管理者による検証を管理します
ONTAP 9

NetApp
April 24, 2024

目次

管理者による検証を管理します

マルチ管理者検証の概要

ONTAP 9.11.1以降では、マルチ管理検証（MAV）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、指定した管理者からの承認がないと実行できないようにすることができます。これにより、侵害を受けた管理者、悪意のある管理者、または経験の浅い管理者が、望ましくない変更やデータの削除を行うことを防止でき

マルチ管理者検証の設定は、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の有効化。"
- "ルールを追加または変更する。"

初期設定後、これらの要素はMAV承認グループ（MAV管理者）の管理者のみが変更できます。

マルチ管理者検証を有効にすると、保護されたすべての処理が完了するために次の3つの手順が必要となります。

- ユーザが処理を開始すると、が実行されます "要求が生成されます。"
- 実行する前に、少なくとも1つは必要です "MAV管理者は承認する必要があります。"
- 承認されると、ユーザーは操作を完了します。

複数管理者による検証は、自動化の負荷が大きいボリュームやワークフローでは使用しないことを想定しています。自動化された各タスクを完了するには承認が必要なためです。 オートメーションとMAVを併用する場合は、MAVの特定の操作にクエリを使用することをお勧めします。たとえば、適用できます `volume delete` MAVルールは、自動化が関係しないボリュームにのみ適用され、特定の命名規則を使用して指定できます。

> MAVの管理者の承認なしでマルチ管理者検証機能を無効にする必要がある場合は、ネットアップサポートに連絡して、次の技術情報アーティクルを記載します。 "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"。

マルチ管理者検証の仕組み

マルチ管理者検証は、次の要素で構成されます。

- 承認権限と拒否権を持つ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。このため、保護された操作を実行または承認する管理者は、それらの操作に対する最低限のRBAC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。"

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*

  管理者による検証機能の設定を制御します。

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

  管理者による検証クレデンシャルを使用して、一連の管理者のメンバーシップを制御します。

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

  管理者による検証が必要な一連のコマンドを制御します。

- `security multi-admin-verify request` 操作

  承認プロセスを制御します。

ルールで保護されたコマンド

マルチ管理者検証を有効にした場合、システム定義のコマンドに加えて次のコマンドも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ようにルールを変更することができます。

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

ONTAP 9.11.1以降のリリースでは、次のコマンドを保護できます。

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

ONTAP 9.13.1以降では、次のコマンドを保護できます。

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

ONTAP 9.14.1以降では、次のコマンドを保護できます。

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

複数管理者による承認の仕組み

保護された操作がMAV保護されたクラスタで入力されると、操作の実行要求が指定されたMAV管理者グループに送信されます。

次の項目を設定できます。

- 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を持つRBACロールが必要です。

- MAV管理者グループの数。
  - MAVグループは、保護された各操作ルールに割り当てられます。

    - 複数のMAVグループの場合、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。
- 保護された操作を実行するために必要なMAV承認の数。
- 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、MAV承認が必要です。

MAV管理者は、保護された操作を実行するための独自の要求を承認できません。そのため、次の

- 管理者が1人だけのクラスタではMAVを有効にしないでください。
- MAVグループにユーザーが1人しかいない場合、MAV管理者は保護された操作を入力できません。通常の管理者は、これらの操作を入力する必要があり、MAV管理者は承認のみを行えます。
- 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、必要な承認数よりも1人大きくなければなりません。 たとえば、保護された操作に2つの承認が必要で、MAV管理者がそれらを実行する場合、MAV管理者グループには3人の承認が必要です。

MAV管理者は、（EMSを使用して）Eメールアラートで承認要求を受信するか、要求キューを照会できます。リクエストを受け取った場合、次の3つのアクションのいずれかを実行できます。

- 承認します
- 拒否（拒否）
- 無視（操作なし）

MAVルールに関連付けられているすべての承認者に電子メール通知が送信されるのは、次の場合です。

- リクエストが作成されました。
- 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す。

リクエスト者が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。

*注：*リクエスト者は、承認グループに属している場合でも、リクエスト者自身のリクエストを承認できません。ただし、E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（つまり、MAV管理者ではない）リクエスタは、電子メール通知を受信しません。

保護された操作の実行の仕組み

保護された操作の実行が承認されると、要求されたユーザーは操作を続行します。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権限の後に評価されます。そのため、操作の実行に十分なRBACアクセス許可がないユーザーはMAV要求プロセスを開始できません。

