マルチ管理者認証の管理
ONTAP 9

NetApp
December 20, 2024

目次

マルチ管理者認証の管理 . . . 1
ONTAPマルチ管理者検証の概要 . . . 1
管理者承認グループの管理 . . . 13
マルチ管理者検証の有効化と無効化 . . . 15
保護されたオペレーションルールの管理 . . . 19
保護された操作の実行を要求 . . . 21
保護された操作要求の管理 . . . 25

マルチ管理者認証の管理

ONTAPマルチ管理者検証の概要

ONTAP 9 .11.1以降では、Multi-Admin Verification（MAV；マルチ管理者認証）を使用して、ボリュームやSnapshotコピーの削除などの特定の処理を、指定した管理者の承認後にのみ実行できるようにすることができます。これにより、侵害された管理者や悪意のある管理者、経験の浅い管理者が望ましくない変更やデータ削除を行うのを防ぐことができます。

マルチ管理者検証の構成は次のとおりです。

- "1つ以上の管理者承認グループを作成します。"
- "マルチ管理者検証機能を有効にします。"
- "ルールを追加または変更する。"

初期設定後にこれらの要素を変更できるのは、MAV承認グループの管理者（MAV管理者）のみです。

マルチ管理者認証が有効な場合、保護対象処理を完了するには次の手順が必要です。

1. ユーザが処理を開始すると、 "要求が生成されます。"
2. 操作を実行する前に、少なくとも1つの"MAV管理者は承認する必要があります。"
3. 承認されると、ユーザーはプロンプトを表示して操作を完了します。

> MAV管理者の承認を得ずにマルチ管理者認証機能を無効にする必要がある場合は、NetAppサポートに連絡し、次の記事を記載してください。 "MAV管理者が利用できない場合にマルチ管理者検証を無効にする方法"

複数管理者による検証は、高度な自動化を伴うボリュームやワークフローでは使用しません。自動化された各タスクは、処理を完了する前に承認が必要になるためです。自動化とMAVを一緒に使用する場合は、特定のMAV操作にクエリを使用することをお勧めします。たとえば、自動化が関係していないボリュームにのみMAVルールを適用し、特定の命名方式でそれらのボリュームを指定でき `volume delete`ます。

> Cloud Volumes ONTAPでは、マルチ管理者認証は使用できません。

マルチ管理者認証の仕組み

マルチ管理者認証は次の要素で構成されます。

- 承認権と拒否権を持つ1人以上の管理者のグループ。
- 保護された操作またはコマンドのセット（a_rules table_）
- a_rulesエンジン_保護されたオペレーションの実行を識別および制御します

MAVルールは、Role-Based Access Control（RBAC；ロールベースアクセス制御）ルールのあとに評価されます。したがって、保護された処理を実行または承認する管理者は、それらの処理に対して最低限必要なRBAC

Privilegesをすでに所有している必要があります。"RBACの詳細については、こちらをご覧ください"です。

システム定義のルール

マルチ管理者検証を有効にすると、システム定義のルール（_guard-rale_rulesとも呼ばれます）によってMAV処理のセットが確立され、MAVプロセス自体が回避されるリスクが含まれます。これらの操作をルールテーブルから削除することはできません。MAVを有効にすると、アスタリスク（）で指定された操作は、実行前に**1**人以上の管理者による承認を必要とします。ただし、 show *コマンドは除きます。

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

  マルチ管理者検証機能の構成を制御します。

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

  マルチ管理者認証資格情報を使用して、管理者セットのメンバーシップを制御します。

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

  複数管理者による検証を必要とする一連のコマンドを制御します。

- `security multi-admin-verify request`運用

  承認プロセスを制御します。

ルール保護コマンド

システム定義の操作に加えて、次のコマンドは、マルチ管理者検証が有効になっている場合にデフォルトで保護されますが、これらのコマンドの保護を解除するルールを変更することができます。

