Gerenciar a verificação de vários administradores

ONTAP 9

NetApp
January 17, 2025

Índice

Gerenciar a verificação de vários administradores

Visão geral da verificação de vários administradores do ONTAP

A partir do ONTAP 9.11,1, você pode usar a verificação multiadministrador (MAV) para garantir que certas operações, como a exclusão de volumes ou cópias Snapshot, possam ser executadas somente após aprovações de administradores designados. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados.

A configuração da verificação de vários administradores consiste em:

- "Criando um ou mais grupos de aprovação de administrador."
- "Habilitando a funcionalidade de verificação de vários administradores."
- "Adicionar ou modificar regras."

Após a configuração inicial, esses elementos só podem ser modificados por administradores em um grupo de aprovação MAV (administradores MAV).

Quando a verificação multi-admin está ativada, a conclusão de cada operação protegida requer estes passos:

1. Quando um utilizador inicia a operação, a "a solicitação é gerada."
2. Antes que a operação possa ser executada, pelo menos uma "O administrador do MAV deve aprovar."
3. Após a aprovação, o usuário é solicitado e conclui a operação.

> Se você precisar desabilitar a funcionalidade de verificação multiadministrador sem a aprovação do administrador do MAV, entre em Contato com o suporte da NetApp e mencione o seguinte artigo da base de dados de Conhecimento: "Como desativar a Verificação Multi-Admin se o administrador do MAV não estiver disponível".

A verificação multiadministrador não se destina a ser usada com volumes ou fluxos de trabalho que envolvam automação pesada, pois cada tarefa automatizada exigiria aprovação antes que a operação pudesse ser concluída. Se você quiser usar automação e MAV juntos, é recomendável usar consultas para operações MAV específicas. Por exemplo, você pode aplicar `volume delete` regras MAV apenas a volumes em que a automação não está envolvida e pode designar esses volumes com um esquema de nomenclatura específico.

> A verificação multi-admin não está disponível com o Cloud Volumes ONTAP.

Como a verificação multi-admin funciona

A verificação multi-admin consiste em:

- Um grupo de um ou mais administradores com poderes de aprovação e veto.
- Um conjunto de operações ou comandos protegidos em uma tabela *rules*.

- Um mecanismo *regras* para identificar e controlar a execução de operações protegidas.

As regras MAV são avaliadas após regras de controle de acesso baseado em função (RBAC). Portanto, os administradores que executam ou aprovam operações protegidas já devem possuir o Privileges RBAC mínimo para essas operações. "Saiba mais sobre o RBAC".

Regras definidas pelo sistema

Quando a verificação multi-admin está ativada, as regras definidas pelo sistema (também conhecidas como regras *guard-rail*) estabelecem um conjunto de operações MAV para conter o risco de contornar o próprio processo MAV. Essas operações não podem ser removidas da tabela de regras. Quando o MAV estiver ativado, as operações designadas por um asterisco (*) requerem aprovação por um ou mais administradores antes da execução, exceto para os comandos **show**.

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

  Controla a configuração da funcionalidade de verificação de vários administradores.

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

  Controle a associação no conjunto de administradores com credenciais de verificação multi-admin.

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

  Controle o conjunto de comandos que exigem verificação multi-admin.

- `security multi-admin-verify request` operações

  Controle o processo de aprovação.

Comandos protegidos por regras

Além das operações definidas pelo sistema, os seguintes comandos são protegidos por padrão quando a verificação multi-admin está ativada, mas você pode modificar as regras para remover a proteção desses comandos.

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

Cada versão do ONTAP fornece mais comandos que você pode escolher para proteger com regras de verificação de vários administradores. Escolha a versão do ONTAP para obter a lista completa de comandos disponíveis para proteção.

