Conceitos

ONTAP 9

NetApp
January 17, 2025

Índice

Conceitos

Servidores de autorização e tokens de acesso

Os servidores de autorização executam várias funções importantes como um componente central dentro da estrutura de autorização do OAuth 2,0.

Servidores de autorização OAuth 2,0

Os servidores de autorização são os principais responsáveis pela criação e assinatura de tokens de acesso. Esses tokens contêm informações de identidade e autorização, permitindo que um aplicativo cliente acesse seletivamente recursos protegidos. Os servidores geralmente são isolados uns dos outros e podem ser implementados de várias maneiras diferentes, incluindo como um servidor dedicado autônomo ou como parte de um produto maior de gerenciamento de identidade e acesso.

> Terminologia diferente às vezes pode ser usada para um servidor de autorização, especialmente quando a funcionalidade OAuth 2,0 é empacotada dentro de um produto ou solução de gerenciamento de identidade e acesso maior. Por exemplo, o termo **provedor de identidade (IDP)** é frequentemente usado de forma intercambiável com **servidor de autorização**.

Administração

Além de emitir tokens de acesso, os servidores de autorização também fornecem serviços administrativos relacionados, normalmente através de uma interface de usuário da Web. Por exemplo, você pode definir e administrar:

- Autenticação de usuários e usuários
- Escopos
- Segregação administrativa através de inquilinos e reinos
- Aplicação da política
- Conexão com vários serviços externos
- Suporte para outros protocolos de identidade (como SAML)

O ONTAP é compatível com servidores de autorização compatíveis com o padrão OAuth 2,0.

Definindo para ONTAP

Você precisa definir um ou mais servidores de autorização para o ONTAP. O ONTAP se comunica com segurança com cada servidor para verificar tokens e executar outras tarefas relacionadas no suporte aos aplicativos cliente.

Os principais aspetos da configuração do ONTAP são apresentados abaixo. Consulte também "Cenários de implantação do OAuth 2,0"para obter mais informações.

Como e onde os tokens de acesso são validados

Existem duas opções para validar tokens de acesso.

- Validação local

O ONTAP pode validar tokens de acesso localmente com base nas informações fornecidas pelo servidor de autorização que emitiu o token. As informações recuperadas do servidor de autorização são armazenadas em cache pelo ONTAP e atualizadas em intervalos regulares.

- Introspeção remota

  Você também pode usar introspeção remota para validar tokens no servidor de autorização. Introspeção é um protocolo que permite que partes autorizadas consultem um servidor de autorização sobre um token de acesso. Ele fornece ao ONTAP uma maneira de extrair determinados metadados de um token de acesso e validar o token. O ONTAP armazena em cache alguns dos dados por motivos de desempenho.

Localização da rede

O ONTAP pode estar atrás de um firewall. Nesse caso, você precisa identificar um proxy como parte da configuração.

Como os servidores de autorização são definidos

Você pode definir um servidor de autorização para o ONTAP usando qualquer uma das interfaces administrativas, incluindo a CLI, o Gerenciador de sistema ou a API REST. Por exemplo, com a CLI você usa o comando `security oauth2 client create`.

Número de servidores de autorização

Você pode definir até oito servidores de autorização para um único cluster ONTAP. O mesmo servidor de autorização pode ser definido mais de uma vez para o mesmo cluster do ONTAP desde que as reivindicações do emissor ou do emissor/público sejam únicas. Por exemplo, com KeyCloak, esse será sempre o caso ao usar reinos diferentes.

Recursos do OAuth 2,0 suportados no ONTAP

O suporte para OAuth 2,0 estava inicialmente disponível com o ONTAP 9.14,1 e continua sendo aprimorado com versões subsequentes. Os recursos do OAuth 2,0 suportados pelo ONTAP são descritos abaixo.

Os recursos introduzidos com uma versão específica do ONTAP são levados para versões futuras.

ONTAP 9.16,1

O ONTAP 9.16,1 expande os recursos padrão do OAuth 2,0 para incluir extensões específicas do Entra ID para grupos nativos de ID do Entra. Isso envolve o uso de GUIDs no token de acesso em vez de nomes. Além disso, a versão adiciona suporte para mapeamento de funções externas para mapear as funções nativas do provedor de identidade para as funções do ONTAP usando o campo "funções" no token de acesso.

