Sicheres Booten auf einem Switch SX350X oder SX550X

Ziel

In diesem Artikel wird der Prozess von Secure Boot erläutert, einer Methode zum Booten mit nur vertrauenswürdiger Software. Diese Funktion ist ab der Firmware-Version 2.4.0.91 aktiviert.

Wenn Sie mit den unten verwendeten Begriffen nicht vertraut sind, lesen Sie Cisco Business: Glossar neuer Begriffe.

Anwendbare Geräte

SX350X

SX550X

Softwareversion

2,4 0,91

Einführung

Secure Boot ist eine Methode zum Laden und Ausführen eines sicheren Images mithilfe einer Vertrauenskette, um das Laden nicht vertrauenswürdiger Software zu vermeiden. Eine Vertrauenskette wird durch Zuweisen von Bildern mit privaten Schlüsseln und mithilfe von Hardware- und Softwaremechanismen zum Überprüfen des geladenen Bildes hergestellt. So können Benutzer sicherstellen, dass beim Laden der Geräte-Firmware keine andere Person Code für Sicherheitsverletzungen hinzugefügt hat.

Wenn ein Benutzer versucht, ein neues Bild zu laden, wird das neue Image in eine temporäre Datei heruntergeladen, die validiert wird. Im Fehlerfall wird die temporäre Datei gelöscht. Wenn das neue Image ungültig ist, schlägt der Installationsvorgang fehl und es wird eine Warnmeldung angezeigt.

Wenn sich Ihre Switches in einer Stack-Topologie befinden

Wenn Sie 2.4.0.91 oder die neueste verfügbare Version auf den aktiven (primären) Switch laden, wird die Firmware auf alle Mitglieder des Stacks geladen. Dies ist unabhängig vom Modell der Produktfamilie, da auf allen Geräten dieselbe Firmware ausgeführt werden muss. Der Stapel funktioniert normal.

Sicherer Bootvorgang

Beim Start druckt das System die Informationen zum sicheren Start auf dem Terminal. Im Folgenden finden Sie die Schritte, die die Geräte vor dem Secure Boot durchgehen.

Boot Read Only Memory (BootROM) validiert *den Bootvorgang*

Booton validiert Universal Boot (*Uboot)*

Uboot validiert das *ROS-Image*

Wenn Secure Boot einen Fehler erkennt, verhindert es, dass das Gerät hochgefahren wird. Wenn dies der Fall ist, wenden Sie sich an Ihren Cisco Partner oder das Technical Assistance Center (TAC), um die nächsten Schritte auszuwählen, die in dieser Situation erforderlich sind. Wenn Sie einen Cisco Partner finden möchten, klicken Sie hier.

Sicheres Booten Syslog

Beim Start druckt das System die Informationen zum sicheren Start:

Sicheres Booten aktiviert/deaktiviert - In Geräten ohne System-on-Chip (SoC) elektrische programmierbare Sicherung (eFuse), z. B. Minimal SYStem (MSYS) Central Processing Unit (CPU), oder wenn sicheres Bit für die Sicherung nicht eingestellt ist, wird der Ausdruck "Secure Boot disabled" (Sicheres Booten deaktiviert) angezeigt. Wenn Secure Boot aktiviert ist, lautet der Ausdruck "Secure Boot Enabled" (Sicheres Booten aktiviert).

Nachdem *BootROM* den *Bootvorgang* validiert hat, wird der Validierungsstatus (*bestanden/fehlgeschlagen*) ausgegeben.

Nachdem der *Bootvorgang* das *Uboot* validiert hat, wird der Validierungsstatus (*bestanden/fehlgeschlagen*) ausgegeben.

Nachdem *Uboot* das *ros-Image* validiert hat, wird der Validierungsstatus (*bestanden/fehlgeschlagen*) ausgegeben.

Hinweis: Bei einem Fehler wird der Startvorgang abgebrochen.

Beispiel für Firmware-Version 2.4.0.91 für sichere Boot-Ausgabe:

Secure Boot-Ausgabe Beispiel Firmware Version 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)
```

Schlussfolgerung

Sie kennen jetzt Secure Boot und wie es Ihnen helfen kann, Ihr Netzwerk zu schützen.