使用 **WebAuthn MFA** 進行驗證與授權

ONTAP 9

NetApp
January 17, 2025

目錄

使用 WebAuthn MFA 進行驗證與授權

WebAuthn 多因素驗證總覽

從 ONTAP 9 。 16.1 開始，系統管理員可以為登入系統管理員的使用者啟用 WebAuthn 多因素驗證（ MFA ）。這可讓系統管理員以 FIDO2 金鑰（例如 YibiKey ）作為第二種驗證形式登入。根據預設，新的和現有的 ONTAP 使用者會停用 WebAuthn MFA 。

第一種驗證方法使用下列驗證類型的使用者和群組可支援 WebAuthn MFA ：

- 使用者：密碼，網域或 nsswitch
- 群組：網域或 nsswitch

當您將 WebAuthn MFA 啟用為使用者的第二種驗證方法之後，系統會要求使用者在登入 System Manager 時登錄硬體驗證者。註冊後，私密金鑰會儲存在驗證者中，而公開金鑰則儲存在 ONTAP 中。

ONTAP 支援每位使用者一個 WebAuthn 認證。如果使用者遺失驗證者，需要更換驗證者，則 ONTAP 管理員需要刪除使用者的 WebAuthn 認證，以便使用者在下次登入時註冊新的驗證者。

啟用 WebAuthn MFA 做為第二種驗證方法的使用者"https://192.168.100.200"，必須使用 FQDN （例如"https://myontap.example.com"）而非 IP 位址（例如）來存取 System Manager 。對於啟用 WebAuthn MFA 的使用者，會拒絕使用 IP 位址登入 System Manager 的嘗試。

為 ONTAP 系統管理員使用者或群組啟用 WebAuthn MFA

身為 ONTAP 管理員，您可以新增已啟用 WebAuthn MFA 選項的新使用者或群組，或是啟用現有使用者或群組的選項，為系統管理員使用者或群組啟用 WebAuthn MFA 。

將 WebAuthn MFA 啟用為使用者或群組的第二種驗證方法之後，下次登入 System Manager 時，系統會要求使用者（或該群組中的所有使用者）登錄硬體 FIDO2 裝置。此登錄由使用者的本機作業系統處理，通常包括插入安全金鑰，建立金鑰，以及輕觸安全金鑰（如果支援）。

建立新使用者或群組時，請啟用 WebAuthn MFA

您可以使用系統管理員或 ONTAP CLI ，建立啟用 WebAuthn MFA 的新使用者或群組。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在 * 使用者 * 下選取 * 新增 * 。
4. 指定使用者或群組名稱，然後在 * 角色 * 的下拉式功能表中選取角色。
5. 指定使用者或群組的登入方法和密碼。

   WebAuthn MFA 支援使用者的「密碼」，「網域」或「 nsswitch 」登入方法，以及群組的「網域」或「 nsswitch 」登入方法。

6. 在 **MFA for HTTP** 欄中，選取 * Enabled* 。
7. 選擇*保存*。

CLI

1. 啟用 WebAuthn MFA ，建立新的使用者或群組。

   在下列範例中，選擇第二種驗證方法的「 publickey 」即可啟用 WebAuthn MFA ：

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

為現有的使用者或群組啟用 **WebAuthn MFA**

您可以為現有的使用者或群組啟用 WebAuthn MFA 。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在使用者和群組清單中，選取您要編輯之使用者或群組的選項功能表。

   WebAuthn MFA 支援使用者的「密碼」，「網域」或「 nsswitch 」登入方法，以及群組的「網域」或「 nsswitch 」登入方法。

4. 在該使用者的 * MFA for HTTP* 欄中，選取 * Enabled* 。
5. 選擇*保存*。

CLI

1. 修改現有的使用者或群組，為該使用者或群組啟用 WebAuthn MFA 。

   在下列範例中，選擇第二種驗證方法的「 publickey 」即可啟用 WebAuthn MFA ：

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

深入瞭解

請造訪 ONTAP 手冊頁面以取得下列命令：

- "建立安全登入"
- "修改安全登入"