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

各ONTAPバージョンでは、マルチ管理者認証ルールで保護できるコマンドが上記以外にも用意されています。保護可能なコマンドの全一覧を確認するには、お使いのONTAPリリースを選択してください。

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. 9.13.1の新しいrule-protectedコマンド
2. 9.14.1の新しいrule-protectedコマンド
3. 9.15.1の新しいrule-protectedコマンド
4. 9.16.1の新しいrule-protectedコマンド

*このコマンドはCLIでのみ使用でき、一部のリリースではSystem Managerでは使用できません。

マルチ管理者承認の仕組み

MAVで保護されたクラスタで保護された操作が入力されると、指定されたMAV管理者グループに操作実行要求が送信されます。

次の設定が可能です。

- MAVグループ内の管理者の名前、連絡先情報、および数。

  MAV管理者には、クラスタ管理者権限のあるRBACロールが必要です。

- MAV管理者グループの数。
  - 保護対象処理ルールごとにMAVグループが割り当てられます。
  - MAVグループが複数ある場合は、どのMAVグループが特定のルールを承認するかを設定できます。
- 保護対象処理を実行するために必要なMAV承認者の数。
- MAV管理者が承認要求に応答する必要がある_承認の失効_期間。
- 要求元の管理者が処理を完了する必要がある_実行のexpiry_period。

これらのパラメータを設定したら、変更するにはMAV承認が必要です。

MAV管理者は、保護された操作の実行要求を自分で承認することはできません。そのため、

- MAVは、管理者が1人だけのクラスタでは有効にしないでください。
- MAVグループに1人しかいない場合、そのMAV管理者は保護された操作を開始できません。通常の管理者は保護された操作を開始する必要があり、MAV管理者は承認のみを実行できます。
- MAV管理者が保護された操作を実行できるようにするには、MAV管理者の数が必要な承認の数より1つ多い必要があります。たとえば、保護された操作に2つの承認が必要で、MAV管理者にそれらの承認を実行させる場合、MAV管理者グループには3人のユーザーが必要です。

MAV管理者は、電子メールアラートで承認リクエストを受信することも（EMSを使用して）、リクエストキューを照会することもできます。リクエストを受け取ると、次の3つのアクションのいずれかを実行できます。

- 承認
- 拒否（拒否）
- 無視（アクションなし）

次の場合、MAVルールに関連付けられたすべての承認者に電子メール通知が送信されます。

- リクエストが作成されます。
- リクエストが承認または拒否された場合。
- 承認されたリクエストが実行されました。

リクエスト者が操作の同じ承認グループに属している場合は、リクエストが承認されると電子メールが送信されます。

> リクエスト者は、自分のリクエストが承認グループに含まれていても、自分のリクエストを承認することはできません（ただし、自分のリクエストの電子メール通知を受け取ることはできます）。承認グループに属していないリクエスト者（つまり、MAV管理者でないリクエスト者）は、電子メール通知を受信しません。

保護された処理の実行の仕組み

保護された操作の実行が承認されると、要求元のユーザーはプロンプトが表示されたときに操作を続行します。処理が拒否された場合、要求元ユーザは処理を続行する前に要求を削除する必要があります。

MAVルールはRBACの権限の後に評価されます。そのため、操作を実行するための十分なRBAC権限を持たないユーザーは、MAV要求プロセスを開始できません。

管理者承認グループの管理

マルチ管理者認証（MAV）を有効にする前に、承認権限または拒否権限を付与する管理者を1人以上含む管理者承認グループを作成する必要があります。マルチ管理者認証を有効にすると、承認グループメンバーシップを変更するには、既存の資格管理者のいずれかによる承認が必要になります。

タスクの内容

既存の管理者をMAVグループに追加したり、新しい管理者を作成したりできます。

MAV機能では、既存のRole-Based Access Control（RBAC；ロールベースアクセス制御）設定が使用されます。潜在的なMAV管理者は、MAV管理者グループに追加する前に、保護された操作を実行するための十分な権限を持っている必要があります。"RBACの詳細については、こちらをご覧ください。"