ONTAP 9.14,1

A partir do ONTAP 9.14,1, os servidores de autorização são suportados através dos seguintes recursos padrão do OAuth 2,0 para aplicativos que usam:

- OAuth 2,0 com os campos padrão, incluindo "iss", "AUD" e "exp", conforme descrito em "RFC6749: O Quadro de autorização OAuth 2,0" e "RFC 7519: JSON Web Token (JWT)". Isso também inclui suporte para identificar exclusivamente usuários através de campos no token de acesso, como "upn", "appid", "sub", "username" ou "Preferred_username".
- Extensões específicas do fornecedor ADFS para nomes de grupos com o campo "grupo".

- Extensões específicas do fornecedor do Azure para UUIDs de grupo com o campo "grupo".
- Extensões ONTAP para suporte de autorização usando funções independentes e nomeadas dentro do escopo do token de acesso OAuth 2,0. Isso inclui os campos "Escopo" e "scp", bem como os nomes de grupos dentro do escopo.

Usando tokens de acesso OAuth 2,0

Os tokens de acesso OAuth 2,0 emitidos pelos servidores de autorização são verificados pelo ONTAP e usados para tomar decisões de acesso baseadas em função para as solicitações de cliente de API REST.

Adquirir um token de acesso

Você precisa adquirir um token de acesso a partir de um servidor de autorização definido para o cluster ONTAP onde você usa a API REST. Para adquirir um token, você deve entrar em Contato diretamente com o servidor de autorização.

O ONTAP não emite tokens de acesso nem redireciona solicitações de clientes para os servidores de autorização.

A forma como você solicita um token depende de vários fatores, incluindo:

- Servidor de autorização e suas opções de configuração
- OAuth 2,0 tipo de concessão
- Ferramenta cliente ou software usada para emitir a solicitação

Tipos de concessão

Um *Grant* é um processo bem definido, incluindo um conjunto de fluxos de rede, usado para solicitar e receber um token de acesso OAuth 2,0. Vários tipos de concessão diferentes podem ser usados dependendo dos requisitos de cliente, ambiente e segurança. Uma lista dos tipos de concessão populares é apresentada na tabela abaixo.

Tipo de concessão	Descrição
Credenciais do cliente	Um tipo de concessão popular baseado no uso apenas de credenciais (como um ID e segredo compartilhado). Presume-se que o cliente tenha uma relação de confiança próxima com o proprietário do recurso.
Palavra-passe	O tipo de concessão de credenciais de senha do proprietário do recurso pode ser usado nos casos em que o proprietário do recurso tenha uma relação de confiança estabelecida com o cliente. Também pode ser útil ao migrar clientes HTTP legados para o OAuth 2,0.
Código de autorização	Este é um tipo de concessão ideal para clientes confidenciais e é baseado em um fluxo baseado em redirecionamento. Ele pode ser usado para obter um token de acesso e atualizar token.

Conteúdo do JWT

Um token de acesso OAuth 2,0 é formatado como JWT. O conteúdo é criado pelo servidor de autorização com base na sua configuração. No entanto, os tokens são opacos para as aplicações cliente. Um cliente não tem razão para inspecionar um token ou estar ciente do conteúdo.

Cada token de acesso JWT contém um conjunto de reivindicações. As reclamações descrevem as caraterísticas do emissor e a autorização com base nas definições administrativas do servidor de autorização. Algumas das reclamações registadas com a norma estão descritas na tabela abaixo. Todas as cordas são sensíveis a maiúsculas e minúsculas.

Pedido de reembolso	Palavra-chave	Descrição
Emissor	iss	Identifica o principal que emitiu o token. O processamento da reclamação é específico da aplicação.
Assunto	sub	O assunto ou usuário do token. O nome é definido para ser global ou localmente único.
Público-alvo	aud	Os destinatários para os quais o token se destina. Implementado como uma matriz de strings.
Expiração	exp	O tempo após o qual o token expira e deve ser rejeitado.

