



Gestion de la vérification multi-administrateurs

ONTAP 9

NetApp
April 24, 2024

Sommaire

- Gestion de la vérification multi-administrateurs 1
 - Présentation de la vérification multi-administrateur 1
 - Gérer les groupes d’approbation des administrateurs 5
 - Activez et désactivez la vérification multi-administration 7
 - Gérer les règles d’opération protégées 11
 - Demander l’exécution d’opérations protégées 14
 - Gérer les demandes d’opérations protégées 17

Gestion de la vérification multi-administrateurs

Présentation de la vérification multi-administrateur

Depuis ONTAP 9.11.1, vous pouvez utiliser la vérification multi-administration (MAV) pour vous assurer que certaines opérations, telles que la suppression de volumes ou de copies Snapshot, ne peuvent être exécutées qu'après approbation d'administrateurs désignés. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables.

La configuration de la vérification multi-administrateurs comprend :

- ["Création d'un ou plusieurs groupes d'approbation administrateur."](#)
- ["Activation de la fonctionnalité de vérification multi-administrateurs."](#)
- ["Ajout ou modification de règles."](#)

Après la configuration initiale, ces éléments ne peuvent être modifiés que par les administrateurs d'un groupe d'approbation MAV (administrateurs MAV).

Lorsque la vérification multi-administrateur est activée, chaque opération protégée nécessite trois étapes :

- Lorsqu'un utilisateur lance l'opération, un ["la demande a été générée."](#)
- Avant de pouvoir être exécuté, au moins un ["L'administrateur MAV doit approuver."](#)
- Après approbation, l'utilisateur termine l'opération.

La vérification multi-administrateurs n'est pas destinée aux volumes ou aux flux de travail nécessitant une automatisation élevée, car chaque tâche automatisée nécessite une approbation avant que l'opération ne puisse être terminée. Si vous souhaitez utiliser l'automatisation et le MAV ensemble, il est recommandé d'utiliser des requêtes pour des opérations MAV spécifiques. Vous pouvez, par exemple, appliquer `volume delete` MAV ne règle que les volumes où l'automatisation n'est pas impliquée et vous pouvez désigner ces volumes avec un schéma de nommage particulier.



Si vous avez besoin de désactiver la fonctionnalité de vérification multi-administrateurs sans l'approbation de l'administrateur MAV, contactez le support NetApp et mentionnez l'article suivant de la base de connaissances : ["Comment désactiver la vérification multi-administrateur si MAV admin n'est pas disponible"](#).

Fonctionnement de la vérification multi-administration

La vérification multi-administrateurs comprend les éléments suivants :

- Groupe d'un ou plusieurs administrateurs ayant des pouvoirs d'approbation et de veto.
- Un ensemble d'opérations ou de commandes protégées dans une table *rules*.
- Un *moteur de règles* pour identifier et contrôler l'exécution des opérations protégées.

Les règles MAV sont évaluées après les règles de contrôle d'accès basé sur des rôles (RBAC). Par conséquent, les administrateurs qui exécutent ou approuvent les opérations protégées doivent déjà posséder le minimum de privilèges RBAC pour ces opérations. ["En savoir plus sur le RBAC."](#)

Règles définies par le système

Lorsque la vérification multi-admin est activée, les règles définies par le système (également appelées règles *Guard-rail*) établissent un ensemble d'opérations MAV pour contenir le risque de contournement du processus MAV lui-même. Ces opérations ne peuvent pas être supprimées de la table des règles. Une fois MAV activé, les opérations désignées par un astérisque (*) nécessitent l'approbation d'un ou de plusieurs administrateurs avant l'exécution, à l'exception des commandes * show*.

- security multi-admin-verify modify fonctionnement*

Contrôle la configuration de la fonctionnalité de vérification multi-administrateur.

- security multi-admin-verify approval-group opérations*

Contrôlez l'appartenance à un ensemble d'administrateurs avec des informations d'identification de vérification multi-administrateur.

- security multi-admin-verify rule opérations*

Contrôler le jeu de commandes qui nécessitent une vérification multi-administrateur.

