Multi-Admin-Verifizierung verwalten

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/multi-admin-verify/index.html on November 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

Multi-Admin-Verifizierung verwalten . . . 1
- Informationen zur ONTAP Multi-Admin-Verifizierung . . . 1
  - Funktionsweise der Multi-Admin-Verifizierung . . . 1
  - Funktionsweise der Genehmigung durch mehrere Administratoren . . . 24
  - Wie die Ausführung geschützter Operationen funktioniert . . . 25
- ONTAP Administrator-Genehmigungsgruppen für MAV verwalten . . . 26
  - System Manager Verfahren . . . 27
  - CLI Prozedur . . . 28
- Multi-Admin-Verifizierung in ONTAP aktivieren oder deaktivieren . . . 30
  - System Manager Verfahren . . . 31
  - CLI Prozedur . . . 33
- Multi-Admin-Verifizierungsregeln für geschützte Vorgänge in ONTAP verwalten . . . 34
  - Regelbeschränkungen . . . 35
  - System Manager Verfahren . . . 35
  - CLI Prozedur . . . 36
  - Verfügbare durch MAV schützbare Operationen . . . 36
- Ausführung von MAV-geschützten Vorgängen in ONTAP anfordern . . . 37
  - System Manager Verfahren . . . 38
  - CLI Prozedur . . . 39
- Verwaltung von MAV geschützten Operationsanforderungen in ONTAP . . . 41

Multi-Admin-Verifizierung verwalten

Informationen zur ONTAP Multi-Admin-Verifizierung

Ab ONTAP 9.11.1 kann die Multi-Admin-Verifizierung (MAV) verwendet werden, um sicherzustellen, dass bestimmte Vorgänge, wie das Löschen von Volumes oder Snapshots, nur nach Genehmigung durch autorisierte Administratoren ausgeführt werden können. Dadurch wird verhindert, dass kompromittierte, böswillige oder unerfahrene Administratoren unerwünschte Änderungen vornehmen oder Daten löschen.

Die Konfiguration der Multi-Admin-Verifizierung umfasst Folgendes:

- "Erstellung einer oder mehrerer Administrator-Genehmigungsgruppen."
- "Aktivierung der Multi-Admin-Verifizierungsfunktion."
- "Hinzufügen oder Ändern von Regeln."

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

Wenn die Multi-Admin-Verifizierung aktiviert ist, sind für den Abschluss jeder geschützten Operation diese Schritte erforderlich:

1. Wenn ein Benutzer den Vorgang initiiert, "Eine Anfrage wird generiert."
2. Bevor die Operation ausgeführt werden kann, muss mindestens eine "Der MAV-Administrator muss zustimmen."
3. Nach der Genehmigung erhält der Benutzer eine Aufforderung und schließt den Vorgang ab.

> Falls Sie die Multi-Admin-Verifizierungsfunktion ohne Zustimmung des MAV-Administrators deaktivieren müssen, wenden Sie sich an den NetApp Support und geben Sie Folgendes an "NetApp Knowledge Base: Wie die Multi-Admin-Verifizierung deaktiviert werden kann, wenn der MAV-Administrator nicht verfügbar ist".

Die Multi-Admin-Verifizierung ist nicht für Volumes oder Workflows mit hohem Automatisierungsgrad vorgesehen, da jede automatisierte Aufgabe vor Abschluss genehmigt werden müsste. Wenn Automatisierung und MAV gemeinsam eingesetzt werden sollen, wird empfohlen, Abfragen für spezifische MAV-Operationen zu verwenden. Beispielsweise könnten `volume delete` MAV-Regeln nur auf Volumes angewendet werden, bei denen keine Automatisierung erfolgt, und diese Volumes könnten mit einem bestimmten Namensschema gekennzeichnet werden.

> Die Multi-Admin-Verifizierung ist bei Cloud Volumes ONTAP nicht verfügbar.

Funktionsweise der Multi-Admin-Verifizierung

Die Multi-Admin-Verifizierung umfasst:

- Eine Gruppe von einem oder mehreren Administratoren mit Genehmigungs- und Vetorechten.
- Eine Reihe geschützter Operationen oder Befehle in einer *Regeltabelle*.
- Eine *Regel-Engine* zur Identifizierung und Steuerung der Ausführung geschützter Operationen.

Genehmigungsgruppen unterstützen stets einzelne Administratoren. Ab ONTAP 9.20.1 können Genehmigungsgruppen auch Gruppen von Identitätsanbietern (IdP), Active Directory (AD) oder LDAP (nsswitch) umfassen. Unterstützte Gruppentypen sind Entra ID, ADFS, AD-Domänengruppen und LDAP-Gruppen. Änderungen an der Gruppenmitgliedschaft eines Benutzers im Identitätsanbieter werden beim nächsten erfolgreichen Login des Benutzers wirksam. Eine MAV Neukonfiguration ist nicht erforderlich.

MAV-Regeln werden nach rollenbasierter Zugriffssteuerung (RBAC) ausgewertet. Daher müssen Administratoren, die geschützte Operationen ausführen oder genehmigen, bereits über die minimalen RBAC-Berechtigungen für diese Operationen verfügen. "Weitere Informationen zu RBAC".

Systemdefinierte Regeln

Wenn die Multi-Admin-Verifizierung (auch als *guard-rail*-Regeln bekannt) aktiviert ist, legen systemdefinierte Regeln eine Reihe von MAV-Operationen fest, um das Risiko einer Umgehung des MAV-Prozesses selbst zu begrenzen. Diese Operationen können nicht aus der Regeltabelle entfernt werden. Sobald MAV aktiviert ist, erfordern mit einem Sternchen (*) gekennzeichnete Operationen vor der Ausführung die Genehmigung durch einen oder mehrere Administratoren, mit Ausnahme von **show**-Befehlen.

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

  Steuert die Konfiguration der Multi-Admin-Verifizierungsfunktionalität.

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

  Die Mitgliedschaft im Administratorenkreis mit Multi-Admin-Verifizierungsberechtigungen wird kontrolliert.

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

  Die Befehlsgruppe, die eine Überprüfung durch mehrere Administratoren erfordert, kann gesteuert werden.

- `security multi-admin-verify request`Operationen

  Den Genehmigungsprozess kontrollieren.

