Expiração do certificado e inscrição automática para reinscrição automática no Cisco IOS CA

Contents

Introduction

Todos os certificados digitais têm um tempo de expiração incorporado no certificado atribuído pelo servidor de autoridade de certificação (AC) emissor durante a inscrição. Quando um certificado digital é usado para a autenticação IPSec de VPN do ISAKMP, há uma verificação automática do tempo de expiração do certificado do dispositivo de comunicação e da hora do sistema no dispositivo (ponto de extremidade de VPN). Isso garante que um certificado usado é válido e não expirou. É também por isso que você *deve* configurar o relógio interno em cada ponto final de VPN (roteador). Se o Network Time Protocol (NTP) (ou Simple Network Time Protocol [SNTP]) não for possível nos roteadores de criptografia VPN, use o comando manual **set clock**.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas em todos os roteadores que executam a imagem cXXXX-advsecurityk9-mz.123-5.9.T para essa respectiva plataforma .

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Quando um certificado digital é considerado expirado ou não expirou?

- Um certificado expirou (inválido) se a hora do sistema for posterior à hora de expiração do certificado ou antes da hora de emissão do certificado.
- Um certificado não expirou (válido) se a hora do sistema for igual ou entre a hora de emissão do certificado e a hora de expiração do certificado.

A finalidade do recurso de inscrição automática é fornecer ao administrador de CA um mecanismo para permitir que um roteador atualmente inscrito se inscreva automaticamente em seu servidor de CA em um percentual configurado do tempo de vida do certificado do roteador. Este é um recurso importante para a capacidade de gerenciamento/suporte dos certificados como um mecanismo de controle. Se você usou uma CA específica para emitir certificados para, potencialmente, milhares de roteadores VPN de filial com um ano de vida (sem inscrição automática), em exatamente um ano do tempo emitido, todos os certificados expiram e todas as filiais perdem a conectividade através do IPSec. Como alternativa, se o recurso de inscrição automática estiver definido como "autoregistrar 70", como neste exemplo, em 70% do tempo de vida do certificado emitido (1 ano), cada roteador emite automaticamente uma nova solicitação de inscrição para o servidor Cisco IOS® CA listado no ponto de confiança.

Observação: uma exceção ao recurso de inscrição automática é que se estiver definido como *menor ou igual a 10*, ele estará em minutos. Se for *maior que 10*, então é uma porcentagem do tempo de vida do certificado.

Há algumas advertências que o administrador da CA do Cisco IOS precisa saber com a inscrição automática. O administrador precisa executar estas ações para que a reinscrição seja bem-sucedida:

1. Conceda ou rejeite manualmente cada solicitação de reinscrição no servidor de CA do Cisco IOS (a menos que "grant auto" seja usado no servidor de CA do Cisco IOS).O servidor de CA do Cisco IOS ainda precisa conceder ou rejeitar cada uma dessas solicitações (com a suposição de que a CA do Cisco IOS não tem "grant auto" ativado). No entanto, nenhuma ação administrativa no roteador que se registra é necessária para iniciar o processo de reinscrição.
2. Salve o novo certificado reinscrito no roteador VPN de reinscrição, se apropriado.Se não houver alterações de configuração não salvas pendentes no roteador, o novo certificado será automaticamente salvo na RAM não volátil (NVRAM). O novo certificado é gravado na NVRAM e o certificado anterior é removido.Se houver alterações de configuração não salvas pendentes, você deverá emitir o comando **copy run start** no roteador que se registra para salvar as alterações de configuração e o novo certificado reinscrito na NVRAM. Quando o comando **copy run start** é concluído, o novo certificado é gravado na NVRAM e o certificado anterior é removido.**Observação:** quando uma nova reinscrição é bem-sucedida, isso *não* revoga o certificado anterior para esse dispositivo inscrito no servidor CA. Quando os dispositivos VPN se comunicam, eles enviam um ao outro o número de série do certificado (um número exclusivo).**Observação:** por exemplo, se você estiver em 70% do tempo de vida do certificado e uma ramificação VPN tiver que se inscrever novamente na CA, essa CA terá dois certificados para esse nome de host. No entanto, o roteador que se registra tem apenas um (o mais novo). Se optar por isso, você poderá revogar administrativamente o certificado antigo ou permitir que ele expire normalmente.**Observação:** as versões de código mais recentes do recurso de inscrição automática têm a opção de "regenerar" os pares de chaves

usados para a inscrição.Esta opção é "não padrão" para regenerar pares de chaves.Se essa opção foi escolhida, saiba o bug da Cisco ID CSCea90136. Essa correção de bug permite que o novo par de chaves seja colocado em arquivos temporários enquanto a nova inscrição de certificado ocorre em um túnel IPSec existente (que está usando o par de chaves antigo).A inscrição automática tem a opção de gerar novas chaves no momento da renovação da certificação. Atualmente, isso causa uma perda de serviço durante o tempo necessário para obter um novo certificado. Isso ocorre porque há uma nova chave, mas não há certificado correspondente a ela.Este recurso mantém a chave antiga e o certificado até que o novo certificado esteja disponível.A geração automática de chave também é implementada para inscrição manual. As chaves são geradas (conforme necessário) para inscrição automática ou manual.Versão encontrada - 12.3PIH03Versão a ser corrigida em - 12.3TVersão aplicada a - 12.3PI03Integrado - NenhumPara obter mais informações, entre em contato com o Suporte Técnico da Cisco.

Informações Relacionadas

- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems