Gestione la verificación de varias administradores

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Gestione la verificación de varias administradores . . . 1
Obtenga más información sobre la verificación multiadministrador de ONTAP . . . 1
Cómo funciona la verificación multi-administrador . . . 1
Cómo funciona la aprobación multi-admin . . . 16
Cómo funciona la ejecución de operaciones protegidas . . . 17
Gestionar grupos de aprobación de administrador de ONTAP para MAV . . . 17
Procedimiento de System Manager . . . 18
Procedimiento de la CLI . . . 18
Habilitar o deshabilitar la verificación multiadministrador en ONTAP . . . 20
Procedimiento de System Manager . . . 21
Procedimiento de la CLI . . . 22
Gestione reglas de verificación multiadministradoras para las operaciones protegidas en ONTAP . . . 24
Restricciones de regla . . . 24
Procedimiento de System Manager . . . 25
Procedimiento de la CLI . . . 25
Solicitar la ejecución de operaciones protegidas por MAV en ONTAP . . . 26
Procedimiento de System Manager . . . 26
Procedimiento de la CLI . . . 27
Gestionar solicitudes de operación protegidas por MAV en ONTAP . . . 30

Gestione la verificación de varias administradores

Obtenga más información sobre la verificación multiadministrador de ONTAP

A partir de ONTAP 9.11.1, puede utilizar la verificación multiadministrador (MAV) para garantizar que determinadas operaciones, como la eliminación de volúmenes o snapshots, solo se puedan ejecutar después de las aprobaciones de los administradores designados. De este modo, se evita que administradores comprometidos, malintencionados o inexpertos realicen cambios no deseados o eliminen datos.

La configuración de la verificación multi-admin consta de:

- "Crear uno o varios grupos de aprobación de administrador."
- "Habilitar la funcionalidad de verificación multi-administrador."
- "Adición o modificación de reglas."

Tras la configuración inicial, estos elementos sólo los pueden modificar los administradores de un grupo de aprobación MAV (administradores MAV).

Cuando la verificación multiadministrador está habilitada, completar todas las operaciones protegidas requiere los siguientes pasos:

1. Cuando un usuario inicia la operación, a. "se genera la solicitud."
2. Antes de que se pueda ejecutar la operación, al menos una "El administrador de MAV debe aprobar."
3. Tras la aprobación, se solicita al usuario y finaliza la operación.

> Si necesita deshabilitar la funcionalidad de verificación de múltiples administradores sin la aprobación del administrador de MAV, comuníquese con el soporte de NetApp y mencione lo siguiente"Base de conocimientos de NetApp : Cómo deshabilitar la verificación de múltiples administradores si el administrador de MAV no está disponible" .

La verificación de varios administradores no está pensada para utilizarse con volúmenes o flujos de trabajo que implican una fuerte automatización, ya que cada tarea automatizada requeriría la aprobación antes de poder completar la operación. Si desea utilizar la automatización y MAV juntos, se recomienda que utilice consultas para operaciones de MAV específicas. Por ejemplo, puede aplicar `volume delete` reglas MAV solo a volúmenes en los que no esté implicada la automatización, y puede designar esos volúmenes con un esquema de nomenclatura particular.

> La verificación multi-admin no está disponible con Cloud Volumes ONTAP.

Cómo funciona la verificación multi-administrador

La verificación multi-admin consta de:

- Grupo de uno o más administradores con facultades de aprobación y veto.

- Conjunto de operaciones o comandos protegidos en una *rules table*.
- Un *motor de reglas* para identificar y controlar la ejecución de operaciones protegidas.

Las reglas de MAV se evalúan después de las reglas de control de acceso basado en funciones (RBAC). Por lo tanto, los administradores que ejecutan o aprueban operaciones protegidas ya deben disponer de privilegios mínimos de RBAC para esas operaciones. "Más información acerca de RBAC".

