Autorização do cliente

ONTAP 9

NetApp
February 12, 2026

Índice

Autorização do cliente

Visão geral e opções para autorização de cliente ONTAP

A implementação do ONTAP OAuth 2,0 foi projetada para ser flexível e robusta, fornecendo os recursos necessários para proteger seu ambiente ONTAP. Existem várias opções de configuração mutuamente exclusivas disponíveis. As decisões de autorização são, em última análise, baseadas nas funções REST do ONTAP contidas ou derivadas dos tokens de acesso OAuth 2,0.

Você só pode usar "Funções REST do ONTAP" ao configurar a autorização para o OAuth 2,0. As funções tradicionais anteriores do ONTAP não são suportadas.

O ONTAP aplica a única opção de autorização mais adequada com base na sua configuração. "Como o ONTAP determina o acesso"Consulte para obter mais informações sobre como o ONTAP toma decisões de acesso ao cliente.

Escopos auto-contidos OAuth 2,0

Esses escopos contêm uma ou mais funções REST personalizadas, cada uma encapsulada em uma única cadeia no token de acesso. Eles são independentes das definições de função do ONTAP. Você precisa configurar as strings de escopo em seu servidor de autorização. Consulte "Escopos OAuth 2,0 independentes" para obter mais informações.

Funções REST do ONTAP local

Uma única função REST nomeada, seja builtin ou personalizado, pode ser usada. A sintaxe do escopo para uma função nomeada é **ONTAP-role-** com codificação URL-ONTAP-role-name>. Por exemplo, se a função ONTAP for `admin` a string Escopo será `ontap-role-admin`.

Usuários

O nome de usuário no token de acesso definido com acesso ao aplicativo "http" pode ser usado. Um usuário é testado na seguinte ordem com base no método de autenticação definido: Senha, domínio (ative Directory), nsswitch (LDAP).

Grupos

Os servidores de autorização podem ser configurados para usar grupos ONTAP para autorização. Se as definições locais do ONTAP forem examinadas, mas não for possível tomar nenhuma decisão de acesso, os grupos do ative Directory ("domínio") ou LDAP ("nsswitch") serão usados. As informações do grupo podem ser especificadas de duas maneiras:

- OAuth 2,0 string de escopo

  Suporta aplicativos confidenciais usando o fluxo de credenciais de cliente onde não há usuário com uma associação de grupo. O escopo deve ser nomeado **ONTAP-group-** com codificação URL-ONTAP-group-name>. Por exemplo, se o grupo for "desenvolvimento", a string de escopo será "ONTAP-group-development".

- Na reclamação "Group" (grupo)

  Isso é destinado a tokens de acesso emitidos pelo ADFS usando o fluxo proprietário do recurso (concessão de senha).

Ver "Trabalhando com grupos OAuth 2.0 ou SAML IdP no ONTAP" para maiores informações.

Escopos OAuth 2.0 autocontidos no ONTAP

Escopos auto-contidos são strings transportadas no token de acesso. Cada uma é uma definição completa de função personalizada e inclui tudo o que a ONTAP precisa para tomar uma decisão de acesso. O escopo é separado e distinto de qualquer uma das funções REST definidas no próprio ONTAP.

Formato da cadeia de escopo

Em um nível base, o escopo é representado como uma cadeia contígua e composto por seis valores separados por dois pontos. Os parâmetros usados na cadeia de escopo são descritos abaixo.

ONTAP literal

O escopo deve começar com o valor literal `ontap` em minúsculas. Isso identifica o escopo como específico do ONTAP.

Cluster

Isso define a que cluster ONTAP o escopo se aplica. Os valores podem incluir:

- UUID do cluster

  Identifica um único cluster.

- Asterisco (*)

  Indica que o escopo se aplica a todos os clusters.

Você pode usar o comando ONTAP CLI `cluster identity show` para exibir o UUID do cluster. Se não for especificado, o escopo se aplica a todos os clusters. Saiba mais sobre `cluster identity show` o "Referência do comando ONTAP"na .

Função

O nome do papel RESTANTE contido no escopo auto-contido. Esse valor não é examinado pelo ONTAP nem correspondido a nenhuma função REST existente definida como ONTAP. O nome é utilizado para registar.

Nível de acesso

Esse valor indica o nível de acesso aplicado ao aplicativo cliente ao usar o endpoint da API no escopo. Existem seis valores possíveis, conforme descrito na tabela abaixo.

Nível de acesso	Descrição
nenhum	Nega todo o acesso ao endpoint especificado.
readonly	Permite apenas acesso de leitura utilizando O GET.
read_create	Permite o acesso de leitura, bem como a criação de novas instâncias de recursos usando POST.

