Manage multi-admin verification

ONTAP 9

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap/multi-admin-verify/index.html on November 13, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Manage multi-admin verification . . . 1
Learn about ONTAP multi-admin verification . . . 1
How multi-admin verification works . . . 1
How multi-admin approval works . . . 24
How protected operation execution works . . . 25
Manage ONTAP administrator approval groups for MAV . . . 26
System Manager procedure . . . 26
CLI procedure . . . 27
Enable or disable multi-admin verification in ONTAP . . . 30
System Manager procedure . . . 31
CLI procedure . . . 32
Manage multi-admin verification rules for protected operations in ONTAP . . . 34
Rule constraints . . . 34
System Manager procedure . . . 35
CLI procedure . . . 35
View available MAV-protectable operations . . . 36
Request execution of MAV protected operations in ONTAP . . . 37
System Manager procedure . . . 37
CLI procedure . . . 38
Manage MAV protected operation requests in ONTAP . . . 40

Manage multi-admin verification

Learn about ONTAP multi-admin verification

Beginning with ONTAP 9.11.1, you can use multi-admin verification (MAV) to ensure that certain operations, such as deleting volumes or snapshots, can be executed only after approvals from designated administrators. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data.

Configuring multi-admin verification consists of:

- Creating one or more administrator approval groups.
- Enabling multi-admin verification functionality.
- Adding or modifying rules.

After initial configuration, these elements can be modified only by administrators in a MAV approval group (MAV administrators).

When multi-admin verification is enabled, the completion of every protected operation requires these steps:

1. When a user initiates the operation, a request is generated.
2. Before the operation can be executed, at least one MAV administrator must approve.
3. Upon approval, the user is prompted and completes the operation.

If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following NetApp Knowledge Base: How to disable Multi-Admin Verification if MAV admin is unavailable.

Multi-admin verification is not intended for use with volumes or workflows that involve heavy automation, because each automated task would require approval before the operation could be completed. If you want to use automation and MAV together, it's recommended that you use queries for specific MAV operations. For example, you could apply `volume delete` MAV rules only to volumes where automation is not involved, and you could designate those volumes with a particular naming scheme.

Multi-admin verification is not available with Cloud Volumes ONTAP.

How multi-admin verification works

Multi-admin verification consists of:

- A group of one or more administrators with approval and veto powers.
- A set of protected operations or commands in a *rules table*.
- A *rules engine* to identify and control execution of protected operations.

Approval groups always support individual administrators. Beginning with ONTAP 9.20.1, approval groups can also include identity provider (IdP), Active Directory (AD), or LDAP (nsswitch) groups. Supported group types include Entra ID, ADFS, AD domain groups, and LDAP groups. Changes to a user's group membership in the identity provider take effect upon

the user's next successful login. No MAV reconfiguration is required.

MAV rules are evaluated after role-based access control (RBAC) rules. Therefore, administrators who execute or approve protected operations must already possess the minimum RBAC privileges for those operations. Learn more about RBAC.

System-defined rules

When multi-admin verification is enabled, system-defined rules (also known as *guard-rail* rules) establish a set of MAV operations to contain the risk of circumventing the MAV process itself. These operations cannot be removed from the rules table. Once MAV is enabled, operations designated by an asterisk (*) require approval by one or more administrators before execution, except for **show** commands.

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

  Controls the configuration of multi-admin verification functionality.

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

  Control membership in the set of administrators with multi-admin verification credentials.

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

  Control the set of commands requiring multi-admin verification.

- `security multi-admin-verify request` operations

  Control the approval process.

Rule-protected commands

In addition to system-defined operations, the following commands are protected by default when multi-admin verification is enabled, but you can modify the rules to remove protection for these commands:

- security login password
- security login unlock
- set

Each ONTAP version provides more commands you can choose to protect with multi-admin verification rules. Choose your ONTAP release for the full list of commands available for protection.

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. New rule-protected command for 9.13.1
2. New rule-protected command for 9.14.1
3. New rule-protected command for 9.15.1
4. New rule-protected command for 9.16.1
5. New rule-protected command for 9.17.1
6. New rule-protected command for 9.18.1
7. New rule-protected command for 9.19.1

*This command is only available with CLI and is unavailable for System Manager in some releases.

How multi-admin approval works

Any time a protected operation is entered on a MAV-protected cluster, an operation execution request is sent to the designated MAV administrator group.

