Gerenciamento de certificados de segurança

Active IQ Unified Manager 9.16

NetApp
November 19, 2024

Índice

Gerenciamento de certificados de segurança

Você pode configurar o HTTPS no servidor do Unified Manager para monitorar e gerenciar seus clusters em uma conexão segura.

Exibindo o certificado de segurança HTTPS

Você pode comparar os detalhes do certificado HTTPS com o certificado recuperado em seu navegador para garantir que a conexão criptografada do navegador com o Unified Manager não esteja sendo intercetada.

Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

A exibição do certificado permite verificar o conteúdo de um certificado regenerado ou exibir nomes Alt de assunto (SAN) a partir dos quais você pode acessar o Unified Manager.

Passo

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

   O certificado HTTPS é exibido na parte superior da página

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

Transferir 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 a uma autoridade de certificação para assinar. Um certificado assinado pela CA ajuda a evitar ataques man-in-the-middle e fornece melhor proteção de segurança do que um certificado autoassinado.

Antes de começar

Tem de ter a função Administrador de aplicações.

Passos

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

Você pode fornecer o arquivo a uma autoridade de certificação para assinar e, em seguida, instalar o certificado assinado.

Instalando um certificado HTTPS assinado e retornado pela CA

Você pode fazer o upload e instalar um certificado de segurança depois que uma Autoridade de certificação o tiver assinado e retornado. O arquivo que você carregar e instalar deve ser uma versão assinada do certificado autoassinado existente. Um certificado assinado pela CA ajuda a evitar ataques 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:

- Fez o download do arquivo de solicitação de assinatura de certificado e o assinou por uma Autoridade de Certificação
- Salva a cadeia de certificados no formato PEM
- Incluídos todos os certificados na cadeia, desde o certificado do servidor Unified Manager até o certificado de assinatura raiz, incluindo quaisquer certificados intermediários presentes

Tem de ter a função Administrador de aplicações.

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 **escolha arquivo…** para localizar o arquivo a ser carregado.
4. Selecione o arquivo e clique em **Instalar** para instalar o arquivo.

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

Exemplo de cadeia de certificados

O exemplo a seguir mostra como o arquivo de 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 que são autoassinados ou CA assinados e são 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 gerados externamente pelo par de chaves público-privadas. Os algoritmos de par 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 carregar deve estar no seguinte formato de entrada.

1. Chave privada do servidor que pertence ao host 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 usados para assinar o certificado acima

Formato para carregar um certificado com um par de chaves EC

As curvas permitidas são "prime256v1" e "ecp384r1". Amostra 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 pertencentes 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-----
```

Depois que o certificado for carregado, você deverá reiniciar a instância do Active IQ Unified Manager para que as alterações entrem em vigor.

Verifica durante o carregamento de certificados gerados externamente

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

- A chave privada na entrada é validada com base no certificado do host na entrada.

- O Nome Comum (CN) no certificado de host é verificado em relação ao FQDN do host.
- O Nome Comum (CN) do certificado de anfitrião não deve estar vazio ou em branco e não deve ser definido como localhost.
- A data de início da validade não deve ser futura e a data de validade do certificado não deve ser anterior.
- Se houver CA ou CA intermediária, a data de início de validade do certificado não deve ser no futuro e a data de 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): "O ActiveIQ Unified Manager não instala um certificado gerado externamente"

Descrições de páginas para gerenciamento de certificados

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

Página certificado HTTPS

A página certificado HTTPS permite exibir o certificado de segurança atual, fazer download de uma solicitação de assinatura de certificado, gerar um novo certificado HTTPS autoassinado ou instalar um novo certificado HTTPS.

Se não tiver gerado um novo certificado HTTPS auto-assinado, o certificado que aparece nesta página é o certificado que foi gerado durante a instalação.

Botões de comando

Os botões de comando permitem executar as seguintes operações:

- * Faça o download do pedido de assinatura de certificado HTTPS*

  Transfere uma solicitação de certificação para o certificado HTTPS atualmente instalado. O navegador solicita que você salve o arquivo <hostname>.csr para que você possa fornecer o arquivo a uma autoridade de certificação para assinar.

- **Instalar certificado HTTPS**

  Permite que você carregue e instale um certificado de segurança depois que uma autoridade de certificação o tiver assinado e devolvido. O novo certificado entra em vigor após reiniciar o servidor de gerenciamento.

- **Regenerate HTTPS Certificate**

  Permite gerar um novo certificado HTTPS autoassinado, que substitui o certificado de segurança atual. O novo certificado entrará em vigor após a reinicialização do Unified Manager.

Caixa de diálogo regenerar certificado HTTPS

A caixa de diálogo regenerar certificado HTTPS permite personalizar as informações de segurança e, em seguida, gerar um novo certificado HTTPS com essas informações.

As informações atuais do certificado são exibidas 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.

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

- **Email**

  Opcional. Um endereço de e-mail para entrar em Contato com sua organização; normalmente, o endereço de e-mail do administrador de certificados ou do departamento DE TI.

- **Empresa**

  Opcional. Normalmente, o nome incorporado da sua empresa.

- **Departamento**

  Opcional. O nome do departamento em sua empresa.

- **Cidade**

  Opcional. A localização da cidade da sua empresa.

- **Estado**

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

- **País**

  Opcional. A localização do país da sua empresa. Este é normalmente 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 localhost 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, localhost)" se quiser remover as informações de identificação local do campo nomes alternativos no certificado. Quando esta caixa de verificação está selecionada, apenas o que introduzir no campo é utilizado no campo nomes alternativos. Quando deixado em branco, o certificado resultante não terá um campo de nomes alternativos.

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

  O algoritmo de chave é definido como RSA. Você pode selecionar um dos tamanhos de chave: 2048, 3072 ou 4096 bits. O tamanho da chave padrão é definido para 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 obter mais informações, "Gerando certificados HTTPS"consulte .

Informações sobre direitos autorais

Informações sobre marcas comerciais