



Gestire la verifica multi-admin

ONTAP 9

NetApp
January 08, 2026

This PDF was generated from <https://docs.netapp.com/it-it/ontap/multi-admin-verify/index.html> on January 08, 2026. Always check docs.netapp.com for the latest.

Sommario

Gestire la verifica multi-admin	1
Ulteriori informazioni sulla verifica multi-admin di ONTAP	1
Come funziona la verifica multi-admin	1
Come funziona l'approvazione multi-admin	16
Come funziona l'esecuzione di operazioni protette	17
Gestire i gruppi di approvazione degli amministratori ONTAP per MAV	17
Procedura di System Manager	18
Procedura CLI	18
Attiva o disattiva la verifica multi-admin in ONTAP	20
Procedura di System Manager	21
Procedura CLI	22
Gestisci regole di verifica con amministratori multipli per operazioni protette in ONTAP	24
Vincoli della regola	24
Procedura di System Manager	25
Procedura CLI	25
Richiedere l'esecuzione di operazioni MAV protette in ONTAP	26
Procedura di System Manager	26
Procedura CLI	27
Gestire le richieste di operazioni protette da MAV in ONTAP	30

Gestire la verifica multi-admin

Ulteriori informazioni sulla verifica multi-admin di ONTAP

A partire da ONTAP 9.11.1, è possibile utilizzare la verifica multi-admin (MAV) per garantire che determinate operazioni, come l'eliminazione di volumi o snapshot, possano essere eseguite solo dopo l'approvazione da parte degli amministratori designati. In questo modo si evita che gli amministratori compromessi, dannosi o inesperti apportino modifiche indesiderate o eliminino dati.

La configurazione della verifica multi-admin comprende:

- "[Creazione di uno o più gruppi di approvazione dell'amministratore.](#)"
- "[Abilitazione della funzionalità di verifica multi-admin.](#)"
- "[Aggiunta o modifica di regole.](#)"

Dopo la configurazione iniziale, questi elementi possono essere modificati solo dagli amministratori di un gruppo di approvazione MAV (amministratori MAV).

Quando la verifica multi-admin è abilitata, il completamento di ogni operazione protetta richiede i seguenti passaggi:

1. Quando un utente avvia l'operazione, un "[la richiesta viene generata.](#)"
2. Prima di poter eseguire l'operazione, almeno uno "[L'amministratore MAV deve approvare.](#)"
3. Dopo l'approvazione, all'utente viene richiesto di completare l'operazione.

 Se è necessario disabilitare la funzionalità di verifica multi-amministratore senza l'approvazione dell'amministratore MAV, contattare l'assistenza NetApp e menzionare quanto segue "[Knowledge Base NetApp : come disabilitare la verifica multi-amministratore se l'amministratore MAV non è disponibile](#)".

La verifica multi-admin non è prevista per l'utilizzo con volumi o flussi di lavoro che comportano un'elevata automazione, perché ogni attività automatizzata richiederebbe l'approvazione prima che l'operazione possa essere completata. Se si desidera utilizzare insieme automazione e MAV, si consiglia di utilizzare query per operazioni MAV specifiche. Ad esempio, è possibile applicare `volume delete` le regole MAV solo ai volumi in cui l'automazione non è coinvolta e designare tali volumi con un particolare schema di denominazione.

 La verifica multiamministratore non è disponibile con Cloud Volumes ONTAP.

Come funziona la verifica multi-admin

La verifica multi-admin consiste in:

- Un gruppo di uno o più amministratori con poteri di approvazione e voto.
- Un insieme di operazioni o comandi protetti in una *tabella di regole*.
- Un *motore di regole* per identificare e controllare l'esecuzione di operazioni protette.

Le regole MAV vengono valutate in base alle regole RBAC (role-based access control). Pertanto, gli

amministratori che eseguono o approvano operazioni protette devono già disporre dei privilegi RBAC minimi per tali operazioni. ["Scopri di più su RBAC"](#).

Regole definite dal sistema

Quando la verifica multi-admin è attivata, le regole definite dal sistema (note anche come regole *guard-rail*) stabiliscono un insieme di operazioni MAV per contenere il rischio di aggirare il processo MAV stesso. Queste operazioni non possono essere rimosse dalla tabella delle regole. Una volta abilitato MAV, le operazioni contrassegnate da un asterisco (*) devono essere approvate da uno o più amministratori prima dell'esecuzione, ad eccezione dei comandi **show**.

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

Controlla la configurazione della funzionalità di verifica multi-admin.

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

Controlla l'appartenenza all'insieme di amministratori con credenziali di verifica multi-admin.

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

Controlla il set di comandi che richiedono la verifica multi-admin.

- `security multi-admin-verify request operazioni`

Controllare il processo di approvazione.

Comandi protetti da regole

Oltre alle operazioni definite dal sistema, i seguenti comandi sono protetti per impostazione predefinita quando è abilitata la verifica multi-amministratore, ma è possibile modificare le regole per rimuovere la protezione per questi comandi:

- "["password di accesso di sicurezza"](#)"
- "["sblocco accesso di sicurezza"](#)"
- "["partenza"](#)"

Ogni versione di ONTAP fornisce più comandi che è possibile scegliere di proteggere con regole di verifica multi-admin. Scegliere la release di ONTAP per l'elenco completo di comandi disponibili per la protezione.