9.16.1

- `cluster date modify` 3
- `cluster log-forwarding create` 3
- `cluster log-forwarding delete` 3
- `cluster log-forwarding modify` 3
- `cluster peer delete`
- `cluster time-service ntp server create` 3
- `cluster time-service ntp server delete` 3
- `cluster time-service ntp server key create` 3
- `cluster time-service ntp server key delete` 3
- `cluster time-service ntp server key modify` 3
- `cluster time-service ntp server modify` 3
- `event config modify`
- `lun delete` 3
- `security anti-ransomware volume attack clear-suspect` 1
- `security anti-ransomware volume disable` 1
- `security anti-ransomware volume event-log modify` 2
- `security anti-ransomware volume pause` 1
- `security anti-ransomware vserver event-log modify` 2
- `security audit modify` 3
- `security ipsec config modify` 3
- `security ipsec policy create` 3
- `security ipsec policy delete` 3
- `security ipsec policy modify` 3
- `security login create`
- `security login delete`
- `security login modify`
- `security 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 aggregate offline 4
- storage encryption disk destroy 3
- storage encryption disk modify 3
- storage encryption disk revert-to-original-state 3
- storage encryption disk sanitize 3
- system bridge run-cli 3
- system controller flash-cache secure-erase run 3
- system controller service-event delete 3
- system health alert delete 3
- system health alert modify 3
- system health policy definition modify 3
- system node autosupport modify 3
- system node autosupport trigger modify 3
- system node coredump delete 3
- system node coredump delete-all 3
- system node hardware nvram-encryption modify 3
- system node run
- system node systemshell
- system script delete 3
- system service-processor ssh add-allowed-addresses 3
- system service-processor ssh remove-allowed-addresses 3
- system smtape restore 3
- system switch ethernet log disable-collection 3
- system switch ethernet log modify 3
- timezone 3
- volume create 3
- volume delete
- volume encryption conversion start 4
- volume encryption rekey start 4
- volume file privileged-delete 3
- volume flexcache delete
- volume modify 3
- volume recovery-queue modify 2
- volume recovery-queue purge 2

- volume recovery-queue purge-all 2
- volume snaplock modify 1
- volume snapshot autodelete modify
- volume snapshot create 3
- volume snapshot delete
- volume snapshot modify 3
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename 3
- volume snapshot restore
- vserver audit create 3
- vserver audit delete 3
- vserver audit disable 3
- vserver audit modify 3
- vserver audit rotate-log 3
- vserver create 2
- vserver consistency-group create 4
- vserver consistency-group delete 4
- vserver consistency-group modify 4
- vserver consistency-group snapshot create 4
- vserver consistency-group snapshot delete 4
- vserver delete 3
- vserver modify 2
- vserver object-store-server audit create 3
- vserver object-store-server audit delete 3
- vserver object-store-server audit disable 3
- vserver object-store-server audit modify 3
- vserver object-store-server audit rotate-log 3
- vserver options 3
- vserver peer delete

- `vserver security file-directory apply` 3
- `vserver security file-directory remove-slag` 3
- `vserver stop` 4
- `vserver vscan disable` 3
- `vserver vscan on-access-policy create` 3
- `vserver vscan on-access-policy delete` 3
- `vserver vscan on-access-policy disable` 3
- `vserver vscan on-access-policy modify` 3
- `vserver vscan scanner-pool create` 3
- `vserver vscan scanner-pool delete` 3
- `vserver vscan scanner-pool modify` 3

9.15.1

- `cluster date modify` 3
- `cluster log-forwarding create` 3
- `cluster log-forwarding delete` 3
- `cluster log-forwarding modify` 3
- `cluster peer delete`
- `cluster time-service ntp server create` 3
- `cluster time-service ntp server delete` 3
- `cluster time-service ntp server key create` 3
- `cluster time-service ntp server key delete` 3
- `cluster time-service ntp server key modify` 3
- `cluster time-service ntp server modify` 3
- `event config modify`
- `lun delete` 3
- `security anti-ransomware volume attack clear-suspect` 1
- `security anti-ransomware volume disable` 1
- `security anti-ransomware volume event-log modify` 2
- `security anti-ransomware volume pause` 1
- `security anti-ransomware vserver event-log modify` 2
- `security audit modify` 3
- `security ipsec config modify` 3
- `security ipsec policy create` 3

- security ipsec policy delete 3
- security ipsec policy modify 3
- security login create
- security login delete
- security login modify
- security key-manager onboard update-passphrase 3
- security saml-sp create 3
- security saml-sp delete 3
- security saml-sp modify 3
- snaplock legal-hold end 3
- storage aggregate delete 3
- storage encryption disk destroy 3
- storage encryption disk modify 3
- storage encryption disk revert-to-original-state 3
- storage encryption disk sanitize 3
- system bridge run-cli 3
- system controller flash-cache secure-erase run 3
- system controller service-event delete 3
- system health alert delete 3
- system health alert modify 3
- system health policy definition modify 3
- system node autosupport modify 3
- system node autosupport trigger modify 3
- system node coredump delete 3
- system node coredump delete-all 3
- system node hardware nvram-encryption modify 3
- system node run
- system node systemshell
- system script delete 3
- system service-processor ssh add-allowed-addresses 3
- system service-processor ssh remove-allowed-addresses 3
- system smtape restore 3
- system switch ethernet log disable-collection 3
- system switch ethernet log modify 3