管理者の承認グループを管理します

Multi-Admin Verification（MAV；マルチ管理者検証）を有効にする前に、1人以上の管理

者が承認権限または拒否権限を付与される管理者承認グループを作成する必要があります。マルチ管理者検証を有効にすると、承認グループのメンバーシップを変更した場合には、既存の資格のある管理者の承認が必要になります。

このタスクについて

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機能は、既存のロールベースアクセス制御（RBAC）設定に対応しています。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。"

MAVを設定して、承認リクエストが保留中であることをMAV管理者に通知できます。そのためには、Eメール通知（特に）を設定する必要があります `Mail From` および `Mail Server` パラメータ—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。MAV管理者は、電子メールアラートを使用しないで、承認キューを手動でチェックする必要があります。

System Manager の手順の略

MAV承認グループを初めて作成する場合は、「System Manager手順 to」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. 管理者による検証を受ける管理者を特定します。
   a. [**Cluster]>[Settings.**]をクリックします
   b. をクリックします → をクリックします
   c. をクリックします + Add [**Users.**]の下にあります
   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. をクリックします → 「セキュリティ」セクションの「*マルチ管理者承認」の横。 （が表示されます ⚙ アイコン（MAVがまだ設定されていない場合）。
      - Name：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。

MAVを有効にした後、既存の設定を編集するにはMAV承認が必要です。

CLI 手順の略

1. に値が設定されていることを確認します `Mail From` および `Mail Server` パラメータ入力するコマンド

```
event config show
```

次のような情報が表示されます。

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

次のパラメータを入力して設定します。

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

2. 管理者による検証を受ける管理者を特定します

実行する処理	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。

実行する処理	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`

マルチ管理者検証を有効または無効にします

Multi-admin Verification（MAV；マルチ管理者検証）は明示的に有効にする必要があります。マルチ管理者検証を有効にした後は、MAV承認グループ（MAV管理者）の管理者による承認が必要になります。

このタスクについて

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の管理者の承認なしでマルチ管理者検証機能を無効にする必要がある場合は、ネットアップサポートに連絡して、次の技術情報アーティクルを記載します。 "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とAutonomous Ransomware Protection（ARP）を使用している場合は、ARPの一時停止、無効化、および疑わしい要求のクリアを担当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。デフォルトの最小数は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。

特定のパラメータについて、これらのパラメータを上書きすることもできます "操作ルール。"

System Manager の手順の略

1. 管理者による検証を受ける管理者を特定します。
   a. **[Cluster]>[Settings.**]をクリックします
   b. をクリックします → をクリックします
   c. をクリックします + Add **[Users.**]の下にあります
   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. 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て、マルチ管理者検証を有効にします。
   a. **[Cluster]>[Settings.**]をクリックします
   b. をクリックします ⚙ 「セキュリティ」セクションの「*マルチ管理者承認」の横。
   c. をクリックします + Add 1つ以上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。

- operation–サポートされているコマンドをリストから選択します。
- Query–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ます。グローバル設定を上書きする場合は、特定のルールに別の値を割り当てます。
  - 必要な承認者の数
  - 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操作
- 保留状態のオープン要求の数

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

マルチ管理者検証を無効にする場合：

1. **[Cluster]>[Settings.**]をクリックします
2. をクリックします ⚙ 「セキュリティ」セクションの「*マルチ管理者承認」の横。
3. [有効]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承認が必要です。

CLI 手順の略

CLIでMAV機能をイネーブルにする前に、少なくとも1つ "MAV管理者グループ" を作成しておく必要があります。

実行する処理	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`
	
	1つ以上を追加して初期設定を完了します "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`

MAV機能を無効にする（MAVの承認が必要）	`security multi-admin-verify modify -enabled false`

保護された操作ルールを管理します

MAV（Multi-admin Verification）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、保護された操作が妨害され、承認の要求が生成されます。

ルールは任意の管理者が適切なRBAC機能を使用してMAVを有効にする前に作成できますが、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MAVルールを作成することはできません。 `volume-snapshot-delete` ルール。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。

ルールで保護されたコマンド

ONTAP 9.11.1以降では、次のコマンドを保護するルールを作成できます。

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

ONTAP 9.13.1以降では、次のコマンドを保護するルールを作成できます。

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

ONTAP 9.14.1以降では、次のコマンドを保護するルールを作成できます。

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

- `vserver modify`

MAV system-defaultコマンドのルール `security multi-admin-verify` "コマンド"を変更することはできません。

マルチ管理者検証を有効にした場合、システム定義のコマンドに加えて次のコマンドも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ように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、オプションでを指定できます `-query` 要求をコマンド機能のサブセットに制限するオプション。。 `-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。