停用 ONTAP System Manager 使用者的 WebAuthn MFA

身為 ONTAP 管理員，您可以使用系統管理員或 ONTAP CLI 編輯使用者或群組，為使用者或群組停用 WebAuthn MFA 。

停用現有使用者或群組的 WebAuthn MFA

您可以隨時停用現有使用者或群組的 WebAuthn MFA 。

如果停用已登錄的認證，則會保留認證。如果您在未來再次啟用認證，則會使用相同的認證，因此使用者在登入時不需要重新登錄。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在使用者和群組清單中，選取您要編輯的使用者或群組。
4. 在該使用者的 * MFA for HTTP* 欄中，選取 * 停用 * 。
5. 選擇*保存*。

CLI

1. 修改現有的使用者或群組，以停用該使用者或群組的 WebAuthn MFA 。

   在下列範例中，選擇「無」作為第二種驗證方法，即可停用 WebAuthn MFA 。

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

深入瞭解

請造訪 ONTAP 手冊頁面以取得此命令：

- "修改安全登入"

檢視 ONTAP WebAuthn MFA 設定並管理認證

身為 ONTAP 管理員，您可以檢視整個叢集的 WebAuthn MFA 設定，並管理 WebAuthn MFA 的使用者和群組認證。

檢視 WebAuthn MFA 的叢集設定

您可以使用 ONTAP CLI 檢視 WebAuthn MFA 的叢集設定。

步驟

1. 檢視 WebAuthn MFA 的叢集設定。您可以選擇使用下列引數指定儲存 VM `vserver` ：

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

檢視支援的公開金鑰 **WebAuthn MFA** 演算法

您可以檢視儲存 VM 或叢集所支援的 WebAuthn MFA 公開金鑰演算法。

步驟

1. 列出支援的公開金鑰 WebAuthn MFA 演算法。您可以選擇使用下列引數指定儲存 VM `vserver` ：

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

檢視已註冊的 **WebAuthn MFA** 認證

身為 ONTAP 管理員，您可以檢視所有使用者的註冊 WebAuthn 認證。使用此程序的非系統管理員使用者只能檢視自己已註冊的 WebAuthn 認證。

步驟

1. 檢視已註冊的 WebAuthn MFA 認證：

```
security webauthn credentials show
```

移除已註冊的 **WebAuthn MFA** 認證

您可以移除已註冊的 WebAuthn MFA 認證。當使用者的硬體金鑰遺失，遭竊或不再使用時，此功能非常實用。當使用者仍擁有原始硬體驗證者，但想要以新的驗證者來取代時，您也可以移除已登錄的認證。移除認證之後，系統會提示使用者註冊替換驗證者。

移除使用者的登錄認證並不會停用使用者的 WebAuthn MFA 。如果使用者遺失硬體驗證者，需要先登入再進行更換，您需要使用這些步驟移除認證，也需要針對使用者移除認證"停用 WebAuthn MFA"。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在使用者和群組清單中，針對您要移除其認證的使用者或群組，選取選項功能表。
4. 選取 * 移除 MFA 以取得 HTTP 認證 * 。
5. 選擇*移除*。

CLI

1. 刪除已註冊的認證。請注意下列事項：
   - 您可以選擇性地指定使用者的儲存 VM 。如果省略，則會在叢集層級移除認證。
   - 您可以選擇性地指定要刪除認證的使用者名稱。如果省略，則會移除目前使用者的認證。

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

深入瞭解

請造訪 ONTAP 手冊頁面以取得下列命令：

- "安全 webauthn 顯示"
- "顯示安全 webauthn 支援的演算法"
- "顯示安全 webauthn 認證"
- "安全 webauthn 認證刪除"