You can configure:

- The names, contact information, and number of administrators in the MAV group.

  A MAV administrator should have an RBAC role with cluster administrator privileges.

- The number of MAV administrator groups.
  - A MAV group is assigned for each protected operation rule.
  - For multiple MAV groups, you can configure which MAV group approves a given rule.
- The number of MAV approvals required to execute a protected operation.
- An *approval expiry* period within which a MAV administrator must respond to an approval request.
- An *execution expiry* period within which the requesting administrator must complete the operation.

Once these parameters are configured, MAV approval is required to modify them.

MAV administrators cannot approve their own requests to execute protected operations. Therefore:

- MAV should not be enabled on clusters with only one administrator.
- If there is only one person in the MAV group, that MAV administrator cannot initiate protected operations; regular administrators must initiate protected operations, and the MAV administrator can only approve.
- If you want MAV administrators to be able to execute protected operations, configure either an approval group with at least one more named approver than the number of required approvals, or an approval group that includes identity provider (IdP), AD, or LDAP groups. Members of configured IdP, AD, or LDAP groups can approve requests without being listed individually as named approvers. In either case, enough eligible approvers other than the requesting administrator must be available to provide the required approvals.

MAV administrators can receive approval requests in email alerts (using EMS) or they can query the request queue. When they receive a request, they can take one of three actions:

- Approve
- Reject (veto)
- Ignore (no action)

Email notifications are sent to all approvers associated with a MAV rule when:

- A request is created.
- A request is approved or vetoed.
- An approved request is executed.

If the requestor is in the same approval group for the operation, they will receive an email when their request is approved.

A requestor can't approve their own requests even if they are in the approval group (although they can get email notifications for their own requests). Requestors who are not in approval groups (that is, who are not MAV administrators) don't receive email notifications.

How protected operation execution works

If execution is approved for a protected operation, the requesting user continues with the operation when prompted. If the operation is vetoed, the requesting user must delete the request before proceeding.

MAV rules are evaluated after RBAC permissions. As a result, a user without sufficient RBAC permissions for operation execution cannot initiate the MAV request process.

MAV rules are evaluated before the protected operation is executed. This means that rules are enforced based on the current state of the system. For example, if a MAV rule is created for `volume modify` with a query of `-size 5GB`, using `volume modify` to resize a 5GB volume to 2GB will require MAV approval, but resizing a 2GB volume to 5GB will not.

Related information

- cluster
- lun
- security
- snaplock legal-hold end

- storage aggregate
- storage encryption
- system

Manage ONTAP administrator approval groups for MAV

Before enabling multi-admin verification (MAV), you must create an admin approval group containing one or more administrators to be granted approve or veto authority. Once you have enabled multi-admin verification, any modifications to approval group membership requires approval from one of the existing qualified administrators.

About this task

You can add existing administrators to a MAV group or create new administrators.

MAV functionality honors existing role-based access control (RBAC) settings. Potential MAV administrators must have sufficient privilege to execute protected operations before they are added to MAV administrator groups. Learn more about RBAC.

You can configure MAV to alert MAV administrators that approval requests are pending. To do so, you must configure email notifications—in particular, the `Mail From` and `Mail Server` parameters—or you can clear these parameters to disable notification. Without email alerts, MAV administrators must check the approval queue manually.

Beginning with ONTAP 9.15.1, you can configure Active Directory (AD) users as MAV administrators. The AD user must be configured as an ONTAP administrator.

Beginning with ONTAP 9.20.1, approval groups can also include identity provider (IdP), Active Directory (AD), or LDAP (nsswitch) groups. Supported group types include Entra ID (formerly Azure AD), ADFS, AD domain groups, and LDAP groups.

Changes to a user's group membership in the identity provider take effect upon the user's next successful login. No MAV reconfiguration is required.

> Before you can add an IdP, AD, or LDAP group to a MAV approval group, the group must already have login access configured and must be registered in the `security login group` table with a role mapping. See the following procedures.

System Manager procedure

If you want to create a MAV approval group for the first time, see the System Manager procedure to enable multi-admin verification.

To modify an existing approval group or create an additional approval group:

1. Identify administrators to receive multi-admin verification.
   a. Select **Cluster > Settings.**
   b. Select → next to **Users, groups, and roles.**
   c. Select + Add under **Users.**
   d. Modify the roster as needed.

