Configurar e implantar

ONTAP 9

NetApp
January 17, 2025

Índice

Configurar e implantar

Prepare-se para implantar o OAuth 2,0 com o ONTAP

Antes de configurar o OAuth 2,0 em um ambiente ONTAP, você deve se preparar para a implantação. Um resumo das principais tarefas e decisões está incluído abaixo. O arranjo das seções é geralmente alinhado com a ordem que você deve seguir. Mas, embora seja aplicável à maioria das implantações, você deve adaptá-lo ao seu ambiente conforme necessário. Você também deve considerar a criação de um plano de implantação formal.

Com base no seu ambiente, pode selecionar a configuração para os servidores de autorização definidos para o ONTAP. Isso inclui os valores de parâmetro que você precisa especificar para cada tipo de implantação. Consulte "Cenários de implantação do OAuth 2,0" para obter mais informações.

Recursos protegidos e aplicativos de clientes

O OAuth 2,0 é uma estrutura de autorização para controlar o acesso a recursos protegidos. Diante disso, um primeiro passo importante com qualquer implantação é determinar quais são os recursos disponíveis e quais clientes precisam acessar.

Identificar aplicativos clientes

Você precisa decidir quais clientes usarão o OAuth 2,0 ao emitir chamadas de API REST e quais endpoints de API eles precisam acessar.

Analise as funções REST do ONTAP e os usuários locais existentes

Você deve rever as definições de identidade do ONTAP existentes, incluindo as funções REST e os usuários locais. Dependendo de como você configura o OAuth 2,0, essas definições podem ser usadas para tomar decisões de acesso.

Transição global para o OAuth 2,0

Embora você possa implementar a autorização do OAuth 2,0 gradualmente, você também pode mover todos os clientes de API REST para o OAuth 2,0 imediatamente definindo um sinalizador global para cada servidor de autorização. Isso permite que as decisões de acesso sejam tomadas com base na configuração existente do ONTAP sem a necessidade de criar escopos autônomos.

Servidores de autorização

Os servidores de autorização desempenham um papel importante na implantação do OAuth 2,0, emitindo tokens de acesso e impondo a política administrativa.

Selecione e instale o servidor de autorização

Você precisa selecionar e instalar um ou mais servidores de autorização. É importante familiarizar-se com as opções de configuração e procedimentos dos seus provedores de identidade, incluindo como definir escopos. Observe que alguns servidores de autorização, incluindo o Microsoft Entra ID, representam grupos usando UUIDs em vez de nomes.

Determine se o certificado de CA raiz de autorização precisa ser instalado

O ONTAP usa o certificado do servidor de autorização para validar os tokens de acesso assinados

apresentados pelos clientes. Para fazer isso, o ONTAP precisa do certificado de CA raiz e de quaisquer certificados intermediários. Estes podem ser pré-instalados com o ONTAP. Se não, você precisa instalá-los.

Avaliar a localização e a configuração da rede

Se o servidor de autorização estiver atrás de um firewall, o ONTAP precisa ser configurado para usar um servidor proxy.

Autenticação e autorização do cliente

Existem vários aspetos da autenticação e autorização do cliente que você precisa considerar.

Escopos auto-contidos ou definições de identidade ONTAP local

Em um alto nível, você pode definir escopos autônomos definidos no servidor de autorização ou confiar nas definições de identidade ONTAP locais existentes, incluindo funções e usuários.

Opções com processamento ONTAP local

Se você usar as definições de identidade do ONTAP, você deve decidir qual aplicar, incluindo:

- Função REST nomeada
- Corresponder a utilizadores locais
- Grupos do ative Directory ou LDAP

Validação local ou introspeção remota

Você precisa decidir se os tokens de acesso serão validados localmente pelo ONTAP ou no servidor de autorização por meio de introspeção. Há também vários valores relacionados a serem considerados, como o intervalo de atualização.

Tokens de acesso restrito ao remetente

Para ambientes que exigem um alto nível de segurança, você pode usar tokens de acesso com restrição de envio baseados em MTLS. Isso requer um certificado para cada cliente.

Grupos como UUIDs e mapeamento de identidade

Se você estiver usando um servidor de autorização que representa grupos usando UUIDs, você precisará Planejar como mapeá-los para nomes de grupos e, possivelmente, para funções associadas.

Interface administrativa

Você pode executar a administração do OAuth 2,0 por meio de qualquer uma das interfaces do ONTAP, incluindo:

- Interface de linha de comando
- System Manager
- API REST

Como os clientes solicitam tokens de acesso

Os aplicativos cliente devem solicitar tokens de acesso diretamente do servidor de autorização. Você precisa decidir como isso será feito, incluindo o tipo de concessão.

Configurar o ONTAP

Há várias tarefas de configuração do ONTAP que você precisa executar.

Defina funções REST e usuários locais

Com base na sua configuração de autorização, pode ser utilizado o processamento de identificação local do ONTAP. Nesse caso, você precisa revisar e definir as funções REST e as definições de usuário. E, dependendo do seu servidor de autorização, isso também pode incluir a administração de grupos com base nos valores UUID.

Configuração central

Há três etapas principais necessárias para executar a configuração principal do ONTAP, incluindo:

- Opcionalmente, instale o certificado raiz (e quaisquer certificados intermediários) para a CA que assinou o certificado do servidor de autorização.
- Defina o servidor de autorização.
- Ative o processamento OAuth 2,0 para o cluster.

Implantar o OAuth 2,0 no ONTAP

A implantação da funcionalidade principal do OAuth 2,0 envolve três etapas principais.

Antes de começar

Você deve se preparar para a implantação do OAuth 2,0 antes de configurar o ONTAP. Por exemplo, você precisa avaliar o servidor de autorização, incluindo como seu certificado foi assinado e se está atrás de um firewall. Consulte "Prepare-se para implantar o OAuth 2,0 com o ONTAP" para obter mais informações.

