

在SNS3700機箱的RMA之後安裝TPM模組

目錄

[簡介](#)

[注意事項](#)

[問題](#)

[解決方案](#)

[驗證](#)

簡介

本文檔介紹在更換機箱的SNS3700伺服器上安裝TPM模組的過程。

注意事項

可信平台模組(TPM)是一個硬體元件，通過儲存加密金鑰來提高伺服器的安全性。

但是，伺服器可以在沒有身份服務引擎(ISE)的情況下運行。



注意：如果您在沒有TPM的伺服器上安裝並運行了ISE應用程式，則需要執行此處所述的過程，以安裝模組並使其可由系統使用。

- 此伺服器支援受信任計算組(TCG)定義的TPM版本2.0(UCSX-TPM-002C)。TPM也基於SPI。
- 不支援aTPM的欄位替換；僅當服務器尚未安裝aTPM後，才能安裝aTPM after-factory。
- 如果返回具有aTPM的伺服器，則必須使用新TPM訂購替換服務器。
- 如果TPM2.0變得無響應，請重新啟動伺服器。

問題

思科製造提供的SNS 3700系列或更高版本包含TPM。

但是，思科服務倉庫提供的SNS 3700系列機箱更換件不包括此類裝置。

必須執行下一個進程才能安裝TPM，並使硬體和軟體都能利用模組的優勢。



解決方案

按給定順序執行後續步驟以安裝模組、初始化模組並利用模組提供的安全功能。

1. 安裝TPMHardware。
2. 在BIOS中啟用TPM。
3. 重新安裝ISE。

使用本文完成步驟1、2和3:[Cisco UCS C220 M6伺服器安裝和維修指南 — 維護伺服器](#)

完成在BIOS中啟用TPM一章中的步驟後，此過程即完成。

要完成步驟4，請導航到下一個連結，並訪問需要在伺服器上安裝的ISE版本的安裝指南：

[安裝和升級指南 — 安裝思科ISE](#)

在安裝指南中，導航到安裝思科ISE部分。

驗證

完成此步驟後，必須安裝並運行ISE。

開啟ISE命令列並運行下一個命令。如果在此處顯示輸出，則表示您已正確安裝TPM。

ISE/user#show tech-support |包括TPM

TPM:存在模組

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。