9.17.1

- cluster date modify³
- cluster log-forwarding create³
- cluster log-forwarding delete³
- cluster log-forwarding modify³
- cluster peer delete
- cluster time-service ntp server create³
- cluster time-service ntp server delete³
- cluster time-service ntp key create³
- cluster time-service ntp key delete³
- cluster time-service ntp key modify³
- cluster time-service ntp server modify³
- event config modify
- event config set-mail-server-password³
- lun delete³
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vserver event-log modify²
- security audit modify³
- security ipsec config modify³
- security ipsec policy create³
- security ipsec policy delete³
- security ipsec policy modify³
- 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-passphrase³
- security saml-sp create³

- 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-delete³
- volume flexcache delete
- volume modify³
- volume rename⁵
- volume recovery-queue modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot create³
- volume snapshot delete
- volume snapshot modify³
- 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 rename³
- volume snapshot restore
- vserver audit create³
- vserver audit delete³
- vserver audit disable³
- vserver audit modify³
- vserver audit rotate-log³
- vserver create²
- vserver consistency-group create⁴
- vserver consistency-group delete⁴
- vserver consistency-group modify⁴
- vserver consistency-group snapshot create⁴
- vserver consistency-group snapshot delete⁴
- vserver delete³
- vserver modify²
- vserver object-store-server audit create³

- vserver object-store-server audit delete³
- vserver object-store-server audit disable³
- vserver object-store-server audit modify³
- vserver object-store-server audit rotate-log³
- vserver object-store-server bucket cors-rule create⁴
- vserver object-store-server bucket cors-rule delete⁴
- vserver options³
- vserver peer delete
- vserver security file-directory apply³
- vserver security file-directory remove-slag³
- vserver stop⁴
- vserver vscan disable³
- vserver vscan on-access-policy create³
- vserver vscan on-access-policy delete³
- vserver vscan on-access-policy disable³
- vserver vscan on-access-policy modify³
- vserver vscan scanner-pool create³
- vserver vscan scanner-pool delete³
- vserver vscan scanner-pool modify³

9.16.1

- cluster date modify³
- cluster log-forwarding create³
- cluster log-forwarding delete³
- cluster log-forwarding modify³
- cluster peer delete
- cluster time-service ntp server create³
- cluster time-service ntp server delete³
- cluster time-service ntp key create³
- cluster time-service ntp key delete³
- cluster time-service ntp key modify³
- cluster time-service ntp server modify³
- event config modify
- event config set-mail-server-password³

- lun delete³
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vserver event-log modify²
- security audit modify³
- security ipsec config modify³
- security ipsec policy create³
- security ipsec policy delete³
- security ipsec policy modify³
- 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-passphrase³
- security saml-sp create³
- security saml-sp delete³
- security saml-sp modify³
- security webauthn credentials delete⁴
- snaplock legal-hold end³
- storage aggregate delete³
- storage aggregate offline⁴
- storage encryption disk destroy³
- storage encryption disk modify³
- storage encryption disk revert-to-original-state³
- storage encryption disk sanitize³
- system bridge run-cli³
- system controller flash-cache secure-erase run³
- system controller service-event delete³
- system health alert delete³
- system health alert modify³

- system health policy definition modify³
- system node autosupport modify³
- system node autosupport trigger modify³
- system node coredump delete³
- system node coredump delete-all³
- system node hardware nvram-encryption modify³
- system node run
- system node systemshell
- system script delete³
- system service-processor ssh add-allowed-addresses³
- system service-processor ssh remove-allowed-addresses³
- system smtape restore³
- system switch ethernet log disable-collection³
- system switch ethernet log modify³
- timezone³
- volume create³
- volume delete
- volume encryption conversion start⁴
- volume encryption rekey start⁴
- volume file privileged-delete³
- volume flexcache delete
- volume modify³
- volume recovery-queue modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot create³
- volume snapshot delete
- volume snapshot modify³
- 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 rename³
- volume snapshot restore
- vserver audit create³
- vserver audit delete³
- vserver audit disable³
- vserver audit modify³
- vserver audit rotate-log³
- vserver create²
- vserver consistency-group create⁴
- vserver consistency-group delete⁴
- vserver consistency-group modify⁴
- vserver consistency-group snapshot create⁴
- vserver consistency-group snapshot delete⁴
- vserver delete³
- vserver modify²
- vserver object-store-server audit create³
- vserver object-store-server audit delete³
- vserver object-store-server audit disable³
- vserver object-store-server audit modify³
- vserver object-store-server audit rotate-log³
- vserver object-store-server bucket cors-rule create⁴
- vserver object-store-server bucket cors-rule delete⁴
- vserver options³
- vserver peer delete
- vserver security file-directory apply³
- vserver security file-directory remove-slag³
- vserver stop⁴
- vserver vscan disable³
- vserver vscan on-access-policy create³
- vserver vscan on-access-policy delete³
- vserver vscan on-access-policy disable³
- vserver vscan on-access-policy modify³

- vserver vscan scanner-pool create³
- vserver vscan scanner-pool delete³
- vserver vscan scanner-pool modify³