承認リクエストが保留中であることをMAV管理者に通知するようにMAVを設定できます。そのためには、Eメール通知（特にパラメータと `Mail Server`パラメータ）を設定する必要があります `Mail From`。または、これらのパラメータをクリアして通知を無効にすることもできます。電子メールアラートがない場合、MAV管理者は承認キューを手動で確認する必要があります。

System Managerの手順

MAV承認グループを初めて作成する場合は、次の手順を参照してください。"マルチ管理者検証を有効にします。"

既存の承認グループを変更する、または追加の承認グループを作成するには、次の手順を実行します。

1. マルチ管理者認証を受ける管理者を指定します。
   a. [**Cluster]>[Settings.**]をクリックします
   b. [Users and Roles]の横にあるをクリックします → 。*
   c. [Users]の下にあるをクリックします + Add 。*
   d. 必要に応じて名簿を変更します。

      詳細については、を参照してください。 "管理者アクセスの制御"

2. MAV承認グループを作成または変更します。
   a. [**Cluster]>[Settings.**]をクリックします
   b. セクションの[マルチ管理者の承認]*の横にあるをクリックします → 。（MAVがまだ設定されていない場合はアイコンが表示され ⚙ ます）。
      - Name：グループ名を入力します。

- Approvers：ユーザのリストから承認者を選択します。
- Email address：Eメール アドレスを入力します。
- Default group：グループを選択します。

MAVを有効にしたあとで既存の設定を編集するには、MAVの承認が必要です。

CLIの手順

1. パラメータと `Mail Server`パラメータに値が設定されていることを確認します `Mail From`。入力：

   `event config show`

   次のように表示されます。

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

   パラメータを設定するには、次のように入力します。

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

2. 複数管理者による検証を受ける管理者の特定

実行する操作	入力するコマンド
現在の管理者を表示します	`security login show`
現在の管理者のクレデンシャルの変更	`security login modify` *`<parameters>`*
新しい管理者アカウントを作成します	`security login create -user-or-group -name` *`admin_name`* `-application ssh -authentication-method password`

3. MAV承認グループを作成します。

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

   - `-vserver`-このリリースでは管理SVMのみがサポートされます。
   - `-name`- MAVグループ名（最大64文字）。
   - `-approvers`- 1人以上の承認者のリスト。

◦ `-email`-リクエストが作成、承認、拒否、または実行されたときに通知される1つ以上の電子メールアドレス。

*例：*次のコマンドは、2つのメンバーと関連付けられたEメールアドレスを持つMAVグループを作成します。

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

4. グループの作成とメンバーシップを確認します。

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

   ◦ 例：*

```
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
```

MAVグループの初期設定を変更するには、次のコマンドを使用します。

*注意：*すべての場合、MAV管理者による承認が必要です。

実行する操作	入力するコマンド
グループの特性を変更するか、既存のメンバー情報を変更します	`security multi-admin-verify approval-group modify [`*parameters*`]`
メンバーを追加または削除します	`security multi-admin-verify approval-group replace [-vserver` *svm_name*`] -name` *group_name* `[-approvers-to-add` *approver1*`[,`*approver2*`…]][-approvers-to-remove` *approver1*`[,`*approver2*`…]]`
グループを削除します	`security multi-admin-verify approval-group delete [-vserver` *svm_name*`] -name` *group_name*

マルチ管理者検証の有効化と無効化

Multi-admin Verification（MAV）は明示的にイネーブルにする必要があります。マルチ管理者認証を有効にすると、削除するにはMAV承認グループの管理者（MAV管理者）によ

る承認が必要になります。

タスクの内容

MAVを有効にすると、MAVを変更または無効にするには、MAV管理者の承認が必要になります。

MAV管理者の承認を得ずにマルチ管理者認証機能を無効にする必要がある場合は、NetAppサポートに連絡し、次の記事を記載してください。 "MAV管理者が利用できない場合にマルチ管理者検証を無効にする方法"