Etapa 1: Instale os certificados de CA raiz do servidor de autorização

O ONTAP inclui um grande número de certificados de CA raiz pré-instalados. Assim, em muitos casos, o certificado para o seu servidor de autorização será imediatamente reconhecido pelo ONTAP sem configuração adicional. Mas dependendo de como o certificado do servidor de autorização foi assinado, talvez seja necessário instalar um certificado de CA raiz e quaisquer certificados intermediários.

Siga as instruções fornecidas abaixo para instalar o certificado, se necessário. Você deve instalar todos os certificados necessários no nível do cluster.

Escolha o procedimento correto com base em como você acessa o ONTAP.

Exemplo 1. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Clique em → ao lado de **certificados**.
4. Na guia **autoridades de certificação confiáveis**, clique em **Adicionar**.
5. Clique em **Importar** e selecione o arquivo de certificado.
6. Complete os parâmetros de configuração para o seu ambiente.
7. Clique em **Add**.

CLI

1. Inicie a instalação:

   ```
   security certificate install -type server-ca
   ```

2. Procure a seguinte mensagem do console:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Abra o arquivo de certificado com um editor de texto.
4. Copie o certificado inteiro, incluindo as seguintes linhas:

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. Cole o certificado no terminal após o prompt de comando.
6. Pressione **Enter** para concluir a instalação.
7. Confirme se o certificado está instalado usando uma das seguintes opções:

   ```
   security certificate show-user-installed

   security certificate show
   ```

Etapa 2: Configurar o servidor de autorização

Você precisa definir pelo menos um servidor de autorização para o ONTAP. Você deve escolher os valores de parâmetro com base em sua configuração e plano de implantação. Reveja "Cenários de implantação do OAuth2" para determinar os parâmetros exatos necessários para a sua configuração.

Para modificar uma definição de servidor de autorização, você pode excluir a definição existente e criar uma nova.

O exemplo fornecido abaixo é baseado no primeiro cenário de implantação simples em "Validação local". Escopos auto-contidos são usados sem um proxy.

Escolha o procedimento correto com base em como você acessa o ONTAP. O procedimento CLI usa variáveis simbólicas que você precisa substituir antes de emitir o comando.

Exemplo 2. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Clique em *** ao lado de *autorização OAuth 2,0**.
4. Selecione **mais opções**.
5. Forneça os valores necessários para sua implantação, como:
   - Nome
   - Aplicação (http)
   - URI do provedor JWKS
   - URI do emissor
6. Clique em **Add**.

CLI

1. Crie a definição novamente:

   ```
   security oauth2 client create -config-name <NAME> -provider-jwks-uri
   <URI_JWKS> -application http -issuer <URI_ISSUER>
   ```

   Por exemplo:

   ```
   security oauth2 client create \
   -config-name auth0 \
   -provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
   realm/protocol/openid-connect/certs \
   -application http \
   -issuer https://superzap.dev.netapp.com:8443/realms/my-realm
   ```

Passo 3: Ative o OAuth 2,0

O passo final é habilitar o OAuth 2,0. Esta é uma configuração global para o cluster ONTAP.

Não ative o processamento do OAuth 2,0 até confirmar que o ONTAP, os servidores de autorização e quaisquer serviços de suporte foram configurados corretamente.

Escolha o procedimento correto com base em como você acessa o ONTAP.

Exemplo 3. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Clique em → ao lado de **autorização OAuth 2,0**.
4. Ativar **autorização OAuth 2,0**.

CLI

1. Ativar OAuth 2,0:

   ```
   security oauth2 modify -enabled true
   ```

2. Confirmar que o OAuth 2,0 está ativado:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Emita uma chamada de API REST usando o OAuth 2,0

A implementação do OAuth 2,0 no ONTAP suporta aplicações cliente API REST. Você pode emitir uma simples chamada de API REST usando curl para começar a usar o OAuth 2,0. O exemplo apresentado abaixo recupera a versão do cluster do ONTAP.

Antes de começar

Você deve configurar e ativar o recurso OAuth 2,0 para seu cluster ONTAP. Isso inclui a definição de um servidor de autorização.

Passo 1: Adquira um token de acesso

Você precisa adquirir um token de acesso para usar com a chamada API REST. A solicitação de token é realizada fora do ONTAP e o procedimento exato depende do servidor de autorização e de sua configuração. Você pode solicitar o token através de um navegador da Web, com um comando curl ou usando uma linguagem de programação.

Para fins de ilustração, um exemplo de como um token de acesso pode ser solicitado ao Keycloak usando curl é apresentado abaixo.

Exemplo de capa-chave

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

Você deve copiar e salvar o token retornado.

Etapa 2: Emita a chamada da API REST

Depois de ter um token de acesso válido, você pode usar um comando curl com o token de acesso para emitir uma chamada de API REST.

Parâmetros e variáveis

As duas variáveis no exemplo curl são descritas na tabela abaixo.

Variável	Descrição
FQDN_IP	O nome de domínio totalmente qualificado ou o endereço IP do LIF de gerenciamento do ONTAP.
ACCESS_TOKEN	O token de acesso OAuth 2,0 emitido pelo servidor de autorização.

Você deve primeiro definir essas variáveis no ambiente de shell Bash antes de emitir o exemplo curl. Por exemplo, na CLI do Linux digite o seguinte comando para definir e exibir a variável FQDN:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

Depois que ambas as variáveis são definidas no seu shell Bash local, você pode copiar o comando curl e colá-lo na CLI. Pressione **Enter** para substituir as variáveis e emitir o comando.

Curl exemplo

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

Informações sobre direitos autorais

Informações sobre marcas comerciais