- `timezone` [3]
- `volume create` [3]
- `volume delete`
- `volume file privileged-delete` [3]
- `volume flexcache delete`
- `volume modify` [3]
- `volume recovery-queue modify` [2]
- `volume recovery-queue purge` [2]
- `volume recovery-queue purge-all` [2]
- `volume snaplock modify` [1]
- `volume snapshot autodelete modify`
- `volume snapshot create` [3]
- `volume snapshot delete`
- `volume snapshot modify` [3]
- `volume snapshot policy add-schedule`
- `volume snapshot policy create`
- `volume snapshot policy delete`
- `volume snapshot policy modify`
- `volume snapshot policy modify-schedule`
- `volume snapshot policy remove-schedule`
- `volume snapshot rename` [3]
- `volume snapshot restore`
- `vserver audit create` [3]
- `vserver audit delete` [3]
- `vserver audit disable` [3]
- `vserver audit modify` [3]
- `vserver audit rotate-log` [3]
- `vserver create` [2]
- `vserver delete` [3]
- `vserver modify` [2]
- `vserver object-store-server audit create` [3]
- `vserver object-store-server audit delete` [3]
- `vserver object-store-server audit disable` [3]
- `vserver object-store-server audit modify` [3]

- vserver object-store-server audit rotate-log 3
- vserver options 3
- vserver peer delete
- vserver security file-directory apply 3
- vserver security file-directory remove-slag 3
- vserver vscan disable 3
- vserver vscan on-access-policy create 3
- vserver vscan on-access-policy delete 3
- vserver vscan on-access-policy disable 3
- vserver vscan on-access-policy modify 3
- vserver vscan scanner-pool create 3
- vserver vscan scanner-pool delete 3
- vserver vscan scanner-pool modify 3

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect 1
- security anti-ransomware volume disable 1
- security anti-ransomware volume event-log modify 2
- security anti-ransomware volume pause 1
- security anti-ransomware vserver event-log modify 2
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify 2
- volume recovery-queue purge 2
- volume recovery-queue purge-all 2
- volume snaplock modify 1
- volume snapshot autodelete modify

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

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect 1
- security anti-ransomware volume disable 1
- security anti-ransomware volume pause 1
- security login create
- security login delete
- security login modify
- 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
- 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. Novo comando protegido por regras para 9.13.1
2. Novo comando protegido por regras para 9.14.1
3. Novo comando protegido por regras para 9.15.1
4. Novo comando protegido por regras para 9.16.1

*Este comando só está disponível com CLI e não está disponível para o System Manager em algumas versões.

Como funciona a aprovação multi-admin

Sempre que uma operação protegida é inserida em um cluster protegido por MAV, uma solicitação de execução de operação é enviada para o grupo de administradores designado MAV.

Você pode configurar:

- Nomes, informações de Contato e número de administradores no grupo MAV.

  Um administrador MAV deve ter uma função RBAC com o administrador de cluster Privileges.

- O número de grupos de administradores do MAV.
  - Um grupo MAV é atribuído para cada regra de operação protegida.
  - Para vários grupos MAV, você pode configurar qual grupo MAV aprova uma determinada regra.
- O número de aprovações MAV necessárias para executar uma operação protegida.
- Um período de expiração de *aprovação* dentro do qual um administrador do MAV deve responder a uma solicitação de aprovação.
- Um período de expiração de *execução* dentro do qual o administrador solicitante deve concluir a operação.

Uma vez configurados esses parâmetros, a aprovação MAV é necessária para modificá-los.

Os administradores do MAV não podem aprovar suas próprias solicitações para executar operações protegidas. Por conseguinte:

- O MAV não deve ser ativado em clusters com apenas um administrador.
- Se houver apenas uma pessoa no grupo MAV, o administrador do MAV não poderá iniciar operações protegidas; os administradores regulares devem iniciar operações protegidas e o administrador do MAV só pode aprovar.
- Se você quiser que os administradores do MAV possam executar operações protegidas, o número de administradores do MAV deve ser maior do que o número de aprovações necessárias. Por exemplo, se duas aprovações forem necessárias para uma operação protegida e você quiser que os administradores do MAV as executem, deve haver três pessoas no grupo de administradores do MAV.

Os administradores do MAV podem receber solicitações de aprovação em alertas de e-mail (usando o EMS) ou podem consultar a fila de solicitações. Quando recebem um pedido, podem tomar uma das três ações:

- Aprovar
- Rejeitar (veto)
- Ignorar (sem ação)

As notificações por e-mail são enviadas a todos os aprovadores associados a uma regra MAV quando:

- Uma solicitação é criada.
- Uma solicitação é aprovada ou vetada.
- Uma solicitação aprovada é executada.

