Gerenciar certificados de segurança

Active IQ Unified Manager

NetApp
October 15, 2025

Índice

Gerenciar certificados de segurança

Você pode configurar HTTPS no servidor do Unified Manager para monitorar e gerenciar seus clusters por meio de uma conexão segura.

Visualizar o certificado de segurança HTTPS

Você pode comparar os detalhes do certificado HTTPS com o certificado recuperado no seu navegador para garantir que a conexão criptografada do seu navegador com o Unified Manager não esteja sendo interceptada.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Visualizar o certificado permite que você verifique o conteúdo de um certificado regenerado ou visualize os Nomes Alt do Assunto (SAN) a partir dos quais você pode acessar o Unified Manager.

Etapa

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.

   O certificado HTTPS é exibido no topo da página

Se precisar visualizar informações mais detalhadas sobre o certificado de segurança do que as exibidas na página Certificado HTTPS, você poderá visualizar o certificado de conexão no seu navegador.

Baixe uma solicitação de assinatura de certificado HTTPS

Você pode baixar uma solicitação de assinatura de certificação para o certificado de segurança HTTPS atual para que você possa fornecer o arquivo para uma Autoridade de Certificação assinar. Um certificado assinado por uma CA ajuda a evitar ataques do tipo man-in-the-middle e fornece melhor proteção de segurança do que um certificado autoassinado.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.
2. Clique em **Baixar solicitação de assinatura de certificado HTTPS**.
3. Salve o `<hostname>.csr` arquivo.

Você pode fornecer o arquivo para uma Autoridade de Certificação assinar e depois instalar o certificado assinado.

Instalar um certificado HTTPS assinado e retornado pela CA

Você pode carregar e instalar um certificado de segurança depois que uma Autoridade

Certificadora o assinar e devolver. O arquivo que você carrega e instala deve ser uma versão assinada do certificado autoassinado existente. Um certificado assinado por uma CA ajuda a evitar ataques do tipo man-in-the-middle e fornece melhor proteção de segurança do que um certificado autoassinado.

*O que. Antes de começar

Você deve ter concluído as seguintes ações:

- Baixou o arquivo de solicitação de assinatura de certificado e o assinou com uma autoridade de certificação
- Salvou a cadeia de certificados no formato PEM
- Incluiu todos os certificados na cadeia, desde o certificado do servidor do Unified Manager até o certificado de assinatura raiz, incluindo quaisquer certificados intermediários presentes

Você deve ter a função de Administrador do Aplicativo.

Se a validade do certificado para o qual um CSR foi criado for superior a 397 dias, a validade será reduzida para 397 dias pela CA antes de assinar e devolver o certificado.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.
2. Clique em **Instalar certificado HTTPS**.
3. Na caixa de diálogo exibida, clique em **Escolher arquivo…** para localizar o arquivo a ser carregado.
4. Selecione o arquivo e clique em **Instalar** para instalar o arquivo.

   Para obter informações, consulte"Instalando um certificado HTTPS gerado usando ferramentas externas" .

Exemplo de cadeia de certificados

O exemplo a seguir mostra como o arquivo da cadeia de certificados pode aparecer:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Instalar um certificado HTTPS gerado usando ferramentas externas

Você pode instalar certificados autoassinados ou assinados por CA e gerados usando uma ferramenta externa como OpenSSL, BoringSSL, LetsEncrypt.

Você deve carregar a chave privada junto com a cadeia de certificados porque esses certificados são pares de chaves pública-privada gerados externamente. Os algoritmos de pares de chaves permitidos são “RSA” e “EC”. A opção **Instalar certificado HTTPS** está disponível na página Certificados HTTPS, na seção Geral. O arquivo que você enviar deve estar no seguinte formato de entrada.

1. Chave privada do servidor que pertence ao host do Active IQ Unified Manager
2. Certificado do servidor que corresponde à chave privada
3. Certificado das CAs em sentido inverso até a raiz, que são usadas para assinar o certificado acima

Formato para carregar um certificado com um par de chaves EC

As curvas permitidas são “prime256v1” e “secp384r1”. Exemplo de certificado com um par EC gerado externamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Formato para carregar um certificado com um par de chaves RSA

Os tamanhos de chave permitidos para o par de chaves RSA pertencente ao certificado de host são 2048, 3072 e 4096. certificado com um **par de chaves RSA** gerado externamente:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Após o upload do certificado, você deve reiniciar a instância do Active IQ Unified Manager para que as alterações entrem em vigor.

Verificações durante o upload de certificados gerados externamente

O sistema realiza verificações ao carregar um certificado gerado usando ferramentas externas. Se alguma das verificações falhar, o certificado será rejeitado. Também há validação incluída para os certificados gerados a partir do CSR dentro do produto e para certificados gerados usando ferramentas externas.