Regelgeschützte Befehle

Zusätzlich zu den systemdefinierten Operationen sind die folgenden Befehle standardmäßig geschützt, wenn die Multi-Admin-Verifizierung aktiviert ist, aber die Regeln können geändert werden, um den Schutz für diese Befehle aufzuheben:

- "security login password"
- "security login unlock"
- "Set"

Jede ONTAP Version bietet mehr Befehle, die mit Multi-Admin-Verifizierungsregeln geschützt werden können. Für die vollständige Liste der zum Schutz verfügbaren Befehle ist die jeweilige ONTAP Version auszuwählen.

9.19.1

- `cluster date modify`[3]
- `cluster log-forwarding create`[3]

- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- placement rebalance performance config modify [7]
- qos adaptive-policy-group create [7]
- qos adaptive-policy-group modify [7]
- qos adaptive-policy-group delete [7]
- qos adaptive-policy-group rename [7]
- qos policy-group create [7]
- qos policy-group modify [7]
- qos policy-group delete [7]
- qos policy-group rename [7]
- qos settings cache modify [7]
- qos settings cluster-options modify [7]
- qos settings nested-qos-svm-vol [7]
- qos settings read-ahead create [7]
- qos settings read-ahead modify [7]
- qos settings read-ahead delete [7]
- qos settings throughput-floors-v2 [7]
- qos workload modify [7]
- qos workload delete [7]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]

- security anti-ransomware volume safe-extension-list add [6]
- security anti-ransomware volume safe-extension-list remove [6]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security dynamic-authorization modify [7]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login password [6]
- security login publickey create
- security login publickey delete
- security login publickey modify
- security login unlock [6]
- security multi-admin-verify modify [6]
- security multi-admin-verify approval-group create [6]
- security multi-admin-verify approval-group delete [6]
- security multi-admin-verify approval-group modify [6]
- security multi-admin-verify approval-group replace [6]
- security multi-admin-verify rule create [6]
- security multi-admin-verify rule delete [6]
- security multi-admin-verify rule modify [6]
- security key-manager external gcp disable [7]
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security us-eo-cybersecurity modify [6]
- security webauthn credentials delete [4]
- set [6]
- snaplock legal-hold end [3]

- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume modify [3]
- volume rename [5]
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume file retention set [6]

- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot rename [6]
- volume snapshot restore [6]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver consistency-group snapshot rename [7]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]

- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.18.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]

- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware volume safe-extension-list add [6]
- security anti-ransomware volume safe-extension-list remove [6]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login password [6]
- security login publickey create
- security login publickey delete
- security login publickey modify
- security login unlock [6]
- security multi-admin-verify modify [6]
- security multi-admin-verify approval-group create [6]
- security multi-admin-verify approval-group delete [6]
- security multi-admin-verify approval-group modify [6]
- security multi-admin-verify approval-group replace [6]
- security multi-admin-verify rule create [6]
- security multi-admin-verify rule delete [6]
- security multi-admin-verify rule modify [6]
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security us-eo-cybersecurity modify [6]

- security webauthn credentials delete [4]
- set [6]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume modify [3]
- volume rename [5]
- volume encryption conversion start [4]

- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume file retention set [6]
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot rename [6]
- volume snapshot restore [6]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]

- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.17.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]

- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]

- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume rename [5]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule

- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]

- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.16.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete

- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]

- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]

- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.15.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]

- `cluster time-service ntp key delete`[3]
- `cluster time-service ntp key modify`[3]
- `cluster time-service ntp server modify`[3]
- `event config modify`
- `event config set-mail-server-password`[3]
- `lun delete`[3]
- `security anti-ransomware volume attack clear-suspect`[1]
- `security anti-ransomware volume disable`[1]
- `security anti-ransomware volume event-log modify`[2]
- `security anti-ransomware volume pause`[1]
- `security anti-ransomware vserver event-log modify`[2]
- `security audit modify`[3]
- `security ipsec config modify`[3]
- `security ipsec policy create`[3]
- `security ipsec policy delete`[3]
- `security ipsec policy modify`[3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase`[3]
- `security saml-sp create`[3]
- `security saml-sp delete`[3]
- `security saml-sp modify`[3]
- `snaplock legal-hold end`[3]
- `storage aggregate delete`[3]
- `storage encryption disk destroy`[3]
- `storage encryption disk modify`[3]
- `storage encryption disk revert-to-original-state`[3]
- `storage encryption disk sanitize`[3]
- `system bridge run-cli`[3]
- `system controller flash-cache secure-erase run`[3]

- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete

- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.14.1

- cluster peer delete
- event config modify

- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create [2]
- vserver modify [2]
- vserver peer delete

9.13.1

- cluster peer delete

- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume pause [1]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

9.12.1/9.11.1

- cluster peer delete
- event config modify
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete

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

1. Neuer regelgeschützter Befehl für 9.13.1
2. Neuer regelgeschützter Befehl für 9.14.1
3. Neuer regelgeschützter Befehl für 9.15.1
4. Neuer regelgeschützter Befehl für 9.16.1
5. Neuer regelgeschützter Befehl für 9.17.1
6. Neuer regelgeschützter Befehl für 9.18.1
7. Neuer regelgeschützter Befehl für 9.19.1

*Dieser Befehl ist nur über die CLI verfügbar und ist in einigen Versionen von System Manager nicht verfügbar.

Funktionsweise der Genehmigung durch mehrere Administratoren

Jedes Mal, wenn eine geschützte Operation auf einem MAV-geschützten Cluster eingeleitet wird, wird eine Ausführungsanforderung für die Operation an die zuständige MAV-Administratorengruppe gesendet.

Sie können Folgendes konfigurieren:

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

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

- Die Anzahl der MAV Administratorgruppen.
  - Für jede geschützte Betriebsregel ist eine MAV Gruppe zugewiesen.
  - Für mehrere MAV-Gruppen lässt sich festlegen, welche MAV-Gruppe eine bestimmte Regel genehmigt.

- Die Anzahl der MAV-Genehmigungen, die zur Durchführung eines geschützten Vorgangs erforderlich sind.
- Eine *Genehmigungsablauffrist*, innerhalb derer ein MAV-Administrator auf eine Genehmigungsanfrage reagieren muss.
- Ein Ablaufzeitraum für die Ausführung, innerhalb dessen der anfragende Administrator den Vorgang abschließen muss.

Sobald diese Parameter konfiguriert sind, ist für deren Änderung die Genehmigung durch MAV erforderlich.