9.15.1

- cluster date modify³
- cluster log-forwarding create³
- cluster log-forwarding delete³
- cluster log-forwarding modify³
- cluster peer delete
- cluster time-service ntp server create³
- cluster time-service ntp server delete³
- cluster time-service ntp key create³
- cluster time-service ntp key delete³
- cluster time-service ntp key modify³
- cluster time-service ntp server modify³
- event config modify
- event config set-mail-server-password³
- lun delete³
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vserver event-log modify²
- security audit modify³
- security ipsec config modify³
- security ipsec policy create³
- security ipsec policy delete³
- security ipsec policy modify³
- 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 modify³
- volume recovery-queue modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot create³
- volume snapshot delete
- volume snapshot modify³
- 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 rename³
- volume snapshot restore
- vserver audit create³
- vserver audit delete³
- vserver audit disable³
- vserver audit modify³
- vserver audit rotate-log³
- vserver create²
- vserver delete³
- vserver modify²
- vserver object-store-server audit create³
- vserver object-store-server audit delete³
- vserver object-store-server audit disable³
- vserver object-store-server audit modify³
- vserver object-store-server audit rotate-log³
- vserver options³
- vserver peer delete
- vserver security file-directory apply³

- vserver security file-directory remove-slag³
- vserver vscan disable³
- vserver vscan on-access-policy create³
- vserver vscan on-access-policy delete³
- vserver vscan on-access-policy disable³
- vserver vscan on-access-policy modify³
- vserver vscan scanner-pool create³
- vserver vscan scanner-pool delete³
- vserver vscan scanner-pool modify³

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vserver event-log modify²
- 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 modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot delete

- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create ²
- vserver modify ²
- vserver peer delete

9.13.1

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

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

9.12.1/9.11.1

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

1. Nuovo comando protetto da regole per 9.13.1
2. Nuovo comando protetto da regole per 9.14.1
3. Nuovo comando protetto da regole per 9.15.1
4. Nuovo comando protetto da regole per 9.16.1
5. Nuovo comando protetto da regole per 9.17.1

*Questo comando è disponibile solo con CLI e non è disponibile per System Manager in alcune versioni.

Come funziona l'approvazione multi-admin

Ogni volta che un'operazione protetta viene inserita in un cluster protetto da MAV, una richiesta di esecuzione dell'operazione viene inviata al gruppo di amministratori MAV designato.

È possibile configurare:

- I nomi, le informazioni di contatto e il numero di amministratori nel gruppo MAV.

Un amministratore MAV deve avere un ruolo RBAC con privilegi di amministratore del cluster.

- Il numero di gruppi di amministratori MAV.

- Viene assegnato un gruppo MAV per ogni regola operativa protetta.
- Per più gruppi MAV, è possibile configurare quale gruppo MAV approva una data regola.

- Il numero di approvazioni MAV richieste per eseguire un'operazione protetta.

- Un periodo di *scadenza dell'approvazione* entro il quale un amministratore MAV deve rispondere a una richiesta di approvazione.

- Un periodo di *scadenza dell'esecuzione* entro il quale l'amministratore richiedente deve completare l'operazione.

Una volta configurati questi parametri, è necessaria l'approvazione MAV per modificarli.

Gli amministratori MAV non possono approvare le proprie richieste di esecuzione di operazioni protette. Pertanto:

- MAV non deve essere abilitato sui cluster con un solo amministratore.
- Se nel gruppo MAV è presente una sola persona, l'amministratore MAV non può avviare operazioni protette; gli amministratori regolari devono avviare operazioni protette e l'amministratore MAV può solo approvare.
- Se si desidera che gli amministratori MAV siano in grado di eseguire operazioni protette, il numero di amministratori MAV deve essere maggiore di uno rispetto al numero di approvazioni richieste. Ad esempio, se sono necessarie due approvazioni per un'operazione protetta e si desidera che gli amministratori MAV le esegano, devono essere presenti tre persone nel gruppo di amministratori MAV.

Gli amministratori MAV possono ricevere richieste di approvazione in avvisi e-mail (tramite EMS) oppure interrogare la coda delle richieste. Quando ricevono una richiesta, possono intraprendere una delle tre azioni seguenti:

- Approvare
- Rifiuto (veto)
- Ignora (nessuna azione)

Le notifiche e-mail vengono inviate a tutti i responsabili dell'approvazione associati a una regola MAV quando:

- Viene creata una richiesta.
- Una richiesta viene approvata o vetoata.
- Viene eseguita una richiesta approvata.

Se il richiedente si trova nello stesso gruppo di approvazione per l'operazione, riceverà un'e-mail quando la richiesta verrà approvata.



Un richiedente non può approvare le proprie richieste anche se fa parte del gruppo di approvazione (anche se può ricevere notifiche e-mail per le proprie richieste). I richiedenti che non fanno parte di gruppi di approvazione (vale a dire, che non sono amministratori MAV) non ricevono notifiche via email.

Come funziona l'esecuzione di operazioni protette

Se l'esecuzione viene approvata per un'operazione protetta, l'utente richiedente continua con l'operazione quando richiesto. Se l'operazione è vetoed, l'utente richiedente deve eliminare la richiesta prima di procedere.

