Certificados

SANtricity 11.9

NetApp
December 16, 2024

Índice

Certificados

Descrição geral dos certificados

O Gerenciamento de certificados permite criar solicitações de assinatura de certificado (CSRs), importar certificados e gerenciar certificados existentes.

O que são certificados?

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet. Existem dois tipos de certificados: Um certificado *assinado* é validado por uma autoridade de certificação (CA) e um certificado *autoassinado* é validado pelo proprietário da entidade em vez de um terceiro.

Saiba mais:

- "Como os certificados funcionam"
- "Terminologia do certificado"

Como faço para configurar certificados?

No Gerenciamento de certificados, você pode configurar certificados para a estação de gerenciamento que hospeda o Unified Manager e também importar certificados para os controladores nos arrays.

Saiba mais:

- "Use certificados assinados pela CA para o sistema de gerenciamento"
- "Importar certificados para matrizes"

Conceitos

Como os certificados funcionam

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet.

Certificados assinados

Os certificados garantem que as comunicações da Web sejam transmitidas de forma encriptada, privada e inalterada, apenas entre o servidor e o cliente especificados. Com o Unified Manager, você pode gerenciar certificados para o navegador em um sistema de gerenciamento de host e as controladoras nos storage arrays descobertos.

Um certificado pode ser assinado por uma autoridade confiável ou pode ser autoassinado. "Assinatura" significa simplesmente que alguém validou a identidade do proprietário e determinou que seus dispositivos podem ser confiáveis. As matrizes de armazenamento são fornecidas com um certificado auto-assinado gerado automaticamente em cada controlador. Você pode continuar usando os certificados autoassinados ou obter certificados assinados pela CA para uma conexão mais segura entre os controladores e os sistemas host.

Embora os certificados assinados pela CA forneçam melhor proteção de segurança (por exemplo, evitando ataques man-in-the-middle), eles também exigem taxas que podem ser caras se você tiver uma rede grande. Em contraste, os certificados autoassinados são menos seguros, mas são gratuitos. Portanto, os certificados autoassinados são mais usados para ambientes de teste internos, não em ambientes de produção.

Um certificado assinado é validado por uma autoridade de certificação (CA), que é uma organização de terceiros confiável. Os certificados assinados incluem detalhes sobre o proprietário da entidade (normalmente, um servidor ou site), data de emissão e expiração do certificado, domínios válidos para a entidade e uma assinatura digital composta por letras e números.

Quando você abre um navegador e insere um endereço da Web, o sistema executa um processo de verificação de certificados em segundo plano para determinar se você está se conetando a um site que inclui um certificado válido assinado pela CA. Geralmente, um site protegido com um certificado assinado inclui um ícone de cadeado e uma designação https no endereço. Se você tentar se conetar a um site que não contenha um certificado assinado pela CA, o navegador exibirá um aviso de que o site não está seguro.

A CA toma medidas para verificar sua identidade durante o processo de inscrição. Eles podem enviar um e-mail para sua empresa registrada, verificar seu endereço comercial e executar uma verificação HTTP ou DNS. Quando o processo de aplicação estiver concluído, a CA envia arquivos digitais para serem carregados em um sistema de gerenciamento de host. Normalmente, esses arquivos incluem uma cadeia de confiança, como segue:

- **Root** — na parte superior da hierarquia está o certificado raiz, que contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização de CA específica. Se você usar a mesma CA para todos os dispositivos de rede, precisará de apenas um certificado raiz.
- **Intermediate** — ramificação fora da raiz são os certificados intermediários. A CA emite um ou mais certificados intermediários para atuar como intermediários entre uma raiz protegida e certificados de servidor.
- **Servidor** — na parte inferior da cadeia está o certificado do servidor, que identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um storage array requer um certificado de servidor separado.