例えば、 `volume snapshot delete` コマンド、 `-query` 次のように設定できます。 `-snapshot !hourly*,!daily*,!weekly*` つまり、hourly、daily、またはweekly属性のプレフィックスが付いたボリュームSnapshotは、MAV保護から除外されます。

```
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、ルールは対応するを指定します `security multi-admin-verify request create` *"protected_operation"* 保護されたオペレーションが入力されると、コマンドが自動的に生成されます。このデフォルトを変更して、が必要になるようにすることができます `request create` コマンドは別 々 に入力します。

デフォルトでは、ルール固有の例外を指定できますが、ルールは次のグローバルMAV設定を継承します。

- 承認者の必要数
- 承認グループ
- 承認の有効期限
- 実行の有効期限

System Manager の手順の略

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. 選択するオプション ⚙ 「セキュリティ」セクションの「*マルチ管理者承認」の横。
3. 選択するオプション + Add ルールを追加するには、既存のルールを変更または削除することもできます。
   - operation–サポートされているコマンドをリストから選択します。
   - Query–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欄のままにします。グローバル設定を上書きする場合は、特定のルールに別の値を割り当てます。
     - 必要な承認者の数
     - 承認グループ

CLI 手順の略

> すべて `security multi-admin-verify rule` コマンドを実行するには、以外のMAV管理者の承認が必要です `security multi-admin-verify rule show`。

実行する処理	入力するコマンド
ルールを作成します	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

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"`

実行する処理	入力するコマンド
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、を参照してください `security multi-admin-verify rule` マニュアルページ

保護された操作の実行を要求します

マルチ管理者検証（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、要求を生成するよう要求します。この要求は、MAV承認グループ（MAV管理者）の1人以上の管理者によって承認される必要があります。または、ダイアログなしでMAV要求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、または要求や有効期限を超えた場合は、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設定に対応しています。つまり、管理者ロールには、MAV設定に関係なく、保護された操作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"。

MAV管理者の場合、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る必要があります。

System Manager の手順の略

ユーザーがメニュー項目をクリックして操作を開始し、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］）

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

- query（要求された処理のパラメータまたは値）
- ユーザーを要求しています
- 要求の有効期限はです
- （の数）保留中の承認者
- （数）承認者の候補

要求が承認されると、要求元ユーザは有効期限内に処理を再試行できます。

ユーザが承認なしで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 手順の略

1. 保護された操作を直接入力するか、MAV requestコマンドを使用します。

   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を管理します

MAV承認グループ（MAV管理者）の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の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。

このタスクについて

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

要求キューからは、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。

状態

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。リクエストが1人の承認者によって却下された場合、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。ユーザは、操作ルールのrequired-approversパラメータを設定できます。ユーザーが必須承認者をルールに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。許可されたユーザーは、操作ルールの承認期限を設定できます。承認期限がルールに設定されていない場合は、グローバル設定の承認期限が適用されます。

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。許可された任意のユーザーは、操作ルールの実行有効期限を設定できます。実行有効期限がルールに設定されていない場合は、グローバル設定の実行有効期限が適用されます。

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（ **Comment** ）

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。状況 `users-permitted` が空の場合、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。

期限切れの要求または実行された要求は、制限が1000件に達したとき、または期限切れの要求が8時間を超えたときにすべて削除されます。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 の手順の略

MAV管理者は、承認リクエストの詳細、リクエストの有効期限、リクエストを承認または却下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］）

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

- query（要求された処理のパラメータまたは値）
- ユーザーを要求しています
- 要求の有効期限はです
- （の数）保留中の承認者
- （数）承認者の候補

MAV管理者は、この画面に追加のコントロールを設定できます。管理者は、個々の操作または操作の選択したグループを承認、拒否、または削除できます。ただし、MAV管理者が要求元ユーザである場合は、独自の要求を承認、拒否、または削除することはできません。

CLI 手順の略

1. 保留中のリクエストが電子メールで通知された場合は、リクエストのインデックス番号と承認期限をメモします。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。

実行する処理	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

実行する処理	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を表示するには、を使用します `-fields` パラメータ）またはすべてのフィールドについて（を使用 `-instance` パラメータ）。
リクエストを削除します	`security multi-admin-verify request delete` *`nn`*

例

次のシーケンスでは、MAV管理者がインデックス番号3のリクエストメールを受信した後、リクエストが承認されます。これはすでに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

次のシーケンスは、MAV管理者がインデックス番号3の要求メールを受信した後、すでに1つの承認がある要求を拒否します。

```
      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: -
```