Reglas definidas por el sistema

Cuando se activa la verificación de varios administradores, las reglas definidas por el sistema (también conocidas como reglas *Guard-Rail*) establecen un conjunto de operaciones MAV para contener el riesgo de eludir el propio proceso MAV. Estas operaciones no se pueden quitar de la tabla de reglas. Una vez activado MAV, las operaciones designadas por un asterisco (*) requieren la aprobación de uno o más administradores antes de la ejecución, excepto los comandos **show**.

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

  Controla la configuración de la funcionalidad de verificación multi-administrador.

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

  Controlar la pertenencia al conjunto de administradores con credenciales de verificación de varios administradores.

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

  Controle el conjunto de comandos que requieren verificación multiadministrador.

- `security multi-admin-verify request` operaciones

  Controle el proceso de aprobación.

Comandos protegidos por reglas

Además de las operaciones definidas por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando la verificación de múltiples administradores está habilitada, pero puede modificar las reglas para eliminar la protección de estos comandos:

- "contraseña de inicio de sesión de seguridad"
- "desbloqueo de inicio de sesión de seguridad"
- "listo"

Cada versión de ONTAP proporciona más comandos que puede elegir de protección con reglas de verificación multiadministrador. Elija la versión de ONTAP para obtener una lista completa de comandos disponibles para proteger.

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 PB/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. Nuevo comando protegido por reglas para 9.13.1
2. Nuevo comando protegido por reglas para 9.14.1
3. Nuevo comando protegido por reglas para 9.15.1
4. Nuevo comando protegido por reglas para 9.16.1
5. Nuevo comando protegido por reglas para 9.17.1

*Este comando solo está disponible con CLI y no está disponible para System Manager en algunas versiones.

Cómo funciona la aprobación multi-admin

Cada vez que se introduce una operación protegida en un cluster protegido MAV, se envía una solicitud de ejecución de operación al grupo de administradores de MAV designado.

Puede configurar:

- Los nombres, la información de contacto y el número de administradores del grupo MAV.

  Un administrador de MAV debe tener una función RBAC con privilegios de administrador de clúster.

- El número de grupos de administradores de MAV.
  - Se asigna un grupo MAV para cada regla de operación protegida.
  - Para varios grupos MAV, puede configurar qué grupo MAV aprueba una regla determinada.
- El número de aprobaciones MAV necesarias para ejecutar una operación protegida.
- Período *de caducidad de aprobación* dentro del cual un administrador MAV debe responder a una solicitud de aprobación.
- Un período *expiration* de ejecución dentro del cual el administrador solicitante debe completar la operación.

Una vez configurados estos parámetros, se requiere la aprobación MAV para modificarlos.

Los administradores de MAV no pueden aprobar sus propias solicitudes para ejecutar operaciones protegidas. Por lo tanto:

- MAV no debe habilitarse en clústeres con un solo administrador.
- Si sólo hay una persona en el grupo MAV, ese administrador de MAV no puede iniciar operaciones protegidas; los administradores normales deben iniciar operaciones protegidas y el administrador de MAV solo puede aprobar.
- Si desea que los administradores de MAV puedan ejecutar operaciones protegidas, el número de administradores de MAV debe ser uno mayor que el número de aprobaciones necesarias. Por ejemplo, si se necesitan dos aprobaciones para una operación protegida y desea que los administradores de MAV las ejecuten, debe haber tres personas en el grupo de administradores de MAV.

Los administradores de MAV pueden recibir solicitudes de aprobación en alertas de correo electrónico (mediante EMS) o pueden consultar la cola de solicitudes. Cuando reciben una solicitud, pueden realizar una de estas tres acciones:

- Aprobar
- Rechazar (veto)
- Ignorar (sin acción)

Las notificaciones de correo electrónico se envían a todos los aprobadores asociados a una regla MAV cuando:

- Se crea una solicitud.
- Se ha aprobado o vetado una solicitud.
- Se ejecuta una solicitud aprobada.

Si el solicitante se encuentra en el mismo grupo de aprobación para la operación, recibirá un correo

electrónico cuando se apruebe su solicitud.

