Avvio sicuro su uno switch SX350X o SX550X

Obiettivo

Lo scopo di questo articolo è quello di spiegare il processo di avvio protetto, un metodo per avviare con solo software attendibile. Questa funzione è abilitata a partire dalla versione firmware 2.4.0.91.

Se non si conoscono alcuni dei termini usati in questo documento, consultare Cisco Business: glossario dei nuovi termini.

Dispositivi interessati

SX350X

SX550X

Versione del software

2.4.0.91

Introduzione

L'avvio protetto è un modo per caricare ed eseguire un'immagine protetta utilizzando una catena di attendibilità per evitare il caricamento di software non attendibile. Viene stabilita una catena di attendibilità assegnando immagini con chiavi private e utilizzando meccanismi hardware e software per verificare l'immagine caricata. In questo modo gli utenti possono essere certi che, quando caricano il firmware del dispositivo, nessun altro utente abbia aggiunto un codice che viola la sicurezza.

Quando un utente tenta di caricare una nuova immagine, questa viene scaricata in un file temporaneo, che viene convalidato. In caso di errore, il file temporaneo viene eliminato. In questo modo, se la nuova immagine non è valida, il processo di installazione avrà esito negativo e verrà visualizzato un messaggio di avviso.

Se gli switch sono in una topologia in stack

Quando si carica la versione 2.4.0.91, o la versione più recente disponibile, sullo switch attivo (primario), il firmware viene caricato su tutti i membri dello stack. Ciò avviene indipendentemente dal modello della famiglia, poiché è necessario che tutti i dispositivi utilizzino lo stesso firmware. Lo stack funzionerà normalmente.

Processo di avvio protetto

Durante l'avvio, il sistema stampa le informazioni sull'avvio protetto sul terminale. Di seguito sono

riportati i passaggi che i dispositivi devono eseguire prima dell'avvio protetto.

La memoria di sola lettura di avvio (BootROM) convalida *l'avvio*

L'avvio convalida l'avvio universale (*Uboot)*

Uboot convalida l'*immagine ROS*

Se l'avvio protetto rileva un errore, impedisce l'avvio del dispositivo. In questo caso, contattare il partner Cisco o il Technical Assistance Center (TAC) per stabilire le fasi successive da seguire in questa situazione. Per trovare un partner Cisco, fare clic qui.

Syslog di avvio protetto

Durante l'avvio, il sistema stampa le informazioni sull'avvio protetto:

Avvio protetto abilitato/disabilitato: nei dispositivi senza fusibili programmabili elettrici (eFuse) System-on-Chip (SoC), ad esempio CPU (Minimal SYS) Central Processing Unit (MSYS), o quando il bit di sicurezza eFuse non è impostato, la stampa sarà "Secure Boot disabled". Se l'opzione Secure Boot è abilitata, la stampa sarà "Secure Boot enabled".

Dopo la convalida dell'*avvio da parte di BootROM*, viene visualizzato lo stato di convalida (*superato/non riuscito*).

Una volta convalidato l'*Uboot*, l'*avvio* visualizza lo stato di convalida (*superato/non riuscito*).

Dopo la convalida dell'*immagine Ro da parte di Uboot*, viene visualizzato lo stato di convalida (*superato/non riuscito*).

Nota: In caso di errore, il processo di avvio verrà interrotto.

Esempio di output Secure Boot versione firmware 2.4.0.91:

Esempio di output Secure Boot versione firmware 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)
```

Conclusioni

L'utente ha acquisito familiarità con Secure Boot e con le modalità di protezione della rete.