Nível de acesso	Descrição
read_modify	Permite acesso de leitura, bem como a capacidade de atualizar os recursos existentes USANDO PATCH.
read_create_modify	Permite todo o acesso, exceto apagar. As operações permitidas incluem GET (read), POST (Create) e PATCH (update).
tudo	Permite acesso total.

SVM

O nome da SVM no cluster ao qual o escopo se aplica. Use o valor * (asterisco) para indicar todos os SVMs.

> Esta funcionalidade não é totalmente suportada com o ONTAP 9.14,1. Você pode ignorar o parâmetro SVM e usar um asterisco como um marcador de posição. Revise o "Notas de versão do ONTAP" para verificar se há suporte futuro à SVM.

URI DA API REST

O caminho completo ou parcial para um recurso ou conjunto de recursos relacionados. A string deve começar com `/api`. Se você não especificar um valor, o escopo se aplica a todos os endpoints da API no cluster do ONTAP.

Exemplos de escopo

Alguns exemplos de escopos auto-contidos são apresentados abaixo.

ONTAP:*:joes-role:read_create_modify:*:/api/cluster

Fornece ao usuário atribuído essa função de leitura, criação e modificação do acesso ao `/cluster` endpoint.

Ferramenta administrativa CLI

Para tornar a administração dos escopos auto-contidos mais fácil e menos propensa a erros, o ONTAP fornece o comando CLI `security oauth2 scope` para gerar strings de escopo com base em seus parâmetros de entrada.

O comando `security oauth2 scope` tem dois casos de uso com base na sua entrada:

- Parâmetros CLI para string de escopo

  Você pode usar esta versão do comando para gerar uma string de escopo com base nos parâmetros de entrada.

- String de escopo para parâmetros CLI

  Você pode usar esta versão do comando para gerar os parâmetros do comando com base na cadeia de carateres de escopo de entrada.

Exemplo

O exemplo a seguir gera uma string de escopo com a saída incluída após o exemplo de comando abaixo. A definição se aplica a todos os clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Saiba mais sobre `security oauth2 scope` o "Referência do comando ONTAP"na .

Mapeamento de funções externas do OAuth 2.0 no ONTAP

Uma função externa é definida em um provedor de identificação configurado para uso pelo ONTAP. Você pode criar e administrar relacionamentos de mapeamento entre essas funções externas e as funções do ONTAP usando a CLI do ONTAP.

Você também pode configurar o recurso de mapeamento de função externa usando a API REST do ONTAP. Saiba mais no "Documentação de automação do ONTAP".

Funções externas em um token de acesso

Aqui está um fragmento de um token de acesso JSON contendo dois papéis externos.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configuração

Você pode usar a interface de linha de comando ONTAP para administrar o recurso de mapeamento de função externa.

Criar

Você pode definir uma configuração de mapeamento de função com o `security login external-role-mapping create` comando. Você precisa estar no nível de privilégio ONTAP **admin** para emitir este comando, bem como as opções relacionadas.

Parâmetros

Os parâmetros usados para criar um mapeamento de grupo são descritos abaixo.

Parâmetro	Descrição
`external-role`	O nome da função definida no provedor de identidade externo.
`provider`	O nome do provedor de identidade. Este deve ser o identificador do sistema.
`ontap-role`	Indica a função ONTAP existente para a qual a função externa está mapeada.

Exemplo

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Saiba mais sobre `security login external-role-mapping create` o "Referência do comando ONTAP"na .

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar
- Eliminar

Informações relacionadas

- "Referência do comando ONTAP"

Como o ONTAP determina o acesso do cliente

Para projetar e implementar adequadamente o OAuth 2,0, você precisa entender como sua configuração de autorização é usada pelo ONTAP para tomar decisões de acesso para os clientes. As principais etapas usadas para determinar o acesso são apresentadas abaixo com base na versão do ONTAP.

Não houve atualizações significativas do OAuth 2,0 com o ONTAP 9.15,1. Se estiver a utilizar a versão 9.15.1, consulte a descrição do ONTAP 9.14,1.

Informações relacionadas

- "Recursos do OAuth 2,0 suportados no ONTAP"

ONTAP 9.16,1

O ONTAP 9.16,1 expande o suporte padrão do OAuth 2,0 para incluir extensões específicas do Microsoft Entra ID para grupos nativos de ID do Entra, bem como mapeamento de funções externas.

Determine o acesso do cliente para o ONTAP 9.16,1

Passo 1: Escopos auto-contidos

Se o token de acesso contiver quaisquer escopos auto-contidos, o ONTAP examina esses escopos primeiro. Se não existirem escopos auto-suficientes, avance para o passo 2.

Com um ou mais escopos independentes presentes, o ONTAP aplica cada escopo até que uma decisão explícita de **PERMITIR** ou **NEGAR** possa ser tomada. Se uma decisão explícita for tomada, o processamento termina.