Se o solicitante estiver no mesmo grupo de aprovação para a operação, ele receberá um e-mail quando a solicitação for aprovada.

> Um solicitante não pode aprovar suas próprias solicitações, mesmo que esteja no grupo de aprovação (embora possa receber notificações por e-mail para suas próprias solicitações). Os solicitantes que não estão em grupos de aprovação (ou seja, que não são administradores MAV) não recebem notificações por e-mail.

Como funciona a execução da operação protegida

Se a execução for aprovada para uma operação protegida, o usuário solicitante continuará com a operação quando solicitado. Se a operação for vetada, o usuário solicitante deverá excluir a solicitação antes de prosseguir.

As regras MAV são avaliadas após as permissões RBAC. Como resultado, um usuário sem permissões RBAC suficientes para execução da operação não pode iniciar o processo de solicitação MAV.

Gerenciar grupos de aprovação de administrador

Antes de ativar a verificação multi-admin (MAV), você deve criar um grupo de aprovação de administrador contendo um ou mais administradores para receber autoridade de aprovação ou veto. Depois de ativar a verificação multi-admin, quaisquer modificações na associação ao grupo de aprovação requerem a aprovação de um dos administradores qualificados existentes.

Sobre esta tarefa

Você pode adicionar administradores existentes a um grupo MAV ou criar novos administradores.

A funcionalidade MAV homenageia as configurações de controle de acesso baseado em função (RBAC) existentes. Os potenciais administradores do MAV devem ter privilégios suficientes para executar operações protegidas antes de serem adicionados aos grupos de administradores do MAV. "Saiba mais sobre o RBAC."

Você pode configurar o MAV para alertar os administradores do MAV de que as solicitações de aprovação estão pendentes. Para fazer isso, você deve configurar notificações por e-mail - em particular, os `Mail From` parâmetros e `Mail Server` - ou você pode limpar esses parâmetros para desativar a notificação. Sem alertas de e-mail, os administradores do MAV devem verificar a fila de aprovação manualmente.

Procedimento do System Manager

Se pretender criar um grupo de aprovação MAV pela primeira vez, consulte o procedimento do Gestor do sistema para "ative a verificação de vários administradores."

Para modificar um grupo de aprovação existente ou criar um grupo de aprovação adicional:

1. Identifique os administradores para receber a verificação de vários administradores.
   a. Clique em **Cluster > Settings.**
   b. Clique → ao lado de **usuários e funções.**
   c. Clique + Add em **Users.**
   d. Modifique a lista conforme necessário.

      Para obter mais informações, consulte "Controle o acesso do administrador."

2. Criar ou modificar o grupo de aprovação MAV:
   a. Clique em **Cluster > Settings.**
   b. Clique → ao lado de **aprovação Multi-Admin** na seção **Segurança**. (Você verá o ⚙ ícone se o MAV ainda não estiver configurado.)
      - Nome: Introduza um nome de grupo.

- Aprovadores: Selecione aprovadores de uma lista de usuários.
- Endereço de e-mail: Insira o(s) endereço(s) de e-mail.
- Grupo padrão: Selecione um grupo.

A aprovação MAV é necessária para editar uma configuração existente assim que o MAV estiver ativado.

Procedimento CLI

1. Verifique se os valores foram definidos para `Mail From` os parâmetros e. `Mail Server` Introduza:

   `event config show`

   O visor deve ser semelhante ao seguinte:

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

   Para configurar estes parâmetros, introduza:

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

2. Identifique os administradores para receber a verificação de vários administradores

Se você quiser…	Introduza este comando
Exibir administradores atuais	`security login show`
Modifique as credenciais dos administradores atuais	`security login modify` *`<parameters>`*
Crie novas contas de administrador	`security login create -user-or-group -name` *`admin_name`* `-application ssh -authentication-method password`

3. Crie o grupo de aprovação MAV:

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

   - `-vserver` - Somente o administrador SVM é suportado nesta versão.
   - `-name` - O nome do grupo MAV, até 64 carateres.
   - `-approvers` - A lista de um ou mais aprovadores.
   - `-email` - Um ou mais endereços de e-mail que são notificados quando uma solicitação é criada,

aprovada, vetada ou executada.

Exemplo: o comando a seguir cria um grupo MAV com dois membros e endereços de e-mail associados.

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

4. Verificar a criação e a associação do grupo:

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

   Exemplo:

```
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
```

Use esses comandos para modificar a configuração inicial do grupo MAV.

Nota: todos exigem aprovação do administrador do MAV antes da execução.