- security multi-admin-verify request exploitation

Contrôler le processus d'approbation.

Commandes protégées par des règles

Outre les commandes définies par le système, les commandes suivantes sont protégées par défaut lorsque la vérification multi-admin est activée, mais vous pouvez modifier les règles afin de supprimer la protection de ces commandes.

- security login password
- security login unlock
- set

Les commandes suivantes peuvent être protégées dans ONTAP 9.11.1 et versions ultérieures.

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

Les commandes suivantes peuvent être protégées à 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`

Les commandes suivantes peuvent être protégées à partir de ONTAP 9.14.1 :

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

Fonctionnement de l’approbation multi-admin

Chaque fois qu’une opération protégée est saisie sur un cluster protégé par MAV, une demande d’exécution d’opération est envoyée au groupe d’administrateurs MAV désigné.

Vous pouvez configurer :

- Les noms, les coordonnées et le nombre d’administrateurs du groupe MAV.

Un administrateur MAV doit avoir un rôle RBAC avec des privilèges d’administrateur de cluster.

- Nombre de groupes d’administrateurs MAV.
 - Un groupe MAV est attribué pour chaque règle d’opération protégée.

- Pour plusieurs groupes MAV, vous pouvez configurer quel groupe MAV approuve une règle donnée.
- Nombre d'approbations MAV nécessaires à l'exécution d'une opération protégée.
- Période_d'expiration_ de l'approbation au cours de laquelle un administrateur MAV doit répondre à une demande d'approbation.
- Période_d'expiration_ de l'exécution pendant laquelle l'administrateur demandeur doit effectuer l'opération.

Une fois ces paramètres configurés, l'approbation MAV est requise pour les modifier.

Les administrateurs MAV ne peuvent pas approuver leurs propres demandes d'exécution d'opérations protégées. Par conséquent :

- MAV ne doit pas être activé sur les clusters avec un seul administrateur.
- S'il n'y a qu'une seule personne dans le groupe MAV, cet administrateur MAV ne peut pas entrer d'opérations protégées ; les administrateurs réguliers doivent les entrer et l'administrateur MAV ne peut approuver que.
- Si vous souhaitez que les administrateurs MAV puissent exécuter des opérations protégées, le nombre d'administrateurs MAV doit être supérieur d'un au nombre d'approbations requises. Par exemple, si deux approbations sont requises pour une opération protégée et que vous voulez que les administrateurs MAV les exécutent, il doit y avoir trois personnes dans le groupe administrateurs MAV.

Les administrateurs MAV peuvent recevoir des demandes d'approbation dans des alertes par e-mail (à l'aide d'EMS) ou interroger la file d'attente des requêtes. Lorsqu'ils reçoivent une demande, ils peuvent effectuer l'une des trois actions suivantes :

- Approuver
- Rejet (veto)
- Ignorer (aucune action)

Les notifications par e-mail sont envoyées à tous les approbateurs associés à une règle MAV lorsque :

- Une demande est créée.
- Une demande est approuvée ou vetotée.
- Une requête approuvée est exécutée.

Si le demandeur se trouve dans le même groupe d'approbation pour l'opération, il recevra un e-mail lorsque sa demande est approuvée.

Remarque : Un demandeur ne peut approuver ses propres demandes, même si elles font partie du groupe d'approbation. Mais ils peuvent obtenir les notifications par e-mail. Les demandeurs qui ne sont pas dans les groupes d'approbation (c'est-à-dire qui ne sont pas des administrateurs MAV) ne reçoivent pas de notifications par e-mail.

Fonctionnement de l'exécution des opérations protégées

Si l'exécution est approuvée pour une opération protégée, l'utilisateur demandeur continue avec l'opération à l'invite. Si l'opération est mise au veto, l'utilisateur requérant doit supprimer la demande avant de continuer.

Les règles MAV sont évaluées après les autorisations RBAC. Par conséquent, un utilisateur sans autorisations RBAC suffisantes pour l'exécution de l'opération ne peut pas lancer le processus de requête MAV.

