Gerenciamento de certificados de segurança

Active IQ Unified Manager 9.7

NetApp
October 22, 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.

Sobre esta tarefa

A exibição do certificado permite verificar o conteúdo de um certificado regenerado ou exibir nomes de URL alternativos a partir dos quais você pode acessar o Unified Manager.

Passos

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

   O certificado HTTPS é exibido na parte superior da página

Depois de terminar

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.

Gerando um certificado de segurança HTTPS

Você pode gerar um novo certificado de segurança HTTPS por vários motivos, incluindo se deseja assinar com uma autoridade de certificação diferente ou se o certificado de segurança atual expirou. O novo certificado substitui o certificado existente.

Antes de começar

Tem de ter a função Administrador de aplicações.

Sobre esta tarefa

Se você não tiver acesso à IU da Web do Unified Manager, poderá regenerar o certificado HTTPS com os mesmos valores usando o console de manutenção.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **certificado HTTPS**.
2. Clique em **Regenerate HTTPS Certificate**.

   A caixa de diálogo Regerate HTTPS Certificate (regenerar certificado HTTPS) é exibida.

3. Selecione uma das opções a seguir, dependendo de como você deseja gerar o certificado:

Se você quiser…	Faça isso…
Regenere o certificado com os valores atuais	Clique na opção **Regenerate usando atributos de certificado atuais**.
Gerar o certificado usando valores diferentes	`Click the *Update the Current Certificate Attributes* option. Os campos Nome Comum e nomes alternativos usarão os valores do certificado existente se você não inserir novos valores. Os outros campos não requerem valores, mas você pode inserir valores, por exemplo, para a Cidade, Estado e país, se quiser que esses valores sejam preenchidos no certificado.` Você pode selecionar 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.

4. Clique em **Yes** para regenerar o certificado.
5. Reinicie o servidor do Unified Manager para que o novo certificado entre em vigor.

Depois de terminar

Verifique as novas informações do certificado visualizando o certificado HTTPS.

Reiniciando a máquina virtual do Unified Manager

Você pode reiniciar a máquina virtual a partir do console de manutenção do Unified Manager. Você deve reiniciar depois de gerar um novo certificado de segurança ou se houver um problema com a máquina virtual.

Antes de começar

O dispositivo virtual está ligado.

Você está conetado ao console de manutenção como usuário de manutenção.

Sobre esta tarefa

Você também pode reiniciar a máquina virtual do vSphere usando a opção **Restart Guest**. Consulte a documentação da VMware para obter mais informações.

Passos

1. Aceda à consola de manutenção.
2. Selecione **Configuração do sistema** > **Reiniciar Máquina Virtual**.

Transferir uma solicitação de assinatura de certificado HTTPS

Você pode baixar uma solicitação 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.

Depois de terminar

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

Instalar um certificado de segurança HTTPS

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.

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.

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.

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-----
```

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 ou instalar um novo certificado HTTPS.

Se não tiver gerado um novo certificado HTTPS, 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 `<hostname>.csr` arquivo 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 certificado HTTPS, 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.

Informações sobre direitos autorais

Informações sobre marcas comerciais