WebAuthn MFAを使用した認証と許可

ONTAP 9

NetApp
December 20, 2024

目次

WebAuthn MFAを使用した認証と許可

WebAuthn多要素認証の概要

ONTAP 9 .16.1以降では、管理者がにログインするユーザに対してWebAuthn多要素認証（MFA）を有効にすることができます。これにより、2つ目の認証形式としてFIDO2キー（YubiKeyなど）を使用したSystem Managerログインが有効になります。デフォルトでは、新規および既存のONTAPユーザに対してWebAuthn MFAは無効になっています。

WebAuthn MFAは、最初の認証方式に次のタイプの認証を使用するユーザおよびグループでサポートされます。

- ユーザ：パスワード、ドメイン、またはnsswitch
- グループ:ドメインまたはnsswitch

ユーザの2つ目の認証方式としてWebAuthn MFAを有効にすると、System Managerにログインしたときにハードウェア認証サーバを登録するように求められます。登録後、秘密鍵はオーセンティケータに格納され、公開鍵はONTAPに格納されます。

ONTAPは、ユーザごとに1つのWebAuthnクレデンシャルをサポートします。ユーザがオーセンティケータを失い、オーセンティケータを交換する必要がある場合、ONTAP管理者はそのユーザのWebAuthnクレデンシャルを削除して、ユーザが次回のログイン時に新しいオーセンティケータを登録できるようにする必要があります。

> 2つ目の認証方式としてWebAuthn MFAを有効にしているユーザは"https://myontap.example.com"、IPアドレス（など"https://192.168.100.200"）ではなくFQDN（など）を使用してSystem Managerにアクセスする必要があります。WebAuthn MFAが有効なユーザの場合、IPアドレスを使用してSystem Managerにログインしようとすると拒否されます。

ONTAP System Managerのユーザまたはグループに対してWebAuthn MFAを有効にする

ONTAP管理者は、[WebAuthn MFA]オプションを有効にして新しいユーザまたはグループを追加するか、既存のユーザまたはグループに対してオプションを有効にすることで、System Managerのユーザまたはグループに対してWebAuthn MFAを有効にできます。

> ユーザまたはグループの2番目の認証方式としてWebAuthn MFAを有効にすると、System Managerに次回ログインしたときに、ユーザ（またはそのグループ内のすべてのユーザ）にハードウェアFIDO2デバイスの登録が求められます。この登録はユーザーのローカルオペレーティングシステムによって処理され、通常はセキュリティキーの挿入、パスキーの作成、セキュリティキーのタッチ（サポートされている場合）で構成されます。

新しいユーザまたはグループの作成時に**WebAuthn MFA**を有効にする

System ManagerまたはONTAP CLIを使用して、WebAuthn MFAを有効にして新しいユーザまたはグループを作成できます。

System Manager

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ユーザとロール]*の横にある矢印アイコンを選択します。
3. [Users]*で[Add]*を選択します。
4. ユーザまたはグループの名前を指定し、* Role *のドロップダウンメニューでロールを選択します。
5. ユーザまたはグループのログイン方法とパスワードを指定します。

   WebAuthn MFAは、ユーザに対しては「password」、「domain」、または「nsswitch」、グループに対しては「domain」または「nsswitch」のログイン方法をサポートしています。

