitzen. "Erfahren Sie mehr über RBAC."

Wenn die Multi-Admin-Überprüfung aktiviert ist, werden durch systemdefinierte Regeln (auch bekannt als *guard-Rail*-Regeln) eine Reihe von MAV-Operationen festgelegt, die das Risiko enthalten, den MAV-Prozess selbst zu umgehen. Diese Vorgänge können nicht aus der Regeltabelle entfernt werden. Wenn MAV aktiviert ist, müssen Operationen, die durch ein Sternchen (*) gekennzeichnet sind, vor der Ausführung von einem oder mehreren Administratoren genehmigt werden, mit Ausnahme von **show**-Befehlen.

- `security multi-admin-verify modify*`

  Steuert die Konfiguration der Verifizierungsfunktion für mehrere Administratoren.

- `security multi-admin-verify approval-group` Betrieb*

  Steuern Sie die Mitgliedschaft im Administratorensatz mit Anmeldeinformationen für die Überprüfung mehrerer Administratoren.

- `security multi-admin-verify rule` Betrieb*

  Steuern Sie die Befehlssatz, für die eine Multi-Admin-Überprüfung erforderlich ist.

- `security multi-admin-verify request` Betrieb

  Kontrollieren Sie den Genehmigungsprozess.

Zusätzlich zu den systemdefinierten Befehlen sind die folgenden Befehle standardmäßig geschützt, wenn die Multi-Admin-Überprüfung aktiviert ist. Sie können jedoch die Regeln ändern, um den Schutz für diese Befehle zu entfernen.

- `security login password`
- `security login unlock`
- `set`

Die folgenden Befehle können in ONTAP 9.11.1 und neueren Versionen gesichert werden.

`cluster peer delete`	`volume snapshot autodelete modify`
`event config modify`	`volume snapshot delete`
`security login create`	`volume snapshot policy add-schedule`
`security login delete`	`volume snapshot policy create`
`security login modify`	`volume snapshot policy delete`
`system node run`	`volume snapshot policy modify`
`system node systemshell`	`volume snapshot policy modify-schedule`
`volume delete`	`volume snapshot policy remove-schedule`
`volume flexcache delete`	`volume snapshot restore`
`volume snaplock modify`	`vserver peer delete`

Funktionsweise der Multi-Admin-Genehmigung

Jedes Mal, wenn ein geschützter Vorgang in einem MAV-geschützten Cluster eingegeben wird, wird eine Anfrage zur Ausführung des Vorgangs an die entsprechende MAV-Administratorgruppe gesendet.

Sie können Folgendes konfigurieren:

- Die Namen, Kontaktinformationen und die Anzahl der Administratoren in der MAV-Gruppe.

  Ein MAV-Administrator sollte über eine RBAC-Rolle mit Cluster-Administratorrechten verfügen.

- Die Anzahl der MAV-Administratorgruppen.
  - Für jede Schutzregel wird eine MAV-Gruppe zugewiesen.
  - Für mehrere MAV-Gruppen können Sie konfigurieren, welche MAV-Gruppe eine bestimmte Regel genehmigt.
- Die Anzahl der erforderlichen MAV-Genehmigungen für die Ausführung eines geschützten Vorgangs.
- Eine Ablauffrist *Genehmigung*, innerhalb derer ein MAV-Administrator auf eine Genehmigungsanfrage antworten muss.
- Eine Ablauffrist *Ausführung*, innerhalb derer der anfragende Administrator den Vorgang abschließen muss.

Sobald diese Parameter konfiguriert sind, muss die MAV-Genehmigung geändert werden.

MAV-Administratoren können ihre eigenen Anforderungen zur Ausführung von geschützten Vorgängen nicht genehmigen. Daher:

- MAV sollte nicht auf Clustern mit nur einem Administrator aktiviert werden.
- Wenn sich nur eine Person in der MAV-Gruppe befindet, kann der MAV-Administrator keine geschützten Vorgänge aufrufen. Regelmäßige Administratoren müssen diese eingeben und der MAV-Administrator kann nur genehmigen.

- Wenn Sie möchten, dass MAV-Administratoren geschützte Vorgänge ausführen können, muss die Anzahl der MAV-Administratoren größer sein als die Anzahl der erforderlichen Genehmigungen. Wenn zum Beispiel zwei Genehmigungen für einen geschützten Vorgang erforderlich sind und Sie möchten, dass MAV-Administratoren diese ausführen, müssen sich drei Personen in der Gruppe MAV-Administratoren befinden.

