動的許可の管理
ONTAP 9

NetApp
February 12, 2026

目次

動的許可の管理

ONTAP動的認証について学ぶ

ONTAP 9.15.1以降では、管理者は動的許可を設定し有効化することで、ONTAPへのリモート アクセス時のセキュリティを強化するとともに、悪意のあるユーザによる攻撃の被害を軽減できます。ONTAP 9.15.1の動的許可は初期段階のフレームワークであり、ユーザにセキュリティ スコアを割り当て、その行動が不審な場合に追加の許可チェックを実施するか、操作を完全に拒否できます。管理者はルールの作成、信頼スコアの割り当て、コマンドの制限を行い、ユーザの特定の行動を許可または拒否するタイミングを指定できます。動的許可の有効化は、クラスタ全体または個別のStorage VMに対して行えます。

動的許可の仕組み

動的許可では、信頼スコア システムに基づき、許可ポリシーに応じた各種信頼レベルをユーザに割り当てます。ユーザの信頼レベルに応じて、その操作を許可または拒否するか、追加の認証を求めることができます。

"動的許可のカスタマイズ"を参照して、基準スコアの重みやその他の動的承認属性を構成する方法の詳細を確認してください。

信頼済みのデバイス

動的許可が使用されている場合、信頼済みのデバイスの定義は、ユーザが認証方法の1つとして公開鍵認証を使用してONTAPにログインするために使用するデバイスです。そのデバイスは、そのユーザのみが対応する秘密鍵を所有しているため、信頼されます。

動的許可の例

例として、3名のユーザがボリュームの削除を試みた場合を考えます。各ユーザの操作試行時には、それぞれのリスクが以下のように評価されます。

- 1番目のユーザは、以前に数回だけ認証に失敗した信頼済みのデバイスからログインしました。そのため、リスクは低いと評価され、追加の認証不要で操作が許可されます。
- 2番目のユーザは、以前に認証に失敗した割合が中程度の信頼済みのデバイスからログインしました。そのため、リスクは中程度と評価され、操作の許可前に追加の認証が求められます。
- 3番目のユーザは、以前に認証に失敗した割合が高い、信頼されていないデバイスからログインしました。そのため、リスクは高いと評価され、操作が拒否されます。

次の手順

- "動的許可の有効化と無効化"
- "動的許可のカスタマイズ"

ONTAPでの動的認可の有効化または無効化

ONTAP 9.15.1以降、管理者は動的認証の設定と有効化を、 `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ユーザ向けに設定をアクティブ化するモードのいずれかで実行できます。動的認証が不要になった場合は、無効にすることができます。動的認証を無効にしても設定はそのまま残り、後で再度有効にする場合に使用できます。

`security dynamic-authorization modify`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-modify.html["ONTAPコマンド リファレンス
"^]を参照してください。

テスト目的での動的許可の有効化

visibilityモードで動的許可を有効化すると、ユーザを誤ってロック アウトする事態を防ぎつつ、機能のテストを行えます。このモードでは、すべての制限対象操作で信頼スコアがチェックされますが、適用はされません。ただし、動的許可の有効時に拒否または追加認証チャレンジの対象となるすべての操作が記録されます。ベストプラクティスとして、目的の設定を適用する前に、このモードでテストすることが推奨されます。

他の動的認証設定をまだ設定していない場合でも、この手順で初めて動的認証を有効化できます。環境に合わせてカスタマイズするためのその他の動的認証設定を設定する手順については、"動的許可のカスタマイズ"を参照してください。

手順

1. グローバル設定を構成し、機能の状態を `visibility`に変更することで、可視性モードで動的認証を有効にします。 `-vserver`パラメータを使用しない場合、コマンドはクラスタ レベルで実行されます。括弧内の値<>を環境に合わせて更新してください。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. `show`コマンドを使用してグローバル構成を表示し、結果を確認します：

```
security dynamic-authorization show
```

enforcedモードでの動的許可の有効化

enforcedモードで動的許可を有効化できます。通常、このモードはvisibilityモードでのテスト実施後に使用します。このモードでは、すべての制限対象操作で信頼スコアがチェックされ、制限条件に該当する場合に操作制限が適用されます。抑制間隔も適用されるため、指定した間隔中は追加の認証チャレンジが行われません。

