Usando Vamos Criptografar Certificados com o Cisco Business Dashboard

Objetivo

Este documento explica como obter um certificado *Vamos Criptografar*, instalá-lo no Cisco Business Dashboard e configurar a renovação automática 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.

O processo descrito neste documento foi automatizado no Cisco Business Dashboard versão 2.2.2 e posterior. Consulte a seção Sistema > Gerenciamento de certificados do Guia de administração para obter mais informações.

Introduction

Vamos criptografar é uma autoridade de certificação que fornece certificados SSL (Secure Sockets Layer) de validação de domínio (DV) gratuitos 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, visite o site Let's Encrypt.

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. O restante deste documento passa pelo processo de emissão de um certificado e automatização da renovação do certificado.

Este documento usa desafios HTTP para validar a propriedade do domínio. Isso exige que o servidor Web do Painel esteja acessível da Internet nas portas padrão TCP/80 e TCP/443. Se o servidor Web não puder ser acessado pela Internet, considere usar os desafios de DNS. Confira o uso de Vamos criptografar o Cisco Business Dashboard com DNS 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.

Passo 2

Para permitir que a renovação do certificado seja automatizada, o cliente do certbot deve ser instalado no Painel. Para instalar o cliente do certbot no servidor do Painel, use os seguintes comandos:

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.

```
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
```

Etapa 3

Em seguida, o servidor Web do Painel precisa ser configurado para hospedar os arquivos de desafio necessários para verificar a propriedade do nome do host. Para fazer isso, criamos um diretório para esses arquivos e atualizamos o arquivo de configuração do servidor web. Em seguida, reiniciamos o aplicativo Painel para que as alterações entrem em vigor. Use os seguintes comandos:

```
cbd:~$sudo mkdir /usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:~$ sudo chmod 755
/usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:~$sudo bash -c 'cat >
/var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf' << EOF
# Localização para arquivos de desafio criados pela localização do certbot /.bem conhecido/acme-
Challenge {
root/usr/lib/ciscobusiness/dashboard/www/letsencrypt;
}
EOF
cbd:~$ cbd:~$sudo chown cbd:cbd /var/lib/ciscobusiness/dashboard/nginx/nginx-loc-
letsencrypt.conf cbd:~$ sudo chmod 640 /var/lib/ciscobusiness/dashboard/nginx/nginx-loc-
letsencrypt.conf cbd:~$cisco-business-dashboard stop cbd:~$cisco-business-dashboard start
```

Passo 4

Solicite um certificado usando o seguinte comando:

```
cbd:~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com —Deployment-hook "cat /etc/letsencrypt/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 /etc/letsencrypt/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 pela conexão com o serviço Web hospedado em cada um dos nomes. Isso significa que o serviço Web do painel deve estar acessível da Internet e hospedado nas portas 80 e 443. O acesso ao aplicativo do painel pode ser restringido usando as configurações de Controle de Acesso na página Sistema > Configurações da Plataforma > Servidor Web na Administração do painel Interface de Usuário (UI). Consulte o Cisco Business Dashboard Administration Guide para obter mais informações.

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.
—Webroot -w ...	Instale os arquivos de desafio no diretório criado acima para que eles possam ser acessados pelo servidor Web do painel.
-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

—Deployment-hook "..."	Guide para obter mais detalhes. 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.

Etapa 5

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

```
cbd:~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com —Deployment-hook "cat /etc/letsencrypt/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 /etc/letsencrypt/live/dashboard.example.com
/privkey.pem -c /tmp/cbdchain.pem"
Salvando o log de depuração em /var/log/letsencrypt/letsencrypt.log
Plug-ins selecionados: Authenticator Webroot, Installer None
```

Etapa 6

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

```
Insira o endereço de e-mail (usado para renovação urgente e avisos de segurança) (Digite 'c'
para
cancelar): user@example.com
```

Etapa 7

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
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)Árvore/(C)Cancelar: R
```

Passo 8

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

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Você gostaria de compartilhar seu endereço de e-mail com a fronteira eletrônica
A Fundação, parceira fundadora do projeto Let's Encrypt e a organização 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.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(S)es/(N)o: Y
```

Passo 9

O certificado foi emitido e pode ser encontrado no subdiretório */etc/letsencrypt/live* no sistema de arquivos:

```
Obtendo um novo certificado
Realizando os seguintes desafios:
desafio http-01 para dashboard.example.com
desafio http-01 para pnpserver.example.com
Usando o caminho do webroot /usr/lib/ciscobusiness/dashboard/www/letsencrypt para todos os
domínios sem correspondência.
Aguardando verificação...
Desafios de limpeza
Executando o comando Deployment-hook: cat
/etc/letsencrypt/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
/etc/letsencrypt/live/dashboard.example.com/privkey.pem -c /tmp/cbdchain.pem
NOTAS IMPORTANTES:
- Parabéns! Seu certificado e sua cadeia foram salvos em:
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem
Seu arquivo de chave foi salvo em:
/etc/letsencrypt/live/dashboard.example.com/privkey.pem
Seu certificado expirará em 2020-10-29. 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 /etc/letsencrypt. 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
cbd:~$ sudo ls /etc/letsencrypt/live/dashboard.example.com
/ cert.pem chain.pem fullchain.pem privkey.pem README
cbd:~$
```

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

Passo 10

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. O pacote de certificado para Ubuntu Linux está configurado para verificar a validade do certificado duas vezes por dia e renová-lo se estiver prestes a expirar, portanto, não é necessário tomar nenhuma ação para manter o certificado atualizado. Para

verificar se as verificações periódicas estão ocorrendo corretamente, aguarde pelo menos doze horas depois de criar o certificado inicialmente e, em seguida, verifique se há mensagens semelhantes ao seguinte no arquivo de log do certbot: `cbd:~$ sudo tail /var/log/letsencrypt/letsencrypt.log`

```
2020-07-31 16:50:52,783:DEBUG:certbot.main:certbot version: 0.31.0
2020-07-31 16:50:52,784:DEBUG:certbot.main:Argumentos: ['-q']
2020-07-31 16:50:52.785:DEBUG:certbot.main:Plug-ins descobertos:
(PluginEntryPoint#manual,
PluginEntryPoint#null,PluginEntryPoint#independente,PluginEntryPoint#webroot)
2020-07-31 16:50:52,793:DEBUG:certbot.log:Nível de log da raiz definido em 30
2020-07-31 16:50:52,793:INFO:certbot.log:Salvando o log de depuração em
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,802:DEBUG:certbot.plugins.select:
Autenticador solicitado <certbot.cli.
_Objeto padrão em 0x7f1152969240> e instalador <certbot.cli.
_Objeto padrão em 0x7f1152969240>
2020-07-31 16:50:52,811:INFO:certbot.renew:Cert ainda não está prestes a ser renovado
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.select:Requested authenticator
Webroot e instalador Nenhum
2020-07-31 16:50:52,812:DEBUG:certbot.renovação:sem falhas de renovação
```

Depois de ter passado tempo suficiente para que a data de vencimento do certificado fosse dentro de trinta dias, o cliente do certbot renovará o certificado e aplicará o certificado atualizado ao aplicativo do painel automaticamente.

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