> Un solicitante no puede aprobar sus propias solicitudes incluso si están en el grupo de aprobación (aunque puede recibir notificaciones por correo electrónico para sus propias solicitudes). Los solicitantes que no se encuentren en grupos de aprobación (es decir, que no sean administradores de MAV) no recibirán notificaciones por correo electrónico.

Cómo funciona la ejecución de operaciones protegidas

Si se aprueba la ejecución para una operación protegida, el usuario solicitante continúa con la operación cuando se le solicita. Si la operación es vetada, el usuario solicitante debe eliminar la solicitud antes de continuar.

Las reglas de MAV se evalúan después de los permisos de RBAC. Como resultado, un usuario sin suficientes permisos de RBAC para la ejecución de la operación no puede iniciar el proceso de solicitud de MAV.

Las reglas MAV se evalúan antes de ejecutar la operación protegida. Esto significa que las reglas se aplican según el estado actual del sistema. Por ejemplo, si se crea una regla MAV para `volume modify` con una consulta de `-size 5GB` , usando `volume modify` Para cambiar el tamaño de un volumen de 5 GB a 2 GB se requerirá la aprobación de MAV, pero para cambiar el tamaño de un volumen de 2 GB a 5 GB no.

Información relacionada

- "clúster"
- "lun"
- "seguridad"
- "extremo de sujeción legal con cierre a presión"
- "agregado de almacenamiento"
- "cifrado del almacenamiento"
- "sistema"

Gestionar grupos de aprobación de administrador de ONTAP para MAV

Antes de habilitar la verificación multi-admin (MAV), debe crear un grupo de aprobación de administrador que contenga a uno o más administradores a los que se les conceda la autorización de aprobación o de veto. Una vez que haya habilitado la verificación de varios administradores, cualquier modificación de la pertenencia al grupo de aprobación requiere la aprobación de uno de los administradores cualificados existentes.

Acerca de esta tarea

Puede agregar administradores existentes a un grupo MAV o crear nuevos administradores.

La funcionalidad MAV cumple la configuración de control de acceso basado en funciones (RBAC) existente. Los posibles administradores de MAV deben tener privilegios suficientes para ejecutar operaciones protegidas antes de agregarlas a los grupos de administradores de MAV. "Más información acerca de RBAC."

Puede configurar MAV para avisar a los administradores de MAV de que las solicitudes de aprobación están pendientes. Para ello, debe configurar las notificaciones por correo electrónico, en particular los `Mail From`

`Mail Server` parámetros y, o bien puede borrar estos parámetros para desactivar la notificación. Sin alertas de correo electrónico, los administradores de MAV deben comprobar manualmente la cola de aprobación.

A partir de ONTAP 9.15.1, puede configurar los usuarios de Active Directory (AD) como administradores de MAV. El usuario de AD debe ser"configurado como administrador de ONTAP" .

Procedimiento de System Manager

Si desea crear un grupo de aprobación MAV por primera vez, consulte el procedimiento de System Manager a. "habilite la verificación multi-admin."

Para modificar un grupo de aprobación existente o crear un grupo de aprobación adicional:

1. Identifique a los administradores para que reciban una verificación de varios administradores.
   a. Haga clic en **clúster > Configuración.**
   b. Haga clic en → junto a **Usuarios y Roles.**
   c. Haga clic en + Add **Usuarios.**
   d. Modifique la planilla según sea necesario.

      Para obtener más información, consulte "Control del acceso de administradores."
2. Crear o modificar el grupo de aprobación MAV:
   a. Haga clic en **clúster > Configuración.**
   b. Haga clic → junto a **Aprobación multiadministrador** en la sección **Seguridad**. (Verá ⚙ el icono si MAV aún no está configurado.)
      - Nombre: Introduzca un nombre de grupo.
      - Autorizadores: Seleccione autorizadores de una lista de usuarios.
      - Dirección de correo electrónico: Introduzca las direcciones de correo electrónico.
      - Grupo predeterminado: Seleccione un grupo.

Se requiere aprobación MAV para editar una configuración existente una vez que MAV está activado.