この手順では、以前に `visibility`モードで動的許可を設定して有効にしていることを前提としています。これを強くお勧めします。

手順

1. `enforced`モードで動的認証を有効にするには、状態を `enforced`に変更します。 `-vserver`パラメータを使用しない場合、コマンドはクラスタ レベルで実行されます。括弧内の値<>を環境に合わせて更新してください。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. `show`コマンドを使用してグローバル構成を表示し、結果を確認します：

```
security dynamic-authorization show
```

動的許可の無効化

追加した認証セキュリティが不要になった場合、動的許可を無効化できます。

手順

1. 動的認証を無効化するには、状態を `disabled`に変更してください。 `-vserver`パラメータを使用しない場合、コマンドはクラスタ レベルで実行されます。括弧内の値<>は環境に合わせて更新してください。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. `show`コマンドを使用してグローバル構成を表示し、結果を確認します：

```
security dynamic-authorization show
```

`security dynamic-authorization show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-show.html["ONTAPコマンド リファレンス
"^]を参照してください。

次の手順

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

ONTAPでの動的認可のカスタマイズ

管理者は、動的許可のさまざまな設定をカスタマイズして、自身がONTAPクラスタにリモートでSSH接続する際のセキュリティを高められます。

セキュリティのニーズに応じて、以下の動的許可設定をカスタマイズできます。

- [動的許可グローバル設定の構成]
- 動的許可の信頼スコア コンポーネントの構成
- 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]

動的許可グローバル設定の構成

保護対象のStorage VM、認証チャレンジの抑制間隔、信頼スコア設定など、動的許可のグローバル設定を構成できます。

```
`security login domain-tunnel create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-modify.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

手順

1. 動的認証のグローバル設定を構成します。 `-vserver`パラメータを使用しない場合、コマンドはクラスタレベルで実行されます。括弧内の値<>を環境に合わせて更新してください：

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

2. 変更後の設定を確認します。

```
security dynamic-authorization show
```

制限されたコマンドの設定

動的認証を有効にすると、この機能にはデフォルトで制限コマンドのセットが含まれます。このリストはニーズに合わせて変更できます。制限コマンドのデフォルトリストについては、"マルチ管理者検証（MAV）のドキュメント"を参照してください。

制限コマンドの追加

動的許可で制限するコマンドのリストにコマンドを追加できます。

`security dynamic-authorization rule create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-rule-create.html["ONTAPコマンド リファレンス
"^]をご覧ください。

手順

1. コマンドを追加します。括弧内の値<>を環境に合わせて更新してください。 `-vserver`パラメータを使用しない場合、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. 変更後の制限コマンド リストを確認します。

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

制限コマンドの削除

動的許可で制限するコマンドのリストからコマンドを削除できます。

`security dynamic-authorization rule delete`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-rule-delete.html["ONTAPコマンド リファレンス
"^]をご覧ください。

手順

1. コマンドを削除します。括弧内の値<>を環境に合わせて更新します。 `-vserver`パラメータを使用しない場合、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. 変更後の制限コマンド リストを確認します。

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

動的許可グループの設定

デフォルトでは、動的認証は有効にするとすぐにすべてのユーザーとグループに適用されます。ただし、`security dynamic-authorization group create`コマンドを使用してグループを作成し、特定のユーザーにのみ動的認証を適用することもできます。

動的許可グループの追加

動的許可グループを追加できます。

`security dynamic-authorization group create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-group-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

手順

1. グループを作成します。括弧内の値<>を環境に合わせて更新してください。 `-vserver`パラメータを使用しない場合、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>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. 変更後の動的許可グループを確認します。

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

動的許可グループの削除

動的許可グループを削除できます。

`security dynamic-authorization group delete`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-group-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

手順

1. グループを削除します。括弧内の値<>を環境に合わせて更新してください。 `-vserver`パラメータを使用しない場合、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>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. 変更後の動的許可グループを確認します。

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

動的許可の信頼スコア コンポーネントの構成

スコア重みの上限を設定することで、スコア基準の優先度を変更したり、リスク スコアから特定の基準を削除したりできます。

ベストプラクティスとして、デフォルトのスコア重み値は残しておき、必要に応じて調整だけ行うことが推奨されます。

`security dynamic-authorization trust-score-component modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-trust-score-component-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

以下に、変更可能なコンポーネントをデフォルトのスコア重みおよび重み（パーセント）とともに示します。

条件	コンポーネント名	デフォルトの未加工スコアの重み	デフォルトのパーセンテージの重み
デバイスの信頼度	`trusted-device`	20	50
ユーザのログイン認証履歴	`authentication-history`	20	50

手順

1. 信頼スコアの構成要素を変更します。括弧内の値<>を環境に合わせて更新してください。 `-vserver`パラメータを指定しない場合、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. 変更後の信頼スコア コンポーネント設定を確認します。

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

ユーザの信頼スコアのリセット

ユーザがシステム ポリシーによりアクセスを拒否されたものの、その身元を証明可能な場合、管理者はそのユーザの信頼スコアをリセットできます。

`security dynamic-authorization user-trust-score reset`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-user-trust-score-reset.html["ONTAPコマンド リファレンス"^]をご覧ください。

手順

1. コマンドを追加します。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、動的許可の信頼スコア コンポーネントの構成を参照してください。括弧<>内の値を環境に合わせて更新してください。`-vserver`パラメータを使用しない場合、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>
```