Consulte "RFC 7519: JSON Web tokens" para obter mais informações.

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).

Consulte "Trabalhar com grupos" para obter mais informações.

Escopos OAuth 2,0 independentes

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.

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.
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
```

Trabalhar com grupos

O ONTAP fornece várias opções para configurar grupos com base no servidor de autorização. Os grupos podem então ser mapeados para funções que são usadas pelo ONTAP para determinar o acesso.

Como os grupos são identificados

Quando você configura um grupo em um servidor de autorização, ele é identificado e transportado em um token de acesso OAuth 2,0 usando um nome ou UUID. Você precisa estar ciente de como o servidor de autorização lida com grupos antes de configurar o ONTAP.

> Se vários grupos forem incluídos em um token de acesso, o ONTAP tentará usar cada um até que haja uma correspondência.

Nomes de grupos

Muitos servidores de autorização identificam e representam grupos usando um nome. Aqui está um fragmento de um token de acesso JSON gerado pelo Serviço de Federação do ative Directory (ADFS) contendo vários grupos. Consulte Gerenciar grupos com nomes para obter mais informações.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

UUUIDs de grupo

Alguns servidores de autorização identificam e representam grupos usando um UUID. Aqui está um fragmento de um token de acesso JSON gerado pelo Microsoft Entra ID contendo vários grupos. Consulte Gerenciar grupos com UUIDs para obter mais informações.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Gerenciar grupos com nomes

Se o servidor de autorização usar nomes para identificar grupos, você precisa garantir que cada grupo esteja definido como ONTAP. Dependendo do seu ambiente de segurança, talvez você já tenha o grupo definido.

Aqui está um exemplo de comando CLI definindo um grupo para ONTAP. Observe que está usando um grupo nomeado do token de acesso de amostra. Você precisa estar no nível de privilégio ONTAP **admin** para emitir o comando.

Exemplo

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

Você também pode configurar esse recurso usando a API REST do ONTAP. Saiba mais no "Documentação de automação do ONTAP".

Gerenciar grupos com UUIDs

Se o servidor de autorização representar grupos usando valores UUID, você precisará executar uma

configuração de duas etapas antes de usar um grupo. A partir do ONTAP 9.16,1, dois recursos de mapeamento estão disponíveis e foram testados com o Microsoft Entra ID. Você precisa estar no nível de privilégio ONTAP **admin** para emitir os comandos CLI.

Você também pode configurar esses recursos usando a API REST do ONTAP. Saiba mais no "Documentação de automação do ONTAP".

Informações relacionadas

- "Comandos CLI do ONTAP"

Mapear um UUID de grupo para um nome de grupo

Se você estiver usando um servidor de autorização que representa grupos usando valores UUID, será necessário mapear os UUIDs do grupo para nomes de grupos. As principais operações da CLI do ONTAP são descritas abaixo.

Criar

Você pode definir uma nova configuração de mapeamento de grupo com o `security login group create` comando. O UUID e o nome do grupo devem corresponder à configuração no servidor de autorização.

Parâmetros

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

Parâmetro	Descrição
`vserver`	Opcionalmente, especifica o nome do SVM (vserver) ao qual o grupo está associado. Se omitido, o grupo está associado ao cluster ONTAP.
`name`	O nome exclusivo do grupo que o ONTAP usará.
`type`	Este valor indica o provedor de identidade do qual o grupo se origina.
`uuid`	Especifica o identificador universalmente exclusivo do grupo, conforme fornecido pelo servidor de autorização.

Aqui está um exemplo de comando CLI definindo um grupo para ONTAP. Observe que está usando um grupo UUID do token de acesso de amostra.

Exemplo

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

Depois de criar o grupo, um identificador inteiro exclusivo somente leitura é gerado para o grupo.

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar

- Eliminar

Você pode usar a `show` opção para recuperar o ID de grupo exclusivo gerado para um grupo. Consulte a documentação de referência dos comandos ONTAP para obter mais informações.

Mapear um UUID de grupo para uma função

Se você estiver usando um servidor de autorização que representa grupos usando valores UUID, você poderá mapear o grupo para uma função. As principais operações da CLI do ONTAP são descritas abaixo. Além disso, você precisa estar no nível de privilégio ONTAP **admin** para emitir os comandos.

> Você precisa primeiro Mapear um UUID de grupo para um nome de grupo e recuperar o ID inteiro exclusivo gerado para o grupo. Você precisará do ID para mapear o grupo para uma função.

Criar

Você pode definir um novo mapeamento de função com o `security login group role-mapping create` comando.

Parâmetros

Os parâmetros usados para mapear um grupo para uma função são descritos abaixo.

Parâmetro	Descrição
`group-id`	Especifica o ID exclusivo gerado para o grupo usando o comando `security login group create`.
`role`	O nome da função ONTAP para o qual o grupo é mapeado.

Exemplo