For more information, see Control administrator access.

2. Beginning with ONTAP 9.20.1, if you want to add an IdP, AD, or LDAP group as a MAV approver, first register the group so it can be referenced in the MAV configuration.
   a. Under **Groups**, select + Add to add a group.

      Enter the group name. The UUID field is required only for Microsoft Entra groups; other identity providers use the group name.

   b. Under **Group to role mapping**, select + Add , select the group, and assign a role with sufficient privileges to approve MAV requests.
3. Create or modify the MAV approval group:
   a. Select **Cluster > Settings.**
   b. Select → next to **Multi-Admin Approval** in the **Security** section. (You will see the ⚙ icon if MAV is not yet configured.)
      - Name: enter a group name.
      - Approvers (users): select individual approvers from a list of users.
      - Approvers (groups): beginning with ONTAP 9.20.1, optionally select one or more registered IdP, AD, or LDAP groups.
      - Email address: enter email address(es).
      - Default group: select a group.

MAV approval is required to edit an existing configuration once MAV is enabled.

CLI procedure

1. Verify that values have been set for the `Mail From` and `Mail Server` parameters. Enter:

   `event config show`

   The display should be similar to the following:

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

   To configure these parameters, enter:

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

   Learn more about `event config show` and `event config modify` in the ONTAP command reference.

2. Identify administrators to participate in multi-admin verification.

If you want to…	Enter this command
Display current administrators	`security login show`
Modify credentials of current administrators	`security login modify <parameters>`
Create new administrator accounts	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

Learn more about `security login show`, `security login modify`, and `security login create` in the ONTAP command reference.

3. Beginning with ONTAP 9.20.1, if you want to add an IdP, AD, or LDAP group as a MAV approver, confirm the group has login access configured, then register it for MAV.

   If the group does not already have login access configured, enter:

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

   Then register the group so it can be referenced in the MAV configuration, and map it to a role:

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

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

   The `-uuid` parameter is required only for Microsoft Entra ID groups. AD domain, ADFS/SAML, and LDAP (nsswitch) groups are identified by name only.

   Example: The following commands register the AD group `mydomain\mav_approvers` for MAV and map it to the `admin` role.

   ```
   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
   ```

   Learn more about `security login group create` and `security login group role-mapping create` in the ONTAP command reference.

4. Create the MAV approval group:

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

- `-vserver` - Only the admin SVM is supported in this release.
- `-name` - The MAV group name, up to 64 characters.
- `-approvers` - The list of one or more individual approvers. For AD users, use the format `domain\user`. For example, `mydomain\pavan`.
- `-groups` - The list of one or more IdP, AD, or LDAP groups to include in the approval group. Each group must already be registered in the `security login group` table with a role mapping.
- `-email` - One or more email addresses that are notified when a request is created, approved, vetoed, or executed.