- A chave privada na entrada é validada em relação ao certificado do host na entrada.
- O Nome Comum (CN) no certificado do host é verificado em relação ao FQDN do host.
- O Nome Comum (CN) do certificado do host não deve estar vazio ou em branco e não deve ser definido como localhost.
- A data de início da validade não deve ser no futuro e a data de expiração da validade do certificado não deve ser no passado.
- Se existir uma CA intermediária ou CA, a data de início da validade do certificado não deve ser no futuro e a data de expiração da validade não deve ser no passado.

> A chave privada na entrada não deve ser criptografada. Se houver chaves privadas criptografadas, elas serão rejeitadas pelo sistema.

Exemplo 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Exemplo 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Exemplo 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Se a instalação do certificado falhar, consulte o artigo da base de conhecimento (KB):https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["O ActiveIQ Unified Manager falha ao instalar um certificado gerado externamente"^]

Descrições de páginas para gerenciamento de certificados

Você pode usar a página Certificado HTTPS para visualizar os certificados de segurança atuais e gerar novos certificados HTTPS.

Página do certificado HTTPS

A página Certificado HTTPS permite que você visualize o certificado de segurança atual, baixe uma solicitação de assinatura de certificado, gere um novo certificado HTTPS autoassinado ou instale um novo certificado HTTPS.

Se você não gerou um novo certificado HTTPS autoassinado, o certificado que aparece nesta página é o certificado que foi gerado durante a instalação.

Botões de comando

Os botões de comando permitem que você execute as seguintes operações:

- **Baixar solicitação de assinatura de certificado HTTPS**

  Baixa uma solicitação de certificação para o certificado HTTPS instalado no momento. Seu navegador solicita que você salve o arquivo <hostname>.csr para que você possa fornecê-lo a uma Autoridade de Certificação para assinatura.

- **Instalar certificado HTTPS**

  Permite que você carregue e instale um certificado de segurança depois que uma Autoridade de Certificação o assinar e devolver. O novo certificado entra em vigor após você reiniciar o servidor de gerenciamento.

- **Regenerar certificado HTTPS**

Permite que você gere um novo certificado HTTPS autoassinado, que substitui o certificado de segurança atual. O novo certificado entrará em vigor após você reiniciar o Unified Manager.

Caixa de diálogo Regenerar certificado HTTPS

A caixa de diálogo Regenerar certificado HTTPS permite que você personalize as informações de segurança e, em seguida, gere um novo certificado HTTPS com essas informações.

As informações atuais do certificado aparecem nesta página.

A seleção “Regenerar usando atributos de certificado atuais” e "Atualizar os atributos de certificado atuais`" permite que você regenere o certificado com as informações atuais ou gere um certificado com novas informações.

- **Nome comum**

  Obrigatório. O nome de domínio totalmente qualificado (FQDN) que você deseja proteger.

  Em configurações de alta disponibilidade do Unified Manager, use o endereço IP virtual.

- **E-mail**

  Opcional. Um endereço de e-mail para entrar em contato com sua organização; normalmente o endereço de e-mail do administrador do certificado ou do departamento de TI.

- **Empresa**

  Opcional. Normalmente, o nome incorporado da sua empresa.

- **Departamento**

  Opcional. O nome do departamento da sua empresa.

- **Cidade**

  Opcional. A localização da sua empresa na cidade.

- **Estado**

  Opcional. Localização do estado ou província, não abreviada, da sua empresa.

- **País**

  Opcional. A localização da sua empresa no país. Normalmente, este é um código ISO de duas letras do país.

- **Nomes alternativos**

  Obrigatório. Nomes de domínio adicionais, não primários, que podem ser usados para acessar este servidor, além do host local existente ou outros endereços de rede. Separe cada nome alternativo com uma vírgula.

  Marque a caixa de seleção “Excluir informações de identificação local (por exemplo, host local)” se desejar remover as informações de identificação local do campo Nomes alternativos no certificado. Quando esta

caixa de seleção estiver marcada, somente o que você inserir no campo será usado no campo Nomes Alternativos. Se deixado em branco, o certificado resultante não terá nenhum campo Nomes Alternativos.

- **TAMANHO DA CHAVE (ALGORITMO DA CHAVE: RSA)**

  O algoritmo principal é definido como RSA. Você pode selecionar um dos tamanhos de chave: 2048, 3072 ou 4096 bits. O tamanho padrão da chave é definido como 2048 bits.

- **PERÍODO DE VALIDADE**

  O período de validade padrão é de 397 dias. Se você tiver atualizado de uma versão anterior, poderá ver a validade do certificado anterior inalterada.

Para mais informações, consulte "Gerando certificados HTTPS".

Informações sobre direitos autorais

Informações sobre marcas comerciais