```
security login group role-mapping create -group-id 1 -role admin
```

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar
- Eliminar

Consulte a documentação de referência dos comandos ONTAP para obter mais informações.

Mapeamento de funções externas

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".

Informações relacionadas

- "Comandos CLI 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
```

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar
- Eliminar

Consulte a documentação de referência dos comandos do ONTAP ou as páginas man da CLI do ONTAP para obter mais informações.

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 de mapeamento de grupo interno será pesquisada. Se houver uma correspondência de grupo e uma função associada, 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. Para obter mais informações, "Trabalhar com grupos"consulte .

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.

Cenários de implantação do OAuth 2,0

Há várias opções de configuração disponíveis ao definir um servidor de autorização para o ONTAP. Com base nessas opções, você pode definir um servidor de autorização apropriado para o seu ambiente usando um dos vários cenários de implantação.

Resumo dos parâmetros de configuração

Existem vários parâmetros de configuração disponíveis ao definir um servidor de autorização para o ONTAP. Estes parâmetros são geralmente suportados em todas as interfaces administrativas.

> O nome usado para um parâmetro ou campo individual pode variar dependendo da interface administrativa do ONTAP. Para acomodar as diferenças nas interfaces administrativas, um único nome genérico é usado para cada parâmetro na tabela. O nome exato usado com uma interface específica deve ser óbvio com base no contexto.

Parâmetro	Descrição
Nome	O nome do servidor de autorização como é conhecido pelo ONTAP.
Aplicação	A aplicação interna do ONTAP à qual a definição se aplica. Este deve ser **http**.
URI do emissor	O FQDN com o caminho que identifica o site ou a organização que emite os tokens.
URI do provedor JWKS	O FQDN com caminho e nome de arquivo onde o ONTAP obtém os conjuntos de chaves da Web JSON usados para validar os tokens de acesso.
Intervalo de atualização do JWKS	O intervalo de tempo que determina com que frequência o ONTAP atualiza informações de certificado do URI JWKS do provedor. O valor é especificado no formato ISO-8601.
Endpoint de introspeção	O FQDN com caminho que o ONTAP usa para executar a validação remota de token por meio de introspeção.
ID do cliente	O nome do cliente, conforme definido no servidor de autorização. Quando esse valor é incluído, você também precisa fornecer o segredo do cliente associado com base na interface.
Proxy de saída	Isso é para fornecer acesso ao servidor de autorização quando o ONTAP está atrás de um firewall. O URI deve estar no formato curl.
Use funções locais, se presentes	Um sinalizador booleano que determina se as definições ONTAP locais são usadas, incluindo uma FUNÇÃO REST nomeada e usuários locais.
Reclamação do utilizador remoto	Um nome alternativo que o ONTAP usa para corresponder aos usuários locais. Use o `sub` campo no token de acesso para corresponder ao nome de usuário local.
Público-alvo	Este campo define os endpoints onde o token de acesso pode ser usado.

Cenários de implantação

Vários cenários comuns de implantação são apresentados abaixo. Eles são organizados com base se a validação de token é realizada localmente pelo ONTAP ou remotamente pelo servidor de autorização. Cada cenário inclui uma lista das opções de configuração necessárias. "Implantar o OAuth 2,0 no ONTAP"Consulte

para obter exemplos dos comandos de configuração.

Depois de definir um servidor de autorização, você pode exibir sua configuração por meio da interface administrativa do ONTAP. Por exemplo, use o comando `security oauth2 client show` com a CLI do ONTAP.