MAVをイネーブルにすると、次のパラメータをグローバルに指定できます。

承認グループ
: グローバル承認グループのリスト。MAV機能を有効にするには、少なくとも1つのグループが必要です。

MAVを自律型ランサムウェア対策（ARP）で使用している場合は、ARPの一時停止、無効化、疑わしい要求のクリアを承認する新規または既存の承認グループを定義します。

必須の承認者
: 保護された操作を実行するために必要な承認者の数。デフォルトの最小値は1です。

必要な承認者の数は、デフォルトの承認グループ内の一意の承認者の総数よりも少なくする必要があります。

承認の有効期限（時間、分、秒）
: MAV管理者が承認要求に応答する必要がある期間。デフォルト値は1時間（1h）、サポートされる最小値は1秒（1s）、サポートされる最大値は14日（14d）です。

実行の有効期限（時間、分、秒）
: 要求元の管理者が::operationを完了する必要がある期間。デフォルト値は1時間（1h）、サポートされる最小値は1秒（1s）、サポートされる最大値は14日（14d）です。

これらのパラメータは、"操作ルール。"

System Managerの手順

1. マルチ管理者認証を受ける管理者を指定します。
   a. **[Cluster]>[Settings.]**をクリックします
   b. [Users and Roles]の横にあるをクリックします → 。*
   c. [Users]の下にあるをクリックします + Add 。*
   d. 必要に応じて名簿を変更します。

      詳細については、を参照してください。 "管理者アクセスの制御"

2. 複数管理者による検証を有効にするには、少なくとも1つの承認グループを作成し、少なくとも1つのルールを追加します。
   a. **[Cluster]>[Settings.]**をクリックします

b. セクションの[マルチ管理者の承認]*の横にあるをクリックします ⚙ 。

c. をクリックし ＋ Add て、少なくとも1つの承認グループを追加します。

- [名前]-グループ名を入力します。
- 承認者–ユーザーのリストから承認者を選択します。
- Eメールアドレス–Eメールアドレスを入力します。
- デフォルトグループ–グループを選択します。

d. ルールを少なくとも1つ追加してください。

- 操作–リストからサポートされているコマンドを選択します。
- クエリ–必要なコマンドオプションと値を入力します。
- オプションのパラメータ。グローバル設定を適用する場合は空白のままにし、特定のルールに別の値を割り当ててグローバル設定を上書きします。
  - 必要な承認者数
  - 承認グループ

e. [詳細設定*]をクリックして、デフォルトを表示または変更します。

- 必要な承認者数（デフォルト：1）
- 実行要求の有効期限（デフォルト：1時間）
- 承認リクエストの有効期限（デフォルト：1時間）
- メールサーバ*
- 送信元Eメールアドレス*

  *これらは、「通知管理」で管理されている電子メール設定を更新します。まだ設定されていない場合は、設定を求めるプロンプトが表示されます。

f. Enable（有効）*をクリックしてMAV初期設定を完了します。

初期設定後、現在のMAVステータスが* Multi-Admin Approval *（マルチ管理者承認）タイルに表示されます。

- ステータス（有効または無効）
- 承認が必要なアクティブな処理
- 保留状態のオープン要求の数

をクリックすると、既存の構成を表示できます →。既存の構成を編集するには、MAVの承認が必要です。

マルチ管理者認証を無効にするには：

1. **[Cluster]>[Settings.]**をクリックします
2. セクションの[マルチ管理者の承認]*の横にあるをクリックします ⚙ 。
3. [Enabled]トグルボタンをクリックします。

   この操作を完了するにはMAVの承認が必要です。

CLIの手順

CLIでMAV機能を有効にする前に、少なくとも1つが"MAV管理者グループ"作成されている必要があります。

実行する操作	入力するコマンド

MAV機能を有効にします	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`
	
	例：次のコマンドは、MAVを1つの承認グループ、2つの必須承認者、およびデフォルトの有効期限で有効にします。
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	少なくとも1つ追加して初期設定を完了する"操作ルール。"