MAV-Administratoren können Genehmigungsanfragen in E-Mail-Benachrichtigungen (über EMS) erhalten oder die Anforderungswarteschlange abfragen. Wenn sie eine Anfrage erhalten, können sie eine von drei Aktionen durchführen:

- Genehmigen
- Ablehnen (Veto)
- Ignorieren (keine Aktion)

E-Mail-Benachrichtigungen werden an alle Genehmiger gesendet, die einer MAV-Regel zugeordnet sind, wenn:

- Eine Anfrage wird erstellt.
- Ein Antrag ist genehmigt oder ein Veto eingelegt.
- Eine genehmigte Anfrage wird ausgeführt.

Wenn sich der Anforderer in derselben Genehmigungsgruppe für den Vorgang befindet, wird er eine E-Mail erhalten, wenn seine Anfrage genehmigt wird.

Hinweis: ein Antragsteller kann seine eigenen Anfragen nicht genehmigen, auch wenn er sich in der Genehmigungsgruppe befindet. Aber sie können die E-Mail-Benachrichtigungen erhalten. Anfragesteller, die sich nicht in Genehmigungsgruppen befinden (d. h. nicht MAV-Administratoren), erhalten keine E-Mail-Benachrichtigungen.

Funktionsweise der geschützten Operation

Wenn die Ausführung für einen geschützten Vorgang genehmigt wird, wird der anfragende Benutzer mit der Operation fortgesetzt, wenn er dazu aufgefordert wird. Wenn der Vorgang ein Vetos hat, muss der anfordernde Benutzer die Anfrage löschen, bevor er fortfahren kann.

MAV-Regeln werden nach RBAC-Berechtigungen evaluiert. Dadurch kann ein Benutzer ohne ausreichende RBAC-Berechtigungen für die Ausführung des Vorgangs den MAV-Anforderungsprozess nicht initiieren.

Management von Genehmigungsgruppen für Administratoren

Bevor Sie die MAV (Multi-Administrator Verification) aktivieren, müssen Sie eine Admin-Genehmigungsgruppe erstellen, die einen oder mehrere Administratoren enthält, die eine Genehmigung oder Veto-Berechtigung erhalten. Sobald Sie die Überprüfung mehrerer Administratoren aktiviert haben, müssen alle Änderungen an der Mitgliedschaft in der Genehmigungsgruppe von einem der vorhandenen qualifizierten Administratoren genehmigt werden.

Über diese Aufgabe

Sie können vorhandene Administratoren einer MAV-Gruppe hinzufügen oder neue Administratoren erstellen.

Die MAV-Funktionalität berücksichtigt vorhandene rollenbasierte RBAC-Einstellungen (Access Control, RBAC). Potenzielle MAV-Administratoren müssen über ausreichende Berechtigungen verfügen, um geschützte Vorgänge auszuführen, bevor sie zu MAV-Administratorgruppen hinzugefügt werden. "Erfahren Sie mehr über RBAC."

Sie können MAV so konfigurieren, dass MAV-Administratoren darauf aufmerksam gemacht werden, dass Genehmigungsanforderungen ausstehen. Dazu müssen Sie E-Mail-Benachrichtigungen konfigurieren, insbesondere die `Mail From` Und `Mail Server` Parameter—oder Sie können diese Parameter löschen, um die Benachrichtigung zu deaktivieren. Ohne E-Mail-Warnmeldungen müssen MAV-Administratoren die Genehmigungswarteschlange manuell prüfen.

System Manager Verfahren

Wenn Sie zum ersten Mal eine MAV-Genehmigungsgruppe erstellen möchten, lesen Sie das Verfahren zu System Manager nach "Aktivieren Sie die Verifizierung für mehrere Administratoren."

So ändern Sie eine vorhandene Genehmigungsgruppe oder erstellen eine zusätzliche Genehmigungsgruppe:

1. Identifizieren Sie die Administratoren, die eine Überprüfung durch mehrere Administratoren erhalten.
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie Auf → Neben **Benutzer und Rollen.**
   c. Klicken Sie Auf + Add Unter **Benutzer.**
   d. Ändern Sie den Dienstplan nach Bedarf.

