動的許可の管理
ONTAP 9

NetApp
June 19, 2024

目次

動的許可の管理

動的許可の概要

ONTAP 9.15.1以降では、管理者は動的な許可を設定して有効にすることで、ONTAPへのリモートアクセスのセキュリティを強化すると同時に、悪意のある攻撃者によって引き起こされる可能性のある損害を軽減することができます。ONTAP 9.15.1では、動的認可により、ユーザーにセキュリティスコアを割り当てるための初期フレームワークが提供されます。また、ユーザーのアクティビティが疑わしい場合は、追加の認可チェックを行ったり、操作を完全に拒否したりすることができます。管理者は、ルールを作成し、信頼スコアを割り当て、コマンドを制限して、特定のアクティビティがユーザーに対して許可または拒否されるタイミングを決定できます。動的許可は、クラスタ全体または個 々 のStorage VMに対して有効にできます。

動的許可の仕組み

動的認可では、信頼スコアリングシステムを使用して、認可ポリシーに応じて異なるレベルの信頼をユーザに割り当てます。ユーザの信頼レベルに基づいて、ユーザが実行するアクティビティを許可または拒否するか、またはユーザにさらなる認証を要求することができます。

たとえば、3人のユーザがボリュームを削除しようとするとします。ユーザーが操作を実行しようとするときに、各ユーザーのリスク評価が検査されます。

- 最初のユーザーが通常の業務時間に信頼できるデバイスからログインするため、リスク評価は低くなります。この操作は追加の認証なしで許可されます。
- 2番目のユーザーは、勤務時間外に自宅の信頼できるデバイスからログインするため、リスク評価は中程度になります。操作が許可される前に、追加の認証を要求されます。
- 3番目のユーザーは、営業時間外の新しい場所にある信頼されていないデバイスからログインします。これにより、リスク評価が高くなり、操作は許可されません。

次のステップ

- "動的許可のカスタマイズ"
- "動的許可の有効化または無効化"

動的許可の有効化または無効化

ONTAP 9.15.1以降では、管理者は動的許可を次のいずれかで設定および有効化できます。 `visibility` 設定をテストするモード、または `enforced` SSH経由で接続するCLIユーザの設定をアクティブにするモード。動的認可が不要になった場合は、ディセーブルにすることができます。ダイナミック許可をディセーブルにしても、コンフィギュレーション設定は使用可能なままであり、後で再度イネーブルにする場合に使用できます。

のパラメータの詳細については、を参照してください。 `security dynamic-authorization modify` コマンドについては、ONTAPのマニュアルページを参照してください。

テストの動的許可を有効にする

表示モードで動的許可を有効にすると、機能をテストして、ユーザが誤ってロックアウトされないようにすることができます。このモードでは、信頼スコアはすべての制限されたアクティビティでチェックされますが、強制はされません。ただし、拒否された、または追加の認証チャレンジの対象となるアクティビティはすべてログに記録されます。ベストプラクティスとして、強制する前に、このモードで目的の設定をテストすることを推奨します。

> この手順を実行すると、他のダイナミック認可設定をまだ設定していない場合でも、初めてダイナミック認可をイネーブルにできます。を参照してください "動的許可のカスタマイズ" その他の動的認証設定を構成して環境に合わせてカスタマイズする手順については、を参照してください。

手順

1. グローバル設定を設定し、機能の状態をに変更することで、可視モードでの動的許可を有効にします。 `visibility`。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。括弧<>の値を環境に合わせて更新します。太字のパラメータは必須です。

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. を使用して結果を確認します。 `show` グローバル設定を表示するコマンドは次のとおりです。

```
security dynamic-authorization show
```

強制モードでの動的許可の有効化

強制モードでダイナミック許可をイネーブルにできます。通常、このモードは、可視化モードでのテストを完了した後に使用します。このモードでは、すべての制限されたアクティビティで信頼スコアがチェックされ、制限条件が満たされるとアクティビティ制限が適用されます。抑制間隔も適用されるため、指定された間隔内での追加の認証チャレンジを防ぐことができます。

> この手順では、でダイナミック認可を設定し、イネーブルにしていることを前提としています。 `visibility` モード。これを強く推奨します。

手順

1. で動的許可を有効にする `enforced` モード（状態をに変更） `enforced`。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。括弧<>の値を環境に合わせて更新します。太字のパラメータは必須です。