Le regole MAV vengono valutate dopo le autorizzazioni RBAC. Di conseguenza, un utente senza autorizzazioni RBAC sufficienti per l'esecuzione dell'operazione non può avviare il processo di richiesta MAV.

Le regole MAV vengono valutate prima dell'esecuzione dell'operazione protetta. Ciò significa che le regole vengono applicate in base allo stato corrente del sistema. Ad esempio, se una regola MAV viene creata per volume modify con una domanda di -size 5GB , utilizzando volume modify per ridimensionare un volume da 5 GB a 2 GB sarà necessaria l'approvazione MAV, ma per ridimensionare un volume da 2 GB a 5 GB non sarà necessaria l'approvazione.

Informazioni correlate

- "[cluster](#)"
- "[lun](#)"
- "[sicurezza](#)"
- "[estremità a tenuta legale a scatto](#)"
- "[aggregato di stoccaggio](#)"
- "[crittografia dello storage](#)"
- "[sistema](#)"

Gestire i gruppi di approvazione degli amministratori ONTAP per MAV

Prima di attivare la verifica multi-amministratore (MAV), è necessario creare un gruppo di approvazione amministratore contenente uno o più amministratori a cui concedere l'autorizzazione di approvazione o voto. Una volta attivata la verifica multi-admin, qualsiasi modifica all'appartenenza al gruppo di approvazione richiede l'approvazione di uno degli amministratori qualificati esistenti.

A proposito di questa attività

È possibile aggiungere amministratori esistenti a un gruppo MAV o creare nuovi amministratori.

La funzionalità MAV rispetta le impostazioni RBAC (role-based access control) esistenti. I potenziali amministratori MAV devono disporre di privilegi sufficienti per eseguire operazioni protette prima di aggiungerli ai gruppi di amministratori MAV. "[Scopri di più su RBAC.](#)"

È possibile configurare MAV per avvisare gli amministratori MAV che le richieste di approvazione sono in sospeso. A tale scopo, è necessario configurare le notifiche e-mail, in particolare l' Mail From e. Mail Server parametri—oppure è possibile cancellare questi parametri per disattivare la notifica. Senza avvisi via email, gli amministratori MAV devono controllare manualmente la coda di approvazione.

A partire da ONTAP 9.15.1, è possibile configurare gli utenti di Active Directory (AD) come amministratori MAV. L'utente AD deve essere "[configurato come amministratore ONTAP](#)".

Procedura di System Manager

Se si desidera creare un gruppo di approvazione MAV per la prima volta, consultare la procedura di System Manager in "[attiva la verifica multi-admin.](#)"

Per modificare un gruppo di approvazione esistente o creare un gruppo di approvazione aggiuntivo:

1. Identificare gli amministratori per ricevere la verifica multi-admin.

- a. Fare clic su **Cluster > Settings**.
- b. Fare clic su accanto a **utenti e ruoli**.
- c. Fare clic su **Add utenti**.
- d. Modificare il registro in base alle esigenze.

Per ulteriori informazioni, vedere "[Controllare l'accesso dell'amministratore.](#)"

2. Creare o modificare il gruppo di approvazione MAV:

- a. Fare clic su **Cluster > Settings**.
- b. Fare clic su accanto a **Multi-Admin Approval** nella sezione **Security**. (Se MAV non è ancora configurato, viene visualizzata l' icona).
 - Name (Nome): Immettere un nome di gruppo.
 - Responsabili dell'approvazione: Selezionare i responsabili dell'approvazione da un elenco di utenti.
 - Email address (Indirizzo email): Inserire gli indirizzi email.
 - Default group (Gruppo predefinito): Selezionare un gruppo.

L'approvazione MAV è necessaria per modificare una configurazione esistente una volta abilitato MAV.

Procedura CLI

1. Verificare che siano stati impostati i valori per Mail From e Mail Server parametri. Inserire:

```
event config show
```

Il display dovrebbe essere simile a quanto segue:

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

Per configurare questi parametri, immettere:

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

Ulteriori informazioni su `event config show` e `event config modify` nella "[Riferimento al comando ONTAP](#)".

2. Identificare gli amministratori per ricevere la verifica multi-admin

Se si desidera...	Immettere questo comando
Visualizza gli amministratori correnti	<code>security login show</code>
Modificare le credenziali degli amministratori correnti	<code>security login modify <parameters></code>
Creare nuovi account amministratore	<code>security login create -user-or-group -name admin_name -application ssh -authentication-method password</code>

Ulteriori informazioni su `security login show`, `security login modify` e `security login create` nella "[Riferimento al comando ONTAP](#)".

3. Creare il gruppo di approvazione MAV:

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

- ° `-vserver` - Solo la SVM amministrativa è supportata in questa versione.
- ° `-name` - Il nome del gruppo MAV, composto da un massimo di 64 caratteri.
- ° `-approvers` - L'elenco di uno o più approvatori. Per gli utenti AD, utilizzare il formato domain\user . Ad esempio, mydomain\pavan .
- ° `-email` - Uno o più indirizzi e-mail che vengono notificati quando una richiesta viene creata, approvata, sottoposta a voto o eseguita.

Esempio: il seguente comando crea un gruppo MAV con due membri e indirizzi e-mail associati.

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

4. Verificare la creazione e l'appartenenza del gruppo:

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

Esempio:

```

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

```

Utilizzare questi comandi per modificare la configurazione iniziale del gruppo MAV.