Certificados autoassinados

Cada controladora no storage inclui um certificado pré-instalado e autoassinado. Um certificado autoassinado é semelhante a um certificado assinado pela CA, exceto que ele é validado pelo proprietário da entidade em vez de um terceiro. Como um certificado assinado pela CA, um certificado autoassinado contém sua própria chave privada e também garante que os dados sejam criptografados e enviados por uma conexão HTTPS entre um servidor e um cliente.

Os certificados autoassinados não são "confiáveis" pelos navegadores. Cada vez que você tenta se conetar a um site que contém apenas um certificado autoassinado, o navegador exibe uma mensagem de aviso. Você deve clicar em um link na mensagem de aviso que permite que você prossiga para o site; ao fazê-lo, você está essencialmente aceitando o certificado auto-assinado.

Certificados para Unified Manager

A interface do Unified Manager é instalada com o Web Services Proxy em um sistema host. Quando você abre um navegador e tenta se conetar ao Unified Manager, o navegador tenta verificar se o host é uma fonte confiável verificando se há um certificado digital. Se o navegador não localizar um certificado assinado pela CA para o servidor, ele abrirá uma mensagem de aviso. A partir daí, você pode continuar para o site para aceitar o certificado autoassinado para essa sessão. Ou, você pode obter certificados digitais assinados de

uma CA para que você não veja mais a mensagem de aviso.

Certificados para controladores

Durante uma sessão do Unified Manager, você pode ver mensagens de segurança adicionais quando tentar acessar um controlador que não tenha um certificado assinado pela CA. Nesse caso, você pode confiar permanentemente no certificado autoassinado ou importar os certificados assinados pela CA para os controladores para que o servidor Proxy de Serviços da Web possa autenticar solicitações de clientes recebidas desses controladores.

Terminologia do certificado

Os termos a seguir se aplicam ao gerenciamento de certificados.

Prazo	Descrição
CA	Uma autoridade de certificação (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam proprietários de sites, o que permite conexões seguras entre clientes e servidores.
CSR	Uma solicitação de assinatura de certificado (CSR) é uma mensagem enviada de um requerente para uma autoridade de certificação (CA). O CSR valida as informações que a CA precisa para emitir um certificado.
Certificado	Um certificado identifica o proprietário de um site para fins de segurança, o que impede que atacantes personifiquem o site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações.
Cadeia de certificados	Uma hierarquia de arquivos que adiciona uma camada de segurança aos certificados. Normalmente, a cadeia inclui um certificado raiz na parte superior da hierarquia, um ou mais certificados intermediários e os certificados de servidor que identificam as entidades.
Certificado intermédio	Um ou mais certificados intermediários ramificam da raiz na cadeia de certificados. A CA emite um ou mais certificados intermediários para atuar como intermediários entre uma raiz protegida e certificados de servidor.
Armazenamento de chaves	Um keystore é um repositório no seu sistema de gerenciamento de host que contém chaves privadas, juntamente com suas chaves públicas e certificados correspondentes. Essas chaves e certificados identificam suas próprias entidades, como os controladores.
Certificado raiz	O certificado raiz está no topo da hierarquia na cadeia de certificados e contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização de CA específica. Se você usar a mesma CA para todos os dispositivos de rede, precisará de apenas um certificado raiz.

Prazo	Descrição
Certificado assinado	Um certificado validado por uma autoridade de certificação (CA). Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente através de uma conexão HTTPS. Além disso, um certificado assinado inclui detalhes sobre o proprietário da entidade (normalmente, um servidor ou site) e uma assinatura digital composta por letras e números. Um certificado assinado usa uma cadeia de confiança e, portanto, é mais frequentemente usado em ambientes de produção. Também referido como um "certificado assinado pela CA" ou um "certificado de gestão".
Certificado auto-assinado	Um certificado autoassinado é validado pelo proprietário da entidade. Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente através de uma conexão HTTPS. Também inclui uma assinatura digital composta por letras e números. Um certificado autoassinado não usa a mesma cadeia de confiança que um certificado assinado pela CA e, portanto, é mais frequentemente usado em ambientes de teste. Também referido como um certificado "pré-instalado".
Certificado do servidor	O certificado do servidor está na parte inferior da cadeia de certificados. Ele identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um sistema de storage requer um certificado de servidor separado.
Loja de confiança	Um repositório de confiança é um repositório que contém certificados de terceiros confiáveis, como CAs.