Validação local

Os cenários de implantação a seguir são baseados no ONTAP executando a validação de token localmente.

Use escopos autônomos sem um proxy

Esta é a implantação mais simples usando apenas escopos auto-contidos do OAuth 2,0. Nenhuma das definições de identidade ONTAP local é usada. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- URI do emissor

Você também precisa adicionar os escopos no servidor de autorização.

Use escopos autônomos com um proxy

Esse cenário de implantação usa os escopos auto-contidos do OAuth 2,0. Nenhuma das definições de identidade ONTAP local é usada. Mas o servidor de autorização está atrás de um firewall e, portanto, você precisa configurar um proxy. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- Proxy de saída
- URI do emissor
- Público-alvo

Você também precisa adicionar os escopos no servidor de autorização.

Use funções de usuário local e mapeamento de nome de usuário padrão com um proxy

Esse cenário de implantação usa funções de usuário local com mapeamento de nomes padrão. A reivindicação de usuário remoto usa o valor padrão de `sub` e, portanto, esse campo no token de acesso é usado para corresponder ao nome de usuário local. O nome de usuário deve ter 40 carateres ou menos. O servidor de autorização está atrás de um firewall, então você também precisa configurar um proxy. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- Usar funções locais, se presentes (`true`)
- Proxy de saída

- Emissor

Tem de se certificar de que o utilizador local está definido como ONTAP.

Use funções de usuário local e mapeamento de nome de usuário alternativo com um proxy

Esse cenário de implantação usa funções de usuário local com um nome de usuário alternativo que é usado para corresponder a um usuário local do ONTAP. O servidor de autorização está atrás de um firewall, então você precisa configurar um proxy. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- Usar funções locais, se presentes (`true`)
- Reclamação do utilizador remoto
- Proxy de saída
- URI do emissor
- Público-alvo

Tem de se certificar de que o utilizador local está definido como ONTAP.

Introspeção remota

As configurações de implantação a seguir são baseadas no ONTAP executando a validação de token remotamente por meio de introspeção.

Use escopos autônomos sem proxy

Esta é uma implantação simples baseada no uso dos escopos auto-contidos do OAuth 2,0. Nenhuma das definições de identidade do ONTAP é usada. Você deve incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- Endpoint de introspeção
- ID do cliente
- URI do emissor

Você precisa definir os escopos, bem como o segredo do cliente e do cliente no servidor de autorização.

Autenticação de cliente usando TLS mútuo

Dependendo de suas necessidades de segurança, você pode configurar opcionalmente o TLS mútuo (MTLS) para implementar uma autenticação de cliente forte. Quando usado com o ONTAP como parte de uma implantação do OAuth 2,0, o MTLS garante que os tokens de acesso são usados apenas pelos clientes aos quais foram emitidos originalmente.

TLS mútuo com OAuth 2,0

O Transport Layer Security (TLS) é usado para estabelecer um canal de comunicação seguro entre dois aplicativos, normalmente um navegador cliente e um servidor da Web. O TLS mútuo estende isso fornecendo uma forte identificação do cliente através de um certificado de cliente. Quando usado em um cluster ONTAP com OAuth 2,0, a funcionalidade base MTLS é estendida criando e usando tokens de acesso restritos ao remetente.

Um token de acesso restrito ao remetente só pode ser usado pelo cliente para o qual foi emitido originalmente. Para suportar esse recurso, uma nova solicitação de confirmação (`cnf`) é inserida no token. O campo contém uma propriedade `x5t#S256` que contém um resumo do certificado de cliente usado ao solicitar o token de acesso. Esse valor é verificado pela ONTAP como parte da validação do token. Os tokens de acesso emitidos por servidores de autorização que não estão restritos ao remetente não incluem a reivindicação de confirmação adicional.

Você precisa configurar o ONTAP para usar o MTLS separadamente para cada servidor de autorização. Por exemplo, o comando CLI `security oauth2 client` inclui o parâmetro `use-mutual-tls` para controlar o processamento MTLS com base em três valores, como mostrado na tabela abaixo.