MAV設定の変更（MAVの承認が必要）	`security multi-admin-verify approval-group modify [-approval-groups group1[,group2…]] [-required-approvers nn ] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`

MAV機能を確認します	`security multi-admin-verify show`
	
	• 例：*
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution Approval Approval`
	`Enabled Approvers Expiry Expiry Groups`
	`------- --------- --------- --------- ----------`
	`true 2 1h 1h mav-grp1`

実行する操作	入力するコマンド
MAV機能を無効にする（MAVの承認が必要）	`security multi-admin-verify modify -enabled false`

保護されたオペレーションルールの管理

マルチ管理者認証（MAV）ルールを作成して、承認が必要な操作を指定します。操作が開始されるたびに、保護された操作が傍受され、承認要求が生成されます。

適切なRBAC機能を持つ管理者は、MAVを有効にする前にルールを作成できますが、MAVを有効にすると、ルールセットを変更するにはMAVの承認が必要になります。

1回の操作で作成できるMAVルールは1つだけです。たとえば、複数のルールを作成することはできません `volume-snapshot-delete`。必要なルール制約は1つのルール内に含める必要があります。

保護するルールを作成できます"これらのコマンド"。各コマンドは、コマンドの保護機能が最初に使用可能になったONTAPバージョン以降で保護できます。

MAV system-defaultコマンドのルールは `security multi-admin-verify` "コマンド"変更できません。

システム定義の操作に加えて、次のコマンドは、マルチ管理者検証が有効になっている場合にデフォルトで保護されますが、これらのコマンドの保護を解除するルールを変更することができます。

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

ルール制約

ルールを作成するときに、オプションを指定して要求をコマンド機能のサブセットに制限することもできます `-query`。 `-query`オプションを使用すると、SVM、ボリューム、Snapshot名などの構成要素を制限することもできます。

たとえば、 `volume snapshot delete`コマンドでを `-query`に設定すると `-snapshot !hourly*,!daily*,!weekly*`、hourly、daily、weeklyのいずれかの属性がプレフィックスされたボリュームSnapshotがMAV保護の対象から除外されます。

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

除外された構成要素はMAVによって保護されず、管理者はそれらを削除または名前変更できます。

デフォルトでは、ルールは、保護された操作が入力されたときに対応するコマンドが自動的に生成されるように指定します `security multi-admin-verify request create "protected_operation"`。このデフォルトを変更して、コマンドを個別に入力するように指定でき `request create`ます。

デフォルトでは、ルールには次のグローバルMAV設定が継承されますが、ルール固有の例外を指定することもできます。

- 必要な承認者数
- 承認グループ
- 承認の有効期限
- 実行有効期間

System Managerの手順

保護された処理ルールを初めて追加する場合は、System Managerの手順を参照してください。"マルチ管理者検証を有効にします。"

既存のルールセットを変更するには：

1. [* Cluster]>[Settings]（設定）*を選択します。
2. セクションの[マルチ管理者の承認]*の横にあるを選択します ⚙ 。
3. 少なくとも1つのルールを追加する場合に選択し ＋ Add ます。既存のルールを変更または削除することもできます。
   - 操作–リストからサポートされているコマンドを選択します。
   - クエリ–必要なコマンドオプションと値を入力します。
   - オプションのパラメータ–グローバル設定を適用する場合は空白のままにし、特定のルールに別の値を割り当ててグローバル設定を上書きします。
     - 必要な承認者数
     - 承認グループ

CLIの手順

を除き、すべての `security multi-admin-verify rule`コマンドを実行する前にMAV管理者の承認が必要です。 `security multi-admin-verify rule show`

実行する操作	入力するコマンド
ルールの作成	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

実行する操作	入力するコマンド

現在の管理者のクレデンシャルの変更	`security login modify <parameters>`
	
	例：次のルールでは、ルートボリュームの削除が承認されている必要があります。
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