Use certificados assinados pela CA para o sistema de gerenciamento

Você pode obter e importar certificados assinados pela CA para acesso seguro ao sistema de gerenciamento que hospeda o Unified Manager.

Antes de começar

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

Sobre esta tarefa

O uso de certificados assinados pela CA é um procedimento de três etapas.

Passo 1: Complete um arquivo CSR

Primeiro, é necessário gerar um arquivo de solicitação de assinatura de certificado (CSR), que identifique sua organização e o sistema host onde o Proxy de Serviços Web e o Unified Manager estão instalados.

Como alternativa, você pode gerar um arquivo CSR usando uma ferramenta como OpenSSL e pular para Passo 2: Envie o arquivo CSR.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Na guia Gerenciamento, selecione **Complete CSR**.
3. Insira as seguintes informações e clique em **Next**:
   - **Organização** — o nome completo e legal de sua empresa ou organização. Inclua sufixos, como Inc. Ou Corp.
   - * Unidade organizacional (opcional) * — a divisão da sua organização que está a lidar com o certificado.
   - **Cidade/localidade** — a cidade onde o seu sistema de acolhimento ou negócio está localizado.
   - **Estado/região (opcional)** — o estado ou a região onde o seu sistema anfitrião ou negócio está localizado.
   - **Código ISO do país** — o código ISO de dois dígitos do seu país (Organização Internacional para Padronização), como os EUA.
4. Insira as seguintes informações sobre o sistema host onde o Proxy de Serviços Web está instalado:
   - **Nome comum** — o endereço IP ou o nome DNS do sistema host onde o Proxy de Serviços Web está instalado. Verifique se esse endereço está correto; ele deve corresponder exatamente ao que você digita para acessar o Unified Manager no navegador. Não inclua http:// ou https://. O nome DNS não pode começar com um curinga.
   - **Endereços IP alternativos** — se o nome comum for um endereço IP, você pode opcionalmente inserir quaisquer endereços IP adicionais ou aliases para o sistema host. Para várias entradas, use um formato delimitado por vírgulas.
   - **Nomes DNS alternativos** — se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o sistema host. Para várias entradas, use um formato delimitado por vírgulas. Se não houver nomes DNS alternativos, mas você inseriu um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um curinga.
5. Certifique-se de que as informações do host estão corretas. Se não estiver, os certificados retornados da CA falharão quando você tentar importá-los.
6. Clique em **Finish**.
7. Vá para Passo 2: Envie o arquivo CSR.

Passo 2: Envie o arquivo CSR

Depois de criar um arquivo de solicitação de assinatura de certificado (CSR), você o enviará a uma Autoridade de Certificação (CA) para receber certificados de gerenciamento assinados para o sistema que hospeda o Unified Manager e o Proxy de Serviços da Web.

Os sistemas e-Series exigem o formato PEM (codificação ASCII Base64) para certificados assinados, que inclui os seguintes tipos de arquivo: .pem, .crt, .cer ou .key.

Passos

1. Localize o ficheiro CSR transferido.

   A localização da pasta do download depende do seu navegador.

2. Envie o arquivo CSR para uma CA (por exemplo, VeriSign ou DigiCert) e solicite certificados assinados no formato PEM.

Depois de enviar um arquivo CSR para a CA, NÃO regenere outro arquivo CSR. Sempre que você gera um CSR, o sistema cria um par de chaves privadas e públicas. A chave pública faz parte da CSR, enquanto a chave privada é mantida no keystore do sistema. Quando você recebe os certificados assinados e os importa, o sistema garante que as chaves privadas e públicas sejam o par original. Se as chaves não corresponderem, os certificados assinados não funcionarão e você deverá solicitar novos certificados à CA.