Em cada configuração, o resultado e a ação tomadas pelo ONTAP dependem do valor do parâmetro de configuração, bem como do conteúdo do token de acesso e do certificado do cliente. Os parâmetros na tabela são organizados do mínimo ao mais restritivo.

Parâmetro	Descrição
nenhum	A autenticação TLS mútua OAuth 2,0 está completamente desativada para o servidor de autorização. A ONTAP não executará a autenticação de certificado de cliente MTLS, mesmo que a reclamação de confirmação esteja presente no token ou um certificado de cliente seja fornecido com a conexão TLS.
pedido	A autenticação TLS mútua do OAuth 2,0 é aplicada se um token de acesso restrito ao remetente for apresentado pelo cliente. Ou seja, o MTLS é aplicado somente se a reivindicação de confirmação (com propriedade `x5t#S256`) estiver presente no token de acesso. Esta é a configuração padrão.
obrigatório	A autenticação TLS mútua OAuth 2,0 é aplicada para todos os tokens de acesso emitidos pelo servidor de autorização. Portanto, todos os tokens de acesso devem ser restritos ao remetente. A autenticação e a solicitação de API REST falharão se a solicitação de confirmação não estiver presente no token de acesso ou se houver um certificado de cliente inválido.

Fluxo de implementação de alto nível

As etapas típicas envolvidas ao usar o MTLS com o OAuth 2,0 em um ambiente ONTAP são apresentadas abaixo. "RFC 8705: Autenticação de cliente TLS mútuo OAuth 2,0 e tokens de acesso com certificado"Consulte para obter mais detalhes.

Passo 1: Criar e instalar um certificado de cliente

O estabelecimento da identidade do cliente é baseado na comprovação do conhecimento de uma chave privada do cliente. A chave pública correspondente é colocada em um certificado X,509 assinado apresentado pelo cliente. Em alto nível, as etapas envolvidas na criação do certificado de cliente incluem:

1. Gere um par de chaves públicas e privadas
2. Crie uma solicitação de assinatura de certificado

3. Envie o arquivo CSR para uma CA conhecida
4. A CA verifica a solicitação e emite o certificado assinado

Normalmente, você pode instalar o certificado de cliente em seu sistema operacional local ou usá-lo diretamente com um utilitário comum, como curl.

Passo 2: Configure o ONTAP para usar o MTLS

Você precisa configurar o ONTAP para usar o MTLS. Esta configuração é feita separadamente para cada servidor de autorização. Por exemplo, com a CLI o comando `security oauth2 client` é usado com o parâmetro opcional `use-mutual-tls` . Consulte "Implantar o OAuth 2,0 no ONTAP" para obter mais informações.

Passo 3: O cliente solicita um token de acesso

O cliente precisa solicitar um token de acesso do servidor de autorização configurado para ONTAP. O aplicativo cliente deve usar o MTLS com o certificado criado e instalado na etapa 1.

Passo 4: O servidor de autorização gera o token de acesso

O servidor de autorização verifica a solicitação do cliente e gera um token de acesso. Como parte disso, ele cria um resumo de mensagem do certificado do cliente que é incluído no token como uma reivindicação de confirmação (campo `cnf`).

Passo 5: O aplicativo cliente apresenta o token de acesso ao ONTAP

O aplicativo cliente faz uma chamada de API REST para o cluster ONTAP e inclui o token de acesso no cabeçalho da solicitação de autorização como um **token de portador**. O cliente deve usar o MTLS com o mesmo certificado usado para solicitar o token de acesso.

Passo 6: O ONTAP verifica o cliente e o token.

O ONTAP recebe o token de acesso em uma solicitação HTTP, bem como o certificado de cliente usado como parte do processamento do MTLS. O ONTAP primeiro valida a assinatura no token de acesso. Com base na configuração, o ONTAP gera um resumo de mensagem do certificado do cliente e compara-o com a reclamação de confirmação **cnf** no token. Se os dois valores corresponderem, o ONTAP confirmou que o cliente que faz a solicitação de API é o mesmo cliente para o qual o token de acesso foi originalmente emitido.

Informações sobre direitos autorais

Informações sobre marcas comerciais