      Weitere Informationen finden Sie unter "Kontrolle des Administratorzugriffs"

2. Erstellen oder Ändern der MAV-Genehmigungsgruppe:
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie Auf → Neben **Multi-Admin-Genehmigung** im Abschnitt **Sicherheit**. (Sie sehen die ⚙ Symbol, wenn MAV noch nicht konfiguriert ist.)
      - Name: Geben Sie einen Gruppennamen ein.
      - Genehmiger: Wählen Sie Genehmiger aus einer Benutzerliste aus.
      - E-Mail-Adresse: E-Mail-Adresse(n) eingeben.
      - Standardgruppe: Wählen Sie eine Gruppe aus.

Eine MAV-Genehmigung ist erforderlich, um eine vorhandene Konfiguration zu bearbeiten, sobald MAV aktiviert ist.

CLI-Verfahren

1. Überprüfen Sie, ob die Werte für die festgelegt wurden `Mail From` Und `Mail Server` Parameter. Geben Sie Ein:

   ```
   event config show
   ```

   Die Anzeige sollte wie folgt lauten:

```
cluster01::> event config show
                           Mail From:  admin@localhost
                         Mail Server:  localhost
                           Proxy URL:  -
                          Proxy User:  -
 Publish/Subscribe Messaging Enabled:  true
```

Um diese Parameter zu konfigurieren, geben Sie Folgendes ein:

`event config modify -mail-from *email_address* -mail-server *server_name*`

2. Identifizieren Sie die Administratoren, die eine Überprüfung durch mehrere Administratoren erhalten

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Zeigen Sie aktuelle Administratoren an	`security login show`
Ändern der Anmeldeinformationen aktueller Administratoren	`security login modify <*parameters*>`
Erstellen neuer Administratorkonten	`security login create -user-or-group -name *admin_name* -application ssh -authentication-method password`

3. Erstellen Sie die MAV-Genehmigungsgruppe:

`security multi-admin-verify approval-group create [ -vserver *svm_name*] -name *group_name* -approvers *approver1*[,*approver2*…] [[-email *address1*], *address1*…]`

   - `-vserver` - Nur die Administrator-SVM wird in diesem Release unterstützt.
   - `-name` - Der MAV-Gruppenname, bis zu 64 Zeichen.
   - `-approvers` - Die Liste eines oder mehrerer Genehmiger.
   - `-email` - Eine oder mehrere E-Mail-Adressen, die benachrichtigt werden, wenn eine Anfrage erstellt, genehmigt, ein Veto eingelegt oder ausgeführt wird.

     Beispiel: mit dem folgenden Befehl wird eine MAV-Gruppe mit zwei Mitgliedern und zugehörigen E-Mail-Adressen erstellt.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. Gruppenerstellung und -Mitgliedschaft überprüfen:

`security multi-admin-verify approval-group show`

Beispiel:

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name        Approvers        Email
-------  ---------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      email
pavan@myfirm.com,julia@myfirm.com
```

Verwenden Sie diese Befehle, um Ihre ursprüngliche MAV-Gruppenkonfiguration zu ändern.

Hinweis: Alle erfordern eine Genehmigung des MAV-Administrators vor der Ausführung.

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Ändern Sie die Gruppeneigenschaften, oder ändern Sie vorhandene Mitgliedsinformationen	`security multi-admin-verify approval-group modify [parameters]`
Mitglieder hinzufügen oder entfernen	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
Gruppe löschen	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

Aktivieren und Deaktivieren der Verifizierung von mehreren Administratoren

Multi-Admin-Verifizierung (MAV) muss explizit aktiviert werden. Sobald Sie die Überprüfung durch mehrere Administratoren aktiviert haben, muss die Genehmigung durch Administratoren in einer MAV-Genehmigungsgruppe (MAV-Administratoren) gelöscht werden.

Über diese Aufgabe

Wenn MAV aktiviert ist, muss MAV durch Ändern oder Deaktivieren der MAV-Administratorfreigabe genehmigt werden.

> Wenn Sie die Verifizierungsfunktion mehrerer Administratoren ohne Genehmigung eines MAV-Administrators deaktivieren müssen, wenden Sie sich an den NetApp Support und erwähnen Sie den folgenden Knowledge Base-Artikel: "So deaktivieren Sie die Multi-Admin-Überprüfung, wenn MAV-Admin nicht verfügbar ist".

Wenn Sie MAV aktivieren, können Sie global die folgenden Parameter angeben.

Genehmigungsgruppen

Eine Liste globaler Genehmigungsgruppen. Um die MAV-Funktionalität zu aktivieren, ist mindestens eine Gruppe erforderlich.

Erforderliche Genehmiger

Die Anzahl der Genehmiger, die für die Ausführung eines geschützten Vorgangs erforderlich sind. Die Standard- und die Mindestzahl ist 1.

Hinweis: die erforderliche Anzahl an Genehmigern muss kleiner als die Gesamtzahl der eindeutigen Genehmiger in den Standardgenehmigungsgruppen sein.

Ablauf der Genehmigung (Stunden, Minuten, Sekunden)

Der Zeitraum, innerhalb dessen ein MAV-Administrator auf eine Genehmigungsanforderung reagieren muss. Der Standardwert ist eine Stunde (1 h), der unterstützte Mindestwert beträgt eine Sekunde (1 s) und der maximal unterstützte Wert beträgt 14 Tage (14d).

Ausführungsablauf (Stunden, Minuten, Sekunden)

Der Zeitraum, in dem der anfragende Administrator den Vorgang: Abschließen muss. Der Standardwert ist eine Stunde (1 h), der unterstützte Mindestwert beträgt eine Sekunde (1 s) und der maximal unterstützte Wert beträgt 14 Tage (14d).

Sie können diese Parameter auch für bestimmte Parameter überschreiben "Betriebsregeln."

System Manager Verfahren

1. Identifizieren Sie die Administratoren, die eine Überprüfung durch mehrere Administratoren erhalten.
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie Auf → Neben **Benutzer und Rollen.**
   c. Klicken Sie Auf + Add Unter **Benutzer.**
   d. Ändern Sie den Dienstplan nach Bedarf.

      Weitere Informationen finden Sie unter "Kontrolle des Administratorzugriffs"

2. Aktivieren Sie die Überprüfung durch mehrere Administratoren, indem Sie mindestens eine Genehmigungsgruppe erstellen und mindestens eine Regel hinzufügen.
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie Auf ⚙ Neben **Multi-Admin-Genehmigung** im Abschnitt **Sicherheit**.
   c. Klicken Sie Auf + Add Um mindestens eine Genehmigungsgruppe hinzuzufügen.
      - Name – Geben Sie einen Gruppennamen ein.
      - Genehmiger – Wählen Sie Genehmiger aus einer Benutzerliste aus.
      - E-Mail-Adresse – Geben Sie die E-Mail-Adresse(n) ein.
      - Standardgruppe – Wählen Sie eine Gruppe aus.
   d. Fügen Sie mindestens eine Regel hinzu.
      - Operation – Wählen Sie einen unterstützten Befehl aus der Liste aus.
      - Abfrage – Geben Sie alle gewünschten Befehlsoptionen und Werte ein.
      - Optionale Parameter; lassen Sie leer, um globale Einstellungen anzuwenden, oder weisen Sie einen anderen Wert für bestimmte Regeln zu, um die globalen Einstellungen zu überschreiben.

        - Erforderliche Anzahl an Genehmigern
        - Genehmigungsgruppen