3. Quando a CA retornar os certificados assinados, vá para Passo 3: Importar certificados de gestão.

Passo 3: Importar certificados de gestão

Depois de receber certificados assinados da Autoridade de Certificação (CA), importe os certificados para o sistema host onde a interface Web Services Proxy e Unified Manager estão instalados.

Antes de começar

- Você recebeu certificados assinados da CA. Esses arquivos incluem o certificado raiz, um ou mais certificados intermediários e o certificado do servidor.
- Se a CA forneceu um arquivo de certificado encadeado (por exemplo, um arquivo .p7b), você deve descompactar o arquivo encadeado em arquivos individuais: O certificado raiz, um ou mais certificados intermediários e o certificado do servidor. Você pode usar o utilitário Windows `certmgr` para descompactar os arquivos (clique com o botão direito do Mouse e selecione **todas as tarefas › Exportar**). A codificação base-64 é recomendada. Quando as exportações estiverem concluídas, um arquivo CER é exibido para cada arquivo de certificado na cadeia.
- Você copiou os arquivos de certificado para o sistema host onde o Proxy de Serviços Web está sendo executado.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Na guia Gerenciamento, selecione **Importar**.

   Abre-se uma caixa de diálogo para importar os ficheiros de certificado.

3. Clique em **Procurar** para selecionar primeiro os arquivos de certificado raiz e intermediário e, em seguida, selecione o certificado do servidor. Se você gerou o CSR a partir de uma ferramenta externa, você também deve importar o arquivo de chave privada que foi criado juntamente com o CSR.

   Os nomes de arquivo são exibidos na caixa de diálogo.

4. Clique em **Importar**.

Resultados

Os arquivos são carregados e validados. As informações do certificado são exibidas na página Gerenciamento de certificados.

Repor certificados de gestão

Você pode reverter o certificado de gerenciamento para o estado original, autoassinado de fábrica.

Antes de começar

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

Sobre esta tarefa

Esta tarefa exclui o certificado de gerenciamento atual do sistema host onde o Proxy de serviços da Web e o Unified Manager estão instalados. Depois que o certificado é redefinido, o sistema host reverte para usando o certificado autoassinado.

Passos

1. Selecione **Definições > certificados**.
2. Selecione a guia **Array Management** e, em seguida, selecione **Reset**.

   Uma caixa de diálogo confirmar certificado de gerenciamento de redefinição é aberta.

3. Digite `reset` o campo e clique em **Reset**.

   Após a atualização do navegador, o navegador pode bloquear o acesso ao site de destino e informar que o site está usando HTTP Strict Transport Security. Essa condição surge quando você volta para certificados autoassinados. Para limpar a condição que está bloqueando o acesso ao destino, você deve limpar os dados de navegação do navegador.

Resultados

O sistema reverte para o uso do certificado autoassinado do servidor. Como resultado, o sistema solicita aos usuários que aceitem manualmente o certificado autoassinado para suas sessões.

Use certificados de matriz

Importar certificados para matrizes

Se necessário, você pode importar certificados para os storages de armazenamento para que eles possam se autenticar com o sistema que hospeda o Unified Manager. Os certificados podem ser assinados por uma autoridade de certificação (CA) ou podem ser autoassinados.

Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Se você estiver importando certificados confiáveis, os certificados devem ser importados para os controladores de storage usando o System Manager.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.

   Esta página mostra todos os certificados reportados para os storages de armazenamento.

3. Selecione um **Importar › certificados** para importar um certificado de CA ou **Importar › certificados de matriz de armazenamento autoassinados** para importar um certificado autoassinado.

   Para limitar a exibição, você pode usar o campo de filtragem **Mostrar certificados que são…** ou pode

classificar as linhas de certificado clicando em um dos cabeçalhos de coluna.

4. Na caixa de diálogo, selecione o certificado e clique em **Importar**.

   O certificado é carregado e validado.

Excluir certificados confiáveis

Você pode excluir um ou mais certificados que não são mais necessários, como um certificado expirado.

