Authentification et autorisation à l'aide de WebAuthn MFA

ONTAP 9

NetApp
January 10, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/authentication-access-control/webauthn-mfa-overview.html on January 10, 2025. Always check docs.netapp.com for the latest.

Sommaire

Authentification et autorisation à l'aide de WebAuthn MFA

Présentation de l'authentification multifacteur WebAuthn

À partir de ONTAP 9.16.1, les administrateurs peuvent activer l'authentification multifacteur (MFA) WebAuthn pour les utilisateurs qui se connectent au Gestionnaire système. Cela permet de se connecter à System Manager en utilisant une clé FIDO2 (telle qu'une YubiKey) comme deuxième forme d'authentification. Par défaut, WebAuthn MFA est désactivé pour les utilisateurs ONTAP nouveaux et existants.

WebAuthn MFA est pris en charge pour les utilisateurs et les groupes qui utilisent les types d'authentification suivants pour la première méthode d'authentification :

- Utilisateurs : mot de passe, domaine ou nsswitch
- Groupes : domaine ou nsswitch

Après avoir activé WebAuthn MFA comme deuxième méthode d'authentification pour un utilisateur, l'utilisateur est invité à enregistrer un authentificateur matériel lors de sa connexion à System Manager. Après l'enregistrement, la clé privée est stockée dans l'authentificateur et la clé publique est stockée dans ONTAP.

ONTAP prend en charge une autorisation WebAuthn par utilisateur. Si un utilisateur perd un authentificateur et doit le remplacer, l'administrateur ONTAP doit supprimer les informations d'identification WebAuthn pour que l'utilisateur puisse enregistrer un nouvel authentificateur lors de la prochaine connexion.

> Les utilisateurs pour lesquels WebAuthn MFA "https://192.168.100.200"est activé comme deuxième méthode d’authentification doivent utiliser le FQDN (par exemple, "https://myontap.example.com") au lieu de l’adresse IP (par exemple,) pour accéder à System Manager. Pour les utilisateurs avec WebAuthn MFA activé, les tentatives de connexion à System Manager à l’aide de l’adresse IP sont rejetées.

Activez WebAuthn MFA pour les utilisateurs ou les groupes ONTAP System Manager

En tant qu'administrateur ONTAP, vous pouvez activer l'authentification WebAuthn MFA pour un utilisateur ou un groupe du Gestionnaire système en ajoutant un nouvel utilisateur ou un nouveau groupe avec l'option WebAuthn MFA activée ou en activant l'option pour un utilisateur ou un groupe existant.

> Après avoir activé WebAuthn MFA comme deuxième méthode d'authentification pour un utilisateur ou un groupe, l'utilisateur (ou tous les utilisateurs de ce groupe) sera invité à enregistrer un périphérique FIDO2 matériel lors de la prochaine connexion à System Manager. Cet enregistrement est géré par le système d'exploitation local de l'utilisateur et consiste généralement à insérer la clé de sécurité, à créer une clé d'authentification et à appuyer sur la clé de sécurité (si elle est prise en charge).

Activez WebAuthn MFA lors de la création d'un nouvel utilisateur ou d'un nouveau groupe

Vous pouvez créer un nouvel utilisateur ou un nouveau groupe avec l'authentification WebAuthn MFA activée via System Manager ou l'interface de ligne de commande ONTAP.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez l'icône en forme de flèche en regard de **utilisateurs et rôles**.
3. Sélectionnez **Ajouter** sous **utilisateurs**.
4. Spécifiez un nom d'utilisateur ou de groupe et sélectionnez un rôle dans le menu déroulant pour **role**.
5. Spécifiez une méthode de connexion et un mot de passe pour l'utilisateur ou le groupe.

   WebAuthn MFA prend en charge les méthodes de connexion « password », « domain » ou « nsswitch » pour les utilisateurs, et « domain » ou « nsswitch » pour les groupes.
6. Dans la colonne **MFA pour HTTP**, sélectionnez **Enabled**.
7. Sélectionnez **Enregistrer**.

CLI

1. Créez un nouvel utilisateur ou un nouveau groupe avec WebAuthn MFA activé.

   Dans l'exemple suivant, WebAuthn MFA est activé en choisissant "publickey" pour la deuxième méthode d'authentification :

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

Activez WebAuthn MFA pour un utilisateur ou un groupe existant

Vous pouvez activer WebAuthn MFA pour un utilisateur ou un groupe existant.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez l'icône en forme de flèche en regard de **utilisateurs et rôles**.
3. Dans la liste des utilisateurs et des groupes, sélectionnez le menu d'options de l'utilisateur ou du groupe que vous souhaitez modifier.

   WebAuthn MFA prend en charge les méthodes de connexion « password », « domain » ou « nsswitch » pour les utilisateurs, et « domain » ou « nsswitch » pour les groupes.
4. Dans la colonne **MFA pour HTTP** de cet utilisateur, sélectionnez **activé**.
5. Sélectionnez **Enregistrer**.

CLI

1. Modifiez un utilisateur ou un groupe existant pour activer WebAuthn MFA pour cet utilisateur ou ce groupe.

   Dans l'exemple suivant, WebAuthn MFA est activé en choisissant "publickey" pour la deuxième méthode d'authentification :

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

En savoir plus >>

Consultez les pages de manuel ONTAP pour obtenir les commandes suivantes :

- "création d'une connexion de sécurité"
- "modification de la connexion de sécurité"

Désactivez WebAuthn MFA pour les utilisateurs du Gestionnaire système ONTAP

En tant qu'administrateur ONTAP, vous pouvez désactiver l'authentification WebAuthn MFA pour un utilisateur ou un groupe en modifiant l'utilisateur ou le groupe à l'aide de System Manager ou de l'interface de ligne de commande ONTAP.

