Usando Vamos Criptografar Certificados com o Cisco Business Dashboard e Validação de DNS

Objetivo

Este documento explica como obter um certificado *Vamos Criptografar* e instalá-lo no Cisco Business Dashboard usando a CLI (Command Line Interface, interface de linha de comando). Se desejar informações gerais sobre como gerenciar certificados, confira o artigo Gerenciar certificados no Cisco Business Dashboard.

Introduction

Vamos criptografar é uma autoridade de certificado que fornece certificados SSL gratuitos de DV (Domain Validation, validação de domínio) para o público usando um processo automatizado. *Vamos Criptografar* fornece um mecanismo de fácil acesso para obter certificados assinados para servidores Web, dando ao usuário final a confiança de que eles estão acessando o serviço correto. Para obter mais informações sobre *Vamos Criptografar*, visite o site Vamos Criptografar.

Usar certificados *Vamos Criptografar* com o Cisco Business Dashboard é razoavelmente simples. Embora o Cisco Business Dashboard tenha alguns requisitos especiais para a instalação de certificado além de apenas disponibilizar o certificado para o servidor web, ainda é possível automatizar a emissão e a instalação do certificado usando as ferramentas de linha de comando fornecidas.

Para emitir e renovar certificados automaticamente, o servidor Web Painel deve estar acessível a partir da Internet. Se esse não for o caso, um certificado pode ser facilmente obtido usando um processo manual e instalado usando as ferramentas de linha de comando. O restante deste documento passa pelo processo de emissão de um certificado e instalação nele.

Se o servidor Web do Painel estiver acessível da Internet nas portas padrão TCP/80 e TCP/443, é possível automatizar o processo de instalação e gerenciamento de certificados. Confira Vamos criptografar o Cisco Business Dashboard para obter detalhes.

Passo 1

A primeira etapa é obter o software que usa o certificado do protocolo ACME. Neste exemplo, estamos usando o cliente certbot, mas há muitas outras opções disponíveis.

Para obter o cliente de certbot, use o Painel ou outro host que execute um sistema operacional tipo Unix (por exemplo, Linux, macOS) e siga as instruções no cliente de certbot para instalar o cliente. Nos menus suspensos nesta página, selecione *Nenhum dos itens acima* para software e seu SO preferido para sistema.

Éimportante observar que neste artigo, seções azuis são prompts e saídas da CLI. O `texto branco` lista comandos. Comandos em cores verdes, incluindo dashboard.example.com, pnpserver.example.com, e user@example.com devem ser substituídos por nomes DNS adequados ao seu ambiente.

Para instalar o cliente do certbot no servidor do Cisco Business Dashboard, use os seguintes comandos:

```
cbd:~$sudo apt update cbd:~$sudo apt install software-properties-common cbd:~$sudo add-apt-repositório ppa:certbot/certbot cbd:~$sudo apt update cbd:~$sudo apt install certbot
```

Passo 2

Crie um diretório de trabalho para conter todos os arquivos associados ao certificado. Observe que esses arquivos incluem informações confidenciais, como a chave privada do certificado e os detalhes da conta do serviço *Vamos Criptografar*. Embora o cliente do certbot crie arquivos com permissões adequadamente restritivas, você deve garantir que o host e a conta que está sendo usada sejam restritos para acesso apenas a equipe autorizada.

Para criar o diretório no Painel, digite os seguintes comandos:

```
cbd:~$mkdir certbot cbd:~/certbot $cd certbot
```

Etapa 3

Solicite um certificado usando o seguinte comando:

```
cbd:~/certbot$certbot certonly — manual — preferenciais dns -d dashboard.example.com -d pnpserver.example.com
—logs-dir . —config-dir . —work-dir . —execute o gancho "cat ~/certbot/live/dashboard.example.com /fullchain.pem /etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem; /usr/bin/cisco-business-dashboard import -t pem -k ~/certbot/live/dashboard.example.com /privkey.pem -c /tmp/cbdchain.pem"
```

Este comando instrui o serviço *Vamos Criptografar* para validar a propriedade dos nomes de host fornecidos solicitando a criação de registros TXT de DNS para cada um dos nomes listados. Depois que os registros TXT tiverem sido criados, o serviço *Vamos Criptografar* confirma que os registros existem e, em seguida, emite o certificado. Finalmente, o certificado é aplicado ao painel usando o utilitário cisco-business-dashboard.