Nota: tutti richiedono l'approvazione dell'amministratore MAV prima dell'esecuzione.

Se si desidera...	Immettere questo comando
Modificare le caratteristiche del gruppo o le informazioni sui membri esistenti	security multi-admin-verify approval-group modify [parameters]
Aggiungere o rimuovere membri	security multi-admin-verify approval-group replace [-vserver <i>svm_name</i>] -name <i>group_name</i> [-approvers-to-add <i>approver1[, approver2...]</i>] [-approvers-to-remove <i>approver1[, approver2...]</i>]
Eliminare un gruppo	security multi-admin-verify approval-group delete [-vserver <i>svm_name</i>] -name <i>group_name</i>

Informazioni correlate

- ["sicurezza multi-admin-verify"](#)

Attiva o disattiva la verifica multi-admin in ONTAP

La verifica multi-admin (MAV) deve essere attivata esplicitamente. Una volta attivata la verifica multi-admin, l'approvazione da parte degli amministratori di un gruppo di approvazione MAV (amministratori MAV) è necessaria per eliminarla.

A proposito di questa attività

Una volta attivato MAV, la modifica o la disattivazione di MAV richiede l'approvazione dell'amministratore MAV.



Se è necessario disabilitare la funzionalità di verifica multi-amministratore senza l'approvazione dell'amministratore MAV, contattare l'assistenza NetApp e menzionare quanto segue ["Knowledge Base NetApp : come disabilitare la verifica multi-amministratore se l'amministratore MAV non è disponibile"](#).

Quando si attiva MAV, è possibile specificare globalmente i seguenti parametri.

Gruppi di approvazione

Un elenco di gruppi di approvazione globali. Per abilitare la funzionalità MAV è necessario almeno un gruppo.



Se si utilizza MAV con la protezione ransomware autonoma (ARP), definire un gruppo di approvazione nuovo o esistente responsabile dell'approvazione della pausa, della disattivazione e dell'eliminazione delle richieste sospette di ARP.

Responsabili dell'approvazione richiesti

Il numero di responsabili dell'approvazione necessari per eseguire un'operazione protetta. Il numero predefinito e minimo è 1.



Il numero richiesto di responsabili dell'approvazione deve essere inferiore al numero totale di responsabili dell'approvazione univoci nei gruppi di approvazione predefiniti.

Scadenza approvazione (ore, minuti, secondi)

Periodo entro il quale un amministratore MAV deve rispondere a una richiesta di approvazione. Il valore predefinito è un'ora (1h), il valore minimo supportato è un secondo (1s) e il valore massimo supportato è 14 giorni (14d).

Scadenza dell'esecuzione (ore, minuti, secondi)

Il periodo entro il quale l'amministratore richiedente deve completare l'operazione::: Il valore predefinito è un'ora (1h), il valore minimo supportato è un secondo (1s) e il valore massimo supportato è 14 giorni (14d).

È inoltre possibile eseguire l'override di uno qualsiasi di questi parametri per specifici "[regole operative](#)."

Procedura di System Manager

1. Identificare gli amministratori per ricevere la verifica multi-admin.
 - a. Fare clic su **Cluster > Settings**.
 - b. Fare clic su accanto a **utenti e ruoli**.
 - c. Fare clic su **Add utenti**.
 - d. Modificare il registro in base alle esigenze.

Per ulteriori informazioni, vedere "[Controllare l'accesso dell'amministratore](#)."
2. Abilitare la verifica multi-admin creando almeno un gruppo di approvazione e aggiungendo almeno una regola.
 - a. Fare clic su **Cluster > Settings**.
 - b. Fare clic su accanto a **Multi-Admin Approval** nella sezione **Security**.
 - c. Fare clic per aggiungere almeno un gruppo di approvazione.
 - Name (Nome): Immettere il nome di un gruppo.
 - Responsabili dell'approvazione: Selezionare i responsabili dell'approvazione da un elenco di utenti.
 - Email address (Indirizzo e-mail) – inserire gli indirizzi e-mail.
 - Default group (Gruppo predefinito) – selezionare un gruppo.
 - d. Aggiungere almeno una regola.

- Operation (funzionamento) – selezionare un comando supportato dall'elenco.
 - Query - immettere le opzioni e i valori dei comandi desiderati.
 - Parametri facoltativi; lasciare vuoto per applicare le impostazioni globali o assegnare un valore diverso per regole specifiche per sostituire le impostazioni globali.
 - Numero richiesto di responsabili dell'approvazione
 - Gruppi di approvazione
- e. Fare clic su **Advanced Settings** (Impostazioni avanzate) per visualizzare o modificare le impostazioni predefinite.
- Numero richiesto di responsabili dell'approvazione (impostazione predefinita: 1)
 - Scadenza richiesta di esecuzione (impostazione predefinita: 1 ora)
 - Scadenza richiesta di approvazione (impostazione predefinita: 1 ora)
 - Server di posta*
 - Da indirizzo email*
- *Questi aggiornano le impostazioni e-mail gestite in "Gestione notifiche". Se non sono ancora stati configurati, viene richiesto di impostarli.
- f. Fare clic su **Enable** (attiva) per completare la configurazione iniziale MAV.