MAV-Administratoren können ihre eigenen Anfragen zur Ausführung geschützter Operationen nicht genehmigen. Daher:

- MAV sollte auf Clustern mit nur einem Administrator nicht aktiviert werden.
- Wenn es in der MAV-Gruppe nur eine Person gibt, kann dieser MAV-Administrator keine geschützten Operationen initiieren; reguläre Administratoren müssen geschützte Operationen initiieren, und der MAV-Administrator kann nur genehmigen.
- Wenn MAV-Administratoren geschützte Vorgänge ausführen können sollen, ist entweder eine Genehmigungsgruppe mit mindestens einem benannten Genehmiger mehr als der Anzahl der erforderlichen Genehmigungen oder eine Genehmigungsgruppe zu konfigurieren, die Identity Provider (IdP)-, AD- oder LDAP-Gruppen umfasst. Mitglieder konfigurierter IdP-, AD- oder LDAP-Gruppen können Anfragen genehmigen, ohne einzeln als benannte Genehmiger aufgeführt zu sein. In beiden Fällen müssen neben dem anfragenden Administrator genügend berechtigte Genehmiger verfügbar sein, um die erforderlichen Genehmigungen zu erteilen.

MAV-Administratoren können Genehmigungsanfragen in E-Mail-Benachrichtigungen (über EMS) erhalten oder die Anfragewarteschlange abfragen. Wenn sie eine Anfrage erhalten, stehen ihnen drei Aktionen zur Auswahl:

- 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.
- Eine Anfrage wird genehmigt oder abgelehnt.
- Ein genehmigter Antrag wird ausgeführt.

Wenn der Antragsteller zur selben Genehmigungsgruppe für den Vorgang gehört, erhält er eine E-Mail, wenn sein Antrag genehmigt wurde.

> Ein Antragsteller kann seine eigenen Anträge nicht genehmigen, selbst wenn er Mitglied der Genehmigungsgruppe ist (obwohl er E-Mail-Benachrichtigungen für seine eigenen Anträge erhalten kann). Antragsteller, die keiner Genehmigungsgruppe angehören (das heißt, die keine MAV-Administratoren sind), erhalten keine E-Mail-Benachrichtigungen.

Wie die Ausführung geschützter Operationen funktioniert

Wird die Ausführung einer geschützten Operation genehmigt, setzt der anfragende Benutzer die Operation nach Aufforderung fort. Wird die Operation abgelehnt, muss der anfragende Benutzer die Anfrage löschen, bevor er fortfahren kann.

MAV-Regeln werden nach den RBAC-Berechtigungen ausgewertet. Daher kann ein Benutzer ohne ausreichende RBAC-Berechtigungen für die Ausführung einer Operation den MAV-Anforderungsprozess nicht initiieren.

MAV-Regeln werden vor der Ausführung des geschützten Vorgangs ausgewertet. Das bedeutet, dass die Regeln auf Basis des aktuellen Systemzustands angewendet werden. Wenn beispielsweise eine MAV-Regel für `volume modify` mit einer Abfrage von `-size 5GB` erstellt wird, erfordert die Verwendung von `volume modify` zur Größenänderung eines 5GB-Volumes auf 2GB eine MAV-Genehmigung, während die Größenänderung eines 2GB-Volumes auf 5GB keine Genehmigung erfordert.

Verwandte Informationen

- "Cluster"
- "LUN"
- "Sicherheit"
- "snaplock Legal-Hold Ende"
- "Speicheraggregat"
- "Speicherverschlüsselung"
- "System"

ONTAP Administrator-Genehmigungsgruppen für MAV verwalten

Bevor die Multi-Admin-Verifizierung (MAV) aktiviert wird, ist eine Administrator-Genehmigungsgruppe zu erstellen, die mindestens einen Administrator mit Genehmigungs- oder Vetorecht enthält. Nach der Aktivierung der Multi-Admin-Verifizierung erfordern Änderungen an der Mitgliedschaft der Genehmigungsgruppe die Zustimmung eines der bestehenden berechtigten Administratoren.

Über diese Aufgabe

Sie können bestehende Administratoren zu einer MAV Gruppe hinzufügen oder neue Administratoren erstellen.

Die MAV-Funktionalität berücksichtigt bestehende Einstellungen der rollenbasierten Zugriffssteuerung (RBAC). Potenzielle MAV-Administratoren müssen über ausreichende Berechtigungen zum Ausführen geschützter Operationen verfügen, bevor sie zu MAV-Administratorgruppen hinzugefügt werden. "Weitere Informationen zu RBAC."

Sie können MAV so konfigurieren, dass MAV-Administratoren über ausstehende Genehmigungsanfragen benachrichtigt werden. Hierfür ist die Konfiguration von E-Mail-Benachrichtigungen erforderlich, insbesondere der `Mail From` und `Mail Server` Parameter, oder diese Parameter können gelöscht werden, um die Benachrichtigung zu deaktivieren. Ohne E-Mail-Benachrichtigungen müssen MAV-Administratoren die Genehmigungswarteschlange manuell prüfen.

Ab ONTAP 9.15.1 ist es möglich, Active Directory (AD)-Benutzer als MAV-Administratoren zu konfigurieren. Der AD-Benutzer muss "Als ONTAP Administrator konfiguriert" sein.

Ab ONTAP 9.20.1 können Genehmigungsgruppen auch Identity Provider (IdP)-, Active Directory (AD)- oder LDAP (nsswitch)-Gruuppen umfassen. Zu den unterstützten Gruppentypen gehören Entra ID (ehemals Azure AD), ADFS, AD-Domänengruppen und LDAP-Gruppen.

Änderungen an der Gruppenzugehörigkeit eines Benutzers beim Identitätsanbieter werden bei der nächsten erfolgreichen Anmeldung des Benutzers wirksam. Eine Neukonfiguration von MAV ist nicht erforderlich.

Bevor Sie eine IdP-, Active Directory- oder LDAP-Gruppe zu einer MAV-Genehmigungsgruppe hinzufügen können, muss die Gruppe bereits über einen konfigurierten Anmeldezugriff verfügen und in der `security login group`Tabelle mit einer Rollenzuordnung registriert sein. Die entsprechenden Verfahren sind nachfolgend aufgeführt.

System Manager Verfahren

Wenn zum ersten Mal eine MAV-Genehmigungsgruppe erstellt werden soll, bietet die System Manager Vorgehensweise weitere Informationen zu "Multi-Admin-Verifizierung aktivieren."