Désactivez WebAuthn MFA pour un utilisateur ou un groupe existant

Vous pouvez désactiver WebAuthn MFA à tout moment pour un utilisateur ou un groupe existant.

Si vous désactivez les informations d'identification enregistrées, les informations d'identification sont conservées. Si vous activez à nouveau les informations d'identification à l'avenir, les mêmes informations d'identification sont utilisées, de sorte que l'utilisateur n'a pas besoin de s'enregistrer à nouveau lors de la connexion.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez l'icône en forme de flèche en regard de **utilisateurs et rôles**.
3. Dans la liste des utilisateurs et des groupes, sélectionnez l'utilisateur ou le groupe à modifier.
4. Dans la colonne **MFA pour HTTP** de cet utilisateur, sélectionnez **Désactivé**.
5. Sélectionnez **Enregistrer**.

CLI

1. Modifiez un utilisateur ou un groupe existant pour désactiver WebAuthn MFA pour cet utilisateur ou ce groupe.

   Dans l'exemple suivant, WebAuthn MFA est désactivé en choisissant « aucun » pour la deuxième méthode d'authentification.

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

En savoir plus >>

Consultez les pages de manuel ONTAP pour obtenir cette commande :

- "modification de la connexion de sécurité"

Afficher les paramètres ONTAP WebAuthn MFA et gérer les informations d'identification

En tant qu'administrateur ONTAP, vous pouvez afficher les paramètres de l'authentification WebAuthn MFA à l'échelle du cluster et gérer les informations d'identification d'utilisateur et de groupe pour l'authentification WebAuthn MFA.

Afficher les paramètres de cluster pour WebAuthn MFA

Vous pouvez afficher les paramètres de cluster pour WebAuthn MFA via l'interface de ligne de commande ONTAP.

Étapes

1. Afficher les paramètres de cluster pour WebAuthn MFA Vous pouvez éventuellement spécifier une VM de stockage à l'aide de l' `vserver`argument suivant :

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

Afficher les algorithmes de clé publique WebAuthn MFA pris en charge

Vous pouvez afficher les algorithmes de clé publique pris en charge pour WebAuthn MFA pour une VM de stockage ou un cluster.

Étapes

1. Répertorie les algorithmes de clé publique WebAuthn MFA pris en charge. Vous pouvez éventuellement spécifier une VM de stockage à l'aide de l' `vserver`argument suivant :

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

Afficher les informations d'identification WebAuthn MFA enregistrées

En tant qu'administrateur ONTAP, vous pouvez afficher les informations d'identification WebAuthn enregistrées pour tous les utilisateurs. Les utilisateurs non administrateurs qui utilisent cette procédure peuvent uniquement afficher leurs propres informations d'identification WebAuthn enregistrées.

Étapes

1. Afficher les informations d'identification WebAuthn MFA enregistrées :

```
security webauthn credentials show
```

Supprimez les informations d'identification WebAuthn MFA enregistrées

Vous pouvez supprimer une information d'identification WebAuthn MFA enregistrée. Ceci est utile lorsqu'une clé matérielle d'un utilisateur a été perdue, volée ou n'est plus utilisée. Vous pouvez également supprimer une information d'identification enregistrée lorsque l'utilisateur dispose toujours de l'authentificateur matériel d'origine, mais souhaite la remplacer par une nouvelle. Une fois les informations d'identification retirées, l'utilisateur est invité à enregistrer l'authentificateur de remplacement.

> La suppression d'une information d'identification enregistrée pour un utilisateur ne désactive pas WebAuthn MFA pour l'utilisateur. Si un utilisateur perd un authentificateur matériel et doit se connecter avant de le remplacer, vous devez supprimer les informations d'identification en suivant ces étapes et également "Désactivez WebAuthn MFA" pour l'utilisateur.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez l'icône en forme de flèche en regard de **utilisateurs et rôles**.
3. Dans la liste des utilisateurs et des groupes, sélectionnez le menu d'options de l'utilisateur ou du groupe dont vous souhaitez supprimer les informations d'identification.
4. Sélectionnez **Supprimer MFA pour les informations d'identification HTTP**.
5. Sélectionnez **Supprimer**.

CLI

1. Supprimez les informations d'identification enregistrées. Notez ce qui suit :
   - Vous pouvez éventuellement spécifier une VM de stockage de l'utilisateur. Si vous omettez le paramètre, les informations d'identification sont supprimées au niveau du cluster.
   - Vous pouvez éventuellement spécifier un nom d'utilisateur de l'utilisateur pour lequel vous supprimez les informations d'identification. Si omis, les informations d'identification sont supprimées pour l'utilisateur actuel.

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

En savoir plus >>

Consultez les pages de manuel ONTAP pour obtenir les commandes suivantes :

- "sécurité webauthn show"
- "les algorithmes pris en charge par le webauthn de sécurité s'affichent"
- "les informations d'identification de sécurité webauthn s'affichent"
- "suppression des informations d'identification de sécurité webauthn"

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.