Se você quiser…	Introduza este comando
Modifique as caraterísticas do grupo ou modifique as informações de membros existentes	`security multi-admin-verify approval-group modify [`*parameters*`]`
Adicionar ou remover membros	`security multi-admin-verify approval-group replace [-vserver` *svm_name*`] -name` *group_name* `[-approvers-to-add` *approver1*`[,`*approver2*`…]][-approvers-to-remove` *approver1*`[,`*approver2*`…]]`
Eliminar um grupo	`security multi-admin-verify approval-group delete [-vserver` *svm_name*`] -name` *group_name*

Ative e desative a verificação de vários administradores

A verificação multi-admin (MAV) deve ser ativada explicitamente. Depois de ativar a verificação multi-admin, a aprovação por administradores em um grupo de aprovação MAV (administradores MAV) é necessária para excluí-la.

Sobre esta tarefa

Uma vez que o MAV está ativado, modificar ou desativar o MAV requer a aprovação do administrador do MAV.

> Se você precisar desabilitar a funcionalidade de verificação multiadministrador sem a aprovação do administrador do MAV, entre em Contato com o suporte da NetApp e mencione o seguinte artigo da base de dados de Conhecimento: "Como desativar a Verificação Multi-Admin se o administrador do MAV não estiver disponível".

Ao ativar o MAV, você pode especificar os seguintes parâmetros globalmente.

Grupos de aprovação

Uma lista de grupos de aprovação globais. É necessário pelo menos um grupo para ativar a funcionalidade MAV.

> Se você estiver usando o MAV com o Autonomous ransomware Protection (ARP), defina um grupo de aprovação novo ou existente que seja responsável por aprovar a pausa ARP, desativar e limpar solicitações suspeitas.

Aprovadores necessários

O número de aprovadores necessários para executar uma operação protegida. O número padrão e mínimo é 1.

> O número necessário de aprovadores deve ser menor que o número total de aprovadores exclusivos nos grupos de aprovação padrão.

Validade da aprovação (horas, minutos, segundos)

O período durante o qual um administrador do MAV deve responder a uma solicitação de aprovação. O valor padrão é de uma hora (1h), o valor mínimo suportado é de um segundo (1s) e o valor máximo suportado é de 14 dias (14d).

Expiração da execução (horas, minutos, segundos)

O período durante o qual o administrador requerente deve concluir a operação::. O valor padrão é de uma hora (1h), o valor mínimo suportado é de um segundo (1s) e o valor máximo suportado é de 14 dias (14d).

Você também pode substituir qualquer um desses parâmetros para específico "regras de operação."

Procedimento do System Manager

1. Identifique os administradores para receber a verificação de vários administradores.
   a. Clique em **Cluster > Settings.**
   b. Clique → ao lado de **usuários e funções.**
   c. Clique + Add em **Users.**
   d. Modifique a lista conforme necessário.

      Para obter mais informações, consulte "Controle o acesso do administrador."
2. Ative a verificação de vários administradores criando pelo menos um grupo de aprovação e adicionando pelo menos uma regra.
   a. Clique em **Cluster > Settings.**

b. Clique ⚙ ao lado de **aprovação Multi-Admin** na seção **Segurança**.
c. Clique + Add para adicionar pelo menos um grupo de aprovação.
   - Name (Nome) – Introduza o nome de um grupo.
   - Aprovadores – Selecione aprovadores de uma lista de usuários.
   - Endereço de e-mail – Digite o(s) endereço(s) de e-mail.
   - Grupo padrão – Selecione um grupo.
d. Adicione pelo menos uma regra.
   - Operação – Selecione um comando suportado na lista.
   - Consulta – Insira quaisquer opções e valores de comando desejados.
   - Parâmetros opcionais; deixe em branco para aplicar configurações globais ou atribua um valor diferente para regras específicas para substituir as configurações globais.
     - Número necessário de aprovadores
     - Grupos de aprovação
e. Clique em **Configurações avançadas** para exibir ou modificar os padrões.
   - Número necessário de aprovadores (padrão: 1)
   - Expiração da solicitação de execução (padrão: 1 hora)
   - Expiração do pedido de aprovação (predefinição: 1hour)
   - Servidor de correio*
   - A partir do endereço de e-mail*

     *Estes atualizam as definições de e-mail geridas em "Gestão de notificações". Você será solicitado a configurá-los se eles ainda não tiverem sido configurados.
f. Clique em **Enable** para concluir a configuração inicial do MAV.

Após a configuração inicial, o status atual do MAV é exibido no mosaico **aprovação Multi-Admin**.