Eine bestehende Genehmigungsgruppe kann geändert oder eine zusätzliche Genehmigungsgruppe erstellt werden:

1. Administratoren für den Erhalt der Multi-Admin-Verifizierung festlegen.
   a. **Cluster > Einstellungen** auswählen.
   b. Die Auswahl von → erfolgt neben **Benutzer, Gruppen und Rollen.**
   c. Unter **Users** erfolgt die Auswahl von + Add .
   d. Die Liste kann bei Bedarf angepasst werden.

      Weitere Informationen sind unter "Administratorzugriff kontrollieren." verfügbar.

2. Ab ONTAP 9.20.1 ist vor dem Hinzufügen einer IdP-, AD- oder LDAP-Gruppe als MAV-Genehmiger zunächst eine Registrierung der Gruppe erforderlich, damit in der MAV-Konfiguration auf sie verwiesen werden kann.
   a. Unter **Gruppen** erfolgt das Hinzufügen einer Gruppe über + Add .

      Eingabe des Gruppennamens. Das UUID-Feld ist nur für Microsoft Entra-Gruppen erforderlich; andere Identitätsanbieter verwenden den Gruppennamen.

   b. Unter **Gruppe-Rollen-Zuordnung** erfolgt die Auswahl von + Add und der Gruppe sowie die Zuweisung einer Rolle mit ausreichenden Berechtigungen zur Genehmigung von MAV-Anfragen.
3. MAV-Genehmigungsgruppe erstellen oder ändern:
   a. **Cluster > Einstellungen** auswählen.
   b. Wählen Sie → neben **Genehmigung durch mehrere Administratoren** im Abschnitt **Sicherheit** aus. (Das ⚙-Symbol wird angezeigt, wenn MAV noch nicht konfiguriert ist.)
      - Name: Einen Gruppennamen eingeben.
      - Genehmiger (Benutzer): Auswahl einzelner Genehmiger aus einer Benutzerliste.
      - Genehmiger (Gruppen): Ab ONTAP 9.20.1 können Sie optional eine oder mehrere registrierte IdP-, Active Directory- oder LDAP-Gruppen auswählen.
      - E-Mail-Adresse: E-Mail-Adresse(n) eingeben.
      - Standardgruppe: eine Gruppe auswählen.

Für die Bearbeitung einer bestehenden Konfiguration ist nach der Aktivierung von MAV eine MAV-Genehmigung erforderlich.

CLI Prozedur

1. Überprüfen Sie, ob für die `Mail From` und `Mail Server` Parameter Werte festgelegt wurden. Folgendes eingeben:

   `event config show`

   Die Anzeige sollte in etwa wie folgt aussehen:

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

   Zum Konfigurieren dieser Parameter wird Folgendes eingegeben:

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

   Weitere Informationen zu `event config show` und `event config modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Es sind Administratoren zu bestimmen, die an der Multi-Admin-Verifizierung teilnehmen.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben
Aktuelle Administratoren anzeigen	`security login show`
Anmeldeinformationen der aktuellen Administratoren ändern	`security login modify <parameters>`
Neue Administratorkonten erstellen	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

   Weitere Informationen zu `security login show`, `security login modify` und `security login create` in der "ONTAP-Befehlsreferenz".

3. Ab ONTAP 9.20.1 ist beim Hinzufügen einer IdP-, AD- oder LDAP-Gruppe als MAV-Genehmiger zunächst zu prüfen, ob für die Gruppe der Anmeldezugriff konfiguriert ist; anschließend ist sie für MAV zu registrieren.

   Falls für die Gruppe noch kein Anmeldezugriff konfiguriert ist, ist Folgendes einzugeben:

   `security login create -user-or-group-name` *`group_name`* `-application http|ssh -authentication-method domain|nsswitch|saml|oauth2 -role` *`role`*

   Anschließend wird die Gruppe registriert, damit in der MAV Konfiguration auf sie verwiesen und sie einer Rolle zugeordnet werden kann:

   `security login group create -vserver` *`svm_name`* `-name` *`group_name`* `[-uuid` *`uuid`*`]`

`security login group role-mapping create -group-id group_id -role role`

Der `-uuid` Parameter ist nur für Microsoft Entra ID-Gruppen erforderlich. Active Directory-Domänengruppen, ADFS/SAML-Gruppen und LDAP-(nsswitch)-Gruuppen werden nur anhand des Namens identifiziert.

Beispiel: Die folgenden Befehle registrieren die Active Directory-Gruppe `mydomain\mav_approvers` für MAV und ordnen sie der `admin` Rolle zu.

```
cluster-1::> security login group create -vserver cluster-1 -name
mydomain\mav_approvers
cluster-1::> security login group show -vserver cluster-1

     Vserver: cluster-1
  Group Name: mydomain\mav_approvers
    Group ID: 1
  Group UUID: -
     Comment: -

cluster-1::> security login group role-mapping create -group-id 1 -role
admin
```

Weitere Informationen zu `security login group create` und `security login group role-mapping create` finden sich in der "ONTAP-Befehlsreferenz".

4. Die MAV-Genehmigungsgruppe erstellen:

   `security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name [-approvers approver1[,approver2…]] [-groups group1[,group2…]] [[-email address1], address1…]`

   - `-vserver` - Nur die Admin-SVM wird in dieser Version unterstützt.
   - `-name` - Der MAV Gruppenname, maximal 64 Zeichen.
   - `-approvers` - Die Liste eines oder mehrerer einzelner Genehmiger. Für AD-Benutzer gilt das Format `domain\user`. Beispielsweise `mydomain\pavan`.
   - `-groups` - Die Liste einer oder mehrerer IdP-, AD- oder LDAP-Gruppen, die in die Genehmigungsgruppe aufgenommen werden sollen. Jede Gruppe muss bereits in der `security login group`Tabelle mit einer Rollenzuordnung registriert sein.
   - `-email` - Eine oder mehrere E-Mail-Adressen, die benachrichtigt werden, wenn eine Anfrage erstellt, genehmigt, abgelehnt oder ausgeführt wird.