    e. Klicken Sie auf **Erweiterte Einstellungen**, um die Standardeinstellungen anzuzeigen oder zu ändern.
        - Erforderliche Anzahl an Genehmigern (Standard: 1)
        - Ablauf der Testsuite (Standard: 1 Stunde)
        - Ablauf der Genehmigungsanforderung (Standard: 1 Stunde)
        - E-Mail-Server*
        - Von E-Mail-Adresse*

        *Diese aktualisieren die unter "Benachrichtigungsverwaltung" verwalteten E-Mail-Einstellungen. Sie werden aufgefordert, sie einzustellen, wenn sie noch nicht konfiguriert wurden.

    f. Klicken Sie auf **Aktivieren**, um die Erstkonfiguration von MAV abzuschließen.

Nach der Erstkonfiguration wird der aktuelle MAV-Status in der Kachel **Multi-Admin Approval** angezeigt.

- Status (aktiviert oder nicht)
- Aktive Vorgänge, für die Genehmigungen erforderlich sind
- Anzahl der offenen Anfragen im Status „ausstehend“

Sie können eine vorhandene Konfiguration anzeigen, indem Sie auf klicken →. Zum Bearbeiten einer vorhandenen Konfiguration ist eine MAV-Genehmigung erforderlich.

So deaktivieren Sie die Multi-Admin-Verifizierung:

1. Klicken Sie Auf **Cluster > Einstellungen.**
2. Klicken Sie Auf ⚙ Neben **Multi-Admin-Genehmigung** im Abschnitt **Sicherheit**.
3. Klicken Sie auf die Schaltfläche zum Wechseln aktiviert.

   Zum Abschluss dieses Vorgangs ist eine MAV-Genehmigung erforderlich.

CLI-Verfahren

Bevor Sie MAV-Funktionalität in der CLI aktivieren, ist mindestens eine davon "MAV-Administratorgruppe" Muss erstellt worden sein.

Wenn Sie… wollen	Geben Sie diesen Befehl ein

MAV-Funktionalität aktivieren	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`
	
	Beispiel : mit dem folgenden Befehl wird MAV mit 1 Genehmigungsgruppe, 2 erforderlichen Genehmigern und Standard-Ablauffristen aktiviert.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Führen Sie die Erstkonfiguration durch Hinzufügen von mindestens einer Konfiguration durch "Betriebsregel."

Änderung einer MAV-Konfiguration (erfordert MAV-Genehmigung)	`security multi-admin-verify approval-group modify [-approval-groups group1 [,group2…]] [-required-approvers nn ] [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`

Überprüfung der MAV-Funktionalität	`security multi-admin-verify show`
	
	Beispiel:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

MAV-Funktionalität deaktivieren (MAV-Genehmigung erforderlich)	`security multi-admin-verify modify -enabled false`

Verwalten von Regeln für geschützte Vorgänge

Sie erstellen MAV-Regeln (Multi-Admin Verification), um Vorgänge zu bestimmen, die genehmigt werden müssen. Sobald ein Vorgang initiiert wird, werden geschützte Vorgänge abgefangen und eine Anfrage zur Genehmigung generiert.

Regeln können erstellt werden, bevor sie MAV durch einen beliebigen Administrator mit entsprechenden RBAC-Funktionen aktivieren. Sobald MAV aktiviert ist, ist bei jeder Änderung der Regelsammlung die Genehmigung durch MAV erforderlich.

In ONTAP 9.11.1 können Sie Regeln für die folgenden Befehle erstellen.

`cluster peer delete`	`volume snapshot autodelete modify`
`event config modify`	`volume snapshot delete`
`security login create`	`volume snapshot policy add-schedule`
`security login delete`	`volume snapshot policy create`
`security login modify`	`volume snapshot policy delete`
`system node run`	`volume snapshot policy modify`
`system node systemshell`	`volume snapshot policy modify-schedule`
`volume delete`	`volume snapshot policy remove-schedule`
`volume flexcache delete`	`volume snapshot restore`
	`vserver peer delete`

Darüber hinaus sind die folgenden Befehle standardmäßig geschützt, wenn MAV aktiviert ist. Sie können jedoch die Regeln ändern, um den Schutz für diese Befehle zu entfernen.

- `security login password`
- `security login unlock`
- `set`

Die Regeln für MAV-System-default-Befehle – das `security multi-admin-verify` Befehle – kann nicht geändert werden.

Beim Erstellen einer Regel können Sie optional die angeben `-query` Option, um die Anforderung auf einen Teil der Befehlsfunktion zu beschränken. Beispiel: Im Befehl „Default set“ `-query` Ist auf festgelegt `-privilege diag`, Das bedeutet, dass eine Anfrage nur dann für den Befehl set generiert wird, wenn -Privilege diag angegeben ist.