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. を使用して結果を確認します。 `show` グローバル設定を表示するコマンドは次のとおりです。

```
security dynamic-authorization show
```

動的許可の無効化

追加された認証セキュリティが不要になった場合は、動的許可をディセーブルにできます。

手順

1. 動的許可を無効にするには、状態をに変更します。 `disabled`。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。括弧<>の値を環境に合わせて更新します。太字のパラメータは必須です。

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. を使用して結果を確認します。 `show` グローバル設定を表示するコマンドは次のとおりです。

```
security dynamic-authorization show
```

次のステップ

（オプション）環境に応じて、を参照してください。 "動的許可のカスタマイズ" 他の動的認可設定を構成します。

動的許可のカスタマイズ

管理者は、動的許可の設定のさまざまな側面をカスタマイズして、ONTAPクラスタへのリモート管理者のSSH接続のセキュリティを強化できます。

セキュリティのニーズに応じて、次の動的認可設定をカスタマイズできます。

- [動的認証グローバル設定の構成]
- [動的認証信頼スコアコンポーネントの設定]
- [カスタム信頼スコアプロバイダの設定]

- [制限されたコマンドの設定]
- [動的許可グループの設定]

動的認証グローバル設定の構成

動的許可のグローバル設定を行うことができます。これには、セキュアなStorage VM、認証チャレンジの抑制間隔、信頼スコアの設定などが含まれます。

のパラメータとデフォルト値の詳細については、 `security dynamic-authorization modify` コマンドについては、ONTAPのマニュアルページを参照してください。

手順

1. 動的認可のグローバル設定を構成します。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。かっこ<>の値を環境に合わせて更新します。

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 作成された構成を表示します。

```
security dynamic-authorization show
```

制限されたコマンドの設定

ダイナミック許可をイネーブルにすると、この機能には制限されたコマンドのデフォルトセットが含まれます。このリストは、必要に応じて変更できます。を参照してください "Multi-Admin Verification（MAV）ドキュメント" デフォルトの制限されたコマンドのリストについては、を参照してください。

制限されたコマンドの追加

動的許可で制限されているコマンドのリストにコマンドを追加できます。

のパラメータとデフォルト値の詳細については、 `security dynamic-authorization rule create` コマンドについては、ONTAPのマニュアルページを参照してください。

手順

1. コマンドを追加します。括弧<>の値を環境に合わせて更新します。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. 表示される制限されたコマンドのリストを表示します。

```
security dynamic-authorization rule show
```

制限されたコマンドを削除する

ダイナミック許可で制限されているコマンドのリストから、コマンドを削除できます。

のパラメータとデフォルト値の詳細については、 `security dynamic-authorization rule delete` コマンドについては、ONTAPのマニュアルページを参照してください。

手順

1. コマンドを削除します。括弧<>の値を環境に合わせて更新します。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. 表示される制限されたコマンドのリストを表示します。

```
security dynamic-authorization rule show
```

動的許可グループの設定

デフォルトでは、動的認可は、イネーブルにするとすぐにすべてのユーザとグループを環境にします。ただし、 `security dynamic-authorization group create` このコマンドを使用すると、ダイナミック認可は特定のユーザだけを環境にすることができます。

動的認可グループを追加します。

ダイナミック認可グループを追加できます。

のパラメータとデフォルト値の詳細については、 `security dynamic-authorization group create` コマンドについては、ONTAPのマニュアルページを参照してください。

手順

1. グループを作成します。括弧<>の値を環境に合わせて更新します。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization group create \
<strong>-group-name <group-name></strong> \
-vserver <storage_VM_name> \
-exclude-users <user1,user2,user3...>
```

2. 作成された動的認可グループを表示します。

```
security dynamic-authorization group show
```

ダイナミック許可グループを削除します。

ダイナミック認可グループを削除できます。

手順

1. グループを削除します。括弧<>の値を環境に合わせて更新します。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization group delete \
<strong>-group-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. 作成された動的認可グループを表示します。