- Estado (ativado ou não)
- Operações ativas para as quais são necessárias aprovações
- Número de solicitações abertas no estado pendente

Você pode exibir uma configuração existente clicando →em . A aprovação MAV é necessária para editar uma configuração existente.

Para desativar a verificação de vários administradores:

1. Clique em **Cluster > Settings.**
2. Clique ⚙ ao lado de **aprovação Multi-Admin** na seção **Segurança**.
3. Clique no botão de alternância ativado.

   A aprovação MAV é necessária para concluir esta operação.

Procedimento CLI

Antes de ativar a funcionalidade MAV na CLI, pelo menos um "Grupo de administradores do MAV"deve ter sido criado.

Se você quiser…	Introduza este comando

Ativar a funcionalidade MAV	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`
	
	Exemplo : o comando a seguir habilita o MAV com 1 grupo de aprovação, 2 aprovadores necessários e períodos de expiração padrão.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Conclua a configuração inicial adicionando pelo menos uma "regra de operação."

Modificar uma configuração MAV (requer aprovação MAV)	`security multi-admin-verify approval-group modify [-approval-groups group1 [,group2…]] [-required-approvers nn ] [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`

Verifique a funcionalidade MAV	`security multi-admin-verify show`
	
	Exemplo:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution Approval Approval`
	`Enabled Approvers Expiry Expiry Groups`
	`------- --------- --------- -------- ----------`
	`true 2 1h 1h mav-grp1`

Se você quiser…	Introduza este comando
Desativar a funcionalidade MAV (requer aprovação MAV)	`security multi-admin-verify modify -enabled false`

Gerenciar regras de operação protegidas

Você cria regras de verificação multi-admin (MAV) para designar operações que exigem aprovação. Sempre que uma operação é iniciada, operações protegidas são intercetadas e uma solicitação de aprovação é gerada.

As regras podem ser criadas antes de ativar o MAV por qualquer administrador com recursos RBAC apropriados, mas uma vez que o MAV está habilitado, qualquer modificação no conjunto de regras requer aprovação MAV.

Apenas uma regra MAV pode ser criada por operação; por exemplo, você não pode fazer várias `volume-snapshot-delete` regras. Quaisquer restrições de regra desejadas devem estar contidas em uma regra.

Você pode criar regras para proteger "estes comandos". Você pode proteger cada comando começando com a versão ONTAP na qual a capacidade de proteção para o comando ficou disponível pela primeira vez.

As regras para os comandos padrão do sistema MAV, o `security multi-admin-verify` "comandos", não podem ser alteradas.

Além das operações definidas pelo sistema, os seguintes comandos são protegidos por padrão quando a verificação multi-admin está ativada, mas você pode modificar as regras para remover a proteção desses comandos.

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

Restrições de regra

Ao criar uma regra, você pode especificar opcionalmente a `-query` opção para limitar a solicitação a um subconjunto da funcionalidade de comando. A `-query` opção também pode ser usada para limitar elementos de configuração, como SVM, volume e nomes de Snapshot.

Por exemplo, no `volume snapshot delete` comando, `-query` pode ser definido como `-snapshot !hourly*,!daily*,!weekly*`, o que significa que instantâneos de volume pré-fixados com atributos de hora em hora, dia ou semanal são excluídos das proteções MAV.

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

Quaisquer elementos de configuração excluídos não seriam protegidos pelo MAV, e qualquer administrador poderia excluí-los ou renomeá-los.

Por padrão, as regras especificam que um comando correspondente `security multi-admin-verify request create "protected_operation"` é gerado automaticamente quando uma operação protegida é inserida. Você pode modificar esse padrão para exigir que o `request create` comando seja inserido separadamente.

Por padrão, as regras herdam as seguintes configurações globais de MAV, embora você possa especificar exceções específicas de regras:

- Número necessário de Aprovadores
- Grupos de aprovação
- Período de validade da aprovação
- Período de expiração da execução

Procedimento do System Manager

Se pretender adicionar uma regra de operação protegida pela primeira vez, consulte o procedimento do Gestor de sistema a. "ative a verificação de vários administradores."

Para modificar o conjunto de regras existente:

1. Selecione **Cluster > Settings**.
2. Selecione ⚙ ao lado de **aprovação Multi-Admin** na seção **Segurança**.
3. + Add Selecione para adicionar pelo menos uma regra; você também pode modificar ou excluir regras existentes.
   - Operação – Selecione um comando suportado na lista.
   - Consulta – Insira quaisquer opções e valores de comando desejados.
   - Parâmetros opcionais – deixe em branco para aplicar configurações globais ou atribua um valor diferente para regras específicas para substituir as configurações globais.
     - Número necessário de aprovadores
     - Grupos de aprovação

Procedimento CLI

Todos `security multi-admin-verify rule` os comandos requerem aprovação do administrador MAV antes da execução, exceto `security multi-admin-verify rule show`.