Dopo la configurazione iniziale, lo stato MAV corrente viene visualizzato nel riquadro **Multi-Admin Approval**.

- Stato (attivato o meno)
- Operazioni attive per le quali sono richieste approvazioni
- Numero di richieste aperte in stato di attesa

È possibile visualizzare una configurazione esistente facendo clic su . L'approvazione MAV è necessaria per modificare una configurazione esistente.

Per disattivare la verifica multi-admin:

1. Fare clic su **Cluster > Settings**.
2. Fare clic su accanto a **Multi-Admin Approval** nella sezione **Security**.
3. Fare clic sul pulsante di attivazione/disattivazione.

Per completare questa operazione è richiesta l'approvazione MAV.

Procedura CLI

Prima di attivare la funzionalità MAV nella CLI, almeno una "[Gruppo di amministratori MAV](#)" deve essere stato creato.

Se si desidera...	Immettere questo comando
Abilitare la funzionalità MAV	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [-required-approvers nn] -enabled true [-execution-expiry [nnh] [nnm] [nns]] [-approval-expiry [nnh] [nnm] [nns]]</pre> <p>Esempio: Il seguente comando abilita MAV con 1 gruppo di approvazione, 2 responsabili dell'approvazione richiesti e periodi di scadenza predefiniti.</p> <pre>cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>Completare la configurazione iniziale aggiungendone almeno una "regola operativa."</p>
Modifica di una configurazione MAV (richiede l'approvazione MAV)	<pre>security multi-admin-verify approval-group modify [-approval-groups group1 [,group2...]] [-required-approvers nn] [-execution-expiry [nnh] [nnm] [nns]] [-approval-expiry [nnh] [nnm] [nns]]</pre>
Verificare la funzionalità MAV	<pre>security multi-admin-verify show</pre> <p>Esempio:</p> <pre>cluster-1::> security multi-admin-verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- ----- true 2 1h 1h mav-grp1</pre>
Disattivare la funzionalità MAV (richiede l'approvazione MAV)	<pre>security multi-admin-verify modify -enabled false</pre>

Informazioni correlate

- "sicurezza multi-admin-verify"

Gestisci regole di verifica con amministratori multipli per operazioni protette in ONTAP

Si creano regole di verifica multi-amministratore (MAV) per designare le operazioni che richiedono l'approvazione. Ogni volta che viene avviata un'operazione, le operazioni protette vengono intercettate e viene generata una richiesta di approvazione.

Le regole possono essere create prima di abilitare MAV da qualsiasi amministratore con funzionalità RBAC appropriate, ma una volta attivata la MAV, qualsiasi modifica al set di regole richiede l'approvazione MAV.

È possibile creare una sola regola MAV per operazione; ad esempio, non è possibile creare più regole volume-snapshot-delete regole. Tutti i vincoli di regola desiderati devono essere contenuti all'interno di una regola.

È possibile creare regole da proteggere "[sono disponibili](#)". È possibile proteggere ogni comando a partire dalla versione di ONTAP in cui era disponibile per la prima volta una funzionalità di protezione per il comando.

Le regole per i comandi MAV di default del sistema, il security multi-admin-verify "[comandi](#)", non può essere modificato.

Oltre alle operazioni definite dal sistema, i seguenti comandi sono protetti per impostazione predefinita quando è abilitata la verifica multi-amministratore, ma è possibile modificare le regole per rimuovere la protezione per questi comandi:

- "password di accesso di sicurezza"
- "sblocco accesso di sicurezza"
- "partenza"

Vincoli della regola

Quando si crea una regola, è possibile specificare facoltativamente l' -query` opzione per limitare la richiesta a un sottoinsieme della funzionalità del comando. Questa ` -query opzione può essere utilizzata anche per limitare gli elementi di configurazione, come SVM, volume e nomi delle snapshot.

Ad esempio, nel volume snapshot delete comando, -query può essere impostato su -snapshot !hourly*, !daily*, !weekly*, il che significa che gli snapshot di volume con attributi orari, giornalieri o settimanali sono esclusi dalle protezioni MAV.

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



Tutti gli elementi di configurazione esclusi non sono protetti da MAV e qualsiasi amministratore può eliminarli o rinominarli.

Per impostazione predefinita, le regole specificano che un comando corrispondente viene generato automaticamente quando si inserisce un `security multi-admin-verify request create "protected_operation"` operazione protetta. È possibile modificare questo valore predefinito per richiedere che il ``request create`` comando venga immesso separatamente.

Per impostazione predefinita, le regole ereditano le seguenti impostazioni MAV globali, anche se è possibile specificare eccezioni specifiche della regola:

- Numero richiesto di approvatori
- Gruppi di approvazione
- Periodo di scadenza dell'approvazione
- Periodo di scadenza dell'esecuzione

Procedura di System Manager

Se si desidera aggiungere una regola operativa protetta per la prima volta, consultare la procedura di System Manager in "[attiva la verifica multi-admin.](#)"

Per modificare il set di regole esistente:

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare accanto a **Multi-Admin Approval** nella sezione **Security**.
3. Selezionare **Add** per aggiungere almeno una regola; è anche possibile modificare o eliminare le regole esistenti.
 - Operation (funzionamento) – selezionare un comando supportato dall'elenco.
 - Query - immettere le opzioni e i valori dei comandi desiderati.
 - Parametri facoltativi: Lasciare vuoto per applicare le impostazioni globali o assegnare un valore diverso per regole specifiche per sostituire le impostazioni globali.
 - Numero richiesto di responsabili dell'approvazione
 - Gruppi di approvazione

Procedura CLI



Tutto `security multi-admin-verify rule` i comandi richiedono l'approvazione dell'amministratore MAV prima dell'esecuzione tranne `security multi-admin-verify rule show`.

