Arranque seguro en un switch SX350X o SX550X

Objetivo

El propósito de este artículo es explicar el proceso de Secure Boot, un método para arrancar solamente con software confiable. Esta función se habilita comenzando con la versión 2.4.0.91 del firmware.

Si no está familiarizado con los siguientes términos, consulte Cisco Business: Glosario de nuevos términos.

Dispositivos aplicables

SX350X

SX550X

Versión del software

2.4.0.91

Introducción

Secure Boot es una manera de cargar y ejecutar una imagen segura usando una cadena de confianza para evitar cargar software no confiable. Se establece una cadena de confianza mediante la asignación de imágenes con claves privadas y el uso de mecanismos de hardware y software para verificar la imagen cargada. Esto permite a los usuarios asegurarse de que, al cargar el firmware del dispositivo, ninguna otra persona ha agregado un código que infringe la seguridad.

Cuando un usuario intenta cargar una nueva imagen, la nueva imagen se descarga en un archivo temporal, que se valida. En caso de error, se elimina el archivo temporal. De esta manera, si la nueva imagen no es válida, el proceso de instalación fallará y mostrará un mensaje de advertencia.

Si los switches se encuentran en una topología apilada

Cuando carga 2.4.0.91, o la última versión disponible, en el switch activo (primario), cargará el firmware en todos los miembros de la pila. Esto es independientemente del modelo de la familia, ya que es un requisito que todos los dispositivos ejecuten el mismo firmware. La pila funcionará normalmente.

Proceso de arranque seguro

Durante el arranque, el sistema imprimirá la información de Secure Boot en el terminal. Estos son los pasos a través de los que los dispositivos verifican antes del arranque seguro.

Memoria de sólo lectura de inicio (BootROM) valida *booton*

Booton valida el arranque universal (*Uboot)*

Uboot valida la *imagen ROS*

Si Secure Boot detecta una falla, impedirá que el dispositivo se inicie. Si esto ocurre, comuníquese con su Cisco Partner o Technical Assistance Center (TAC) para determinar los siguientes pasos a seguir en esta situación. Si necesita encontrar un partner de Cisco, haga clic aquí.

Registro del sistema de arranque seguro

Durante el arranque, el sistema imprimirá la información de Secure Boot:

Secure Boot enabled/disabled (Activado/desactivado): en los dispositivos sin fusible programable eléctrico System-on-Chip (SoC) (Fusible), como la unidad de procesamiento central (CPU) Minimal SYStem (MSYS), o cuando el bit seguro eFuse no está configurado, la impresión será "Secure Boot disabled" (Arranque seguro desactivado). Si se habilita Secure Boot, la impresión será "Secure Boot enabled" (Arranque seguro activado).

Después de que *BootROM* valide el *booton*, imprime el estado de validación (*pasado/fallido*).

Después de que *booton* valide el *arranque*, imprime el estado de validación (*pasado/fallido*).

Después de que *Uboot* valide la *imagen ros*, imprime el estado de validación (*pasado/fallido*).

Nota: En caso de falla, el proceso de inicio se detendrá.

Ejemplo de firmware de salida de arranque seguro versión 2.4.0.91:

Ejemplo de firmware de salida de arranque seguro versión 2.5.0.83:

```
BootROM - 1.73
Booting from NAND flash, Secure modeBootROM: RSA Public key verification PASSED
BootROM: CSK block signature verification PASSED
BootROM: Boot header signature verification PASSED
BootROM: Flash ID verification PASSED


General initialization - Version: 1.0.0
AVS selection from EFUSE disabled (Skip reading EFUSE values)
Overriding default AVS value to: 0x23
Detected Device ID 6811
High speed PHY - Version: 2.0

Init Customer board mvHwsPexConfig: Link is Gen1, check the EP capability
PCIe, Idx 0: Link upgraded to Gen2 based on client capabilities
High speed PHY - Ended Successfully
DDR3 Training Sequence - Ver TIP-1.55.0
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
DDR3 Training Sequence - Ended Successfully
BootROM: Image checksum verification PASSED
BootROM: Boot image signature verification PASSED


Armada38x Booton: Apr 17 2018 21:23:48 ver. 2.1.3
efuse secure mode: ON

Press x to choose XMODEM...
Booting from NAND flash
Verify secure U-Boot pass
Running UBOOT...


U-Boot 2013.01 (Jun 18 2019 - 16:47:25) Marvell version: 2016_T1.0.eng_drop_v10 2.5.18

Loading system/images/active-image ...
Verify ROS secure Image pass, efuse is programmed
Uncompressing Linux... done, booting the kernel.
I2C frequency 100 kHz (Tclk 200 MHz, freq_m 12, freq_n 3)
```

Conclusión

Ya está familiarizado con Secure Boot y cómo puede ayudar a proteger su red.