Usar certificados

SANtricity software

NetApp
March 17, 2026

Índice

Usar certificados

Use certificados assinados por CA para controladores no SANtricity System Manager

Você pode obter certificados assinados por CA para comunicações seguras entre os controladores e o navegador usado para acessar SANtricity System Manager.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Você precisa saber o endereço IP ou os nomes DNS de cada controlador.

Sobre esta tarefa

Utilizar certificados assinados por uma CA é um procedimento de três etapas.

Etapa 1: preencha os CSRs para os controladores

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR) para cada controlador no array de storage.

Sobre esta tarefa

Esta tarefa descreve como gerar um arquivo CSR a partir do System Manager. O CSR fornece informações sobre sua organização e, ou o endereço IP ou o nome DNS do controlador. Durante esta tarefa, um arquivo CSR é gerado se o array de storage tiver um controlador e dois arquivos CSR se tiver dois controladores.

> Alternativamente, você pode gerar um arquivo CSR usando uma ferramenta como OpenSSL e pode pular para Etapa 2: enviar os arquivos CSR.

Passos

1. Selecione **Configurações › Certificados**.
2. Na aba Array Management, selecione **Complete CSR**.

> Se você vir uma caixa de diálogo solicitando que aceite um certificado autoassinado para o segundo controlador, clique em **Accept Self-Signed Certificate** para prosseguir.

3. Insira as seguintes informações e clique em **Avançar**:
   - **Organização** — O nome completo e legal da sua empresa ou organização. Inclua sufixos, como Inc. ou Corp.
   - **Unidade organizacional (opcional)** — A divisão da sua organização que está lidando com o certificado.
   - **Cidade/Localidade** — A cidade onde seu array de storage ou empresa está localizado.
   - **Estado/Região (opcional)** — O estado ou região onde seu array de storage ou empresa está localizado.
   - **Código ISO do país** — O código ISO (Organização Internacional de Normalização) de dois dígitos do seu país, como US.

Alguns campos podem estar preenchidos previamente com as informações apropriadas, como o endereço IP do controlador. Não altere os valores preenchidos previamente, a menos que tenha certeza de que estão incorretos. Por exemplo, se você ainda não concluiu um CSR, o endereço IP do controlador está definido como “localhost.” Nesse caso, você deve alterar “localhost” para o nome DNS ou endereço IP do controlador.

4. Verifique ou insira as seguintes informações sobre o controlador A em seu array de storage:
   - **Nome comum do Controlador A** — O endereço IP ou o nome DNS do controlador A é exibido por padrão. Certifique-se de que este endereço esteja correto; ele deve corresponder exatamente ao que você digita para acessar System Manager no navegador. O nome DNS não pode começar com um caractere curinga.
   - **Endereços IP alternativos do Controlador A** — Se o nome comum for um endereço IP, você pode, opcionalmente, inserir quaisquer endereços IP adicionais ou aliases para o controlador A. Para múltiplas entradas, use um formato separado por vírgulas.
   - **Nomes DNS alternativos do controlador A** — Se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o controlador A. Para várias entradas, use o formato separado por vírgulas. Se não houver nomes DNS alternativos, mas você tiver inserido um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um caractere curinga. Se o array de storage tiver apenas um controlador, o botão **Finish** estará disponível.

     Se o array de storage tiver dois controladores, o botão **Next** estará disponível.

Não clique no link **Pular esta etapa** ao criar inicialmente uma solicitação CSR. Este link é fornecido em situações de recuperação de erros. Em casos raros, uma solicitação CSR pode falhar em um controlador, mas não no outro. Este link permite que você pule a etapa de criação de uma solicitação CSR no controlador A, caso ela já esteja definida, e continue para a próxima etapa para recriar uma solicitação CSR no controlador B.

5. Se houver apenas um controlador, clique em **Concluir**. Se houver dois controladores, clique em **Avançar** para inserir as informações do controlador B (como acima) e, em seguida, clique em **Concluir**.

   Para um único controlador, um arquivo CSR é baixado para o seu sistema local. Para dois controladores, dois arquivos CSR são baixados. O local da pasta de download depende do seu navegador.

6. Vá para Etapa 2: enviar os arquivos CSR.

Etapa 2: enviar os arquivos CSR

Após criar os arquivos de solicitação de assinatura de certificado (CSR), envie os arquivos para uma autoridade certificadora (CA). E-Series systems 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 os arquivos CSR baixados.
2. Envie os arquivos CSR para uma Autoridade Certificadora (por exemplo, Verisign ou DigiCert), e solicite certificados assinados no formato PEM.

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

3. Quando a CA retornar os certificados assinados, vá para Etapa 3: importar certificados assinados para controladores.

Etapa 3: importar certificados assinados para controladores

Após receber os certificados assinados da Certificate Authority (CA), importe os arquivos dos controladores.

Antes de começar

- A Autoridade Certificadora (CA) retornou arquivos de certificado assinados. Esses arquivos incluem o certificado raiz, um ou mais certificados intermediários e os certificados do servidor.
- Se a CA forneceu um arquivo de certificado em cadeia (por exemplo, um arquivo .p7b), você deve descompactar o arquivo em cadeia em arquivos individuais: o certificado raiz, um ou mais certificados intermediários e os certificados de servidor que identificam os controladores. Você pode usar o utilitário do Windows `certmgr` para descompactar os arquivos (clique com o botão direito e selecione **All Tasks › Export**). A codificação Base-64 é recomendada. Quando as exportações forem concluídas, um arquivo CER será exibido para cada arquivo de certificado na cadeia.
- Você copiou os arquivos de certificado para o sistema host onde acessa System Manager.

Passos

1. Selecione o menu: Configurações[Certificados]
2. Na guia Array Management, selecione **Import**.

   Uma caixa de diálogo é aberta para importar o(s) arquivo(s) de certificado.

3. Clique nos botões **Procurar** para primeiro selecionar os arquivos de certificado raiz e intermediário e, em seguida, selecione cada certificado de servidor para os controladores. Os arquivos raiz e intermediário são os mesmos para ambos os controladores. Somente os certificados de servidor são exclusivos para cada controlador. Se você gerou o CSR a partir de uma ferramenta externa, você também deve importar o arquivo de chave privada que foi criado junto com o CSR.

   Os nomes dos arquivos são exibidos na caixa de diálogo.

4. Clique em **Importar**.

   Os arquivos são carregados e validados.

Resultado

A sessão é encerrada automaticamente. Você deve fazer login novamente para que os certificados entrem em vigor. Ao fazer login novamente, os novos certificados assinados pela CA são usados para sua sessão.

Redefinir certificados de gerenciamento em SANtricity System Manager

Você pode reverter os certificados nos controladores de certificados assinados por CA para os certificados autoassinados definidos de fábrica.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Os certificados assinados pela CA devem ser importados previamente.

Sobre esta tarefa

A função Reset exclui os arquivos de certificado assinados pela CA de cada controlador. Os controladores voltarão então a usar certificados autoassinados.

Passos

1. Selecione **Configurações › Certificados**.
2. Na guia Array Management, selecione **Reset**.

   Uma caixa de diálogo Confirm Reset Management Certificates será aberta.

3. Digite `reset` no campo e clique em **Redefinir**.

   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 ocorre quando você volta a usar certificados autoassinados. Para limpar a condição que está bloqueando o acesso ao destino, você deve limpar os dados de navegação do navegador.

Resultados

Os controladores voltam a usar certificados autoassinados. Como resultado, o sistema solicita aos usuários que aceitem manualmente o certificado autoassinado para suas sessões.

Visualizar informações do certificado importado no SANtricity System Manager

Na página Certificados, você pode visualizar o tipo de certificado, a autoridade emissora e o intervalo de datas de validade dos certificados para o array de storage.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.

Passos

1. Selecione **Configurações › Certificados**.
2. Selecione uma das abas para visualizar informações sobre os certificados.

Aba	Descrição
Gerenciamento de array	Visualize informações sobre os certificados assinados pela CA importados para cada controlador, incluindo o arquivo root, o(s) arquivo(s) intermediate e o(s) arquivo(s) server.
Confiável	Visualize informações sobre todos os outros tipos de certificados importados para os controladores. Use o campo de filtro em **Mostrar certificados que são…** para visualizar certificados instalados pelo usuário ou pré-instalados. • **Instalados pelo usuário** — Certificados que um usuário carregou para o array de storage, que podem incluir certificados confiáveis quando o controlador atua como cliente (em vez de servidor), certificados LDAPS e certificados de Federação de Identidade. • **Pré-instalado** — Certificados autoassinados incluídos com o array de storage.
Gerenciamento de chaves	Veja informações sobre os certificados assinados pela CA importados para um servidor de gerenciamento de chaves externo.

Importar certificados para controladores ao atuar como clientes no SANtricity System Manager

Se o controlador rejeitar uma conexão por não conseguir validar a cadeia de confiança de um servidor de rede, você pode importar um certificado da guia Trusted que permite ao controlador (atuando como cliente) aceitar comunicações desse servidor.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Os arquivos de certificado estão instalados no seu sistema local.