Procedimiento de la CLI

1. Compruebe que se han definido valores para los `Mail From` `Mail Server` parámetros y. Introduzca:

   ```
   event config show
   ```

   La pantalla debe ser similar a la siguiente:

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

Para configurar estos parámetros, introduzca:

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

Obtenga más información sobre `event config show` y `event config modify` en el "Referencia de comandos del ONTAP".

2. Identifique a los administradores para que reciban una verificación de varios administradores

Si desea…	Introduzca este comando
Mostrar los administradores actuales	`security login show`
Modifique las credenciales de los administradores actuales	`security login modify <parameters>`
Crear nuevas cuentas de administrador	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

Obtenga más información acerca de `security login show`, `security login modify` y `security login create` en el "Referencia de comandos del ONTAP".

3. Cree el grupo de aprobación MAV:

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

- `-vserver` - Solo el admin SVM es compatible en esta versión.
- `-name` - El nombre del grupo MAV, hasta 64 caracteres.
- `-approvers`- La lista de uno o más aprobadores. Para los usuarios de AD, utilice el formato `domain\user` . Por ejemplo, `mydomain\pavan` .
- `-email` - Una o más direcciones de correo electrónico que son notificadas cuando una solicitud es creada, aprobada, vetada o ejecutada.

  Ejemplo: el siguiente comando crea un grupo MAV con dos miembros y direcciones de correo electrónico asociadas.

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

4. Verificar la creación y pertenencia a grupos:

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

Ejemplo:

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

Utilice estos comandos para modificar la configuración inicial del grupo MAV.

Nota: todos requieren la aprobación del administrador de MAV antes de la ejecución.

Si desea…	Introduzca este comando
Modifique las características del grupo o modifique la información de miembro existente	`security multi-admin-verify approval-group modify [parameters]`
Agregar o quitar miembros	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
Eliminar un grupo	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

Información relacionada

- "verificación de seguridad multiadministrador"

Habilitar o deshabilitar la verificación multiadministrador en ONTAP

La verificación de varios administradores (MAV) se debe habilitar explícitamente. Una vez activada la verificación de varios administradores, se requiere la aprobación de un grupo de aprobación MAV (administradores MAV) para eliminarlo.

Acerca de esta tarea

Una vez que MAV está activado, la modificación o desactivación de MAV requiere la aprobación del administrador de MAV.

> Si necesita deshabilitar la funcionalidad de verificación de múltiples administradores sin la aprobación del administrador de MAV, comuníquese con el soporte de NetApp y mencione lo siguiente"Base de conocimientos de NetApp : Cómo deshabilitar la verificación de múltiples administradores si el administrador de MAV no está disponible" .

Al activar MAV, puede especificar los siguientes parámetros globalmente.

Grupos de aprobación

Lista de grupos de aprobación globales. Se necesita al menos un grupo para activar la funcionalidad MAV.

Si utiliza MAV con protección autónoma contra ransomware (ARP), defina un grupo de aprobación nuevo o existente que sea responsable de aprobar la pausa de ARP, deshabilitar y borrar solicitudes sospechosas.

Autorizadores requeridos

Número de autorizadores necesarios para ejecutar una operación protegida. El número predeterminado y el número mínimo son 1.

El Núm. Necesario de aprobadores debe ser menor que el Núm. Total de aprobadores únicos en los grupos de aprobación por defecto.

Caducidad de la aprobación (horas, minutos, segundos)

El período dentro del cual un administrador MAV debe responder a una solicitud de aprobación. El valor predeterminado es una hora (1h), el valor mínimo soportado es un segundo (1s) y el valor máximo soportado es 14 días (14d).

Caducidad de la ejecución (horas, minutos, segundos)

El período dentro del cual el administrador solicitante debe completar la operación:. El valor predeterminado es una hora (1h), el valor mínimo soportado es un segundo (1s) y el valor máximo soportado es 14 días (14d).

También puede sustituir cualquiera de estos parámetros para especificarlos "reglas de funcionamiento."

