Autenticação e autorização usando WebAuthn MFA

ONTAP 9

NetApp
January 17, 2025

Índice

Autenticação e autorização usando WebAuthn MFA 1
Visão geral da autenticação multifator WebAuthn 1
Habilite o MFA WebAuthn para usuários ou grupos do Gerenciador de sistema do ONTAP 1
Desative o WebAuthn MFA para usuários do Gerenciador de sistema do ONTAP 3
Veja as configurações de MFA do ONTAP WebAuthn e gerencie credenciais 4

Autenticação e autorização usando WebAuthn MFA

Visão geral da autenticação multifator WebAuthn

A partir do ONTAP 9.16,1, os administradores podem ativar a autenticação multifator WebAuthn (MFA) para usuários que fazem login no Gerenciador de sistema. Isso permite logins do System Manager usando uma chave FIDO2 (como uma YubiKey) como uma segunda forma de autenticação. Por padrão, o WebAuthn MFA está desativado para usuários novos e existentes do ONTAP.

O WebAuthn MFA é compatível com usuários e grupos que usam os seguintes tipos de autenticação para o primeiro método de autenticação:

- Usuários: Senha, domínio ou nsswitch
- Grupos: Domínio ou nsswitch

Depois de ativar o WebAuthn MFA como o segundo método de autenticação para um usuário, o usuário é solicitado a Registrar um autenticador de hardware ao fazer login no System Manager. Após o Registro, a chave privada é armazenada no autenticador e a chave pública é armazenada no ONTAP.

O ONTAP suporta uma credencial WebAuthn por usuário. Se um usuário perder um autenticador e precisar substituí-lo, o administrador do ONTAP precisará excluir a credencial WebAuthn do usuário para que o usuário possa Registrar um novo autenticador no próximo login.

> Os usuários que têm o WebAuthn MFA habilitado como um segundo método de autenticação precisam usar o FQDN (por exemplo, "https://myontap.example.com") em vez do endereço IP (por exemplo, "https://192.168.100.200") para acessar o System Manager. Para usuários com WebAuthn MFA habilitado, as tentativas de fazer login no System Manager usando o endereço IP são rejeitadas.

Habilite o MFA WebAuthn para usuários ou grupos do Gerenciador de sistema do ONTAP

Como administrador do ONTAP, você pode ativar o WebAuthn MFA para um usuário ou grupo do Gerenciador de sistema adicionando um novo usuário ou grupo com a opção de WebAuthn MFA ativada ou habilitando a opção para um usuário ou grupo existente.

> Depois de ativar o WebAuthn MFA como o segundo método de autenticação para um usuário ou grupo, o usuário (ou todos os usuários desse grupo) será solicitado a Registrar um dispositivo FIDO2 de hardware no próximo login no System Manager. Esse Registro é gerenciado pelo sistema operacional local do usuário e geralmente consiste em inserir a chave de segurança, criar uma chave de acesso e tocar na chave de segurança (se suportada).

Ative o WebAuthn MFA ao criar um novo usuário ou grupo

Você pode criar um novo usuário ou grupo com o WebAuthn MFA habilitado usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Selecione **Adicionar** em **usuários**.
4. Especifique um nome de usuário ou grupo e selecione uma função no menu suspenso para **função**.
5. Especifique um método de login e uma senha para o usuário ou grupo.

   WebAuthn MFA suporta métodos de login de "senha", "domínio" ou "nsswitch" para usuários e "domínio" ou "nsswitch" para grupos.

6. Na coluna **MFA para HTTP**, selecione **Enabled**.
7. Selecione **Guardar**.

CLI

1. Crie um novo usuário ou grupo com o WebAuthn MFA habilitado.

   No exemplo a seguir, o WebAuthn MFA é habilitado escolhendo "publikey" para o segundo método de autenticação:

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

Ative o WebAuthn MFA para um usuário ou grupo existente

Você pode ativar o WebAuthn MFA para um usuário ou grupo existente.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Na lista de utilizadores e grupos, selecione o menu de opções para o utilizador ou grupo que pretende editar.

   WebAuthn MFA suporta métodos de login de "senha", "domínio" ou "nsswitch" para usuários e "domínio" ou "nsswitch" para grupos.