Sobre esta tarefa

Pode ser necessário importar certificados da guia Confiáveis se você quiser permitir que outro servidor entre em contato com os controladores (por exemplo, um servidor LDAP ou um servidor syslog que usa TLS).

Passos

1. Selecione **Configurações › Certificados**.
2. Na aba Trusted, selecione **Importar**.

   Uma caixa de diálogo é aberta para importar os arquivos de certificado confiáveis.

3. Clique em **Procurar** para selecionar os arquivos de certificado dos controladores.

   Os nomes dos arquivos são exibidos na caixa de diálogo.

4. Clique em **Importar**.

Resultados

Os arquivos são carregados e validados.

${post_edited_translations.segment}

${post_edited_translations.segment}

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Um servidor DNS está configurado em ambos os controladores, o que permite o uso de um domínio totalmente qualificado para o servidor OCSP. Esta tarefa está disponível na página Hardware.
- Se você deseja especificar seu próprio servidor OCSP, você deve saber a URL desse servidor.

Sobre esta tarefa

A verificação automática de revogação é útil nos casos em que a CA emitiu um certificado indevidamente ou uma chave privada foi comprometida.

Durante essa tarefa, você pode configurar um servidor OCSP ou usar o servidor especificado no arquivo de certificado. O servidor OCSP determina se a CA revogou algum certificado antes da data de expiração programada e, em seguida, bloqueia o usuário de acessar um site se o certificado estiver revogado.

Passos

1. Selecione **Configurações › Certificados**.
2. Selecione a guia **Trusted**.

   Você também pode ativar a verificação de revogação na guia **Key Management**.

3. Clique em **Tarefas incomuns** e, em seguida, selecione **Ativar verificação de revogação** no menu suspenso.
4. Selecione **Desejo ativar a verificação de revogação**, para que uma marca de seleção apareça na caixa de seleção e campos adicionais apareçam na caixa de diálogo.
5. No campo **Endereço do servidor OCSP**, você pode opcionalmente inserir uma URL para um servidor OCSP. Se você não inserir um endereço, o sistema usará a URL do servidor OCSP do arquivo de certificado.
6. Clique em **Test Address** para garantir que o sistema consiga abrir uma conexão com o URL especificado.
7. Clique em **Salvar**.

Resultados

Se o array de storage tentar se conectar a um servidor com um certificado revogado, a conexão é negada e um evento é registrado.

Excluir certificados confiáveis no SANtricity System Manager

Você pode excluir os certificados instalados pelo usuário importados anteriormente da guia Confiáveis.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Se você estiver atualizando um certificado confiável para uma nova versão, o certificado atualizado deve ser importado antes de excluir o certificado antigo.

> Você pode perder o acesso a um sistema se excluir um certificado usado para autenticar os controladores e outro servidor, como um servidor LDAP, antes de importar um certificado de substituição.

Sobre esta tarefa

Esta tarefa descreve como excluir certificados instalados pelo usuário. Os certificados autoassinados pré-instalados não podem ser excluídos.

Passos

1. Selecione **Configurações › Certificados**.
2. Selecione a guia **Trusted**.

   A tabela mostra os certificados confiáveis do array de storage.
3. Na tabela, selecione o certificado que você deseja remover.
4. Clique em **Tarefas incomuns › Excluir**.

   Uma caixa de diálogo Confirmar Exclusão de Certificado Confiável é aberta.
5. Digite `delete` no campo e clique em **Excluir**.

Use certificados assinados por CA para autenticação com um servidor de gerenciamento de chaves no SANtricity System Manager

Para garantir a comunicação segura entre um servidor de gerenciamento de chaves e os controladores do array de storage, você deve configurar os conjuntos de certificados apropriados.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.

Sobre esta tarefa

A autenticação entre os controladores e um servidor de gerenciamento de chaves é um procedimento de duas etapas.

Etapa 1: preencha e envie o CSR para autenticação com um servidor de gerenciamento de chaves

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR) e, em seguida, usar o CSR para solicitar um certificado de cliente assinado de uma autoridade de certificação (CA) confiável pelo servidor de gerenciamento de chaves. Você também pode criar e baixar um certificado de cliente do servidor

de gerenciamento de chaves usando o arquivo CSR baixado. Um certificado de cliente valida os controladores do array de storage, permitindo que o servidor de gerenciamento de chaves confie em suas solicitações do Key Management Interoperability Protocol (KMIP).

