Démarrage sécurisé sur un commutateur SX350X ou SX550X

Objectif

L'objectif de cet article est d'expliquer le processus de démarrage sécurisé, une méthode de démarrage avec seulement des logiciels de confiance. Cette fonctionnalité est activée à partir de la version 2.4.0.91 du micrologiciel.

Si vous ne connaissez pas les termes utilisés ci-dessous, consultez Cisco Business : Glossaire des nouveaux termes.

Périphériques pertinents

SX350X

SX550X

Version du logiciel

2.4.0.91

Introduction

Secure Boot est un moyen de charger et d'exécuter une image sécurisée à l'aide d'une chaîne de confiance pour éviter de charger des logiciels non fiables. Une chaîne de confiance est établie en attribuant des images avec des clés privées et en utilisant des mécanismes matériels et logiciels pour vérifier l'image chargée. Cela permet aux utilisateurs de s'assurer que lorsqu'ils chargent le micrologiciel du périphérique, aucune autre personne n'a ajouté de code de violation de sécurité.

Lorsqu'un utilisateur tente de charger une nouvelle image, la nouvelle image est téléchargée dans un fichier temporaire, qui est validé. En cas d'erreur, le fichier temporaire est supprimé. De cette manière, si la nouvelle image n'est pas valide, le processus d'installation échoue et affiche un message d'avertissement.

Si vos commutateurs sont dans une topologie empilée

Lorsque vous chargez 2.4.0.91, ou la dernière version disponible, sur le commutateur actif (principal), il charge le micrologiciel sur tous les membres de la pile. Ceci est indépendamment du modèle de la famille, car il est nécessaire que tous les périphériques exécutent le même micrologiciel. La pile fonctionne normalement.

Processus de démarrage sécurisé

Au démarrage, le système imprime les informations de démarrage sécurisé sur le terminal. Voici les étapes que les périphériques doivent suivre avant le démarrage sécurisé.

Boot Read Only Memory (BootROM) valide le *démarrage*

Booton valide le démarrage universel (*Uboot)*

Uboot valide l'*image ROS*

Si le démarrage sécurisé détecte une défaillance, il empêche le périphérique de démarrer. Si cela se produit, contactez votre centre d'assistance technique ou partenaire Cisco (TAC) pour déterminer les prochaines étapes à suivre dans cette situation. Si vous devez trouver un partenaire Cisco, cliquez ici.

Syslog de démarrage sécurisé

Au démarrage, le système imprime les informations de démarrage sécurisé :

Démarrage sécurisé activé/désactivé : dans les périphériques sans module de fusion programmable électrique (eFuse) System-on-Chip (SoC), tel que le processeur central (MSYS) Minimal SYStem (MSYS), ou lorsque le bit sécurisé eFuse n'est pas défini, l'impression sera “ ” de démarrage sécurisé désactivé. Si le démarrage sécurisé est activé, l'impression sera “ ” de démarrage sécurisé.

Une fois que *BootROM* valide l'*amorçage*, il imprime l'état de validation (*passé/échoué*).

Une fois que *le démarrage* a validé l'*Uboot*, il imprime l'état de validation (*passé/échoué*).

Une fois *Uboot* validé l'*image ros*, il imprime l'état de validation (*réussi/échoué*).

Note: En cas d'échec, le processus de démarrage s'arrête.

Exemple de sortie de démarrage sécurisé version 2.4.0.91 :

Exemple de sortie de démarrage sécurisé version 2.5.0.83 du micrologiciel :

```
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)
```

Conclusion

Vous connaissez maintenant Secure Boot et comment il peut vous aider à protéger votre réseau.