Os parâmetros no comando são necessários pelas seguintes razões:

certonly	Solicite um certificado e baixe os arquivos. Não tente instalá-los. No caso do Cisco Business Dashboard, o certificado não é usado apenas pelo servidor Web, mas também pelo serviço PnP e outras funções. Como resultado, o cliente do certbot não consegue instalar o certificado automaticamente.
--manual	Não tente autenticar automaticamente com o serviço *Vamos Criptografar*. Trabalhe interativamente com o usuário para se autenticar.
—preferido-desafia dns	Autentique usando registros TXT DNS.
-d dashboard.example.com -d pnpserver.example.com	Os FQDNs que devem ser incluídos no certificado. O nome listado será incluído no campo Nome comum do certificado, e todos os nomes serão listados no campo Assunto-Alt-Nome. O nome pnpserver.<domain> é um nome especial usado pelo recurso Network Plug and Play ao executar a descoberta de DNS. Consulte o Cisco Business Dashboard Administration Guide para obter mais detalhes.
—logs-dir . —config-dir . —work-dir .	Use o diretório atual para todos os arquivos de trabalho criados durante o processo.
—Deployment-hook "..."	Use o utilitário de linha de comando cisco-business-dashboard para pegar a chave privada e a cadeia de

certificados recebidos do serviço *Vamos Criptografar* e carregá-los no aplicativo de painel da mesma forma como se os arquivos fossem carregados através da Interface de Usuário (UI) do Painel.

O certificado raiz que ancora a cadeia de certificados também é adicionado ao arquivo de certificado aqui. Isso é exigido por determinadas plataformas sendo implantadas usando Network Plug and Play.

A instalação automática do certificado usando a opção —Deployment-hook só é possível quando o cliente do certbot está sendo executado no servidor do painel. Se o cliente do certbot estiver sendo executado em um computador diferente, a chave privada e os arquivos de certificado da cadeia completa devem ser copiados para o servidor do painel e instalados usando os comandos:

-cat <arquivo de certificado completo> /etc/ssl/certs/DST_Root_CA_X3.pem >/tmp/cbdchain.pem

cisco-business-dashboard import -t pem -k <private key file> -c /tmp/cbdchain.pem

Passo 4

Execute o processo de criação do certificado seguindo as instruções geradas pelo cliente do certbot:

```
cbd:~/certbot$certbot certonly — manual — preferenciais dns -d dashboard.example.com -d
pnpserver.example.com
—logs-dir . —config-dir . —work-dir . —execute o gancho "cat ~/certbot/live/
dashboard.example.com /fullchain.pem /etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem;
/usr/bin/cisco-business-dashboard import -t pem -k ~/certbot/live/dashboard.example.com
/privkey.pem -c tmp/cbdchain.pem"
Salvando o log de depuração em /home/cisco/certbot/letsencrypt.log
Plug-ins selecionados: Manual do Autenticador, Instalador Nenhum
```

Etapa 5

Digite o endereço de e-mail ou **C** para Cancelar.

```
Insira o endereço de e-mail (usado para renovações urgentes e avisos de segurança) (Digite 'c'
para cancelar): user@example.com
Iniciando nova conexão HTTPS (1): acme-v02.api.letsencrypt.org
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Etapa 6

Digite **A** para concordar ou **C** para cancelar.

```
Leia os Termos de serviço em
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. Você deve
concordar para se registrar no servidor ACME em
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Digite A para concordar ou C para cancelar.
(A)Árvore/(C)Cancelar: R
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Etapa 7

Digite **Y** para Sim ou **N** para Não.

```
Você gostaria de compartilhar seu endereço de e-mail com a fronteira eletrônica
Fundação, parceiro fundador do projeto Vamos Criptografar e sem fins lucrativos
organização que desenvolve o Certbot? Gostaríamos de enviar um e-mail sobre nosso trabalho
criptografando a web, as notícias do EFF, as campanhas e as maneiras de apoiar a liberdade
digital.
Digite Y para Sim ou N para Não.
(S)es/(N)o: Y
Obtendo um novo certificado
Realizando os seguintes desafios:
desafio dns-01 para dashboard.example.com
desafio dns-01 para pnpserver.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Passo 8

Digite **Y** para Sim ou **N** para Não.