  Example: The following command creates a MAV group with two individual approvers and one Entra ID group.

  ```
  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. Verify group creation and membership:

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

   Example:

   ```
   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
   ```

Use these commands to modify your initial MAV group configuration.

Note: All require MAV administrator approval before execution.

If you want to…	Enter this command
Modify the group characteristics or modify existing member information	`security multi-admin-verify approval-group modify [-vserver svm_name] -name group_name [-approvers approver1 [,approver2…]] [-groups group1[, group2…]] [[-email address1], address1… ]`
Add or remove members	`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…]]`
Delete a group	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

Related information

- security multi-admin-verify

Enable or disable multi-admin verification in ONTAP

Multi-admin verification (MAV) must be enabled explicitly. Once you have enabled multi-admin verification, approval by administrators in a MAV approval group (MAV administrators) is required to delete it.

About this task

Once MAV is enabled, modifying or disabling MAV requires MAV administrator approval.

If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following NetApp Knowledge Base: How to disable Multi-Admin Verification if MAV admin is unavailable.

When you enable MAV, you can specify the following parameters globally.

Approval groups

A list of global approval groups. At least one group is required to enable MAV functionality.

If you are using MAV with Autonomous Ransomware Protection, define a new or existing approval group that is responsible for approving ransomware protection pause, disable, and clear suspect requests.

Required approvers

The number of approvers required to execute a protected operation. The default and minimum number is 1.

The required number of approvers must be less than the total number of unique approvers in the default approval groups.

Approval expiry (hours, minutes, seconds)

The period within which a MAV administrator must respond to an approval request. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).

Execution expiry (hours, minutes, seconds)

The period within which the requesting administrator must complete the:: operation. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).

You can also override any of these parameters for specific operation rules.

System Manager procedure

1. Identify administrators to receive multi-admin verification.
   a. Select **Cluster > Settings.**
   b. Select → next to **Users, groups, and roles.**
   c. Select + Add under **Users.**
   d. Modify the roster as needed.

      For more information, see Control administrator access.
2. Beginning with ONTAP 9.20.1, if you want to use an IdP, AD, or LDAP group as a MAV approver, register the group and map it to a role:
   a. Under **Groups**, select + Add to add a group. The UUID field is required only for Microsoft Entra groups; other identity providers use the group name.
   b. Under **Group to role mapping**, select + Add , select the group, and assign a role with sufficient privileges to approve MAV requests.
3. Enable multi-admin verification by creating at least one approval group and adding at least one rule.
   a. Select **Cluster > Settings.**
   b. Select ⚙ next to **Multi-Admin Approval** in the **Security** section.
   c. Select + Add to add at least one approval group.
      - Name – Enter a group name.
      - Approvers (users) – Select approvers from a list of users.
      - Approvers (groups) – Beginning with ONTAP 9.20.1, optionally select one or more registered IdP, AD, or LDAP groups.
      - Email address – Enter email address(es).
      - Default group – Select a group.
   d. Add at least one rule.
      - Operation – Select a supported command from the list.
      - Query – Enter any desired command options and values.
      - Optional parameters; leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
        - Required number of approvers

        - Approval groups

    e. Select **Advanced Settings** to view or modify defaults.
        - Required number of approvers (default: 1)
        - Execution request expiry (default: 1 hour)
        - Approval request expiry (default: 1hour)
        - Mail server*
        - From email address*

        *These update the email settings managed under "Notification Management". You are prompted to set them if they have not yet been configured.

    f. Select **Enable** to complete MAV initial configuration.

After initial configuration, the current MAV status is displayed in the **Multi-Admin Approval** tile.

- Status (enabled or not)
- Active operations for which approvals are required
- Number of open requests in pending state

You can display an existing configuration by selecting →. MAV approval is required to edit an existing configuration.

To disable multi-admin verification:

1. Select **Cluster > Settings.**
2. Select ⚙ next to **Multi-Admin Approval** in the **Security** section.
3. Select the Enabled toggle button.

   MAV approval is required to complete this operation.

CLI procedure

Before enabling MAV functionality at the CLI, at least one MAV administrator group must have been created.

If you want to…	Enter this command

Enable MAV functionality	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`
	
	Example : the following command enables MAV with 1 approval group, 2 required approvers, and default expiry periods.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Complete initial configuration by adding at least one operation rule.

Modify a MAV configuration (requires MAV approval)	`security multi-admin-verify approval-group modify [-approval-groups group1 [,group2…]] [-required-approvers nn ] [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`

Verify MAV functionality	`security multi-admin-verify show`
	
	Example:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution Approval Approval`
	`Enabled Approvers Expiry Expiry Groups`
	`------- --------- --------- -------- ----------`
	`true 2 1h 1h mav-grp1`

Disable MAV functionality (requires MAV approval)	`security multi-admin-verify modify -enabled false`

Related information

- security multi-admin-verify

Manage multi-admin verification rules for protected operations in ONTAP

You create multi-admin verification (MAV) rules to designate operations requiring approval. Whenever an operation is initiated, protected operations are intercepted and a request for approval is generated.

Rules can be created before enabling MAV by any administrator with appropriate RBAC capabilities, but once MAV is enabled, any modification to the rule set requires MAV approval.

Only one MAV rule can be created per operation; for example, you cannot make multiple `volume-snapshot-delete` rules. Any desired rule constraints must be contained within one rule.

You can create rules to protect these commands. You can protect each command beginning with the ONTAP version in which protection capability for the command first became available.

The rules for MAV system-default commands, the `security multi-admin-verify` commands, cannot be altered.

In addition to system-defined operations, the following commands are protected by default when multi-admin verification is enabled, but you can modify the rules to remove protection for these commands:

- security login password
- security login unlock
- set

Rule constraints

When you create a rule, you can optionally specify the `-query` option to limit the request to a subset of the command functionality. The `-query` option can also be used to limit configuration elements, such as the SVM, the volume, and snapshot names.

For example, in the `volume snapshot delete` command, `-query` can be set to `-snapshot !hourly*,!daily*,!weekly*`, meaning that volume snapshots prefixed with hourly, daily, or weekly attributes are excluded from MAV protections.

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

Any excluded configuration elements would not be protected by MAV, and any administrator could delete or rename them.

By default, rules specify that a corresponding `security multi-admin-verify request create "protected_operation"` command is generated automatically when a protected operation is entered. You

can modify this default to require that the `request create` command be entered separately.

By default, rules inherit the following global MAV settings, although you can specify rule-specific exceptions:

- Required Number of Approvers
- Approval Groups
- Approval Expiry period
- Execution Expiry period

System Manager procedure

If you want to add a protected operation rule for the first time, see the System Manager procedure to enable multi-admin verification.

To modify the existing rule set:

1. Select **Cluster > Settings**.
2. Select ⚙ next to **Multi-Admin Approval** in the **Security** section.
3. Select + Add to add at least one rule; you can also modify or delete existing rules.
   - Operation – Select a supported command from the list.
   - Query – Enter any desired command options and values.
   - Optional parameters – Leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
     - Required number of approvers
     - Approval groups

CLI procedure

ⓘ All `security multi-admin-verify rule` commands require MAV administrator approval before execution except `security multi-admin-verify rule show`.

If you want to…	Enter this command
Create a rule	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [-approval-groups group1[,group2…]] [parameters]`

If you want to…	Enter this command

Modify credentials of current administrators	`security login modify <parameters>`
	
	Example: the following rule requires approval to delete the root volume.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`
	
	Use the `-approval-groups` parameter to specify one or more MAV approval groups for this rule, overriding the global approval groups setting for this operation only.

Modify a rule	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Delete a rule	`security multi-admin-verify rule delete -operation "protected_operation"`
Show rules	`security multi-admin-verify rule show`
View all available MAV-protectable operations	`security multi-admin-verify registered-operations show`

View available MAV-protectable operations

Beginning with ONTAP 9.20.1, you can display all operations that can be protected by MAV on the current cluster. This can help you create a rule without consulting external documentation to determine valid operation names.

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

Example:

```
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
...
```

The list of operations varies by ONTAP version and cluster personality.

You can filter the output by operation name using the `-operation` parameter, including wildcard matching.

Example:

```
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
...
```

Related information

- security multi-admin-verify rule
- security login modify

Request execution of MAV protected operations in ONTAP

When you initiate a protected operation or command on a cluster enabled for multi-admin verification (MAV), ONTAP automatically intercepts the operation and asks to generate a request, which must be approved by one or more administrators in a MAV approval group (MAV administrators). Alternatively, you can create a MAV request without the dialog.

If approved, you must then respond to the query to complete the operation within the request expiry period. If vetoed, or if the request or expiry periods are exceeded, you must delete the request and resubmit.

MAV functionality honors existing RBAC settings. That is, your administrator role must have sufficient privilege to execute a protected operation without regard to MAV settings. Learn more about RBAC.

If you are a MAV administrator, your requests to execute protected operations must also be approved by a MAV administrator.

System Manager procedure

When a user clicks on a menu item to initiate an operation and the operation is protected, a request for approval is generated and the user receives a notification similar to the following:

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

The **Multi-Admin Requests** window is available when MAV is enabled, showing pending requests based on the user's login ID and MAV role (approver or not). For each pending request, the following fields are displayed:

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

  If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- (Number of) Potential Approvers

When the request is approved, the requesting user can retry the operation within the expiry period.

If the user retries the operation without approval, a notification is displayed similar to the following:

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

CLI procedure

1. Enter the protected operation directly or using the MAV request command.

   Examples – to delete a volume, enter one of the following commands:

   - `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. Check the status of the request and respond to the MAV notice.
   a. If the request is approved, respond to the CLI message to complete the operation.

      Example:

```
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. If the request is vetoed, or the expiry period has passed, delete the request, and either resubmit or contact the MAV administrator.