4. Na coluna **MFA para HTTP** para esse usuário, selecione **Enabled**.
5. Selecione **Guardar**.

CLI

1. Modifique um usuário ou grupo existente para ativar o WebAuthn MFA para esse usuário ou grupo.

   No exemplo a seguir, o WebAuthn MFA é habilitado escolhendo "publikey" para o segundo método de autenticação:

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

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "login de segurança criar"
- "modificação de início de sessão de segurança"

Desative o WebAuthn MFA para usuários do Gerenciador de sistema do ONTAP

Como administrador do ONTAP, você pode desativar o WebAuthn MFA para um usuário ou grupo editando o usuário ou grupo com o Gerenciador do sistema ou a CLI do ONTAP.

Desative o WebAuthn MFA para um usuário ou grupo existente

Você pode desativar o WebAuthn MFA para um usuário ou grupo existente a qualquer momento.

Se desativar as credenciais registadas, as credenciais são retidas. Se você ativar as credenciais novamente no futuro, as mesmas credenciais serão usadas, para que o usuário não precise se Registrar novamente ao fazer login.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Na lista de utilizadores e grupos, selecione o utilizador ou grupo que pretende editar.
4. Na coluna **MFA para HTTP** para esse usuário, selecione **Disabled**.
5. Selecione **Guardar**.

CLI

1. Modifique um usuário ou grupo existente para desativar o WebAuthn MFA para esse usuário ou grupo.

   No exemplo a seguir, o WebAuthn MFA é desativado escolhendo "nenhum" para o segundo método de autenticação.

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

Saiba mais

Visite as páginas do manual do ONTAP para este comando:

- "modificação de início de sessão de segurança"

Veja as configurações de MFA do ONTAP WebAuthn e gerencie credenciais

Como administrador do ONTAP, você pode exibir configurações de MFA WebAuthn em todo o cluster e gerenciar credenciais de usuário e grupo para o MFA WebAuthn.

Exibir configurações de cluster para WebAuthn MFA

Você pode exibir as configurações de cluster para WebAuthn MFA usando a CLI do ONTAP.

Passos

1. Veja as configurações do cluster para WebAuthn MFA. Opcionalmente, você pode especificar uma VM de armazenamento usando o `vserver` argumento:

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

Veja algoritmos de chave pública suportados do WebAuthn MFA

Você pode exibir os algoritmos de chave pública compatíveis para WebAuthn MFA para uma VM de armazenamento ou para um cluster.

Passos

1. Liste os algoritmos de chave pública suportados do WebAuthn MFA. Opcionalmente, você pode especificar uma VM de armazenamento usando o `vserver` argumento:

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

Veja as credenciais do WebAuthn MFA registradas

Como administrador do ONTAP, você pode exibir as credenciais de WebAuthn registradas para todos os usuários. Os utilizadores não administradores que utilizam este procedimento só podem ver as suas próprias credenciais WebAuthn registadas.

Passos

1. Veja as credenciais do WebAuthn MFA registradas:

```
security webauthn credentials show
```

Remova uma credencial WebAuthn MFA registrada

Você pode remover uma credencial WebAuthn MFA registrada. Isso é útil quando a chave de hardware de um usuário foi perdida, roubada ou não está mais em uso. Você também pode remover uma credencial registrada quando o usuário ainda tem o autenticador de hardware original, mas deseja substituí-la por uma nova. Depois de remover a credencial, o usuário será solicitado a Registrar o autenticador de substituição.

> ⓘ A remoção de uma credencial registrada para um usuário não desativa o WebAuthn MFA para o usuário. Se um usuário perder um autenticador de hardware e precisar fazer login antes de substituí-lo, você precisará remover a credencial usando estas etapas e também "Desative o WebAuthn MFA" para o usuário.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Na lista de usuários e grupos, selecione o menu de opções para o usuário ou grupo cujas credenciais deseja remover.
4. Selecione **Remover MFA para credenciais HTTP**.
5. Selecione **Remover**.

CLI

1. Elimine as credenciais registadas. Observe o seguinte:
   - Opcionalmente, você pode especificar uma VM de storage do usuário. Se omitida, a credencial é removida no nível do cluster.
   - Opcionalmente, você pode especificar um nome de usuário do usuário para o qual você está excluindo a credencial. Se omitida, a credencial é removida para o usuário atual.

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

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "segurança webauthn show"
- "os algoritmos suportados por webauthn de segurança são mostrados"
- "credenciais webauthn de segurança são exibidas"
- "credenciais de segurança webauthn excluídas"

Informações sobre direitos autorais

Informações sobre marcas comerciais