```
smci-vsim20::> security multi-admin-verify rule show
                                                 Required  Approval
Vserver Operation                                Approvers Groups
------- ---------------------------------------- --------- -------------
vs01    set                                      -         -
          Query: -privilege diagnostic
```

Standardmäßig wird durch Regeln ein entsprechendes festgelegt `security multi-admin-verify request create "protected_operation"` Der Befehl wird automatisch generiert, wenn ein geschützter Vorgang eingegeben wird. Sie können diese Standardeinstellung so ändern, dass sie den erfordert `request create` Befehl separat eingegeben.

Standardmäßig erben Regeln die folgenden globalen MAV-Einstellungen, obwohl regelspezifische Ausnahmen angegeben werden können:

- Erforderliche Anzahl der Genehmiger
- Genehmigungsgruppen
- Ablauffrist der Genehmigung
- Ablauffrist der Ausführung

System Manager Verfahren

Wenn Sie zum ersten Mal eine Regel für geschützte Vorgänge hinzufügen möchten, lesen Sie die Verfahren zu System Manager nach "Aktivieren Sie die Verifizierung für mehrere Administratoren."

So ändern Sie den vorhandenen Regelsatz:

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie Auf ⚙ Neben **Multi-Admin-Genehmigung** im Abschnitt **Sicherheit**.
3. Klicken Sie Auf + Add Zum Hinzufügen von mindestens einer Regel können Sie auch vorhandene Regeln ändern oder löschen.
   - Operation – Wählen Sie einen unterstützten Befehl aus der Liste aus.
   - Abfrage – Geben Sie alle gewünschten Befehlsoptionen und Werte ein.
   - Optionale Parameter: Lassen Sie das Feld leer, um globale Einstellungen anzuwenden, oder weisen Sie einen anderen Wert für bestimmte Regeln zu, um die globalen Einstellungen zu überschreiben.
     - Erforderliche Anzahl an Genehmigern
     - Genehmigungsgruppen

CLI-Verfahren

ⓘ Alle `security multi-admin-verify rule` Befehle erfordern vor der Ausführung eine Genehmigung des MAV-Administrators außer `security multi-admin-verify rule show`.

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Erstellen Sie eine Regel	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

Ändern der Anmeldeinformationen aktueller Administratoren	`security login modify <parameters>`
	
	Beispiel: Die folgende Regel erfordert die Genehmigung, um das Root-Volume zu löschen.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0`

Regel ändern	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Löschen Sie eine Regel	`security multi-admin-verify rule delete -operation "protected_operation"`
Regeln anzeigen	`security multi-admin-verify rule show`

Details zur Befehlssyntax finden Sie im `security multi-admin-verify rule` Man-Pages.

Anforderung einer Ausführung geschützter Vorgänge

Wenn Sie einen geschützten Vorgang oder einen geschützten Befehl für ein Cluster initiieren, das für die MAV-Überprüfung (Multi-Admin Verification) aktiviert ist, fängt ONTAP den Vorgang automatisch ab und fordert zur Generierung einer Anfrage auf, die von einem oder mehreren Administratoren in einer MAV Approval Group (MAV Administrators) genehmigt werden muss. Alternativ können Sie auch eine MAV-Anfrage ohne Dialog erstellen.

Wenn die Anfrage genehmigt ist, müssen Sie die Anfrage entsprechend beantworten, um den Vorgang innerhalb der Ablauffrist des Antrags abzuschließen. Wenn ein Veto eingelegt oder die Anfrage oder die Ablauffristen überschritten werden, müssen Sie die Anfrage löschen und erneut einreichen.

Die MAV-Funktionalität berücksichtigt vorhandene RBAC-Einstellungen. Das heißt, Ihre Administratorrolle muss über ausreichende Berechtigungen verfügen, um einen geschützten Vorgang auszuführen, ohne die MAV-Einstellungen zu berücksichtigen. "Erfahren Sie mehr über RBAC".

Wenn Sie ein MAV-Administrator sind, müssen Ihre Anfragen zur Ausführung von geschützten Vorgängen auch von einem MAV-Administrator genehmigt werden.

System Manager Verfahren

Wenn ein Benutzer auf einen Menüpunkt klickt, um einen Vorgang zu starten und der Vorgang zu schützen, wird eine Anfrage zur Genehmigung generiert und der Benutzer erhält eine Benachrichtigung wie folgt:

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

Das Fenster **Multi-Admin Requests** steht zur Verfügung, wenn MAV aktiviert ist und ausstehende Anfragen basierend auf der Anmelde-ID des Benutzers und der MAV-Rolle (Genehmiger oder nicht) angezeigt werden. Für jede ausstehende Anforderung werden die folgenden Felder angezeigt:

- Betrieb
- Index (Zahl)
- Status (ausstehend, genehmigt, abgelehnt, ausgeführt oder abgelaufen)

  Wird eine Anfrage von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.

- Abfrage (alle Parameter oder Werte für die angeforderte Operation)
- Benutzer Wird Angefordert
- Die Anfrage Läuft Ab Am
- (Anzahl der ausstehenden Genehmiger
- (Anzahl der möglichen Genehmiger

Wenn die Anfrage genehmigt wird, kann der anfragende Benutzer den Vorgang innerhalb des Ablaufzeitraums wiederholen.

Wenn der Benutzer den Vorgang ohne Genehmigung erneut versucht, wird eine Benachrichtigung wie folgt angezeigt:

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

CLI-Verfahren

1. Geben Sie den geschützten Vorgang direkt oder mit dem Befehl MAV Request ein.

   Beispiele – um ein Volume zu löschen, geben Sie einen der folgenden Befehle ein:

   - `volume delete`

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
       auto-generated and requires approval.
```