信頼スコアの閲覧

ユーザは、ログイン セッションにおける自分の信頼スコアを閲覧できます。

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
```

`security login whoami`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-whoami.html["ONTAPコマンド リファレンス"^]をご覧ください。

カスタム信頼スコア プロバイダの設定

すでに外部の信頼スコア プロバイダからスコア設定方法を受信している場合、動的許可設定にカスタム プロバイダを追加できます。

開始する前に

- カスタム信頼スコア プロバイダはJSON応答を返せなくてはなりません。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、配列要素ではなくスカラーである必要があります。
  - 信頼スコアを返すフィールドは、 `trust_score.value`などのネストされたフィールドにすることができます。
  - JSON応答に、信頼スコアの数値を返すフィールドが含まれている必要があります。ネイティブでこのフィールドが存在しない場合は、この値を返すラッパー スクリプトを作成できます。
- 提供する値は信頼スコアとリスク スコアのいずれかを指定できます。信頼スコアとリスク スコアの違いは、前者は信頼度が高いほどスコアが高くなるのに対し、後者はその反対であることです。たとえば、スコア範囲が0～100で信頼スコアが90の場合、スコアの信頼度が非常に高いとみなされ、通常は追加チャレンジなしで「許可」されます。反対に、スコア範囲が0～100でリスク スコアが90の場合、リスクが高いとみなされ、通常は追加チャレンジなしで「拒否」されます。
- カスタム信頼スコア プロバイダはONTAP REST API経由でアクセス可能である必要があります。
- カスタム信頼スコア プロバイダは、いずれかのサポート対象パラメータで設定可能である必要があります。サポート対象パラメーター一覧にない設定が必要なカスタム信頼スコア プロバイダは使用できません。

`security dynamic-authorization trust-score-component create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-trust-score-component-create.html["ONTAPコマンド リファレンス"^]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ーを追加します。括弧内の値<>を環境に合わせて更新してください。 `-vserver`パラメータを使用しない場合、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. 変更後の信頼スコア プロバイダ設定を確認します。

```
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

外部の信頼スコア プロバイダとの通信にタグを使用できます。こうすることで、機密情報を漏えいさせることなく、URLで信頼スコア プロバイダに情報を送信できます。

`security dynamic-authorization trust-score-component create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-trust-score-component-create.html["ONTAPコマンド リファレンス"^]を参照してください。

手順

1. トラスト スコア プロバイダ タグを有効にします。括弧内の値<>を環境に合わせて更新してください。`-vserver`パラメータを使用しない場合、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