     Beispiel: Der folgende Befehl erstellt eine MAV-Gruppe mit zwei einzelnen Genehmigern und einer Entra ID Gruppe.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -groups entra-group-mav-approvers -email
```

```
pavan@myfirm.com,julia@myfirm.com
```

5. Gruppenerstellung und Mitgliedschaft überprüfen:

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

   Beispiel:

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

Diese Befehle dienen zur Änderung der ursprünglichen MAV Gruppenkonfiguration.

Hinweis: Alle erfordern die Genehmigung durch den MAV-Administrator, bevor sie ausgeführt werden.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben
Gruppenmerkmale oder vorhandene Mitgliederinformationen ändern	`security multi-admin-verify approval-group modify [-vserver svm_name] -name group_name [-approvers approver1 [,approver2…]] [-groups group1[, group2…]] [[-email address1], address1… ]`
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…]] [-groups-to-add group1[,group2…]][-groups-to-remove group1[,group2…]]`
Gruppe löschen	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Multi-Admin-Verifizierung in ONTAP aktivieren oder deaktivieren

Multi-Admin-Verifizierung (MAV) muss explizit aktiviert werden. Nach der Aktivierung der

Multi-Admin-Verifizierung ist die Genehmigung durch Administratoren einer MAV-Genehmigungsgruppe (MAV-Administratoren) erforderlich, um sie zu löschen.

Über diese Aufgabe

Sobald MAV aktiviert ist, erfordert die Änderung oder Deaktivierung von MAV die Genehmigung des MAV-Administrators.

> Falls Sie die Multi-Admin-Verifizierungsfunktion ohne Zustimmung des MAV-Administrators deaktivieren müssen, wenden Sie sich an den NetApp Support und geben Sie Folgendes an "NetApp Knowledge Base: Wie die Multi-Admin-Verifizierung deaktiviert werden kann, wenn der MAV-Administrator nicht verfügbar ist".

Wenn MAV aktiviert ist, können die folgenden Parameter global festgelegt werden.

Genehmigungsgruppen

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

> Wenn MAV mit Autonomous Ransomware Protection verwendet wird, sollte eine neue oder bestehende Genehmigungsgruppe definiert werden, die für die Genehmigung von Anfragen zum Pausieren, Deaktivieren und Löschen von verdächtigem Ransomware-Schutz zuständig ist.

Erforderliche Genehmiger

Die Anzahl der Genehmiger, die zur Ausführung einer geschützten Operation erforderlich ist. Die Standard- und Mindestanzahl beträgt 1.

> Die erforderliche Anzahl an Genehmigern muss kleiner sein als die Gesamtzahl der eindeutigen Genehmiger in den Standard Genehmigungsgruppen.

Ablauf der Genehmigung (Stunden, Minuten, Sekunden)

Die Frist, innerhalb derer ein MAV-Administrator auf eine Genehmigungsanfrage reagieren muss. Der Standardwert beträgt eine Stunde (1h), der minimale unterstützte Wert ist eine Sekunde (1s), und der maximal unterstützte Wert ist 14 Tage (14d).

Ablauf der Ausführung (Stunden, Minuten, Sekunden)

Der Zeitraum, innerhalb dessen der anfragende Administrator die Operation abschließen muss. Der Standardwert beträgt eine Stunde (1h), der minimale unterstützte Wert ist eine Sekunde (1s), und der maximal unterstützte Wert ist 14 Tage (14d).

Sie können auch jeden dieser Parameter für bestimmte "Betriebsregeln." überschreiben.

System Manager Verfahren

1. Administratoren für den Erhalt der Multi-Admin-Verifizierung festlegen.
   a. **Cluster > Einstellungen** auswählen.
   b. Die Auswahl von → erfolgt neben **Benutzer, Gruppen und Rollen.**
   c. Unter **Users** erfolgt die Auswahl von + Add .
   d. Die Liste kann bei Bedarf angepasst werden.

      Weitere Informationen sind unter "Administratorzugriff kontrollieren." verfügbar.

2. Ab ONTAP 9.20.1 müssen Sie, wenn Sie eine IdP-, AD- oder LDAP-Gruppe als MAV-Genehmiger verwenden möchten, die Gruppe registrieren und einer Rolle zuordnen:
   a. Unter **Gruppen** erfolgt das Hinzufügen einer Gruppe über + Add . Das UUID-Feld ist nur für Microsoft Entra Gruppen erforderlich; andere Identitätsanbieter verwenden den Gruppennamen.
   b. Unter **Gruppe-Rollen-Zuordnung** erfolgt die Auswahl von + Add und der Gruppe sowie die Zuweisung einer Rolle mit ausreichenden Berechtigungen zur Genehmigung von MAV-Anfragen.
3. Die Multi-Admin-Verifizierung wird aktiviert, indem mindestens eine Genehmigungsgruppe erstellt und mindestens eine Regel hinzugefügt wird.
   a. **Cluster > Einstellungen** auswählen.
   b. Wählen Sie neben **Genehmigung durch mehrere Administratoren** im Abschnitt **Sicherheit** aus.
   c. Über + Add lässt sich mindestens eine Genehmigungsgruppe hinzufügen.
      - Name – Ein Gruppenname wird eingegeben.
      - Genehmiger (Benutzer): Auswahl von Genehmigern aus einer Liste von Benutzern.
      - Genehmiger (Gruppen) – Ab ONTAP 9.20.1 ist optional die Auswahl einer oder mehrerer registrierter IdP-, AD- oder LDAP-Gruppen möglich.
      - E-Mail-Adresse – E-Mail-Adresse(n) eingeben.
      - Standardgruppe – Eine Gruppe auswählen.
   d. Fügen Sie mindestens eine Regel hinzu.
      - Betrieb – Ein unterstützter Befehl aus der Liste kann ausgewählt werden.
      - Abfrage – Beliebige gewünschte Befehlsoptionen und Werte eingeben.
      - Optionale Parameter; leer lassen, um die globalen Einstellungen anzuwenden, oder einen anderen Wert für spezifische Regeln zuweisen, um die globalen Einstellungen zu überschreiben.
        - Erforderliche Anzahl an Genehmigern
        - Genehmigungsgruppen
   e. Mit **Erweiterte Einstellungen** können die Standardeinstellungen angezeigt oder geändert werden.
      - Erforderliche Anzahl an Genehmigern (Standard: 1)
      - Ablauf der Ausführungsanforderung (Standard: 1 Stunde)
      - Ablauf der Genehmigungsanfrage (Standard: 1 Stunde)
      - Mailserver*
      - Von E-Mail-Adresse*

      *Diese Einstellungen aktualisieren die E-Mail-Einstellungen, die unter „Benachrichtigungsverwaltung“ verwaltet werden. Eine Aufforderung zur Festlegung erfolgt, falls sie noch nicht konfiguriert wurden.
   f. Zum Abschließen der MAV Erstkonfiguration ist **Aktivieren** auszuwählen.

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 bestehende Konfiguration anzeigen, indem Sie → auswählen. Zum Bearbeiten einer bestehenden Konfiguration ist eine MAV Genehmigung erforderlich.

Deaktivieren der Multi-Admin-Verifizierung:

1. **Cluster > Einstellungen** auswählen.
2. Wählen Sie ⚙ neben **Genehmigung durch mehrere Administratoren** im Abschnitt **Sicherheit** aus.
3. Es ist die Umschaltfläche „Enabled“ auszuwählen.

   Für die Durchführung dieses Vorgangs ist eine MAV-Genehmigung erforderlich.

CLI Prozedur

Bevor die MAV-Funktionalität über die CLI aktiviert werden kann, muss mindestens ein "MAV Administratorgruppe" erstellt worden sein.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben

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: Der folgende Befehl aktiviert MAV mit 1 Genehmigungsgruppe, 2 erforderlichen Genehmigern und Standardablaufzeiten.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Die Erstkonfiguration wird abgeschlossen, indem mindestens ein "Betriebsregel." hinzugefügt wird

Eine MAV Konfiguration ändern (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]]`

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben

MAV-Funktionalität verifizieren	`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 (erfordert MAV-Genehmigung)	`security multi-admin-verify modify -enabled false`

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Multi-Admin-Verifizierungsregeln für geschützte Vorgänge in ONTAP verwalten

Sie erstellen Regeln zur Verifizierung durch mehrere Administratoren (MAV), um Vorgänge zu kennzeichnen, die eine Genehmigung erfordern. Immer wenn ein Vorgang initiiert wird, werden geschützte Vorgänge abgefangen und eine Genehmigungsanfrage erstellt.

Regeln können vor der Aktivierung von MAV von jedem Administrator mit entsprechenden RBAC-Funktionen erstellt werden, aber sobald MAV aktiviert ist, erfordert jede Änderung am Regelsatz die Genehmigung durch MAV.

Pro Operation kann nur eine MAV-Regel erstellt werden; beispielsweise können nicht mehrere `volume-snapshot-delete` Regeln erstellt werden. Alle gewünschten Regelbeschränkungen müssen in einer einzigen Regel enthalten sein.

Sie können Regeln zum Schutz von "diese Befehle" erstellen. Jeder Befehl kann ab der ONTAP Version geschützt werden, in der die Schutzfunktion für den jeweiligen Befehl erstmals verfügbar war.

Die Regeln für die MAV-Systemstandardbefehle, die `security multi-admin-verify` "Befehle", können nicht geändert werden.

Zusätzlich zu den systemdefinierten Operationen sind die folgenden Befehle standardmäßig geschützt, wenn die Multi-Admin-Verifizierung aktiviert ist, aber die Regeln können geändert werden, um den Schutz für diese Befehle aufzuheben:

- "security login password"
- "security login unlock"
- "Set"

Regelbeschränkungen

Beim Erstellen einer Regel kann optional die `-query` Option angegeben werden, um die Anfrage auf eine Teilmenge der Befehlsfunktionalität zu beschränken. Die `-query` Option kann ebenfalls verwendet werden, um Konfigurationselemente wie die SVM, das Volume und Snapshot-Namen einzuschränken.

Beispielsweise kann im `volume snapshot delete` Befehl `-query` auf `-snapshot !hourly*,!daily*,!weekly*` gesetzt werden, was bedeutet, dass Volume-Snapshots mit dem Präfix „hourly“, „daily“ oder „weekly“ vom MAV-Schutz ausgeschlossen werden.