Se si desidera...	Immettere questo comando
Creare una regola	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>

Se si desidera...	Immettere questo comando
Modificare le credenziali degli amministratori correnti	<pre>security login modify <parameters></pre> <p>Esempio: La seguente regola richiede l'approvazione per eliminare il volume root.</p> <pre>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</pre>
Modificare una regola	<pre>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</pre>
Eliminare una regola	<pre>security multi-admin-verify rule delete -operation "protected_operation"</pre>
Mostra regole	<pre>security multi-admin-verify rule show</pre>

Informazioni correlate

- "[regola di verifica multi-amministrazione di sicurezza](#)"
- "[modifica dell'accesso di sicurezza](#)"

Richiedere l'esecuzione di operazioni MAV protette in ONTAP

Quando si avvia un'operazione o un comando protetto su un cluster abilitato per la verifica multi-admin (MAV), ONTAP intercetta automaticamente l'operazione e chiede di generare una richiesta, che deve essere approvata da uno o più amministratori in un gruppo di approvazione MAV (amministratori MAV). In alternativa, è possibile creare una richiesta MAV senza la finestra di dialogo.

Se approvata, è necessario rispondere alla richiesta per completare l'operazione entro il periodo di scadenza della richiesta. In caso di voto o di superamento dei termini di richiesta o scadenza, è necessario eliminare la richiesta e reinviarla.

La funzionalità MAV rispetta le impostazioni RBAC esistenti. In altri termini, il ruolo di amministratore deve disporre di privilegi sufficienti per eseguire un'operazione protetta, indipendentemente dalle impostazioni MAV. "[Scopri di più su RBAC](#)".

Se sei un amministratore MAV, le tue richieste di eseguire operazioni protette devono essere approvate anche da un amministratore MAV.

Procedura di System Manager

Quando un utente fa clic su una voce di menu per avviare un'operazione e l'operazione è protetta, viene generata una richiesta di approvazione e l'utente riceve una notifica simile a quanto segue:

Approval request to delete the volume was sent.

Track the request ID 356 from Events & Jobs > Multi-Admin Requests.

La finestra **Richieste multi-amministratore** è disponibile quando MAV è attivato, mostrando le richieste in sospeso in base all'ID di accesso dell'utente e al ruolo MAV (approvatore o meno). Per ogni richiesta in sospeso, vengono visualizzati i seguenti campi:

- Operazione
- Indice (numero)
- Stato (in sospeso, approvato, rifiutato, eseguito o scaduto)

Se una richiesta viene respinta da un responsabile dell'approvazione, non sono possibili ulteriori azioni.

- Query (qualsiasi parametro o valore per l'operazione richiesta)
- Utente richiedente
- La richiesta scade il
- (Numero di) approvatori in sospeso
- (Numero di) potenziali responsabili dell'approvazione

Una volta approvata la richiesta, l'utente richiedente può riprovare l'operazione entro il periodo di scadenza.

Se l'utente tenta di eseguire nuovamente l'operazione senza approvazione, viene visualizzata una notifica simile alla seguente:

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

Procedura CLI

1. Inserire l'operazione protetta direttamente o utilizzando il comando di richiesta MAV.

Esempi – per eliminare un volume, immettere uno dei seguenti comandi:

◦ volume delete

```
cluster-1::*> volume delete -volume voll -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. Controllare lo stato della richiesta e rispondere all'avviso MAV.

a. Se la richiesta viene approvata, rispondere al messaggio CLI per completare l'operazione.

Esempio:

```
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. Se la richiesta è stata vetoata o il periodo di scadenza è scaduto, eliminarla e reinviarla o contattare l'amministratore MAV.

Esempio:

```

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".

```

Informazioni correlate

- ["sicurezza multi-admin-verify"](#)

Gestire le richieste di operazioni protette da MAV in ONTAP

Quando gli amministratori di un gruppo di approvazione MAV (amministratori MAV) vengono informati di una richiesta di esecuzione di un'operazione in sospeso, devono rispondere con un messaggio di approvazione o di voto entro un periodo di tempo stabilito (scadenza dell'approvazione). Se non si riceve un numero sufficiente di approvazioni, il richiedente deve eliminare la richiesta e presentarne un'altra.

A proposito di questa attività

Le richieste di approvazione sono identificate con numeri di indice, inclusi nei messaggi e-mail e nelle visualizzazioni della coda di richiesta.



Le richieste in stato terminale possono essere sovrascritte o rimosse automaticamente. Utilizzare il ["registro di controllo"](#) per rivedere le richieste precedenti.

È possibile visualizzare le seguenti informazioni dalla coda di richiesta:

Operazione

Operazione protetta per la quale viene creata la richiesta.