ルールを変更します	`security multi-admin-verify rule modify -operation “protected_operation” [parameters]`
ルールを削除します。	`security multi-admin-verify rule delete -operation “protected_operation”`
ルールを表示します	`security multi-admin-verify rule show`

コマンド構文の詳細については、マニュアルページを参照して `security multi-admin-verify rule`ください。

保護された操作の実行を要求

Multi-Admin Verification（MAV）が有効になっているクラスタで保護された操作またはコマンドを開始すると、ONTAPは自動的に操作を代行受信し、MAV承認グループの1人以上の管理者（MAV管理者）が承認する必要がある要求の生成を要求します。または、ダイアログなしでMAVリクエストを作成することもできます。

承認された場合は、クエリに応答して、要求の有効期限内に処理を完了する必要があります。拒否された場合、要求数の上限を超えた場合、または有効期限を過ぎた場合は、要求を削除して再送信する必要があります。

MAV機能は、既存のRBAC設定を遵守します。つまり、MAVの設定に関係なく、管理者ロールには、保護対象処理を実行するための十分な権限が必要です。"RBACの詳細については、こちらをご覧ください"です。

MAV管理者の場合は、保護された操作を実行する要求もMAV管理者によって承認されている必要があります。

System Managerの手順

ユーザーがメニュー項目をクリックして操作を開始し、その操作が保護されると、承認要求が生成され、次のような通知がユーザーに送信されます。

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

[*Multi-Admin Requests]ウィンドウは、MAVが有効な場合に使用できます。このウィンドウには、ユーザのログインIDとMAVロール（承認者または未承認）に基づいて保留中のリクエストが表示されます。保留中の要求ごとに、次のフィールドが表示されます。

- 操作
- インデックス（数値）
- ステータス（[保留中]、[承認済み]、[却下済み]、[実行済み]、または[期限切れ]）

  1人の承認者によってリクエストが却下された場合、それ以上のアクションは実行できません。

- クエリ（要求された操作のパラメータまたは値）
- 要求しているユーザ
- リクエストの有効期限：
- （の数）保留中の承認者
- （数）潜在的承認者数

要求が承認されると、要求したユーザは有効期限内に操作を再試行できます。

ユーザーが承認せずに操作を再試行すると、次のような通知が表示されます。

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

CLIの手順

1. 保護された動作を直接入力するか、MAV requestコマンドを使用して入力します。

   例–ボリュームを削除するには、次のいずれかのコマンドを入力します。

   - `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. リクエストのステータスを確認し、MAV通知に応答します。
   a. 要求が承認されたら、CLIメッセージに応答して処理を完了します。
      - 例：*

```
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. 要求が拒否された場合、または有効期限が過ぎた場合は、要求を削除し、再送信するかMAV管理者に連絡してください。

   - 例：*