6. [MFA for HTTP]列で、*[Enabled]*を選択します。
7. [保存（ Save ）] を選択します。

CLI

1. WebAuthn MFAを有効にして新しいユーザまたはグループを作成します。

   次の例では、2番目の認証方式として「publickey」を選択してWebAuthn MFAを有効にしています。

```
security login create -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

既存のユーザまたはグループに対して**WebAuthn MFA**を有効にする

既存のユーザまたはグループに対してWebAuthn MFAを有効にすることができます。

System Manager

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ユーザとロール]*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、編集するユーザまたはグループのオプションメニューを選択します。

   WebAuthn MFAは、ユーザに対しては「password」、「domain」、または「nsswitch」、グループに対しては「domain」または「nsswitch」のログイン方法をサポートしています。
4. そのユーザの* MFA for HTTP 列で Enabled *を選択します。
5. [保存（ Save ）] を選択します。

CLI

1. 既存のユーザまたはグループを変更して、そのユーザまたはグループに対してWebAuthn MFAを有効にします。

   次の例では、2番目の認証方式として「publickey」を選択してWebAuthn MFAを有効にしています。

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

詳細

これらの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。

- "security login create"
- "security login modify"

ONTAP System ManagerユーザのWebAuthn MFAを無効にする

ONTAP管理者は、System ManagerまたはONTAP CLIでユーザまたはグループを編集することで、ユーザまたはグループのWebAuthn MFAを無効にできます。

既存のユーザまたはグループに対して**WebAuthn MFA**を無効にする

既存のユーザまたはグループのWebAuthn MFAはいつでも無効にできます。

登録済みクレデンシャルを無効にしても、クレデンシャルは保持されます。今後クレデンシャルを再度有効にすると、同じクレデンシャルが使用されるため、ユーザがログイン時に再登録する必要はありません。

System Manager

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ユーザとロール]*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、編集するユーザまたはグループを選択します。
4. そのユーザの* MFA for HTTP 列で Disabled *を選択します。
5. [保存（ Save ）] を選択します。

CLI

1. 既存のユーザまたはグループを変更して、そのユーザまたはグループのWebAuthn MFAを無効にします。

   次の例では、2番目の認証方式として「none」を選択してWebAuthn MFAを無効にしています。

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method none \
                      -application http \
                      -role admin
```

詳細

この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。

- "security login modify"

ONTAP WebAuthn MFA設定の表示とクレデンシャルの管理

ONTAP管理者は、クラスタ全体のWebAuthn MFA設定を表示し、WebAuthn MFAのユーザおよびグループのクレデンシャルを管理できます。

WebAuthn MFAのクラスタ設定を表示します。

ONTAP CLIを使用して、WebAuthn MFAのクラスタ設定を表示できます。

手順

1. WebAuthn MFAのクラスタ設定を表示します。必要に応じて、引数を使用してStorage VMを指定できます `vserver`。

```
security webauthn show -vserver <storage_vm_name>
```

サポートされている公開鍵**WebAuthn MFA**アルゴリズムの表示

Storage VMまたはクラスタのWebAuthn MFAでサポートされている公開鍵アルゴリズムを表示できます。

手順

1. サポートされている公開鍵WebAuthn MFAアルゴリズムを列挙します。必要に応じて、引数を使用してStorage VMを指定できます `vserver`。

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

登録済み**WebAuthn MFA**クレデンシャルの表示

ONTAP管理者は、すべてのユーザの登録済みWebAuthnクレデンシャルを表示できます。この手順を使用する管理者以外のユーザは、自分の登録済みWebAuthnクレデンシャルのみを表示できます。

手順

1. 登録されたWebAuthn MFAクレデンシャルを表示します。

```
security webauthn credentials show
```

登録済み**WebAuthn MFA**クレデンシャルの削除

登録済みのWebAuthn MFAクレデンシャルを削除できます。これは、ユーザーのハードウェアキーが紛失したり、盗まれたり、使用されなくなったりした場合に便利です。ユーザーが元のハードウェアオーセンティケータを持っていて、新しいものに置き換えたい場合は、登録されたクレデンシャルを削除することもできます。クレデンシャルを削除すると、ユーザは交換用オーセンティケータを登録するように求められます。

ユーザの登録済みクレデンシャルを削除しても、そのユーザのWebAuthn MFAは無効になりません。ユーザがハードウェアオーセンティケータを紛失し、交換する前にログインする必要がある場合は、次の手順とユーザの手順を使用してクレデンシャルを削除する"WebAuthn MFAを無効にする"必要があります。

System Manager

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [ユーザとロール]*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、クレデンシャルを削除するユーザまたはグループのオプションメニューを選択します。
4. [HTTPクレデンシャルのMFAを削除する]*を選択します。
5. 「* 削除」を選択します。

CLI

1. 登録済みクレデンシャルを削除します。次の点に注意してください。
   - 必要に応じて、ユーザのStorage VMを指定できます。省略すると、クラスタレベルでクレデンシャルが削除されます。
   - 必要に応じて、クレデンシャルを削除するユーザのユーザ名を指定できます。省略すると、現在のユーザのクレデンシャルが削除されます。

```
security webauthn credentials delete -vserver <storage_vm_name>
-username <username>
```

詳細

これらの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。

- "security webauthn show"
- "サポートされるセキュリティwebauthn - algorithms show"
- "security webauthn credentials show"
- "セキュリティwebauthnクレデンシャルの削除"

著作権に関する情報

商標に関する情報