Gérer les groupes d'approbation des administrateurs

Avant d'activer la vérification multi-administrateur (MAV), vous devez créer un groupe d'approbation administrateur contenant un ou plusieurs administrateurs à accorder ou à accorder une autorité d'approbation ou de veto. Une fois que vous avez activé la vérification multi-administrateur, toute modification de l'appartenance au groupe d'approbation nécessite l'approbation de l'un des administrateurs qualifiés existants.

Description de la tâche

Vous pouvez ajouter des administrateurs existants à un groupe MAV ou créer de nouveaux administrateurs.

La fonctionnalité MAV permet de définir les paramètres existants de contrôle d'accès basé sur des rôles (RBAC). Les administrateurs MAV potentiels doivent disposer de privilèges suffisants pour exécuter des opérations protégées avant d'être ajoutés aux groupes d'administrateurs MAV. ["En savoir plus sur le RBAC."](#)

Vous pouvez configurer MAV pour avertir les administrateurs MAV que les demandes d'approbation sont en attente. Pour ce faire, vous devez configurer les notifications par e-mail, en particulier, le `Mail From` et `Mail Server` paramètres—ou vous pouvez effacer ces paramètres pour désactiver la notification. Sans alertes par e-mail, les administrateurs MAV doivent vérifier manuellement la file d'attente d'approbation.

Procédure de System Manager

Si vous souhaitez créer un groupe d'approbation MAV pour la première fois, reportez-vous à la procédure System Manager à ["activation de la vérification multi-administrateurs"](#)

Pour modifier un groupe d'approbation existant ou créer un groupe d'approbation supplémentaire :

1. Identifiez les administrateurs pour qu'ils reçoivent une vérification multi-administrateur.
 - a. Cliquez sur **Cluster > Paramètres**.
 - b. Cliquez sur ➔ À côté de **utilisateurs et rôles**.
 - c. Cliquez sur ➕ **Add** Sous **utilisateurs**.
 - d. Modifiez la liste si nécessaire.

Pour plus d'informations, voir ["Contrôlez l'accès administrateur."](#)

2. Créer ou modifier le groupe d'approbation MAV :
 - a. Cliquez sur **Cluster > Paramètres**.
 - b. Cliquez sur ➔ En regard de **Multi-Admin Approval** dans la section **Security**. (Vous verrez le ⚙ Si MAV n'est pas encore configuré.)
 - Nom : entrez un nom de groupe.
 - Approbateurs : sélectionnez des approbateurs dans une liste d'utilisateurs.
 - Adresse e-mail : saisissez une ou plusieurs adresses e-mail.
 - Groupe par défaut : sélectionnez un groupe.

Une approbation MAV est requise pour modifier une configuration existante une fois que MAV est activé.

Procédure CLI

1. Vérifier que les valeurs ont été définies pour le Mail From et Mail Server paramètres. Entrez :

```
event config show
```

L'affichage doit être similaire à ce qui suit :

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

Pour configurer ces paramètres, entrez :

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

2. Identifiez les administrateurs pour qu'ils reçoivent une vérification multi-administrateur

Si vous voulez...	Saisissez cette commande
Afficher les administrateurs actuels	<code>security login show</code>
Modifier les informations d'identification des administrateurs actuels	<code>security login modify <parameters></code>
Créer de nouveaux comptes d'administrateur	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

3. Créer le groupe d'approbation MAV :

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

- -vserver - Seul le SVM d'admin est pris en charge dans cette version.
- -name - Le nom du groupe MAV, jusqu'à 64 caractères.
- -approvers - La liste d'un ou plusieurs approbateurs.
- -email - Une ou plusieurs adresses e-mail qui sont notifiées lors de la création, de l'approbation, du veto ou de l'exécution d'une demande.

Exemple : la commande suivante crée un groupe MAV avec deux membres et des adresses e-mail associées.


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

4. Vérifier la création et l'appartenance de groupe :

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

Exemple:

```
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
```

Utilisez ces commandes pour modifier votre configuration initiale du groupe MAV.

Remarque : tous exigent l'approbation de l'administrateur MAV avant l'exécution.