> Os arquivos CSR gerados externamente por meio de pares de chaves pública e privada podem ser importados através da caixa de diálogo Criar Chave de Segurança Externa. Para obter mais informações sobre como importar um arquivo CSR gerado externamente, consulte "Etapa 2: importar certificados para o servidor de gerenciamento de chaves".

Passos

1. Selecione **Configurações › Certificados**.
2. Na guia Key Management, selecione **Complete CSR**.
3. Insira as seguintes informações:
   - **Nome comum** — Um nome que identifica o cliente. É prática comum que o nome comum corresponda aos requisitos do servidor KMS para convenções de nomenclatura de certificados de cliente. O nome comum geralmente ajuda o KMS a identificar o certificado do cliente quando este é apresentado durante um handshake.
   - **Organização** — O nome completo e legal da sua empresa ou organização. Inclua sufixos, como Inc. ou Corp.
   - **Unidade organizacional (opcional)** — A divisão da sua organização que está lidando com o certificado.
   - **Cidade/Localidade** — A cidade ou localidade onde sua organização está localizada.
   - **Estado/Região (opcional)** — O estado ou região onde sua organização está localizada.
   - **Código ISO do país** — O código ISO (International Organization for Standardization) de dois dígitos, como US, onde sua organização está localizada.
4. Clique em **Download**.

   Um arquivo CSR é salvo em seu sistema local.

5. Solicite um certificado de cliente assinado pela CA que seja confiável para o servidor de gerenciamento de chaves.

   > É comum que o servidor de gerenciamento de chaves possua um recurso que gera certificados assinados diretamente, pois funciona como sua própria CA.

6. Quando você tiver um certificado de cliente, acesse Etapa 2: importar certificados para o servidor de gerenciamento de chaves.

Etapa 2: importar certificados para o servidor de gerenciamento de chaves

Como próximo passo, você importa certificados para autenticação entre o array de storage e o servidor de gerenciamento de chaves. Existem dois tipos de certificados: o certificado do cliente valida os controladores do array de storage, enquanto o certificado do servidor de gerenciamento de chaves valida o servidor. Você deve carregar tanto o arquivo de certificado do cliente para os controladores quanto o arquivo de certificado do servidor para o servidor de gerenciamento de chaves.

Antes de começar

- Você possui um arquivo de certificado de cliente assinado (consulte Etapa 1: preencha e envie o CSR para autenticação com um servidor de gerenciamento de chaves), e copiou esse arquivo para o host onde

está acessando System Manager. Um certificado de cliente valida os controladores do array de storage, permitindo que o servidor de gerenciamento de chaves confie em suas solicitações do Key Management Interoperability Protocol (KMIP).

- Você deve obter um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando System Manager. Um certificado de servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, então o array de storage pode confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

> Para obter mais informações sobre o certificado do servidor, consulte a documentação do seu key management server.

Passos

1. Selecione **Configurações › Certificados**.
2. Na guia Key Management, selecione **Import**.

   Uma caixa de diálogo é aberta para importar os arquivos de certificado.

3. Ao lado de **Selecionar certificado do cliente**, clique no botão **Procurar** para selecionar o arquivo de certificado do cliente para os controladores do array de storage.

   O nome do arquivo é exibido na caixa de diálogo.

4. Se você gerou um arquivo de certificado externamente usando um par de chaves privada e pública, clique no botão **Procurar** ao lado de **Selecionar arquivo de chave privada** para selecionar o arquivo de certificado para os controladores do array de storage.

   O nome do arquivo é exibido na caixa de diálogo.

5. Ao lado de **Selecionar certificado do servidor de gerenciamento de chaves**, clique no botão **Procurar** para selecionar o arquivo de certificado do servidor para o seu servidor de gerenciamento de chaves. Você pode escolher um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

   O nome do arquivo é exibido na caixa de diálogo.

6. Clique em **Importar**.

   Os arquivos são carregados e validados.

Exportar certificados do servidor de gerenciamento de chaves no SANtricity System Manager

Você pode salvar um certificado para um servidor de gerenciamento de chaves na sua máquina local.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Os certificados devem ser importados previamente.

Passos

1. Selecione **Configurações › Certificados**.
2. Selecione a guia **Gerenciamento de Chaves**.
3. Na tabela, selecione o certificado que deseja exportar e clique em **Export**.

   Uma caixa de diálogo Salvar é aberta.

4. Digite um nome de arquivo e clique em **Save**.

Informações sobre direitos autorais

Informações sobre marcas comerciais