Example:

```
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".
```

Related information

- security multi-admin-verify

Manage MAV protected operation requests in ONTAP

When administrators in a MAV approval group (MAV administrators) are notified of a pending operation execution request, they must respond with an approve or veto message within a fixed time (approval expiry). If a sufficient number of approvals are not received, the requester must delete the request and make another.

About this task

Approval requests are identified with index numbers, which are included in email messages and displays of the request queue.

`multi-admin-verify` requests in a terminal state may be overwritten or removed automatically. Use the audit log to review previous requests.

Beginning with ONTAP 9.20.1, members of a configured IdP, AD, or LDAP approver group can

approve or veto requests without being listed as named approvers. Changes to a user's group membership in the identity provider take effect upon the user's next successful login. No MAV reconfiguration is required.

The following information from the request queue can be displayed:

Operation
The protected operation for which the request is created.

Query
The object (or objects) upon which the user wants to apply the operation.

State
The current state of the request; pending, approved, rejected, expired, executed. If a request is rejected by one approver, no further actions are possible.

Required approvers
The number of MAV administrators that are required to approve the request. A user can set the required-approvers parameter for the operation rule. If a user does not set the required-approvers to the rule, then the required-approvers from the global setting is applied.

Pending approvers
The number of MAV administrators that are still required to approve the request for the request to be marked as approved.

Potential approver groups
Beginning with ONTAP 9.20.1, the IdP, AD, or LDAP groups whose members are eligible to approve or veto the request.

Approval expiry
The period within which a MAV administrator must respond to an approval request. Any authorized user can set the approval-expiry for an operation rule. If approval-expiry is not set for the rule, then the approval-expiry from the global setting is applied.

Execution expiry
The period within which the requesting administrator must complete the operation. Any authorized user can set the execution-expiry for an operation rule. If execution-expiry is not set for the rule, then the execution-expiry from the global setting is applied.

Users approved
The MAV administrators who have approved the request.

User vetoed
The MAV administrators who have vetoed the request.

Storage VM (vserver)
The SVM with which the request is associated with. Only the admin SVM is supported in this release.

User requested
The username of the user who created the request.

Time created

The time when the request is created.

Time approved

The time when the request state changed to approved.

Comment

Any comments that are associated with the request.

Users permitted

The list of users permitted to perform the protected operation for which the request is approved. If `users-permitted` is empty, then any user with appropriate permissions can perform the operation.

System Manager

MAV administrators receive email messages with details of the approval request, request expiry period, and a link to approve or reject the request. They can access an approval dialog by selecting the link in the email or navigate to **Events & Jobs > Multi-Admin Requests** in System Manager.

The **Multi-Admin Requests** window is available when multi-admin verification is enabled, showing pending requests based on the user's login ID and MAV role (approver or not). Select **My Approvals** to list only the requests that the logged-in user is eligible to act on, including requests available through membership in an IdP, AD, or LDAP approver group.

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

  If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- Potential Approvers (beginning with ONTAP 9.20.1, this includes users eligible as named approvers and through membership in an eligible IdP, AD, or LDAP approver group)

MAV administrators have additional controls in this window; they can approve, reject, or delete individual operations, or selected groups of operations. However, if the MAV administrator is the Requesting User, they cannot approve, reject or delete their own requests.

CLI

1. When notified of pending requests by email, note the request's index number and approval expiry period. The index number can also be displayed using the **show** or **show-pending** options in the following table.
2. Approve or veto the request.

If you want to…	Enter this command
Approve a request	`security multi-admin-verify request approve` *nn*
Veto a request	`security multi-admin-verify request veto` *nn*
Show all requests, pending requests, or a single request	`security multi-admin-verify request { show | show-pending } [`*nn*`] { -fields` *field1*`[,`*field2*`…] | [-instance ] }` You can show all requests in the queue or only pending requests. If you enter the index number, only information for that is displayed. You can display information about specific fields (by using the `-fields` parameter) or about all fields (by using the `-instance` parameter).
Delete a request	`security multi-admin-verify request delete` *nn*

Example:

The following sequence approves a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```
          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: -
```

Beginning with ONTAP 9.20.1, the `security multi-admin-verify request show` command includes a `Potential Approver Groups` field that lists any IdP, AD, or LDAP groups whose members are eligible to approve or veto the request.

Example:

The following sequence vetoes a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```
      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: -
```

Related information

- security multi-admin-verify

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.