```
smci-vsim20::> security multi-admin-verify rule show
                                                Required  Approval
Vserver Operation                               Approvers Groups
------- --------------------------------------- --------- -------------
vs01    volume snapshot delete                  -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

Ausgeschlossene Konfigurationselemente wären durch MAV nicht geschützt, und jeder Administrator könnte sie löschen oder umbenennen.

Standardmäßig ist festgelegt, dass ein entsprechender `security multi-admin-verify request create "protected_operation"` Befehl automatisch generiert wird, wenn eine geschützte Operation aufgerufen wird. Diese Standardeinstellung kann so geändert werden, dass der `request create` Befehl separat eingegeben werden muss.

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

- Erforderliche Anzahl an Genehmigern
- Genehmigungsgruppen
- Ablaufzeitraum der Genehmigung
- Ablaufzeitraum für die Ausführung

System Manager Verfahren

Wenn zum ersten Mal eine Regel für geschützte Vorgänge hinzugefügt werden soll, bietet die System Manager-Vorgehensweise weitere Informationen zu "Multi-Admin-Verifizierung aktivieren."

Das bestehende Regelwerk kann wie folgt geändert werden:

1. **Cluster > Einstellungen** auswählen.
2. Wählen Sie neben **Genehmigung durch mehrere Administratoren** im Abschnitt **Sicherheit** aus.
3. Wählen Sie + Add, um mindestens eine Regel hinzuzufügen; Sie können auch bestehende Regeln

ändern oder löschen.

- Betrieb – Ein unterstützter Befehl aus der Liste kann ausgewählt werden.
- Abfrage – Beliebige gewünschte Befehlsoptionen und Werte eingeben.
- Optionale Parameter – Leer lassen, um die globalen Einstellungen anzuwenden, oder für bestimmte Regeln einen anderen Wert zuweisen, um die globalen Einstellungen zu überschreiben.
  - Erforderliche Anzahl an Genehmigern
  - Genehmigungsgruppen

CLI Prozedur

Alle `security multi-admin-verify rule`Befehle erfordern vor ihrer Ausführung die Genehmigung durch den MAV-Administrator, außer `security multi-admin-verify rule show`.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben
Regel erstellen	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [-approval-groups group1[,group2…]] [parameters]`

Anmeldeinformationen der aktuellen Administratoren ändern	`security login modify <parameters>`
	
	Beispiel: Die folgende Regel erfordert eine Genehmigung zum Löschen des Root Volume.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`
	
	Mit dem `-approval-groups` Parameter lassen sich eine oder mehrere MAV-Genehmigungsgruppen für diese Regel angeben, wodurch die globale Genehmigungsgruppeneinstellung nur für diesen Vorgang überschrieben wird.