```
security dynamic-authorization group show
```

動的認証信頼スコアコンポーネントの設定

スコアリング基準の優先度を変更したり、リスクスコアリングから特定の基準を削除したりするために、最大スコアウェイトを設定できます。

ベストプラクティスとして、デフォルトのスコアウェイト値はそのままにし、必要な場合にのみ調整することを推奨します。

のパラメータとデフォルト値の詳細については、 `security dynamic-authorization trust-score-component modify` コマンドについては、ONTAPのマニュアルページを参照してください。

変更可能なコンポーネントは、デフォルトのスコアとパーセンテージの重みとともに次のとおりです。

基準	コンポーネント名	デフォルトの未加工スコアの重み	デフォルトの重量パーセンテージ
信頼できるデバイス	`trusted-device`	20	50です
ユーザログイン認証履歴	`authentication-history`	20	50です

手順

1. 信頼スコアコンポーネントを変更します。括弧<>の値を環境に合わせて更新します。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. 結果の信頼スコアコンポーネントの設定を表示します。

```
security dynamic-authorization trust-score-component show
```

ユーザーの信頼スコアをリセットする

ユーザーがシステムポリシーのためにアクセスを拒否され、IDを証明できる場合、管理者はユーザーの信頼スコアをリセットできます。

のパラメータとデフォルト値の詳細については、 `security dynamic-authorization user-trust-score reset` コマンドについては、ONTAPのマニュアルページを参照してください。

手順

1. コマンドを追加します。を参照してください [動的認証信頼スコアコンポーネントの設定] リセット可能な信頼スコアコンポーネントのリストについては、を参照してください。括弧<>の値を環境に合わせて更新します。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

信頼スコアの表示

ユーザは、ログインセッションの独自の信頼スコアを表示できます。

手順

1. 信頼スコアを表示します。

```
security login whoami
```

次のような出力が表示されます。

```
User: admin
Role: admin
Trust Score: 50
```

カスタム信頼スコアプロバイダの設定

外部の信頼スコアプロバイダーからスコアリングメソッドをすでに受信している場合は、カスタムプロバイダーを動的認可設定に追加できます。

作業を開始する前に

- カスタム信頼スコアプロバイダはJSON応答を返す必要があります。次の構文要件を満たす必要があります。
  - 信頼スコアを返すフィールドは、配列の要素ではなくスカラーフィールドである必要があります。
  - 信頼スコアを返すフィールドは、次のようにネストされたフィールドにすることができます。`trust_score.value`。
  - JSON応答内に数値の信頼スコアを返すフィールドが必要です。これがネイティブで利用できない場合は、この値を返すラッパースクリプトを記述できます。
- 提供される値は、信頼スコアまたはリスクスコアのいずれかです。違いは、信頼スコアが昇順で、高いスコアが高い信頼レベルを示し、リスクスコアが降順であることです。たとえば、0～100のスコア範囲の信頼スコアが90の場合は、スコアが非常に信頼性が高く、追加のチャレンジなしで「許可」になる可能性があることを示します。 スコアの範囲が0～100の場合、リスクスコアが90の場合は、リスクが高く、追加のチャレンジなしで「拒否」になる可能性があります。
- カスタム信頼スコアプロバイダには、ONTAP REST API経由でアクセスできる必要があります。
- カスタム信頼スコアプロバイダは、サポートされているパラメータのいずれかを使用して設定する必要があります。サポートされているパラメータリストにない設定を必要とするカスタム信頼スコアプロバイダはサポートされません。

のパラメータとデフォルト値の詳細については、 `security dynamic-authorization trust-score-component create` コマンドについては、ONTAPのマニュアルページを参照してください。

手順

1. カスタム信頼スコアプロバイダを追加します。括弧<>の値を環境に合わせて更新します。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. 結果の信頼スコアプロバイダ設定を表示します。

```
security dynamic-authorization trust-score-component show
```

カスタム信頼スコアプロバイダタグの設定

タグを使用して外部の信頼スコアプロバイダーと通信できます。これにより、機密情報を公開することなく、URL内の情報を信頼スコアプロバイダーに送信できます。

のパラメータとデフォルト値の詳細については、 `security dynamic-authorization trust-score-component create` コマンドについては、ONTAPのマニュアルページを参照してください。

手順

1. 信頼スコアプロバイダタグを有効にします。括弧<>の値を環境に合わせて更新します。使用しない場合は、 `-vserver` パラメータを指定すると、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です。

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

例：

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

著作権に関する情報

商標に関する情報