Certificaatbeëindiging en automatische inschrijving voor automatische herinschrijving op Cisco IOS CA

Inhoud

Inleiding

Alle digitale certificaten hebben een ingebouwde verlooptijd in het certificaat die tijdens de inschrijving wordt toegewezen door de server van de instantie van afgifte (CA). Wanneer een digitaal certificaat wordt gebruikt voor VPN-verificatie van ISAKMP, is er een automatische controle van de verlooptijd van het certificaat van het communicatiemiddel en de systeemtijd op het apparaat (VPN-eindpunt). Dit waarborgt dat een gebruikt certificaat geldig is en niet is verlopen. Het is ook waarom u de interne kloktijd op elk VPN-eindpunt (router) *moet* instellen. Als Network Time Protocol (NTP) (of Simple Network Time Protocol [SNTP]) niet mogelijk is op de VPN-cryptorouters, gebruikt u de handmatige **ingestelde** klokopdracht.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op alle routers die de cXXXX-adversie-k9-mz.123-5.9.T-afbeelding voor dat respectieve platform uitvoeren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Wanneer wordt een digitaal certificaat geacht te zijn verlopen of niet te zijn verlopen?

- Een certificaat is verlopen (ongeldig) als de systeemtijd na de verlooptijd van het certificaat of vóór de afgegeven tijd van het certificaat valt.
- Een certificaat is niet verlopen (geldig) indien de systeemtijd op of tussen de afgegeven tijd van het certificaat en de verlopen tijd van het certificaat ligt.

Het doel van de optie Auto-inschrijving is om de CA-beheerder een mechanisme te geven om een momenteel ingeschreven router toe te staan om automatisch opnieuw in te schrijven met zijn CA-server op een ingesteld percentage van de levensduur van het routercertificaat. Dit is een belangrijk kenmerk voor de beheersbaarheid/de ondersteunbaarheid van de certificaten als controlemechanisme. Als u een bepaalde CA gebruikte om certificaten uit te geven aan potentieel duizenden routers van tak VPN met een leven van één jaar (zonder Auto-inschrijving), dan in precies één jaar van de uitgegeven tijd, verlopen alle certificaten en alle takken verliezen connectiviteit door IPSec. In plaats hiervan geeft elke router automatisch een nieuw inschrijvingsverzoek uit aan de Cisco IOS® CA server die in het betrouwbaar punt is opgesomd, als de optie Auto-inschrijven 70" is ingesteld, zoals in dit voorbeeld, dan 70% van de levensduur van het uitgegeven certificaat (1 jaar).

Opmerking: Eén uitzondering op de optie Auto-inschrijven is dat als deze *op minder dan of gelijk aan 10* is ingesteld, dit in minuten is. Als het *meer dan 10* is, dan is het een percentage van de levensduur van het certificaat.

Er zijn een aantal voorbehouden waarvan de Cisco IOS CA-beheerder zich bewust moet zijn van de automatische inschrijving. De beheerder moet deze acties uitvoeren om de herinschrijving succesvol te laten zijn:

1. Geef elk herinschrijvingsverzoek handmatig op de Cisco IOS CA-server of verwerp het (tenzij "beurs" wordt gebruikt op de Cisco IOS CA-server).De Cisco IOS CA server moet nog steeds elk van deze verzoeken verlenen of afwijzen (met de veronderstelling dat Cisco IOS CA geen "subsidie auto" heeft ingeschakeld). Er is echter geen administratieve actie op de inschrijvende router vereist om het herregistratieproces te starten.
2. Sla het nieuwe heringevoerde certificaat op in de VPN-router die u opnieuw instelt, indien nodig.Als er geen onopgeslagen configuratieveranderingen in de router in behandeling zijn, dan wordt het nieuwe certificaat automatisch opgeslagen in Non-Volatile RAM (NVRAM). Het nieuwe certificaat wordt in NVRAM geschreven en het vorige certificaat wordt verwijderd.Als er niet-opgeslagen configuratieveranderingen in het wachten zijn, moet u de opdracht van de **loopstart van het kopieerprogramma** op de het registreren van de router uitgeven om de configuratieveranderingen en het nieuwe opnieuw ingeschreven certificaat in NVRAM op te slaan. Zodra de opdracht **Start** van **kopie** is voltooid, wordt het nieuwe certificaat in NVRAM geschreven en wordt het vorige certificaat verwijderd.**Opmerking:** Wanneer een nieuwe inschrijving succesvol is, trekt dat het vorige certificaat voor dat ingeschreven apparaat op de CA server *niet* in. Wanneer VPN-apparaten communiceren, verzenden ze elkaar het certificaatserienummer (een uniek nummer).**Opmerking:** Als u bijvoorbeeld 70% van de levensduur van het certificaat hebt en een VPN-tak is om opnieuw in te schrijven bij de CA, dan heeft CA twee certificaten voor die hostname. Hoe dan ook, de inrolrouter heeft er

slechts één (de nieuwere). Als u dit wenst, kunt u het oude certificaat administratief intrekken of het normaal laten verlopen.**Opmerking:** De nieuwere codeversies van de optie Auto-inschrijving hebben een optie om de key-paren die voor inschrijving zijn gebruikt te "regenereren".Deze optie is "geen standaard" om belangrijke paren te regenereren.Als deze optie geselecteerd is, moet u zich bewust zijn van Cisco bug-ID CSCea90136. Deze bug-oplossing maakt het mogelijk dat het nieuwe sleutelpaar in tijdelijke bestanden wordt gezet terwijl de nieuwe certificaatinschrijving plaats vindt via een bestaande IPSec-tunnel (dat het oude toetsenbord gebruikt).Automatische inschrijving heeft de optie om nieuwe sleutels te genereren bij certificatieverlenging. Op dit moment leidt dit tot verlies van betekening of kennisgeving gedurende de tijd die nodig is om een nieuw certificaat te verkrijgen. Dit komt doordat er een nieuwe sleutel is, maar geen certificaat dat bij het besluit past.Deze optie behoudt de oude toets en het oude certificaat totdat het nieuwe certificaat beschikbaar is.Automatische sleutelgeneratie wordt ook geïmplementeerd voor handmatige inschrijving. Er worden sleutels gegenereerd (indien nodig) voor automatische of handmatige inschrijving.Versie gevonden - 12.3PIH03Versie vast te stellen in - 12.3TVersie van toepassing op - 12.3PI03Geïntegreerd in - geenNeem voor extra informatie contact op met Cisco Technical Support.

Gerelateerde informatie

- IPsec-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen