Secure-start op een SX350X of SX550X switch

Doel

Dit artikel heeft als doel het proces van Secure Boot uit te leggen, een methode om op te starten met alleen vertrouwde software. Deze optie is ingeschakeld vanaf firmware versie 2.4.0.9.1.

Als u niet bekend bent met de onderstaande termen, raadpleegt u Cisco Business: Lijst van termen van nieuwe termen.

Toepasselijke apparaten

SX350X-software

SX550X-software

Softwareversie

2.4.0.91

Inleiding

Secure Boot is een manier om een beveiligde afbeelding te laden en uit te voeren met behulp van een vertrouwensketen om te voorkomen dat onvertrouwde software wordt geladen. Er wordt een vertrouwensketen ingesteld door afbeeldingen met privé-sleutels toe te wijzen en door hardware- en softwaremechanismen te gebruiken om het geladen beeld te controleren. Hiermee kunnen gebruikers er zeker van zijn dat wanneer ze software laden geen andere persoon een veiligheidsoverslagcode heeft toegevoegd.

Wanneer een gebruiker een nieuwe afbeelding probeert te laden, wordt de nieuwe afbeelding gedownload naar een tijdelijk bestand, dat gevalideerd is. Bij een fout wordt het tijdelijke bestand verwijderd. Als de nieuwe afbeelding niet geldig is, wordt het installatieproces mislukt en geeft het een waarschuwingsbericht weer.

Als uw switches in een stapelbare topologie staan

Wanneer u 2.4.0.91, of de nieuwste beschikbare versie, op de actieve (primaire) schakelaar laadt, zal het de firmware op alle leden van de stapel laden. Dit is ongeacht het model binnen de familie, omdat het een vereiste is dat alle apparaten de zelfde firmware draaien. De stapel werkt normaal.

Secure-blogproces

Tijdens het opstarten drukt het systeem informatie over het beveiligde opstarten op de terminal af. Hier zijn de stappen die de apparaten voor de Secure Boot controleren.

Opstarten Read Only Memory (BootROM) bevestigt de *startknop*

Booton bevestigt Universal Boot (*Ubooster)*

De computer bevestigt de *ROS-afbeelding*

Als de Secure Boot een storing detecteert, voorkomt u dat het apparaat opstart. Als dit voorkomt, neem dan contact op met uw Cisco partner of Technical Assistance Center (TAC) om de volgende stappen te ondernemen in deze situatie. Als u een Cisco-partner wilt vinden, klikt u hier.

Secure Boot Syslog

Tijdens het opstarten drukt het systeem informatie over Secure Boot af:

Secure Boot Enabled/Off - in apparaten zonder System-on-Chip (SoC) elektrische programmeerbare zekering (Fuse), zoals Mini SYStem (MSYS) Central Processing Unit (CPU), of wanneer Fuse Secure-bit niet is ingesteld, wordt de printout "Secure Boot Enabled" genoemd. Als Secure Boot is ingeschakeld, wordt de printout ingeschakeld.

Nadat *BootROM* de *booton* bevestigt, drukt het de validatiestatus (*aangenomen/mislukt*) af.

Nadat *booton* de *Uboogenot* bevestigt, drukt het de validatiestatus (*aangenomen/mislukt*) af.

Nadat *Uboot* de *rockafbeelding* gevalideerd heeft, drukt deze de validatiestatus (*doorgegeven/mislukt*) af.

Opmerking: De start stopt als het apparaat uitvalt.

Secure Boot uitvoer voorbeeld firmware versie 2.4.0.91:

Secure Boot uitvoer voorbeeld firmware versie 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)
```

Conclusie

U bent nu bekend met Secure Boot en de manier waarop dit uw netwerk kan helpen beschermen.