- `security multi-admin-verify request create “volume delete”`

```
Error: command failed: The security multi-admin-verify request (index
3)
       requires approval.
```

2. Den Status der Anfrage überprüfen und auf die MAV-Benachrichtigung antworten.
   a. Wenn der Antrag genehmigt wird, beantworten Sie die CLI-Meldung, um den Vorgang abzuschließen.

      Beispiel:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. Wenn der Antrag gegen ein Vetos gestellt wird oder die Ablauffrist abgelaufen ist, löschen Sie die Anfrage, und senden Sie sie erneut oder wenden Sie sich an den MAV-Administrator.

Beispiel:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Managen Sie Anforderungen für geschützte Vorgänge

Wenn Administratoren einer MAV-Genehmigungsgruppe (MAV-Administratoren) über eine Anfrage zur Ausführung eines ausstehenden Vorgangs benachrichtigt werden, müssen sie innerhalb eines festgelegten Zeitraums mit einer Genehmigungs- oder Veto-Nachricht (Ablauf der Genehmigung) antworten. Wenn keine ausreichende Anzahl von Genehmigungen eingegangen ist, muss der Anfordernde die Anfrage löschen und eine andere erstellen.

Über diese Aufgabe

Genehmigungsanforderungen werden mit Indexnummern identifiziert, die in E-Mail-Nachrichten und Anzeigen der Anforderungswarteschlange enthalten sind.

Die folgenden Informationen aus der Anforderungswarteschlange können angezeigt werden:

Betrieb

Der geschützte Vorgang, für den die Anforderung erstellt wird.

Abfrage

Das Objekt (oder die Objekte), auf das der Benutzer die Operation anwenden möchte.

Bundesland

Der aktuelle Status der Anfrage; ausstehend, genehmigt, abgelehnt, abgelaufen, Ausgeführt. Wird eine Anfrage von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.

Erforderliche Genehmiger

Die Anzahl der MAV-Administratoren, die zur Genehmigung der Anfrage erforderlich sind. Ein Benutzer kann den Parameter erforderliche Genehmiger für die Operationssegel festlegen. Wenn ein Benutzer die erforderlichen Genehmiger nicht auf die Regel setzt, werden die erforderlichen Genehmiger aus der globalen Einstellung angewendet.

Ausstehende Genehmiger

Die Anzahl der MAV-Administratoren, die noch erforderlich sind, um die Anfrage zu genehmigen, die als genehmigt gekennzeichnet werden soll.

Ablauf der Genehmigung

Der Zeitraum, innerhalb dessen ein MAV-Administrator auf eine Genehmigungsanforderung reagieren muss. Jeder autorisierte Benutzer kann den Genehmigungssatz für eine Betriebsregel festlegen. Wenn für die Regel kein Genehmigungssatz festgelegt ist, wird der Genehmigungssatz aus der globalen Einstellung angewendet.

Ablauf der Ausführung

Der Zeitraum, in dem der anfordernde Administrator den Vorgang abschließen muss. Jeder autorisierte Benutzer kann das Ablaufdatum für eine Betriebsregel festlegen. Wenn für die Regel kein Ausführungs-Expiry festgelegt ist, wird das Ausführen-Expiry aus der globalen Einstellung angewendet.

Anwender genehmigt

Die MAV-Administratoren, die den Antrag genehmigt haben.

Vetoed durch den Benutzer

Die MAV-Administratoren, die den Antrag gegen das Vetos gestellt haben.

