Gestione la verificación de varias administradores

ONTAP 9

NetApp
April 16, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/multi-admin-verify/index.html on April 16, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestione la verificación de varias administradores . . . 1
Información general de verificación de varios administradores . . . 1
Administrar grupos de aprobación de administradores . . . 5
Habilitar y deshabilitar la verificación de varios administradores . . . 7
Gestione reglas de operaciones protegidas . . . 11
Solicite la ejecución de operaciones protegidas . . . 14
Gestione solicitudes de operaciones protegidas . . . 17

Gestione la verificación de varias administradores

Información general de verificación de varios administradores

A partir de ONTAP 9.11.1, puede utilizar la verificación multiprotocolo (MAV) para garantizar que determinadas operaciones, como la eliminación de volúmenes o copias snapshot, solo se puedan ejecutar tras las aprobaciones de 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 multi-administrador está habilitada, la finalización de cada operación protegida requiere tres pasos:

- Cuando un usuario inicia la operación, un "se genera la solicitud."
- Antes de que pueda ejecutarse, al menos uno "El administrador de MAV debe aprobar."
- Tras la aprobación, el usuario completa la operación.

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 conjuntamente, se recomienda utilizar consultas para operaciones MAV específicas. Por ejemplo, puede aplicar `volume delete` MAV sólo rige para volúmenes en los que la automatización no está involucrada, y puede designar dichos volúmenes con un esquema de nomenclatura en particular.

> Si necesita deshabilitar la funcionalidad de verificación multi-admin sin la aprobación del administrador de MAV, póngase en contacto con el soporte de NetApp y mencione el siguiente artículo de la base de conocimientos: "Cómo deshabilitar la verificación de administrador múltiple si el administrador de MAV no está disponible".

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` operación*

  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 los comandos definidos por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando se habilita la verificación multi-administrador, pero se pueden modificar las reglas para quitar la protección de estos comandos.

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

Los siguientes comandos pueden protegerse en ONTAP 9.11.1 y versiones posteriores.

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

Los siguientes comandos se pueden proteger a partir de ONTAP 9.13.1:

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

Los siguientes comandos se pueden proteger a partir de ONTAP 9.14.1:

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

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 introducir operaciones protegidas; los administradores regulares deben introducirlas y el administrador de MAV sólo puede aprobarlas.
- 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.

Nota: Un solicitante no puede aprobar sus propias solicitudes, incluso si están en el grupo de aprobación. Pero pueden recibir las notificaciones por correo electrónico. 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.

Administrar grupos de aprobación de administradores

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 administradores potenciales 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 concreto, el `Mail From` y.. `Mail Server` parámetros—o puede borrar estos parámetros para deshabilitar la notificación. Sin alertas de correo electrónico, los administradores de MAV deben comprobar manualmente la cola de aprobación.

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 En **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 en → Junto a **aprobación Multi-Admin** en la sección **Seguridad**. (Verá la ⚙ 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 establecido valores para `Mail From` y.. `Mail Server` parámetros. 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`*

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`

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 se admite la SVM de administrador en esta versión.
   - `-name` - El nombre del grupo MAV, hasta 64 caracteres.
   - `-approvers` - La lista de uno o más aprobadores.
   - `-email` - Una o varias direcciones de correo electrónico que se notifican cuando se crea, aprueba, vetó o ejecuta una solicitud.

     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`*

Habilitar y deshabilitar la verificación de varios administradores

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 multi-admin sin la aprobación del administrador de MAV, póngase en contacto con el soporte de NetApp y mencione el siguiente artículo de la base de conocimientos: "Cómo deshabilitar la verificación de administrador múltiple 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 anular cualquiera de estos parámetros para un parámetro específico "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 En **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 en ⚙ Junto a **aprobación Multi-Admin** en la sección **Seguridad**.
   c. Haga clic en + Add 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 mostrar 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 en ⚙ Junto a **aprobación Multi-Admin** 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, al menos una "Grupo de administradores MAV" debe haber sido creado.

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`

Gestione reglas de operaciones protegidas

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.

Comandos protegidos por reglas

Puede crear reglas para proteger los siguientes comandos que comienzan con ONTAP 9.11.1.

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

Puede crear reglas para proteger los siguientes comandos que comienzan con ONTAP 9.13.1:

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

Puede crear reglas para proteger los siguientes comandos que comienzan con ONTAP 9.14.1:

- `volume recovery-queue modify`
- `volume recovery-queue purge`

- `volume recovery-queue purge-all`
- `vserver modify`

Las reglas para los comandos MAV system-default, el `security multi-admin-verify` "comandos", no se puede modificar.

Además de los comandos definidos por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando se habilita la verificación multi-administrador, pero se pueden modificar las reglas para quitar la protección de estos comandos.

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

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. La `-query` La opción también se puede usar para limitar elementos de configuración, como los nombres de la SVM, del volumen y de las snapshots.

Por ejemplo, en la `volume snapshot delete` comando, `-query` se puede establecer en `-snapshot !hourly*,!daily*,!weekly*`, Lo que significa que las instantáneas de volumen con el prefijo de atributos por hora, diario o semanal 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 corresponde `security multi-admin-verify request create "protected_operation"` el comando se genera automáticamente cuando se introduce una operación protegida. Puede modificar este valor predeterminado para requerir que el `request create` el comando se introduce 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 añadir 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 Multi-Admin** en la sección **Seguridad**.
3. Seleccione + Add para agregar al menos una regla, también puede modificar o eliminar 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

> Todo `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]`

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`

Para obtener detalles de sintaxis de comandos, consulte `security multi-admin-verify rule` páginas de manual.

Solicite la ejecución de operaciones protegidas

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".
```

Gestione solicitudes de operaciones protegidas

Cuando se notifica a los administradores de un grupo de aprobación MAV (administradores MAV) de una solicitud de ejecución de operación pendiente, deben responder con un mensaje de aprobación o de veto dentro de un período de tiempo fijo (caducidad de la aprobación). Si no se recibe un número suficiente de aprobaciones, el solicitante debe 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.

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 y, a continuación, cualquier usuario con los permisos adecuados puede realizar la operación.

Todas las solicitudes vencidas o ejecutadas se eliminan cuando se alcanza un límite de 1000 solicitudes o cuando el tiempo de vencimiento es superior a 8 horas para las solicitudes caducadas. Las solicitudes de

vetoed se eliminan una vez marcadas como caducadas.

Procedimiento de System Manager

Los administradores de MAV reciben mensajes de correo electrónico con detalles sobre la solicitud de aprobación, el período de caducidad de la solicitud y un vínculo para aprobar o rechazar la solicitud. Pueden acceder a un diálogo de aprobación haciendo clic en el enlace del correo electrónico o navegue hasta **Eventos y trabajos>solicitudes** en System Manager.

La ventana **Requests** está disponible cuando está habilitada la verificación de varios administradores, mostrando solicitudes pendientes basadas en el ID de inicio de sesión del usuario y la función 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.

Procedimiento de la CLI

1. Cuando se le notifique por correo electrónico acerca de las solicitudes pendientes, anote el número de índice y el período de caducidad de la aprobación de la solicitud. El número de índice también se puede mostrar utilizando las opciones **show** o **show-anPending** que se mencionan 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 la `-fields` parámetro) o 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 de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.