Si vous voulez...	Saisissez cette commande
Modifier les caractéristiques du groupe ou modifier les informations du membre existant	<code>security multi-admin-verify approval-group modify [<i>parameters</i>]</code>
Ajouter ou supprimer des membres	<code>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>]</code>
Supprimer un groupe	<code>security multi-admin-verify approval-group delete [-vserver <i>svm_name</i>] -name <i>group_name</i></code>

Activez et désactivez la vérification multi-administration

La vérification multi-administrateur (MAV) doit être activée explicitement. Une fois que vous avez activé la vérification multi-administrateur, l'approbation par les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) est requise pour la supprimer.

Description de la tâche

Une fois MAV activé, la modification ou la désactivation de MAV nécessite l'approbation de l'administrateur MAV.



Si vous avez besoin de désactiver la fonctionnalité de vérification multi-administrateurs sans l'approbation de l'administrateur MAV, contactez le support NetApp et mentionnez l'article suivant de la base de connaissances : ["Comment désactiver la vérification multi-administrateur si MAV admin n'est pas disponible"](#).

Lorsque vous activez MAV, vous pouvez spécifier globalement les paramètres suivants.

Groupes d'approbation

Une liste de groupes d'approbation globaux. Au moins un groupe est requis pour activer la fonctionnalité MAV.



Si vous utilisez MAV avec la protection anti-ransomware autonome (ARP), définissez un nouveau groupe d'approbation ou un groupe d'approbation existant chargé d'approuver la pause ARP, de désactiver et d'effacer les demandes suspectes.

Approbateurs requis

Nombre d'approbateurs requis pour exécuter une opération protégée. La valeur par défaut et le nombre minimum sont 1.



Le nombre requis d'approbateurs doit être inférieur au nombre total d'approbateurs uniques dans les groupes d'approbation par défaut.

Expiration de l'approbation (heures, minutes, secondes)

Période pendant laquelle un administrateur MAV doit répondre à une demande d'approbation. La valeur par défaut est une heure (1h), la valeur minimale prise en charge est une seconde (1s) et la valeur maximale prise en charge est de 14 jours (14d).

Expiration de l'exécution (heures, minutes, secondes)

Période pendant laquelle l'administrateur requérant doit effectuer l'opération :: La valeur par défaut est une heure (1h), la valeur minimale prise en charge est une seconde (1s) et la valeur maximale prise en charge est de 14 jours (14d).


Vous pouvez également remplacer n'importe lequel de ces paramètres pour un particulier ["règles de fonctionnement"](#).

Procédure de System Manager

1. Identifiez les administrateurs pour qu'ils reçoivent une vérification multi-administrateur.
 - a. Cliquez sur **Cluster > Paramètres**.
 - b. Cliquez sur À côté de **utilisateurs et rôles**.
 - c. Cliquez sur **Add** Sous **utilisateurs**.
 - d. Modifiez la liste si nécessaire.

Pour plus d'informations, voir ["Contrôlez l'accès administrateur"](#).

2. Activez la vérification multi-administration en créant au moins un groupe d'approbation et en ajoutant au moins une règle.
 - a. Cliquez sur **Cluster > Paramètres**.
 - b. Cliquez sur En regard de **Multi-Admin Approval** dans la section **Security**.


- c. Cliquez sur  **Add** pour ajouter au moins un groupe d'approbation.
- Nom – Entrez un nom de groupe.
 - Approbateurs : sélectionnez des approbateurs dans une liste d'utilisateurs.
 - Adresse e-mail – Entrez une ou plusieurs adresses e-mail.
 - Groupe par défaut : sélectionnez un groupe.
- d. Ajoutez au moins une règle.
- Opération – sélectionnez une commande prise en charge dans la liste.
 - Requête – saisissez les options et les valeurs de commande souhaitées.
 - Paramètres facultatifs ; laissez vide pour appliquer des paramètres globaux ou attribuez une valeur différente pour des règles spécifiques afin de remplacer les paramètres globaux.
 - Nombre requis d'approbateurs
 - Groupes d'approbation
- e. Cliquez sur **Paramètres avancés** pour afficher ou modifier les valeurs par défaut.
- Nombre d'approbateurs requis (par défaut : 1)
 - Expiration de la demande d'exécution (par défaut : 1 heure)
 - Expiration de la demande d'approbation (par défaut : 1 heure)
 - Serveur de messagerie*
 - De l'adresse e-mail*
- *Ces paramètres mettent à jour les paramètres de messagerie gérés sous "gestion des notifications". Vous êtes invité à les définir si elles n'ont pas encore été configurées.
- f. Cliquez sur **Activer** pour terminer la configuration initiale du MAV.