Procedimiento de System Manager

1. Identifique a los administradores para que reciban una verificación de varios administradores.
   a. Haga clic en **clúster > Configuración.**
   b. Haga clic en → junto a **Usuarios y Roles.**
   c. Haga clic en + Add **Usuarios.**
   d. Modifique la planilla según sea necesario.

      Para obtener más información, consulte "Control del acceso de administradores."

2. Active la verificación de varios administradores creando al menos un grupo de aprobación y agregando al menos una regla.
   a. Haga clic en **clúster > Configuración.**
   b. Haga clic ⚙ junto a **Aprobación multiadministrador** en la sección **Seguridad**.
   c. Haga + Add clic para agregar al menos un grupo de aprobación.
      - Nombre: Introduzca un nombre de grupo.
      - Autorizadores: Seleccione autorizadores de una lista de usuarios.
      - Dirección de correo electrónico: Introduzca las direcciones de correo electrónico.
      - Grupo predeterminado: Seleccione un grupo.
   d. Agregue al menos una regla.

- Operación: Seleccione un comando admitido de la lista.
- Query: Introduzca los valores y las opciones de comandos que desee.
- Parámetros opcionales; déjelo en blanco para aplicar la configuración global o asigne un valor diferente para reglas específicas para anular la configuración global.
  - Número requerido de aprobadores
  - Grupos de aprobación

e. Haga clic en **Configuración avanzada** para ver o modificar los valores predeterminados.
   - Número requerido de autorizadores (valor predeterminado: 1)
   - Caducidad de la solicitud de ejecución (valor predeterminado: 1 hora)
   - Caducidad de la solicitud de aprobación (valor predeterminado: 1 hora)
   - Servidor de correo*
   - Desde la dirección de correo electrónico*

     *Estos actualizan la configuración de correo electrónico administrada en "Notification Management". Se le pedirá que los configure si aún no se han configurado.

f. Haga clic en **Activar** para completar la configuración inicial de MAV.

Después de la configuración inicial, el estado actual de MAV se muestra en el mosaico **Multi-Admin Approval**.

- Estado (habilitado o no)
- Operaciones activas para las que se necesitan aprobaciones
- Número de solicitudes abiertas en estado pendiente

Puede visualizar una configuración existente haciendo clic en →. Se requiere aprobación MAV para editar una configuración existente.

Para deshabilitar la verificación multi-admin:

1. Haga clic en **clúster > Configuración.**
2. Haga clic ⚙ junto a **Aprobación multiadministrador** en la sección **Seguridad**.
3. Haga clic en el botón de alternar habilitado.

   Se requiere la aprobación MAV para completar esta operación.

Procedimiento de la CLI

Antes de activar la funcionalidad MAV en la CLI, "Grupo de administradores MAV"se debe haber creado al menos una.

Si desea…	Introduzca este comando

Active la funcionalidad de MAV	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`
	
	Ejemplo : el siguiente comando habilita MAV con 1 grupo de aprobación, 2 aprobadores requeridos y períodos de caducidad predeterminados.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Complete la configuración inicial agregando al menos una "regla de operación."

Modificar una configuración de MAV (requiere aprobación de MAV)	`security multi-admin-verify approval-group modify [-approval-groups group1 [,group2…]] [-required-approvers nn ] [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`

Verifique la funcionalidad de MAV	`security multi-admin-verify show`
	
	Ejemplo:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

Desactivar la función MAV (requiere la aprobación MAV)	`security multi-admin-verify modify -enabled false`

Información relacionada

- "verificación de seguridad multiadministrador"

Gestione reglas de verificación multiadministradoras para las operaciones protegidas en ONTAP

Se crean reglas de verificación de varios administradores (MAV) para designar operaciones que requieren aprobación. Siempre que se inicia una operación, las operaciones protegidas se interceptan y se genera una solicitud de aprobación.

Las reglas se pueden crear antes de habilitar MAV por cualquier administrador con las capacidades RBAC adecuadas, pero una vez que MAV está activado, cualquier modificación del conjunto de reglas requiere la aprobación de MAV.

Sólo se puede crear una regla MAV por operación; por ejemplo, no se pueden crear varias `volume-snapshot-delete` reglas. Cualquier restricción de regla deseada debe estar contenida dentro de una regla.

