证书到期和自动注册的自动重新注册到Cisco IOS CA

目录

简介

所有数字证书在注册期间由颁发证书颁发机构(CA)服务器分配的证书中都有内置的过期时间。当数字证书用于ISAKMP的VPN IPSec身份验证时，会自动检查通信设备的证书过期时间和设备（VPN终端）上的系统时间。 这可确保使用的证书有效且未过期。这也是您必须在每*个VPN*终端（路由器）上设置内部时钟的原因。 如果VPN加密路由器上不能使用网络时间协议(NTP)（或简单网络时间协议[SNTP]），则使用手动**set clock**命令。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于为相应平台运行cXXXX-advsecurityk9-mz.123-5.9.T映像的所有路由器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

数字证书何时被视为过期或未过期？

- 如果系统时间在证书到期时间之后或证书的签发时间之前，则证书已过期（无效）。

- 如果系统时间在证书的签发时间或证书的过期时间之间，则证书未过期（有效）。

Auto-enroll（自动注册）功能旨在为CA管理员提供一种机制，允许当前注册的路由器在路由器证书的已配置生命周期百分比上自动向其CA服务器重新注册。这是证书作为控制机制的可管理性/可支持性的重要功能。如果您使用特定CA向可能有数千个分支VPN路由器颁发证书，其寿命为一年（无自动注册），则在颁发时间的整整一年内，所有证书都将过期，所有分支机构都会通过IPSec失去连接。或者，如果自动注册功能设置为“自动注册70”（如本例中所示），则在已颁发证书（1年）的70%生命期内，每台路由器会自动向信任点中列出的Cisco IOS® CA服务器发出新注册请求。

注：自动登记功能的一个例外是，如果设置为小于或等于*10，则*它以分钟为单位。如果大于*10,*则表示证书生命期的百分比。

Cisco IOS CA管理员在自动注册时需要注意一些警告。管理员需要执行以下操作才能成功重新注册：

1. 手动授予或拒绝Cisco IOS CA服务器上的每个重新注册请求（除非Cisco IOS CA服务器上使用“grant auto”）。Cisco IOS CA服务器仍需要授予或拒绝这些请求中的每个请求（假设Cisco IOS CA未启用“grant auto”）。 但是，启动重新注册过程无需对注册路由器执行任何管理操作。
2. 在重新注册VPN路由器中保存新的重新注册证书（如果适用）。如果路由器中没有未保存的配置更改挂起，则新证书将自动保存到非易失性RAM(NVRAM)。 新证书写入NVRAM，并删除之前的证书。如果有未保存的配置更改挂起，则必须在注册路由器上发出**copy run start**命令，以便将配置更改和新的重新注册证书保存到NVRAM中。完成**copy run start命**令后，新证书将写入NVRAM，并删除之前的证书。**注意：**当新的重新注册成功时，不会*撤*销CA服务器上该注册设备的先前证书。当VPN设备通信时，它们会相互发送证书序列号（唯一编号）。**注意：**例如，如果您处于证书生命期的70%，并且VPN分支机构要向CA重新注册，则该CA具有该主机名的两个证书。但是，注册路由器只有一个（较新的）。 如果选择，可以管理性撤销旧证书，或允许其正常过期。**注意：**较新的代码版本的“自动注册”(Auto-enroll)功能具有“重新生成”用于注册的密钥对的选项。此选项为“不默认”以重新生成密钥对。如果选择此选项，请注意Cisco Bug ID CSCea90136。此Bug修复允许在新证书注册通过现有IPSec隧道（使用旧密钥对）时将新密钥对放入临时文件中。Auto-enroll可选择在认证续约时生成新密钥。目前，这会导致在获取新证书所需的时间内丢失服务。这是因为有新密钥，但没有与其匹配的证书。此功能将保留旧密钥和证书，直到新证书可用。自动密钥生成也用于手动注册。生成密钥（根据需要）以进行自动或手动注册。找到的版本 — 12.3PIH03要修复的版本 — 12.3T应用于 — 12.3PI03的版本集成 — 无有关其他信息，请联系思科技术支持。

相关信息

- IPSec 支持页面
- 技术支持 - Cisco Systems