Storage-VM (vServer)

Der SVM, der die Anforderung zugeordnet ist. In dieser Version wird nur die Admin-SVM unterstützt.

Der Benutzer wurde angefordert

Der Benutzername des Benutzers, der die Anforderung erstellt hat.

Uhrzeit erstellt

Die Uhrzeit, zu der die Anfrage erstellt wurde.

Nach Genehmigung der Zeit

Die Zeit, zu der der Antragsstatus in „genehmigt“ geändert wurde.

Kommentar

Kommentare, die mit der Anfrage verknüpft sind.

Benutzer erlaubt

Die Liste der Benutzer, für die der geschützte Vorgang ausgeführt werden kann, für den die Anforderung genehmigt wird. Wenn `users-permitted` Ist leer, dann kann jeder Benutzer mit entsprechenden

Berechtigungen den Vorgang durchführen.

Alle abgelaufenen oder ausgeführten Anfragen werden gelöscht, wenn ein Limit von 1000 Anfragen erreicht wird oder wenn die abgelaufene Zeit länger als 8 Stunden für abgelaufene Anfragen ist. Vetos-Anträge werden gelöscht, sobald sie als abgelaufen markiert sind.

System Manager Verfahren

MAV-Administratoren erhalten E-Mail-Nachrichten mit Details der Genehmigungsanforderung, Ablauffrist anfordern und einen Link zum Genehmigen oder Ablehnen der Anfrage. Sie können über den Link in der E-Mail auf ein Genehmigungsdialogfeld zugreifen oder im System Manager zu **Events & Jobs>Requests** navigieren.

Das Fenster **Requests** steht zur Verfügung, wenn die Multi-Admin-Überprüfung aktiviert ist und ausstehende Anfragen basierend auf der Anmelde-ID und der MAV-Rolle des Benutzers (Genehmiger oder nicht) angezeigt werden.

- Betrieb
- Index (Zahl)
- Status (ausstehend, genehmigt, abgelehnt, ausgeführt oder abgelaufen)

  Wird eine Anfrage von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.

- Abfrage (alle Parameter oder Werte für die angeforderte Operation)
- Benutzer Wird Angefordert
- Die Anfrage Läuft Ab Am
- (Anzahl der ausstehenden Genehmiger
- (Anzahl der möglichen Genehmiger

MAV-Administratoren verfügen in diesem Fenster über zusätzliche Steuerelemente. Sie können einzelne Vorgänge oder ausgewählte Gruppen von Operationen genehmigen, ablehnen oder löschen. Wenn der MAV-Administrator jedoch der anfragende Benutzer ist, kann er seine eigenen Anforderungen nicht genehmigen, ablehnen oder löschen.

CLI-Verfahren

1. Wenn Sie über ausstehende Anfragen per E-Mail benachrichtigt werden, notieren Sie die Indexnummer der Anfrage und den Ablauf der Genehmigung. Die Indexnummer kann auch mit den unten genannten Optionen **show** oder **show-exwaring** angezeigt werden.
2. Genehmigen oder Vereinen der Anfrage.

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Genehmigen einer Anfrage	`security multi-admin-verify request approve` *nn*
Veto auf eine Anfrage	`security multi-admin-verify request veto` *nn*

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Zeigt alle Anfragen, ausstehende Anfragen oder eine einzelne Anforderung an	`security multi-admin-verify request { show
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  Sie können alle Anfragen in der Warteschlange oder nur ausstehende Anforderungen anzeigen. Wenn Sie die Indexnummer eingeben, werden nur die entsprechenden Informationen angezeigt. Sie können Informationen zu bestimmten Feldern anzeigen (mithilfe von `-fields` Parameter) oder über alle Felder (mit dem `-instance` Parameter).
Löschen Sie eine Anfrage	`security multi-admin-verify request delete` *nn*

Beispiel:

Die folgende Sequenz genehmigt einen Antrag, nachdem der MAV-Administrator die Anfrage-E-Mail mit der Indexnummer 3 erhalten hat, die bereits eine Genehmigung hat.

```
          cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

Beispiel:

Die folgende Sequenz vetoes einen Antrag, nachdem der MAV-Administrator die Anfrage-E-Mail mit der Nummer 3 erhalten hat, die bereits eine Genehmigung hat.

```
      cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```