Puede crear reglas para proteger "estos comandos". Puede proteger cada comando comenzando por la versión de ONTAP, en la que se encuentra disponible la funcionalidad de protección para el comando primero.

Las reglas para los comandos MAV por defecto del sistema `security multi-admin-verify` "comandos", , no se pueden modificar.

Además de las operaciones definidas por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando la verificación de múltiples administradores está habilitada, pero puede modificar las reglas para eliminar la protección de estos comandos:

- "contraseña de inicio de sesión de seguridad"
- "desbloqueo de inicio de sesión de seguridad"
- "listo"

Restricciones de regla

Al crear una regla, puede especificar opcionalmente la `-query` opción para limitar la solicitud a un subconjunto de la funcionalidad del comando. `-query`La opción también puede usarse para limitar elementos de configuración, como los nombres de la SVM, de los volúmenes y de snapshots.

Por ejemplo, en el `volume snapshot delete` comando, `-query` se puede definir en `-snapshot !hourly*,!daily*,!weekly*`, lo que significa que las instantáneas de volumen con el prefijo de atributos por hora, por día o por semana se excluyen de las protecciones MAV.

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

MAV no protegería ningún elemento de configuración excluido y cualquier administrador podría suprimirlos o cambiarles el nombre.

De forma predeterminada, las reglas especifican que el `security multi-admin-verify request create "protected_operation"` comando correspondiente se genera automáticamente cuando se introduce una operación protegida. Puede modificar este valor predeterminado para requerir que `request create` el comando se introduzca por separado.

De forma predeterminada, las reglas heredan la siguiente configuración global de MAV, aunque se pueden especificar excepciones específicas de reglas:

- Número de aprobadores requerido
- Grupos de aprobación
- Período de caducidad de la aprobación
- Periodo de caducidad de ejecución

Procedimiento de System Manager

Si desea agregar una regla de operación protegida por primera vez, consulte el procedimiento de System Manager a. "habilite la verificación multi-admin."

Para modificar el conjunto de reglas existente:

1. Seleccione **Cluster > Settings**.
2. Seleccione junto a **Aprobación multiadministrador** en la sección **Seguridad**.
3. Seleccione esta opción + Add para agregar al menos una regla; también puede modificar o suprimir las reglas existentes.
   - Operación: Seleccione un comando admitido de la lista.
   - Query: Introduzca los valores y las opciones de comandos que desee.
   - Parámetros opcionales: Dejar en blanco para aplicar la configuración global o asignar un valor diferente para reglas específicas para anular la configuración global.
     - Número requerido de aprobadores
     - Grupos de aprobación

Procedimiento de la CLI

Todos `security multi-admin-verify rule` los comandos requieren la aprobación del administrador de MAV antes de la ejecución, excepto `security multi-admin-verify rule show`.

Si desea…	Introduzca este comando
Cree una regla	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

Si desea…	Introduzca este comando

Modifique las credenciales de los administradores actuales	`security login modify <parameters>`
	
	Ejemplo: La siguiente regla requiere aprobación para eliminar el volumen raíz.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

Modificar una regla	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Eliminar una regla	`security multi-admin-verify rule delete -operation "protected_operation"`
Muestra las reglas	`security multi-admin-verify rule show`

Información relacionada

- "regla de verificación de seguridad multiadministrador"
- "modificación del inicio de sesión de seguridad"

Solicitar la ejecución de operaciones protegidas por MAV en ONTAP

Cuando inicia una operación o comando protegido en un clúster habilitado para la verificación de varios administradores (MAV), ONTAP intercepta automáticamente la operación y solicita generar una solicitud, que debe ser aprobada por uno o más administradores de un grupo de aprobación de MAV (administradores de MAV). También puede crear una solicitud MAV sin el diálogo.

Si se aprueba, deberá responder a la consulta para completar la operación dentro del período de caducidad de la solicitud. Si se ha vetado o si se han superado los períodos de solicitud o caducidad, debe eliminar la solicitud y volver a enviarla.

La funcionalidad MAV cumple la configuración de RBAC existente. Es decir, la función de administrador debe tener privilegios suficientes para ejecutar una operación protegida sin tener en cuenta la configuración de MAV. "Más información acerca de RBAC".

Si es administrador de MAV, sus solicitudes de ejecución de operaciones protegidas también deben ser aprobadas por un administrador de MAV.

Procedimiento de System Manager

Cuando un usuario hace clic en un elemento de menú para iniciar una operación y la operación está protegida, se genera una solicitud de aprobación y el usuario recibe una notificación similar a la siguiente:

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

La ventana **solicitudes de administrador múltiple** está disponible cuando MAV está activado, mostrando solicitudes pendientes basadas en el ID de inicio de sesión del usuario y la función MAV (aprobador o no). Para cada solicitud pendiente, se muestran los siguientes campos:

- Funcionamiento
- Índice (número)
- Estado (pendiente, aprobado, rechazado, ejecutado o caducado)

  Si un aprobador rechaza una solicitud, no es posible realizar ninguna otra acción.

- Consulta (cualquier parámetro o valor para la operación solicitada)
- Usuario solicitante
- La solicitud caduca el
- (Número de) aprobadores pendientes
- (Número de) posibles aprobadores

Una vez aprobada la solicitud, el usuario solicitante puede volver a intentar la operación dentro del período de caducidad.

Si el usuario vuelve a intentar la operación sin aprobación, se muestra una notificación similar a la siguiente:

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

Procedimiento de la CLI

1. Introduzca la operación protegida directamente o mediante el comando MAV Request.

   Ejemplos: Para eliminar un volumen, introduzca uno de los siguientes comandos:

   - `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. Compruebe el estado de la solicitud y responda al aviso de MAV.
   a. Si se aprueba la solicitud, responda al mensaje de la CLI para completar la operación.

      Ejemplo:

```
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. Si se vetó la solicitud o el período de caducidad ha pasado, elimine la solicitud y vuelva a enviarla o póngase en contacto con el administrador de MAV.

Ejemplo:

```
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".
```

Información relacionada

- "verificación de seguridad multiadministrador"

Gestionar solicitudes de operación protegidas por MAV en ONTAP

Cuando a los administradores de un grupo de aprobación MAV (administradores MAV) se les notifica sobre una solicitud de ejecución de operación pendiente, deben responder con un mensaje de aprobación o veto dentro de un tiempo fijo (vencimiento de la aprobación). Si no se recibe un número suficiente de aprobaciones, el solicitante deberá eliminar la solicitud y realizar otra.

Acerca de esta tarea

Las solicitudes de aprobación se identifican con números de índice, que se incluyen en los mensajes de correo electrónico y se muestran en la cola de solicitudes.

`multi-admin-verify`Las solicitudes en un estado terminal pueden sobrescribirse o eliminarse automáticamente. Utilice el"registro de auditoría" para revisar solicitudes anteriores.

Se puede mostrar la siguiente información de la cola de solicitudes:

Funcionamiento

La operación protegida para la que se crea la solicitud.

Consulta

El objeto (u objetos) sobre el que el usuario desea aplicar la operación.

Estado

El estado actual de la solicitud; pendiente, aprobado, rechazado, caducado, ejecutado. Si un aprobador rechaza una solicitud, no es posible realizar ninguna otra acción.

Autorizadores requeridos

El número de administradores de MAV que se necesitan para aprobar la solicitud. Un usuario puede establecer el parámetro aprobadores requeridos para la regla de operación. Si un usuario no establece los aprobadores requeridos en la regla, se aplican los autorizadores requeridos de la configuración global.

Aprobadores pendientes

El número de administradores de MAV que todavía deben aprobar la solicitud para que se marque como aprobada.

Caducidad de la aprobación

El período dentro del cual un administrador MAV debe responder a una solicitud de aprobación. Cualquier usuario autorizado puede definir la fecha de caducidad de la aprobación de una regla de operación. Si no se ha establecido la fecha de caducidad de la regla, se aplicará la fecha de caducidad de la aprobación del valor global.

Caducidad de la ejecución

El período en el que el administrador solicitante debe completar la operación. Cualquier usuario autorizado puede establecer la caducidad de la ejecución de una regla de operación. Si no se ha definido la caducidad de la ejecución para la regla, se aplicará la caducidad de la ejecución desde el valor global.

Usuarios aprobados

Los administradores de MAV que han aprobado la solicitud.

El usuario ha vetado

Los administradores de MAV que han vetado la solicitud.

VM de almacenamiento (Vserver)

La SVM con la que se asocia la solicitud. Solo esta versión admite la SVM de administrador.

Usuario solicitado

Nombre de usuario del usuario que creó la solicitud.

Hora de creación

Hora a la que se crea la solicitud.

Tiempo aprobado

Hora a la que el estado de la solicitud cambió a aprobado.

Comentar

Cualquier comentario asociado a la solicitud.

Se permiten usuarios

Lista de usuarios autorizados para realizar la operación protegida para la que se aprueba la solicitud. Si `users-permitted` está vacío, cualquier usuario con los permisos adecuados puede realizar la operación.

System Manager

Los administradores de MAV reciben mensajes de correo electrónico con detalles de la solicitud de aprobación, el período de vencimiento de la solicitud y un enlace para aprobar o rechazar la solicitud. Pueden acceder a un cuadro de diálogo de aprobación haciendo clic en el enlace del correo electrónico o navegando a **Eventos y trabajos > Solicitudes** en el Administrador del sistema.

La ventana **Solicitudes** está disponible cuando la verificación de múltiples administradores está habilitada y muestra las solicitudes pendientes según el ID de inicio de sesión del usuario y el rol MAV (aprobador o no).

- Funcionamiento
- Índice (número)
- Estado (pendiente, aprobado, rechazado, ejecutado o caducado)

  Si un aprobador rechaza una solicitud, no es posible realizar ninguna otra acción.

- Consulta (cualquier parámetro o valor para la operación solicitada)
- Usuario solicitante
- La solicitud caduca el
- (Número de) aprobadores pendientes
- (Número de) posibles aprobadores

Los administradores de MAV tienen controles adicionales en esta ventana; pueden aprobar, rechazar o eliminar operaciones individuales o grupos de operaciones seleccionados. Sin embargo, si el administrador MAV es el usuario solicitante, no puede aprobar, rechazar o eliminar sus propias solicitudes.

CLI

1. Cuando se le notifique por correo electrónico sobre solicitudes pendientes, anote el número de índice de la solicitud y el período de vencimiento de la aprobación. El número de índice también se puede mostrar utilizando las opciones **show** o **show-pending** mencionadas a continuación.
2. Aprobar o vetar la solicitud.

Si desea…	Introduzca este comando
Aprobar una solicitud	`security multi-admin-verify request approve` *nn*
Vetar una solicitud	`security multi-admin-verify request veto` *nn*
Mostrar todas las solicitudes, solicitudes pendientes o una sola solicitud	`security multi-admin-verify request { show

Si desea…	Introduzca este comando
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  Puede mostrar todas las solicitudes de la cola o sólo las solicitudes pendientes. Si introduce el número de índice, solo se mostrará la información correspondiente. Puede mostrar información sobre campos específicos (mediante el `-fields` parámetro) o sobre todos los campos (mediante el `-instance` parámetro).
Eliminar una solicitud	`security multi-admin-verify request delete` *nn*

Ejemplo:

La siguiente secuencia aprueba una solicitud después de que el administrador de MAV haya recibido el correo electrónico de solicitud con el número de índice 3, que ya tiene una aprobación.

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


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

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

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

Ejemplo:

En la siguiente secuencia se vetará una solicitud después de que el administrador MAV haya recibido el correo electrónico de solicitud con el número de índice 3, que ya tiene una aprobación.

```
      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: -
```

Información relacionada

- "verificación de seguridad multiadministrador"

Información de copyright

Información de la marca comercial