Après la configuration initiale, l'état actuel du MAV est affiché dans la mosaïque **Multi-Admin Approval**.

- État (activé ou non)
- Opérations actives pour lesquelles des approbations sont requises
- Nombre de demandes ouvertes à l'état en attente

Vous pouvez afficher une configuration existante en cliquant sur . L'approbation MAV est requise pour modifier une configuration existante.

Pour désactiver la vérification multi-administrateur :

1. Cliquez sur **Cluster > Paramètres**.
2. Cliquez sur  En regard de **Multi-Admin Approval** dans la section **Security**.
3. Cliquez sur le bouton bascule activé.

L'approbation MAV est requise pour effectuer cette opération.

Procédure CLI

Avant d'activer la fonctionnalité MAV au niveau de la CLI, au moins une "[Groupe administrateur MAV](#)" doit avoir été créé.

Si vous voulez...	Saisissez cette commande
Activer la fonctionnalité MAV	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn] -enabled true [-execution-expiry [nnh][nm][nns]] [-approval-expiry [nnh][nm][nns]]</pre> <p>Exemple : la commande suivante active MAV avec 1 groupe d'approbation, 2 approbateurs requis et périodes d'expiration par défaut.</p> <pre>cluster-1::> security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>Terminez la configuration initiale en ajoutant au moins une configuration "règle de fonctionnement."</p>
Modifier une configuration MAV (nécessite l'approbation MAV)	<pre>security multi-admin-verify approval- group modify [-approval-groups group1 [,group2...]] [-required-approvers nn] [-execution-expiry [nnh][nm][nns]] [-approval-expiry [nnh][nm][nns]]</pre>
Vérifier la fonctionnalité MAV	<pre>security multi-admin-verify show</pre> <p>Exemple:</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>
Désactiver la fonctionnalité MAV (nécessite l'approbation MAV)	<pre>security multi-admin-verify modify -enabled false</pre>

Gérer les règles d'opération protégées

Vous créez des règles de vérification multi-administration (MAV) pour désigner des opérations nécessitant une approbation. Chaque fois qu'une opération est lancée, des opérations protégées sont interceptées et une demande d'approbation est générée.

Les règles peuvent être créées avant d'activer MAV par tout administrateur disposant des fonctionnalités RBAC appropriées, mais une fois MAV activé, toute modification de l'ensemble de règles nécessite l'approbation MAV.

Une seule règle MAV peut être créée par opération ; par exemple, vous ne pouvez pas en créer plusieurs `volume-snapshot-delete` règles. Toutes les contraintes de règle souhaitées doivent être contenues dans une règle.

Commandes protégées par des règles

Vous pouvez créer des règles pour protéger les commandes suivantes à partir de ONTAP 9.11.1.

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

Vous pouvez créer des règles pour protéger les commandes suivantes à 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`

Vous pouvez créer des règles pour protéger les commandes suivantes à partir de ONTAP 9.14.1 :

- `volume recovery-queue modify`

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

Les règles pour les commandes par défaut du système MAV, le `security multi-admin-verify` "**commandes**", ne peut pas être modifié.

Outre les commandes définies par le système, les commandes suivantes sont protégées par défaut lorsque la vérification multi-admin est activée, mais vous pouvez modifier les règles afin de supprimer la protection de ces commandes.

