

使用外部CA將ISE 3.3與Stealthwatch 7.5.1整合

目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[設定](#)

[A部分：安全網路分析\(Stealthwatch\)憑證組態](#)

[第I部分 — 為安全網路分析pxGrid客戶端證書生成CSR](#)

[第二部分 — 使用外部CA建立安全網路分析pxGrid客戶端證書](#)

[第III部分 — 將Secure Network Analytics pxGrid Client Certificate新增到Manager](#)

[第IV部分 — 將CA根證書匯入Manager信任儲存](#)

[B部分：思科身分識別服務引擎3.3憑證組態](#)

[第I部分 — 生成ISE伺服器pxGrid證書](#)

[第二部分 — 使用外部CA建立ISE伺服器pxGrid證書](#)

[第III部分 — 將CA根證書匯入ISE信任儲存](#)

[第IV部分 — 將ISE證書繫結到證書簽名請求\(CSR\)](#)

[整合](#)

[驗證](#)

[疑難排解](#)

[DNS解析問題](#)

[解決方案](#)

[未知CA錯誤或缺少受信任證書](#)

[解決方案](#)

[已知瑕疵](#)

簡介

本文檔介紹使用pxGrid連線將ISE 3.3與安全網路分析(Stealthwatch)整合的過程。

必要條件

思科建議瞭解以下主題：

- 身分識別服務引擎
- 平台交換網格(pxGrid)
- 安全網路分析(Stealthwatch)
- TLS/SSL證書。
- Windows Server 2016上的PKI

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎(ISE)版本3.3補丁4
- 安全網路分析(Stealthwatch)7.5.1
- Windows server 2016作為外部證書頒發機構(CA)伺服器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

A部分：安全網路分析(Stealthwatch)憑證組態

第I部分 — 為安全網路分析pxGrid客戶端證書生成CSR

1. 登入Stealthwatch管理控制檯(SMC)。
2. 從主選單中選擇「配置」>「全域性」>「集中管理」。



Dashboard



Monitor



Investigate



Report



Configure

Configure X

Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

Central Management

User Management

Manager

UDP Director

External Lookup

System

| | |
|------------------------------|----------------------------|
| 思科錯誤ID 18119 | ISE正在選擇不受支援的密碼ITLS伺服器呼叫資料包 |
| 思科錯誤ID 01634 | 無法使用EPS條件隔離裝置 |

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）。