Query

Oggetto (o oggetti) su cui l'utente desidera applicare l'operazione.

Stato

Lo stato corrente della richiesta: In sospeso, approvato, rifiutato, scaduto, eseguito. Se una richiesta viene respinta da un responsabile dell'approvazione, non sono possibili ulteriori azioni.

Responsabili dell'approvazione richiesti

Il numero di amministratori MAV necessari per approvare la richiesta. Un utente può impostare il parametro required-approvers per la regola dell'operazione. Se un utente non imposta i responsabili dell'approvazione richiesti sulla regola, vengono applicati i responsabili dell'approvazione richiesti dall'impostazione globale.

Responsabili dell'approvazione in sospeso

Il numero di amministratori MAV che sono ancora necessari per approvare la richiesta per essere contrassegnati come approvati.

Scadenza approvazione

Periodo entro il quale un amministratore MAV deve rispondere a una richiesta di approvazione. Qualsiasi utente autorizzato può impostare la scadenza dell'approvazione per una regola dell'operazione. Se la regola non è impostata su approvazione-scadenza, viene applicata l'approvazione-scadenza dall'impostazione globale.

Scadenza dell'esecuzione

Il periodo entro il quale l'amministratore richiedente deve completare l'operazione. Qualsiasi utente autorizzato può impostare la scadenza dell'esecuzione per una regola dell'operazione. Se la regola non è impostata su execution-expiry, viene applicata l'impostazione di execution-execution-expiry dall'impostazione globale.

Approvati dagli utenti

Gli amministratori MAV che hanno approvato la richiesta.

Veto dell'utente

Gli amministratori MAV che hanno posto il voto alla richiesta.

Storage VM (vserver)

SVM a cui è associata la richiesta. Solo la SVM amministrativa è supportata in questa release.

Richiesto dall'utente

Il nome utente dell'utente che ha creato la richiesta.

Ora di creazione

L'ora in cui viene creata la richiesta.

Tempo approvato

L'ora in cui lo stato della richiesta è cambiato in approvato.

Commento

Eventuali commenti associati alla richiesta.

Utenti consentiti

L'elenco degli utenti autorizzati a eseguire l'operazione protetta per cui la richiesta è approvata. Se `users-permitted` è vuoto, quindi qualsiasi utente con autorizzazioni appropriate può eseguire l'operazione.

System Manager

Gli amministratori MAV ricevono messaggi di posta elettronica con i dettagli della richiesta di approvazione, il periodo di scadenza della richiesta e un collegamento per approvare o rifiutare la richiesta. Possono accedere a una finestra di dialogo di approvazione cliccando sul collegamento nell'e-mail oppure andando su **Eventi e lavori > Richieste** in Gestione sistema.

La finestra **Richieste** è disponibile quando è abilitata la verifica multi-amministratore e mostra le richieste in sospeso in base all'ID di accesso dell'utente e al ruolo MAV (approvatore o meno).

- Operazione
- Indice (numero)
- Stato (in sospeso, approvato, rifiutato, eseguito o scaduto)

Se una richiesta viene respinta da un responsabile dell'approvazione, non sono possibili ulteriori azioni.

- Query (qualsiasi parametro o valore per l'operazione richiesta)
- Utente richiedente
- La richiesta scade il
- (Numero di) approvatori in sospeso
- (Numero di) potenziali responsabili dell'approvazione

Gli amministratori MAV dispongono di controlli aggiuntivi in questa finestra; possono approvare, rifiutare o eliminare singole operazioni o gruppi di operazioni selezionati. Tuttavia, se l'amministratore MAV è l'utente richiedente, non può approvare, rifiutare o eliminare le proprie richieste.

CLI

1. Quando si riceve una notifica via e-mail delle richieste in sospeso, annotare il numero di indice della richiesta e il periodo di scadenza dell'approvazione. Il numero di indice può essere visualizzato anche utilizzando le opzioni **show** o **show-pending** menzionate di seguito.
2. Approvare o veto la richiesta.

Se si desidera...	Immettere questo comando
Approvare una richiesta	<code>security multi-admin-verify request approve nn</code>
Veto di una richiesta	<code>security multi-admin-verify request veto nn</code>
Mostra tutte le richieste, le richieste in sospeso o una singola richiesta	<code>'security multi-admin-verify request { show</code>

Se si desidera...	Immettere questo comando
show-pending } [nn] { -fields field1[,field2...]	[-instance] }` È possibile visualizzare tutte le richieste nella coda o solo quelle in sospeso. Se si inserisce il numero di indice, vengono visualizzate solo le informazioni relative a tale valore. È possibile visualizzare informazioni su campi specifici utilizzando -fields o su tutti i campi (utilizzando il -instance parametro).
Eliminare una richiesta	security multi-admin-verify request delete nn

Esempio:

La seguente sequenza approva una richiesta dopo che l'amministratore MAV ha ricevuto l'email di richiesta con il numero di indice 3, che ha già un'approvazione.

```
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: -
```

Esempio:

La seguente sequenza veta una richiesta dopo che l'amministratore MAV ha ricevuto l'email di richiesta con il numero di indice 3, che ha già un'approvazione.

```
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: -
```

Informazioni correlate

- ["sicurezza multi-admin-verify"](#)

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.