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

Contraintes de règle

Lorsque vous créez une règle, vous pouvez éventuellement spécifier le `-query` option permettant de limiter la demande à un sous-ensemble de la fonctionnalité de la commande. Le `-query` Option peut également être utilisée pour limiter les éléments de configuration tels que la SVM, le volume et les noms des snapshots.

Par exemple, dans le `volume snapshot delete` commande `-query` peut être défini sur `-snapshot !hourly*,!daily*,!weekly*`, Ce qui signifie que les instantanés de volume préfixés avec des attributs horaires, quotidiens ou hebdomadaires sont exclus des protections MAV.

```
smci-vsim20::> security multi-admin-verify rule show
```

		Required	Approval
		Approvers	Groups
-----	-----	-----	-----
vs01	volume snapshot delete	-	-
	Query: -snapshot !hourly*,!daily*,!weekly*		



Tous les éléments de configuration exclus ne seraient pas protégés par MAV, et tout administrateur pourrait les supprimer ou les renommer.

Par défaut, les règles spécifient qu'un correspondant `security multi-admin-verify request create` "*protected_operation*" la commande est générée automatiquement lorsqu'une opération protégée est saisie. Vous pouvez modifier cette valeur par défaut pour exiger que la `request create` la commande doit être saisie séparément.

Par défaut, les règles héritent des paramètres généraux MAV suivants, bien que vous puissiez spécifier des exceptions spécifiques aux règles :

- Nombre requis d'approbateurs
- Groupes d'approbation
- Période d'expiration de l'approbation

- Période d'expiration de l'exécution

Procédure de System Manager

Pour ajouter une règle d'opération protégée pour la première fois, reportez-vous à la procédure de System Manager à ["activation de la vérification multi-administrateurs"](#)

Pour modifier le jeu de règles existant :

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez  En regard de **Multi-Admin Approval** dans la section **Security**.
3. Sélectionnez **+ Add** pour ajouter au moins une règle, vous pouvez également modifier ou supprimer des règles existantes.
 - Opération – sélectionnez une commande prise en charge dans la liste.
 - Requête – saisissez les options et les valeurs de commande souhaitées.
 - Paramètres facultatifs – laissez vide pour appliquer des paramètres globaux ou attribuez une valeur différente pour des règles spécifiques afin de remplacer les paramètres globaux.
 - Nombre requis d'approbateurs
 - Groupes d'approbation

Procédure CLI



Tout `security multi-admin-verify rule` Les commandes exigent l'approbation de l'administrateur MAV avant leur exécution, sauf `security multi-admin-verify rule show`.

Si vous voulez...	Saisissez cette commande
Créer une règle	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>
Modifier les informations d'identification des administrateurs actuels	<code>security login modify <parameters></code> Exemple : la règle suivante nécessite l'approbation pour supprimer le volume racine. <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code>
Modifier une règle	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
Supprimer une règle	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>

Si vous voulez...	Saisissez cette commande
Afficher les règles	<code>security multi-admin-verify rule show</code>

Pour plus d'informations sur la syntaxe de commande, reportez-vous à la section `security multi-admin-verify rule` pages de manuel.

Demander l'exécution d'opérations protégées

Lorsque vous lancez une opération ou une commande protégée sur un cluster activé pour la vérification multi-administrateur (MAV), ONTAP intercepte automatiquement l'opération et demande de générer une requête qui doit être approuvée par un ou plusieurs administrateurs d'un groupe d'approbation MAV (administrateurs MAV). Vous pouvez également créer une requête MAV sans la boîte de dialogue.

Si elle est approuvée, vous devez alors répondre à la requête pour terminer l'opération dans le délai d'expiration de la requête. Si vous vous êtes opposé ou si les périodes de demande ou d'expiration sont dépassées, vous devez supprimer la demande et la renvoyer.

La fonctionnalité MAV permet de définir les paramètres RBAC existants. C'est-à-dire que votre rôle d'administrateur doit disposer de privilèges suffisants pour exécuter une opération protégée sans tenir compte des paramètres MAV. ["En savoir plus sur le RBAC"](#).

Si vous êtes administrateur MAV, vos demandes d'exécution d'opérations protégées doivent également être approuvées par un administrateur MAV.

