在SNS3700机箱的RMA后安装TPM模块

目录

简介

考虑事项

问题

解决方案

确认

简介

本文档介绍在更换机箱的SNS3700服务器上安装TPM模块的过程。

考虑事项

可信平台模块(TPM)是一个硬件组件，通过存储加密密钥来提高服务器的安全性。

但是，服务器可以在没有身份服务引擎(ISE)的情况下运行身份服务引擎。

⚠ 警告：如果您在没有TPM的服务器上安装并运行ISE应用，您需要执行此处记录的过程以安装模块并使其可由系统使用。

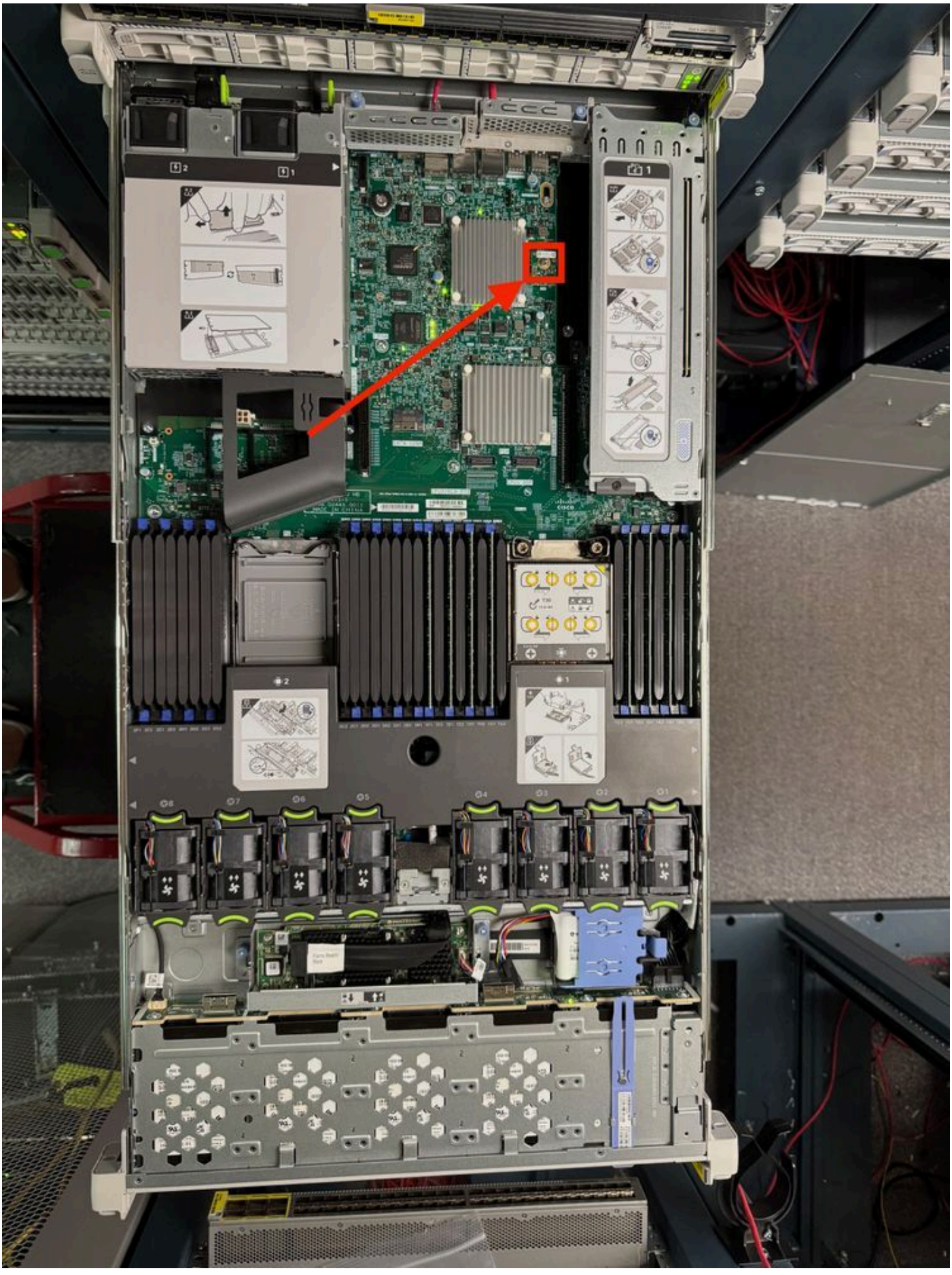
- 此服务器支持受信任计算组(TCG)定义的TPM版本2.0(UCSX-TPM-002C)。 TPM也基于SPI。
- 无法更换TPM。这意味着，如果模块已安装，则无法移除和更换，因为已使用防篡改螺钉进行安装。
- 如果主板中缺少TPM，则可以安装模块。
- 如果返回了带有aTPM的服务器，则必须使用新TPM订购替换服务器。
- 如果TPM2.0变为无响应，请重新启动服务器。

问题

SNS 3700系列或更高版本包含思科制造提供的TPM。

但是，思科服务站提供的SNS 3700系列机箱更换件不包含此类设备。

必须执行下一个过程才能安装TPM并使硬件和软件都能利用模块的优势。



映像1. TPM模块在SNS 3700系列设备中的位置

解决方案

按照给定顺序执行后续步骤，以安装模块、初始化模块并利用模块提供的安全功能。

1. 安装TPMHardware。
2. 在BIOS中启用TPM。
3. 重新安装ISE。

使用本文完成步骤1、2和3:Cisco UCS C220 M6服务器安装和维修指南 — 维护服务器

完成在BIOS中启用TPM一章中的步骤后，此过程即告完成。

要完成第4步，请导航到下一个链接，并访问需要在服务器上安装的ISE版本的安装指南：

安装和升级指南 — 安装思科ISE

在安装指南中，导航到安装思科ISE部分。

确认

完成此步骤后，您必须安装并运行ISE。

打开ISE命令行并运行下一个命令。如果在此处显示输出，则意味着您已正确安装TPM。

ISE/user#show tech-support |包含TPM

TPM:存在模块

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。