Se você quiser…	Introduza este comando
Crie uma regra	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

Modifique as credenciais dos administradores atuais	`security login modify <parameters>`
	
	Exemplo: A regra a seguir requer aprovação para excluir o volume raiz.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

Modificar uma regra	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Excluir uma regra	`security multi-admin-verify rule delete -operation "protected_operation"`
Mostrar regras	`security multi-admin-verify rule show`

Para obter detalhes da sintaxe do comando, consulte as `security multi-admin-verify rule` páginas man.

Solicitar a execução de operações protegidas

Quando você inicia uma operação ou comando protegidos em um cluster habilitado para verificação multi-admin (MAV), o ONTAP interceta automaticamente a operação e solicita a geração de uma solicitação, que deve ser aprovada por um ou mais administradores em um grupo de aprovação MAV (administradores MAV). Alternativamente, você pode criar uma solicitação MAV sem a caixa de diálogo.

Se aprovado, você deve responder à consulta para concluir a operação dentro do período de expiração da solicitação. Se vetado, ou se a solicitação ou os períodos de expiração forem excedidos, você deverá excluir a solicitação e reenviar.

A funcionalidade MAV homenageia as configurações RBAC existentes. Ou seja, sua função de administrador deve ter privilégio suficiente para executar uma operação protegida sem considerar as configurações de MAV. "Saiba mais sobre o RBAC".

Se você for um administrador do MAV, suas solicitações para executar operações protegidas também devem

ser aprovadas por um administrador do MAV.

Procedimento do System Manager

Quando um usuário clica em um item de menu para iniciar uma operação e a operação é protegida, uma solicitação de aprovação é gerada e o usuário recebe uma notificação semelhante à seguinte:

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

A janela **pedidos Multi-Admin** está disponível quando o MAV está ativado, mostrando solicitações pendentes com base no ID de login do usuário e na função MAV (aprovador ou não). Para cada solicitação pendente, os seguintes campos são exibidos:

- Operação
- Índice (número)
- Estado (pendente, aprovado, rejeitado, executado ou expirado)

  Se uma solicitação for rejeitada por um aprovador, nenhuma outra ação será possível.

- Consulta (quaisquer parâmetros ou valores para a operação solicitada)
- Utilizador a solicitar
- A solicitação expira em
- (Número de) Aprovadores pendentes
- (Número de) potenciais Aprovadores

Quando a solicitação for aprovada, o usuário solicitante poderá tentar novamente a operação dentro do período de expiração.

Se o utilizador voltar a tentar a operação sem aprovação, é apresentada uma notificação semelhante à seguinte:

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

Procedimento CLI

1. Introduzir diretamente a operação protegida ou através do comando pedido MAV.

   Exemplos – para excluir um volume, digite um dos seguintes comandos:

   - `volume delete`

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
       auto-generated and requires approval.
```

- `security multi-admin-verify request create “volume delete”`

```
Error: command failed: The security multi-admin-verify request (index
3)
       requires approval.
```

2. Verifique o status da solicitação e responda ao aviso MAV.
   a. Se a solicitação for aprovada, responda à mensagem CLI para concluir a operação.

      Exemplo:

```
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 a solicitação for vetada ou se o período de expiração tiver passado, exclua a solicitação e envie novamente ou entre em Contato com o administrador do MAV.

Exemplo:

```
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".
```

Gerenciar solicitações de operação protegidas

Quando os administradores de um grupo de aprovação MAV (administradores MAV) são notificados de uma solicitação de execução de operação pendente, eles devem responder com uma mensagem de aprovação ou veto dentro de um período de tempo fixo (expiração da aprovação). Se um número suficiente de aprovações não for recebido, o solicitante deve excluir a solicitação e fazer outra.

Sobre esta tarefa

As solicitações de aprovação são identificadas com números de índice, que são incluídos em mensagens de e-mail e exibições da fila de solicitações.

As seguintes informações da fila de pedidos podem ser exibidas:

Operação
A operação protegida para a qual a solicitação é criada.

Consulta
O objeto (ou objetos) sobre o qual o usuário deseja aplicar a operação.

Estado

O estado atual da solicitação; pendente, aprovado, rejeitado, expirado, executado. Se uma solicitação for rejeitada por um aprovador, nenhuma outra ação será possível.