```
NOTE: O IP desta máquina será registrado publicamente como tendo solicitado isto
certificado. Se você estiver executando o certbot no modo manual em uma máquina que não esteja
seu servidor, por favor, certifique-se de que está bem com isso.
Você está bem com seu IP sendo registrado?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Digite Y para Sim ou N para Não.
(S)es/(N)o: Y
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Implante um registro TXT DNS com o nome
_acme-Challenge.dashboard.example.com com o seguinte valor:
3AzDTqNGXb8kSkhqXXYWE2iZrFAVCGT2B8oZNGyBwhc
```

Passo 9

Um registro TXT DNS para validar a propriedade do nome de host dashboard.example.com deve ser criado na infraestrutura DNS. As etapas necessárias para fazer isso estão fora do escopo deste documento e dependerão do provedor de DNS sendo usado. Depois de criado, valide se o registro está disponível usando uma ferramenta de consulta DNS, como Dig.

O processo de desafio de DNS pode ser automatizado para determinados provedores de DNS. Consulte Plug-ins DNS para obter mais detalhes.

Pressione **Enter** no teclado.

```
Antes de continuar, verifique se o registro está implantado.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Pressione Enter para continuar
```

Passo 10

Você receberá uma saída CLI semelhante. Crie e verifique registros TXT adicionais para cada nome a ser incluído no certificado. Repita a Etapa 9 para cada nome especificado no comando certbot.

Pressione **Enter** no teclado.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Implante um registro TXT DNS com o nome
_acme-Challeng.pnpserver.example.com com o seguinte valor:
Txruc89x8dVaHmLHJII0oA2ILmIY83XYl13yYakjNuc
Antes de continuar, verifique se o registro está implantado.
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Pressione Enter para continuar
```

Passo 11

O certificado foi emitido e pode ser encontrado no subdiretório *ao vivo* no sistema de arquivos:

```
Aguardando verificação...
Desafios de limpeza
Caminho(s) fora do padrão; pode não funcionar com crontab instalado pelo gerenciador de pacotes
do sistema operacional
Executando o comando Deployment-hook: cat ~/certbot/live/dashboard.example.com/fullchain.pem
/etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem; /usr/bin/cisco-business-dashboard import
-t pem -k ~/certbot/live/dashboard.example.com/privkey.pem -c /tmp/cbdchain.pem
NOTAS IMPORTANTES:
- Parabéns! Seu certificado e sua cadeia foram salvos em:
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem
Seu arquivo de chave foi salvo em:
/home/cisco/certbot/live/dashboard.example.com/privkey.pem
Seu certificado expirará em 2020-11-11. Para obter um novo
versão deste certificado no futuro, basta executar o certbot
novamente. Para renovar *todos* os certificados de forma não interativa, execute
"certbot renew"
- Suas credenciais de conta foram salvas em seu Certbot
diretório de configuração em /home/cisco/certbot. Você deveria fazer um
backup seguro desta pasta agora. Este diretório de configuração irá
também contêm certificados e chaves privadas obtidas pelo Certbot
fazer backups regulares desta pasta é ideal.
- Se você gosta do Certbot, considere apoiar nosso trabalho:
Doando para ISRG / Vamos criptografar: https://letsencrypt.org/donate
Doando para o EFF: https://eff.org/donate-le
```

Etapa 12

Insira os seguintes comandos:

```
cbd:~/certbot$cd live/dashboard.example.com/ cbd:~/certbot/live/dashboard.example.com$ls
cert.pem chain.pem fullchain.pem privkey.pem README
```

O diretório que contém os certificados tem permissões restritas para que somente o usuário da cisco possa visualizar os arquivos. O arquivo *privkey.pem*, em particular, é sensível e o acesso a esse arquivo deve ser restrito apenas a pessoal autorizado.

O painel deve estar em execução com o novo certificado. Se você abrir a Interface de Usuário (UI) do Painel em um navegador da Web inserindo qualquer um dos nomes especificados ao criar o certificado na barra de endereços, o navegador da Web deverá indicar que a conexão é confiável e segura.

Observe que os certificados emitidos por *Vamos Criptografar* têm períodos de vida relativamente curtos - atualmente 90 dias. Para garantir que o certificado permaneça válido, você precisará repetir o processo descrito acima antes que os 90 dias estejam prontos.

Para obter mais informações sobre o uso do cliente certbot, consulte a página de documentação do certbot.