Eine Regel ändern	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Eine Regel löschen	`security multi-admin-verify rule delete -operation "protected_operation"`
Regeln anzeigen	`security multi-admin-verify rule show`
Alle verfügbaren MAV-geschützten Operationen	`security multi-admin-verify registered-operations show`

Verfügbare durch MAV schützbare Operationen

Ab ONTAP 9.20.1 können Sie alle Operationen anzeigen, die im aktuellen Cluster durch MAV geschützt werden können. Dies erleichtert die Erstellung einer Regel, ohne externe Dokumentation zur Ermittlung

gültiger Operationsnamen konsultieren zu müssen.

```
security multi-admin-verify registered-operations show
```

Beispiel:

```
cluster1::> security multi-admin-verify registered-operations show
Operation
----------------------------------------
cluster peer delete
security login delete
security login modify
volume delete
volume move start
volume snapshot delete
...
```

Die Liste der Operationen variiert je nach ONTAP Version und Cluster-Persönlichkeit.

Sie können die Ausgabe anhand des Operationsnamens mithilfe des Parameters `-operation` filtern, einschließlich des Abgleichs mit Platzhaltern.

Beispiel:

```
cluster1::> security multi-admin-verify registered-operations show
-operation security*
Operation
---------------------------------
security anti-ransomware volume attack clear-suspect
security anti-ransomware volume disable
security anti-ransomware volume event-log modify
security audit modify
security login delete
...
```

Verwandte Informationen

- "Regel für die Multi-Admin-Verify-Sicherheit"
- "security login modify"

Ausführung von MAV-geschützten Vorgängen in ONTAP anfordern

Wenn ein geschützter Vorgang oder Befehl auf einem Cluster mit aktivierter Multi-Admin-Verifizierung (MAV) initiiert wird, fängt ONTAP den Vorgang automatisch ab und fordert die Generierung einer Anfrage an, die von einem oder mehreren Administratoren einer

MAV-Genehmigungsgruppe (MAV-Administratoren) genehmigt werden muss. Alternativ ist es möglich, eine MAV-Anfrage ohne den Dialog zu erstellen.

Wird der Antrag genehmigt, ist innerhalb der Antragsfrist auf die Anfrage zu antworten, um den Vorgang abzuschließen. Wird der Antrag abgelehnt oder sind die Antrags- oder Ablauffristen überschritten, ist der Antrag zu löschen und erneut einzureichen.

Die MAV-Funktionalität berücksichtigt bestehende RBAC-Einstellungen. Das heißt, Ihre Administratorrolle muss über ausreichende Berechtigungen verfügen, um einen geschützten Vorgang unabhängig von den MAV-Einstellungen auszuführen. "Weitere Informationen zu RBAC".

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

System Manager Verfahren

Wenn ein Benutzer auf einen Menüpunkt klickt, um eine Operation auszulösen und die Operation geschützt ist, wird eine Genehmigungsanfrage generiert und der Benutzer erhält eine Benachrichtigung, die in etwa wie folgt aussieht:

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

Das Fenster **Anfragen mehrerer Administratoren** ist verfügbar, wenn MAV aktiviert ist und zeigt ausstehende Anfragen basierend auf der Anmelde-ID des Benutzers und der MAV-Rolle (Genehmiger oder nicht) an. Für jede ausstehende Anfrage werden die folgenden Felder angezeigt:

- Betrieb
- Index (Nummer)
- Status (Ausstehend, Genehmigt, Abgelehnt, Ausgeführt oder Abgelaufen)

  Wird ein Antrag von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.
- Abfrage (beliebige Parameter oder Werte für die angeforderte Operation)
- Anfordernder Benutzer
- Anfrage läuft am
- (Anzahl der) ausstehenden Genehmiger
- (Anzahl) potenzieller Genehmiger

Wenn die Anfrage genehmigt wird, kann der anfragende Benutzer den Vorgang innerhalb der Ablauffrist erneut ausführen.

Wenn der Benutzer den Vorgang ohne Genehmigung wiederholt, wird eine Benachrichtigung ähnlich der folgenden angezeigt:

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

CLI Prozedur

1. Die geschützte Operation kann direkt oder mit dem MAV-Anforderungsbefehl ausgeführt werden.

   Beispiele: Zum Löschen eines Volumes kann einer der folgenden Befehle verwendet werden:

   - `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. Der Status der Anfrage und die Antwort auf die MAV-Mitteilung werden geprüft.

   a. Wenn die Anfrage genehmigt wird, erfolgt eine Antwort auf die CLI-Nachricht, 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. Wird der Antrag abgelehnt oder ist die Frist abgelaufen, sollte der Antrag gelöscht und entweder erneut eingereicht oder der MAV-Administrator kontaktiert werden.