Aprovadores necessários

O número de administradores MAV que são necessários para aprovar a solicitação. Um usuário pode definir o parâmetro de aprovadores necessários para a regra de operação. Se um usuário não definir os aprovadores necessários para a regra, os aprovadores necessários da configuração global serão aplicados.

Aprovadores pendentes

O número de administradores MAV que ainda são obrigados a aprovar a solicitação para que a solicitação seja marcada como aprovada.

Validade da aprovação

O período durante o qual um administrador do MAV deve responder a uma solicitação de aprovação. Qualquer utilizador autorizado pode definir a validade da aprovação para uma regra de operação. Se a expiração da aprovação não for definida para a regra, então a expiração da aprovação do ajuste global é aplicada.

Expiração da execução

O período durante o qual o administrador requerente deve concluir a operação. Qualquer usuário autorizado pode definir a expiração de execução para uma regra de operação. Se a execução-expiração não estiver definida para a regra, então a execução-expiração da configuração global será aplicada.

Usuários aprovados

Os administradores do MAV que aprovaram a solicitação.

Vetado pelo utilizador

Os administradores do MAV que vetaram a solicitação.

VM de storage (vserver)

O SVM com o qual a solicitação está associada. Somente o SVM admin é compatível nesta versão.

Utilizador solicitado

O nome de usuário do usuário que criou a solicitação.

Hora criada

A hora em que a solicitação é criada.

Hora aprovada

A hora em que o estado da solicitação foi alterado para aprovado.

Comentário

Quaisquer comentários associados à solicitação.

Usuários permitidos

A lista de utilizadores autorizados a realizar a operação protegida para a qual a solicitação foi aprovada. Se `users-permitted` estiver vazio, qualquer usuário com permissões apropriadas pode executar a operação.

Todas as solicitações expiradas ou executadas são excluídas quando um limite de 1000 solicitações é atingido

ou quando o tempo expirado é maior que 8hrs para solicitações expiradas. As solicitações vetadas são excluídas depois que forem marcadas como expiradas.

Procedimento do System Manager

Os administradores do MAV recebem mensagens de e-mail com detalhes da solicitação de aprovação, período de expiração da solicitação e um link para aprovar ou rejeitar a solicitação. Eles podem acessar uma caixa de diálogo de aprovação clicando no link no e-mail ou navegar para **Eventos & trabalhos>solicitações** no System Manager.

A janela **Requests** está disponível quando a verificação multi-admin está ativada, mostrando solicitações pendentes com base no ID de login do usuário e na função MAV (aprovador ou não).

- Operação
- Índice (número)
- Estado (pendente, aprovado, rejeitado, executado ou expirado)

  Se uma solicitação for rejeitada por um aprovador, nenhuma outra ação será possível.

- Consulta (quaisquer parâmetros ou valores para a operação solicitada)
- Utilizador a solicitar
- A solicitação expira em
- (Número de) Aprovadores pendentes
- (Número de) potenciais Aprovadores

Os administradores do MAV têm controles adicionais nesta janela; eles podem aprovar, rejeitar ou excluir operações individuais ou grupos selecionados de operações. No entanto, se o administrador MAV for o Usuário solicitante, ele não poderá aprovar, rejeitar ou excluir seus próprios pedidos.

Procedimento CLI

1. Quando notificado de solicitações pendentes por e-mail, observe o número de índice e o período de expiração da aprovação da solicitação. O número do índice também pode ser exibido usando as opções **show** ou **show-pending** mencionadas abaixo.
2. Aprovar ou vetar o pedido.

Se você quiser…	Introduza este comando
Aprovar uma solicitação	`security multi-admin-verify request approve` *nn*
Veto um pedido	`security multi-admin-verify request veto` *nn*
Mostrar todas as solicitações, solicitações pendentes ou uma única solicitação	`security multi-admin-verify request { show

Se você quiser…	Introduza este comando
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  Você pode mostrar todas as solicitações na fila ou apenas solicitações pendentes. Se introduzir o número do índice, apenas são apresentadas informações para esse número. Você pode exibir informações sobre campos específicos (usando o `-fields` parâmetro) ou sobre todos os campos (usando o `-instance` parâmetro).
Eliminar um pedido	`security multi-admin-verify request delete` *nn*

Exemplo:

A sequência a seguir aprova uma solicitação após o administrador do MAV receber o e-mail da solicitação com o índice número 3, que já tem uma aprovação.

```
          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: -
```

Exemplo:

A sequência a seguir veta uma solicitação depois que o administrador do MAV recebeu o e-mail da solicitação com o índice número 3, que já tem uma aprovação.

```
      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: -
```

Informações sobre direitos autorais

Informações sobre marcas comerciais