```
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".
```

保護された操作要求の管理

MAV承認グループの管理者（MAV管理者）に保留中の操作実行要求が通知された場合、一定の期間（承認期限）内に承認または拒否メッセージで応答する必要があります。十分な数の承認が得られない場合、リクエスト者はそのリクエストを削除して別のリクエストを作成する必要があります。

タスクの内容

承認リクエストはインデックス番号で識別され、電子メールメッセージやリクエストキューの表示に含まれます。

要求キューから次の情報を表示できます。

操作
: 要求が作成される保護された操作。

クエリ
: ユーザーが操作を適用するオブジェクト。

都道府県

リクエストの現在の状態（保留中、承認済み、却下済み、期限切れ） 実行済み。1人の承認者によってリクエストが却下された場合、それ以上のアクションは実行できません。

必須の承認者

リクエストを承認するために必要なMAV管理者の数。ユーザーは、操作ルールに必要な承認者パラメータを設定できます。ユーザーがルールに必須承認者を設定していない場合は、グローバル設定の必須承認者が適用されます。

保留中の承認者

リクエストを承認済みとしてマークするためにリクエストを承認する必要があるMAV管理者の数。

承認の有効期限

MAV管理者が承認要求に応答する必要がある期間。承認されたユーザーは誰でも、操作ルールの承認期限を設定できます。ルールにapproval-expiryが設定されていない場合は、グローバル設定のapproval-expiryが適用されます。

実行の有効期限

要求元の管理者が処理を完了する必要のある期間。許可されたユーザーは誰でも、操作ルールの実行期限を設定できます。ルールにexecution-expiryが設定されていない場合は、グローバル設定のexecution-expiryが適用されます。

ユーザーが承認しました

リクエストを承認したMAV管理者。

ユーザが拒否しました

リクエストを拒否したMAV管理者。

Storage VM（SVM）

要求が関連付けられているSVM。このリリースでは管理SVMのみがサポートされます。

ユーザが要求しました

要求を作成したユーザのユーザ名。

作成時刻

リクエストが作成された時刻。

承認された時間

リクエストの状態が承認済みに変更された時刻。

コメント

リクエストに関連付けられているコメント。

ユーザが許可されました

リクエストが承認された保護された操作の実行を許可されているユーザーのリスト。が空の場合は `users-permitted`、適切な権限を持つすべてのユーザが処理を実行できます。

期限切れまたは実行されたすべての要求は、要求数の上限に達した場合、または期限切れの要求の有効期限が8時間を超えた場合に削除されます。拒否された要求は、期限切れとしてマークされると削除されます。

System Managerの手順

MAV管理者は、承認要求の詳細、要求の有効期限、および要求を承認または拒否するためのリンクが記載された電子メールメッセージを受信します。承認ダイアログにアクセスするには、Eメール内のリンクをクリックするか、System Managerで* Events & Jobs > Requests *（イベントとジョブ>要求）に移動します。

[*Requests]ウィンドウは、マルチ管理者検証がイネーブルの場合に使用でき、ユーザのログインIDおよびMAVロール（アプルーバまたはそれ以外）に基づいて保留中の要求が表示されます。

- 操作
- インデックス（数値）
- ステータス（[保留中]、[承認済み]、[却下済み]、[実行済み]、または[期限切れ]）

  1人の承認者によってリクエストが却下された場合、それ以上のアクションは実行できません。

- クエリ（要求された操作のパラメータまたは値）
- 要求しているユーザ
- リクエストの有効期限：
- （の数）保留中の承認者
- （数）潜在的承認者数

MAV管理者は、このウィンドウで追加のコントロールを使用できます。個 々 の操作、または選択した操作グループを承認、却下、または削除できます。ただし、MAV管理者が要求ユーザである場合は、自分の要求を承認、拒否、または削除することはできません。

CLIの手順

1. 保留中のリクエストが電子メールで通知されたら、リクエストのインデックス番号と承認の有効期限をメモします。インデックス番号は、以下の* show または show-pending *オプションを使用して表示することもできます。
2. 要求を承認または拒否します。

実行する操作	入力するコマンド
リクエストを承認します	`security multi-admin-verify request approve` *nn*
要求を拒否します	`security multi-admin-verify request veto` *nn*
すべての要求、保留中の要求、または単一の要求を表示します	`security multi-admin-verify request { show

実行する操作	入力するコマンド
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  キュー内のすべての要求を表示することも、保留中の要求だけを表示することもできます。インデックス番号を入力すると、その要求の情報のみが表示されます。特定のフィールドに関する情報（パラメータを使用）またはすべてのフィールドに関する情報（パラメータを使用）を表示でき `-fields`ます `-instance`。
リクエストを削除します	`security multi-admin-verify request delete` *nn*

例：

次のシーケンスは、MAV管理者がインデックス番号3のリクエスト電子メールを受信した後、リクエストを承認します。インデックス番号3はすでに1つの承認を持っています。

```
          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: -
```

例：

次のシーケンスでは、MAV管理者がインデックス番号3の要求電子メールを受信した後、要求が拒否されます。この電子メールにはすでに1つの承認が設定されています。

```
      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: -
```

著作権に関する情報

商標に関する情報