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".
```

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Verwaltung von MAV geschützten Operationsanforderungen in ONTAP

Wenn Administratoren in einer MAV-Genehmigungsgruppe (MAV-Administratoren) über eine ausstehende Ausführungsanfrage benachrichtigt werden, müssen sie innerhalb einer festgelegten Frist (Ablauf der Genehmigung) mit einer Genehmigungs- oder Ablehnungsnachricht antworten. Wenn nicht genügend Genehmigungen eingehen, muss der Anfragende die Anfrage löschen und eine neue stellen.

Über diese Aufgabe

Genehmigungsanfragen werden mit Indexnummern gekennzeichnet, die in E-Mail-Nachrichten und in der Anzeige der Anfragewarteschlange enthalten sind.

`multi-admin-verify`Anfragen im Endstatus können automatisch überschrieben oder entfernt werden. Die "Revisionsprotokoll" kann zur Überprüfung vorheriger Anfragen verwendet werden.

Ab ONTAP 9.20.1 können Mitglieder einer konfigurierten Genehmigergruppe für IdP, AD oder LDAP Anfragen genehmigen oder ablehnen, ohne als namentlich genannte Genehmiger aufgeführt zu sein. Änderungen an der Gruppenzugehörigkeit eines Benutzers im Identitätsanbieter werden bei der nächsten erfolgreichen Anmeldung des Benutzers wirksam. Eine Neukonfiguration von MAV ist nicht erforderlich.

Folgende Informationen aus der Anfragewarteschlange können angezeigt werden:

Betrieb
: Die geschützte Operation, für die die Anfrage erstellt wird.

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

Status
: Der aktuelle Status des Antrags: ausstehend, genehmigt, abgelehnt, abgelaufen, ausgeführt. Wird ein Antrag von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.

Erforderliche Genehmiger
: Die Anzahl der MAV-Administratoren, die die Anfrage genehmigen müssen. Ein Benutzer kann den

Parameter required-approvers für die Vorgangsregel festlegen. Wenn ein Benutzer required-approvers für die Regel nicht festlegt, wird der Wert required-approvers aus der globalen Einstellung angewendet.

Ausstehende Genehmiger

Die Anzahl der MAV-Administratoren, die noch erforderlich sind, um die Anfrage zu genehmigen, damit die Anfrage als genehmigt markiert wird.

Potenzielle Genehmigergruppen

Ab ONTAP 9.20.1 sind dies die IdP-, Active Directory- oder LDAP-Gruppen, deren Mitglieder berechtigt sind, die Anfrage zu genehmigen oder abzulehnen.

Ablauf der Genehmigung

Die Frist, innerhalb derer ein MAV-Administrator auf eine Genehmigungsanfrage reagieren muss. Jeder autorisierte Benutzer kann die Genehmigungsfrist für eine Vorgangsregel festlegen. Ist keine Genehmigungsfrist für die Regel festgelegt, wird die Genehmigungsfrist aus der globalen Einstellung angewendet.

Ablauf der Ausführung

Der Zeitraum, innerhalb dessen der anfragende Administrator den Vorgang abschließen muss. Jeder autorisierte Benutzer kann das Ausführungsablaufdatum für eine Vorgangsregel festlegen. Wenn kein Ausführungsablaufdatum für die Regel festgelegt ist, wird das Ausführungsablaufdatum aus der globalen Einstellung übernommen.

Genehmigte Nutzer

Die MAV-Administratoren, die den Antrag genehmigt haben.

Benutzer hat sein Veto eingelegt

Die MAV-Administratoren, die den Antrag abgelehnt haben.

Storage VM (vserver)

Die SVM, der die Anfrage zugeordnet ist. In dieser Version wird nur die admin SVM unterstützt.

Benutzeranfrage

Der Benutzername des Benutzers, der die Anfrage erstellt hat.

Erstellungszeit

Der Zeitpunkt, zu dem die Anfrage erstellt wurde.

Genehmigungszeit

Der Zeitpunkt, zu dem sich der Status der Anfrage auf „genehmigt“ geändert hat.

Kommentar

Alle Kommentare, die mit der Anfrage in Verbindung stehen.

Zugelassene Benutzer

Die Liste der Benutzer, die berechtigt sind, die geschützte Operation durchzuführen, für die die Anfrage genehmigt wurde. Wenn `users-permitted`leer ist, kann jeder Benutzer mit den entsprechenden Berechtigungen die Operation durchführen.

System Manager

MAV-Administratoren erhalten E-Mails mit Details zur Genehmigungsanfrage, deren Gültigkeitsdauer und

einem Link zur Genehmigung oder Ablehnung der Anfrage. Sie können den Genehmigungsdialog über den Link in der E-Mail aufrufen oder in System Manager zu **Events & Jobs > Multi-Admin Requests** navigieren.

Das Fenster **Multi-Admin Requests** ist verfügbar, wenn die Multi-Admin-Verifizierung aktiviert ist, und zeigt ausstehende Anfragen basierend auf der Anmelde-ID des Benutzers und der MAV-Rolle (Genehmiger oder nicht) an. Mit **My Approvals** werden nur die Anfragen aufgelistet, für die der angemeldete Benutzer berechtigt ist zu handeln, einschließlich Anfragen, die über die Mitgliedschaft in einer IdP-, Active Directory- oder LDAP-Genehmigergruppe verfügbar sind.

- Betrieb
- Index (Nummer)
- Status (Ausstehend, Genehmigt, Abgelehnt, Ausgeführt oder Abgelaufen)

  Wird ein Antrag von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.
- Abfrage (beliebige Parameter oder Werte für die angeforderte Operation)
- Anfordernder Benutzer
- Anfrage läuft am
- (Anzahl der) ausstehenden Genehmiger
- Potenzielle Genehmiger (ab ONTAP 9.20.1 umfasst dies Benutzer, die als benannte Genehmiger oder durch Mitgliedschaft in einer berechtigten IdP-, Active Directory- oder LDAP-Genehmigergruppe infrage kommen)

MAV-Administratoren verfügen in diesem Fenster über zusätzliche Steuerungsmöglichkeiten; sie können einzelne Vorgänge oder ausgewählte Gruppen von Vorgängen genehmigen, ablehnen oder löschen. Wenn der MAV-Administrator jedoch der Requesting User ist, kann er seine eigenen Anfragen nicht genehmigen, ablehnen oder löschen.

CLI

1. Wenn Sie per E-Mail über ausstehende Anfragen benachrichtigt werden, sollten Sie die Indexnummer und die Gültigkeitsdauer der Genehmigung der Anfrage beachten. Die Indexnummer kann auch mithilfe der Optionen **show** oder **show-pending** in der folgenden Tabelle angezeigt werden.
2. Den Antrag genehmigen oder ablehnen.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben
Eine Anfrage genehmigen	`security multi-admin-verify request approve` *nn*
Einen Antrag ablehnen	`security multi-admin-verify request veto` *nn*
Alle Anfragen, ausstehende Anfragen oder eine einzelne Anfrage anzeigen	`security multi-admin-verify request { show

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  Sie können alle Anfragen in der Warteschlange oder nur ausstehende Anfragen anzeigen. Bei Eingabe der Indexnummer werden nur die Informationen dazu angezeigt. Informationen zu bestimmten Feldern (mithilfe des `-fields` Parameters) oder zu allen Feldern (mithilfe des `-instance` Parameters) können angezeigt werden.
Eine Anfrage löschen	`security multi-admin-verify request delete` *nn*

Beispiel:

Die folgende Sequenz genehmigt eine Anfrage, 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
Potential Approver Groups: entra-group-mav-approvers
   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: -
```

Ab ONTAP 9.20.1 enthält der `security multi-admin-verify request show` Befehl ein `Potential Approver Groups` Feld, in dem alle IdP-, AD- oder LDAP-Gruppen aufgeführt sind, deren Mitglieder berechtigt sind, die Anfrage zu genehmigen oder abzulehnen.

Beispiel:

Die folgende Sequenz legt ein Veto gegen eine Anfrage ein, 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         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: -
```

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

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.