Antes de começar

Importe o novo certificado antes de excluir o antigo.

> Esteja ciente de que a exclusão de um certificado raiz ou intermediário pode afetar vários storages, já que esses storages podem compartilhar os mesmos arquivos de certificado.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.
3. Selecione um ou mais certificados na tabela e clique em **Excluir**.

   > A função **Delete** não está disponível para certificados pré-instalados.

   A caixa de diálogo confirmar Excluir certificado confiável é aberta.

4. Confirme a exclusão e clique em **Excluir**.

   O certificado é removido da tabela.

Resolver certificados não confiáveis

Certificados não confiáveis ocorrem quando um storage array tenta estabelecer uma conexão segura com o Unified Manager, mas a conexão não consegue confirmar como segura.

Na página certificado, você pode resolver certificados não confiáveis importando um certificado autoassinado da matriz de armazenamento ou importando um certificado de autoridade de certificação (CA) emitido por um terceiro confiável.

Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de Administrador de Segurança.
- Se você pretende importar um certificado assinado pela CA:
  - Você gerou uma solicitação de assinatura de certificado (arquivo .CSR) para cada controlador na matriz de armazenamento e a enviou para a CA.
  - A CA retornou arquivos de certificado confiáveis.
  - Os ficheiros de certificado estão disponíveis no sistema local.

Sobre esta tarefa

Talvez seja necessário instalar certificados de CA confiáveis adicionais se alguma das seguintes opções for verdadeira:

- Recentemente, você adicionou uma matriz de armazenamento.
- Um ou ambos os certificados expiram.
- Um ou ambos os certificados são revogados.
- Um ou ambos os certificados estão faltando um certificado raiz ou intermediário.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.

   Esta página mostra todos os certificados reportados para os storages de armazenamento.

3. Selecione um **Importar › certificados** para importar um certificado de CA ou **Importar › certificados de matriz de armazenamento autoassinados** para importar um certificado autoassinado.

   Para limitar a exibição, você pode usar o campo de filtragem **Mostrar certificados que são…** ou pode classificar as linhas de certificado clicando em um dos cabeçalhos de coluna.

4. Na caixa de diálogo, selecione o certificado e clique em **Importar**.

   O certificado é carregado e validado.

Gerenciar certificados

Ver certificados

Você pode ver informações resumidas de um certificado, que inclui a organização usando o certificado, a autoridade que emitiu o certificado, o período de validade e as impressões digitais (identificadores exclusivos).

Antes de começar

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione um dos seguintes separadores:
   - **Gerenciamento** — mostra o certificado para o sistema que hospeda o Proxy de Serviços Web. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade de certificação (CA). Ele permite acesso seguro ao Unified Manager.
   - **Trusted** — mostra os certificados que o Unified Manager pode acessar para matrizes de armazenamento e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos a partir de uma autoridade de certificação (CA) ou podem ser autoassinados.
3. Para ver mais informações sobre um certificado, selecione sua linha, selecione as elipses no final da linha e clique em **Exibir** ou **Exportar**.

Exportar certificados

Você pode exportar um certificado para exibir seus detalhes completos.

Antes de começar

Para abrir o ficheiro exportado, tem de ter uma aplicação de visualizador de certificados.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione um dos seguintes separadores:
   - **Gerenciamento** — mostra o certificado para o sistema que hospeda o Proxy de Serviços Web. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade de certificação (CA). Ele permite acesso seguro ao Unified Manager.
   - **Trusted** — mostra os certificados que o Unified Manager pode acessar para matrizes de armazenamento e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos a partir de uma autoridade de certificação (CA) ou podem ser autoassinados.
3. Selecione um certificado na página e, em seguida, clique nas elipses no final da linha.
4. Clique em **Exportar** e salve o arquivo de certificado.
5. Abra o arquivo no aplicativo visualizador de certificados.

Informações sobre direitos autorais

Informações sobre marcas comerciais