Se o ONTAP não conseguir tomar uma decisão de acesso explícito, avance para o passo 2.

Passo 2: Verifique o sinalizador de funções locais

ONTAP examina o parâmetro booleano `use-local-roles-if-present` . O valor deste sinalizador é definido separadamente para cada servidor de autorização definido como ONTAP.

- Se o valor for `true`, avance para o passo 3.
- Se o valor estiver `false` a processar termina e o acesso for negado.

Passo 3: Nomeado ONTAP REST role

Se o token de acesso contiver uma FUNÇÃO REST nomeada `scope` no campo ou `scp`, ou como uma reivindicação, o ONTAP usará a função para tomar a decisão de acesso. Isso sempre resulta em uma decisão **ALLOW** ou **DENY** e o processamento termina.

Se não houver nenhuma função REST nomeada ou a função não for encontrada, continue para a etapa 4.

Passo 4: Usuários

Extraia o nome de usuário do token de acesso e tente combiná-lo com os usuários que têm acesso ao aplicativo "http". Os usuários são examinados com base no método de autenticação na seguinte ordem:

- palavra-passe
- Domínio (ative Directory)
- Nsswitch (LDAP)

Se um usuário correspondente for encontrado, o ONTAP usará a função definida para que o usuário tome uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se um usuário não for correspondido ou se não houver nome de usuário no token de acesso, continue para a etapa 5.

Passo 5: Grupos

Se um ou mais grupos forem incluídos, o formato será examinado. Se os grupos forem representados como UUIDs, uma tabela interna de mapeamento de grupos será pesquisada. Se houver uma correspondência de grupo e uma função associada, o ONTAP usará a função definida para o grupo para tomar uma decisão de acesso. Isso sempre resulta em uma decisão **ALLOW** ou **DENY** e o processamento será encerrado. Para mais informações, consulte "Trabalhando com grupos OAuth 2.0 ou SAML IdP no ONTAP" .

Se os grupos forem representados como nomes e configurados com autorização de domínio ou nsswitch, o ONTAP tentará combiná-los com um grupo do ative Directory ou LDAP, respetivamente. Se

houver uma correspondência de grupo, o ONTAP usará a função definida para o grupo tomar uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se não houver correspondência de grupo ou se não houver nenhum grupo no token de acesso, o acesso será negado e o processamento será concluído.

ONTAP 9.14,1

O OAuth 2,0 inicial suportado é introduzido com o ONTAP 9.14,1 com base nos recursos padrão do OAuth 2,0.

Determine o acesso do cliente para o ONTAP 9.14,1

Passo 1: Escopos auto-contidos

Se o token de acesso contiver quaisquer escopos auto-contidos, o ONTAP examina esses escopos primeiro. Se não existirem escopos auto-suficientes, avance para o passo 2.

Com um ou mais escopos independentes presentes, o ONTAP aplica cada escopo até que uma decisão explícita de **PERMITIR** ou **NEGAR** possa ser tomada. Se uma decisão explícita for tomada, o processamento termina.

Se o ONTAP não conseguir tomar uma decisão de acesso explícito, avance para o passo 2.

Passo 2: Verifique o sinalizador de funções locais

ONTAP examina o parâmetro booleano `use-local-roles-if-present` . O valor deste sinalizador é definido separadamente para cada servidor de autorização definido como ONTAP.

- Se o valor for `true`, avance para o passo 3.
- Se o valor estiver `false` a processar termina e o acesso for negado.

Passo 3: Nomeado ONTAP REST role

Se o token de acesso contiver uma FUNÇÃO REST nomeada `scope` no campo ou `scp`, o ONTAP usará a função para tomar a decisão de acesso. Isso sempre resulta em uma decisão **ALLOW** ou **DENY** e o processamento termina.

Se não houver nenhuma função REST nomeada ou a função não for encontrada, continue para a etapa 4.

Passo 4: Usuários

Extraia o nome de usuário do token de acesso e tente combiná-lo com os usuários que têm acesso ao aplicativo "http". Os usuários são examinados com base no método de autenticação na seguinte ordem:

- palavra-passe
- Domínio (ative Directory)
- Nsswitch (LDAP)

Se um usuário correspondente for encontrado, o ONTAP usará a função definida para que o usuário tome uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se um usuário não for correspondido ou se não houver nome de usuário no token de acesso, continue para a etapa 5.

Passo 5: Grupos

Se um ou mais grupos forem incluídos e configurados com autorização de domínio ou nsswitch, o ONTAP tentará combiná-los com um grupo do ative Directory ou LDAP, respetivamente.

Se houver uma correspondência de grupo, o ONTAP usará a função definida para o grupo tomar uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se não houver correspondência de grupo ou se não houver nenhum grupo no token de acesso, o acesso será negado e o processamento será concluído.

Informações sobre direitos autorais

Informações sobre marcas comerciais