Procédure de System Manager

Lorsqu'un utilisateur clique sur un élément de menu pour lancer une opération et que l'opération est protégée, une demande d'approbation est générée et l'utilisateur reçoit une notification semblable à ce qui suit :

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

La fenêtre **Multi-Admin Requests** est disponible lorsque MAV est activé, affichant les demandes en attente basées sur l'ID de connexion et le rôle MAV de l'utilisateur (approbateur ou non). Pour chaque demande en attente, les champs suivants sont affichés :

- Fonctionnement
- Index (nombre)
- État (en attente, approuvé, rejeté, exécuté ou expiré)

Si une demande est rejetée par un approbateur, aucune autre action n'est possible.

- Requête (tous les paramètres ou valeurs de l'opération demandée)
- Utilisateur demandeur
- La demande expire le

- (Nombre de) approbateurs en attente
- (Nombre de) approbateurs potentiels

Lorsque la demande est approuvée, l'utilisateur demandeur peut relancer l'opération dans la période d'expiration.

Si l'utilisateur tente de nouveau l'opération sans approbation, une notification s'affiche comme suit :

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

Procédure CLI

1. Entrez directement l'opération protégée ou à l'aide de la commande MAV request.

Exemples – pour supprimer un volume, entrez l'une des commandes suivantes :

° 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. Vérifier l'état de la demande et répondre à l'avis MAV.

- a. Si la requête est approuvée, répondez au message de l'interface de ligne de commande pour terminer l'opération.

Exemple:

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

```
    Request Index: 3
      Operation: volume delete
        Query: -vserver vs0 -volume voll1
        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 voll1 -vserver vs0
```

Info: Volume "voll1" 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 voll_*" 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 "voll1" in Vserver "vs0" ?
{y|n}: y

- b. Si la demande est voetotée ou si la période d'expiration est passée, supprimez la demande et relancez ou contactez l'administrateur MAV.

Exemple:

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

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll1
    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 voll1 -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".
```

Gérer les demandes d'opérations protégées

Lorsque les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) sont avertis d'une demande d'exécution d'opération en attente, ils doivent répondre par un message d'approbation ou de veto dans un délai fixe (expiration de l'approbation). Si un nombre suffisant d'approbations n'est pas reçu, le demandeur doit supprimer la demande et en faire une autre.

Description de la tâche

Les demandes d'approbation sont identifiées par des numéros d'index, qui sont inclus dans les e-mails et sont affichées dans la file d'attente des demandes.

Les informations suivantes de la file d'attente de demandes peuvent être affichées :

Fonctionnement

Opération protégée pour laquelle la demande est créée.

Requête

Objet (ou objets) sur lequel l'utilisateur souhaite appliquer l'opération.

État

État actuel de la demande ; en attente, approuvé, rejeté, expiré, exécuté. Si une demande est rejetée par un approbateur, aucune autre action n'est possible.

Approbateurs requis

Nombre d'administrateurs MAV requis pour approuver la demande. Un utilisateur peut définir le paramètre approbateurs requis pour la règle d'opération. Si un utilisateur ne définit pas les approbateurs requis sur la règle, les approbateurs requis du paramètre global sont appliqués.

Approbateurs en attente

Nombre d'administrateurs MAV toujours requis pour approuver la demande pour que la demande soit marquée comme approuvée.

Expiration de l'approbation

Période pendant laquelle un administrateur MAV doit répondre à une demande d'approbation. Tout utilisateur autorisé peut définir la règle d'approbation-expiration d'une opération. Si l'approbation-expiration n'est pas définie pour la règle, l'approbation-expiration du paramètre global est appliquée.

Expiration de l'exécution

Période pendant laquelle l'administrateur requérant doit terminer l'opération. Tout utilisateur autorisé peut définir une règle d'exécution-expiration pour une opération. Si exécution-expiration n'est pas définie pour la règle, l'exécution-expiration du paramètre global est appliquée.

Utilisateurs approuvés

Les administrateurs MAV qui ont approuvé la demande.

L'utilisateur a refusé son droit d'veto

Les administrateurs MAV qui ont opposé leur veto à la demande.

VM de stockage (vServer)

SVM avec lequel la requête est associée. Seule le SVM d'administration est pris en charge dans cette version.

Utilisateur demandé

Nom d'utilisateur de l'utilisateur qui a créé la demande.

Heure de création

Heure de création de la demande.

Heure d'approbation

Heure à laquelle l'état de la demande passe à approuvé.

Commentaire

Tout commentaire associé à la demande.

Utilisateurs autorisés

Liste des utilisateurs autorisés à effectuer l'opération protégée pour laquelle la demande est approuvée. Si `users-permitted` est vide, alors tout utilisateur disposant des autorisations appropriées peut effectuer l'opération.

Toutes les demandes expirées ou exécutées sont supprimées lorsqu'une limite de 1000 demandes est atteinte ou lorsque la durée d'expiration est supérieure à 8 heures pour les demandes expirées. Les demandes de veto

sont supprimées dès qu'elles sont marquées comme expirées.

Procédure de System Manager

Les administrateurs MAV reçoivent des e-mails contenant les détails de la demande d'approbation, la période d'expiration de la demande et un lien pour approuver ou rejeter la demande. Ils peuvent accéder à une boîte de dialogue d'approbation en cliquant sur le lien dans l'e-mail ou accédez à **Events & Jobs> requêtes** dans System Manager.

La fenêtre **requêtes** est disponible lorsque la vérification multi-administrateur est activée, affichant les demandes en attente basées sur l'ID de connexion de l'utilisateur et le rôle MAV (approbateur ou non).

- Fonctionnement
- Index (nombre)
- État (en attente, approuvé, rejeté, exécuté ou expiré)

Si une demande est rejetée par un approbateur, aucune autre action n'est possible.

- Requête (tous les paramètres ou valeurs de l'opération demandée)
- Utilisateur demandeur
- La demande expire le
- (Nombre de) approbateurs en attente
- (Nombre de) approbateurs potentiels

Les administrateurs MAV disposent de contrôles supplémentaires dans cette fenêtre ; ils peuvent approuver, rejeter ou supprimer des opérations individuelles ou des groupes d'opérations sélectionnés. Toutefois, si l'administrateur MAV est l'utilisateur qui demande, il ne peut approuver, rejeter ou supprimer ses propres demandes.

Procédure CLI

1. Lorsqu'une demande est signalée par courrier électronique en attente, notez le numéro d'index de la demande et la période d'expiration de l'approbation. Le numéro d'index peut également être affiché à l'aide des options **show** ou **show-Pending** mentionnées ci-dessous.
2. Approuver ou opposer un veto à la demande.

Si vous voulez...	Saisissez cette commande
Approuver une demande	<code>security multi-admin-verify request approve nn</code>
Veto sur une demande	<code>security multi-admin-verify request veto nn</code>
Affiche toutes les demandes, les demandes en attente ou une seule demande	<code>`security multi-admin-verify request { show</code>

Si vous voulez...	Saisissez cette commande
show-pending } [nn] { -fields <i>field1</i> [, <i>field2</i> ...]	[-instance] }` Vous pouvez afficher toutes les demandes dans la file d'attente ou uniquement les demandes en attente. Si vous saisissez le numéro d'index, seules les informations pour ce numéro sont affichées. Vous pouvez afficher des informations sur des champs spécifiques (en utilisant le <code>-fields</code> paramètre) ou à propos de tous les champs (en utilisant le <code>-instance</code> paramètre).
Supprimer une demande	<code>security multi-admin-verify request delete nn</code>

Exemple :

La séquence suivante approuve une demande après que l'administrateur MAV ait reçu l'e-mail de demande avec l'index numéro 3, qui a déjà une approbation.

```

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: -

```

Exemple :

La séquence suivante affiche une demande après que l'administrateur MAV ait reçu l'e-mail de demande avec l'index numéro 3, qui a déjà une approbation.

```
cluster1::> security multi-admin-verify request show-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: -
```


Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.