有關思科安全管理裝置(SMA)的「開拓者」CLI命令的管理詳細資訊

目錄

[簡介](#)
[必要條件](#)
[為什麼](#)
[影響](#)
[解決方案](#)
[命令列示例](#)
[命名語法示例](#)
[疑難排解](#)

簡介

從AsyncOS 11.4開始，並繼續AsyncOS 12.x for Security Management Appliance(SMA),Web使用者介面(UI)經歷了重新設計以及資料的內部處理。本文的重點是探討瀏覽新重新設計的Web使用者介面的能力變化。 通過實施技術更先進的設計，思科致力於改善使用者體驗。

作者：Chris Arellano，思科TAC工程師。

必要條件

註：「管理」介面是預設介面，在SMA上的首次配置期間顯示。在**網路> IP介面**中，不允許刪除。 因此，驗證服務時總是使用預設介面。

在啟用**trailblazerconfig**之前，確保已驗證以下專案：

1. SMA已升級且正在運行AsyncOS版本12.x（或更高版本）
2. 在**Network > IP Interfaces**中，管理介面已啟用**Appliance Management > HTTPS 必須在防火牆**上開啟**Appliance Management** > HTTPS埠
3. 在**Network > IP Interfaces**中，管理介面都啟用了**AsyncOS API > HTTP**和**AsyncOS > HTTPS。 必須在防火牆**上**開啟AsyncOS API > HTTP**和**AsyncOS API** > HTTPS埠
4. 「開拓者」埠必須通過防火牆開啟 預設為4431
5. 確保DNS可以解析管理介面「主機名」
   即**nslookup** sma.hostname返回IP地址
6. 確保DNS可以解析「*這是垃圾郵件隔離區的預設接*口」配置為訪問垃圾郵件隔離區的主機名/URL

為什麼

12.x下一代SMA(NGSMA)GUI已重新實施為單頁應用程式(SPA)，該應用程式可下載到客戶端(IE、Chrome、Firefox)以提高使用者體驗。 SPA與SMA的多個內部伺服器通訊，每個伺服器執行不同的服務。

SPA與SMA通訊中的CORS（跨源資源共用）限制會導致多個模組之間通訊的一些障礙。

- CORS是一項安全功能，旨在防止惡意命令在與其他內部服務的已建立通訊線路內執行。

內部伺服器可通過NGSMA通過不同的編號TCP埠訪問。每個TCP埠都需要單獨的證書批准才能與客戶端通訊。 無法與NGSMA的內部伺服器進行通訊，從而造成問題。

影響

下一代網路介面包括「/euq-login」和「ng-login」。

AMP思科威脅響應(CTR)整合報告。

解決方案

代表不同模組的TCP連線埠的簡單範例要求每個連線埠接受憑證。 如果SMA上不存在受信任的簽名證書，則當瀏覽器向模組發起透明通訊時，需要多個證書接受。 對於可能不瞭解TCP埠6443、443、4431需求的使用者，該體驗可能會導致混淆。

為了克服這些挑戰，思科實施了Nginx在客戶端（瀏覽器客戶端）和伺服器（通過特定埠可訪問的服務）之間執行代理功能。 Nginx（格式為NGINX或nginx）是一種Web伺服器，也可以用作反向代理、負載均衡器、郵件代理和HTTP快取。

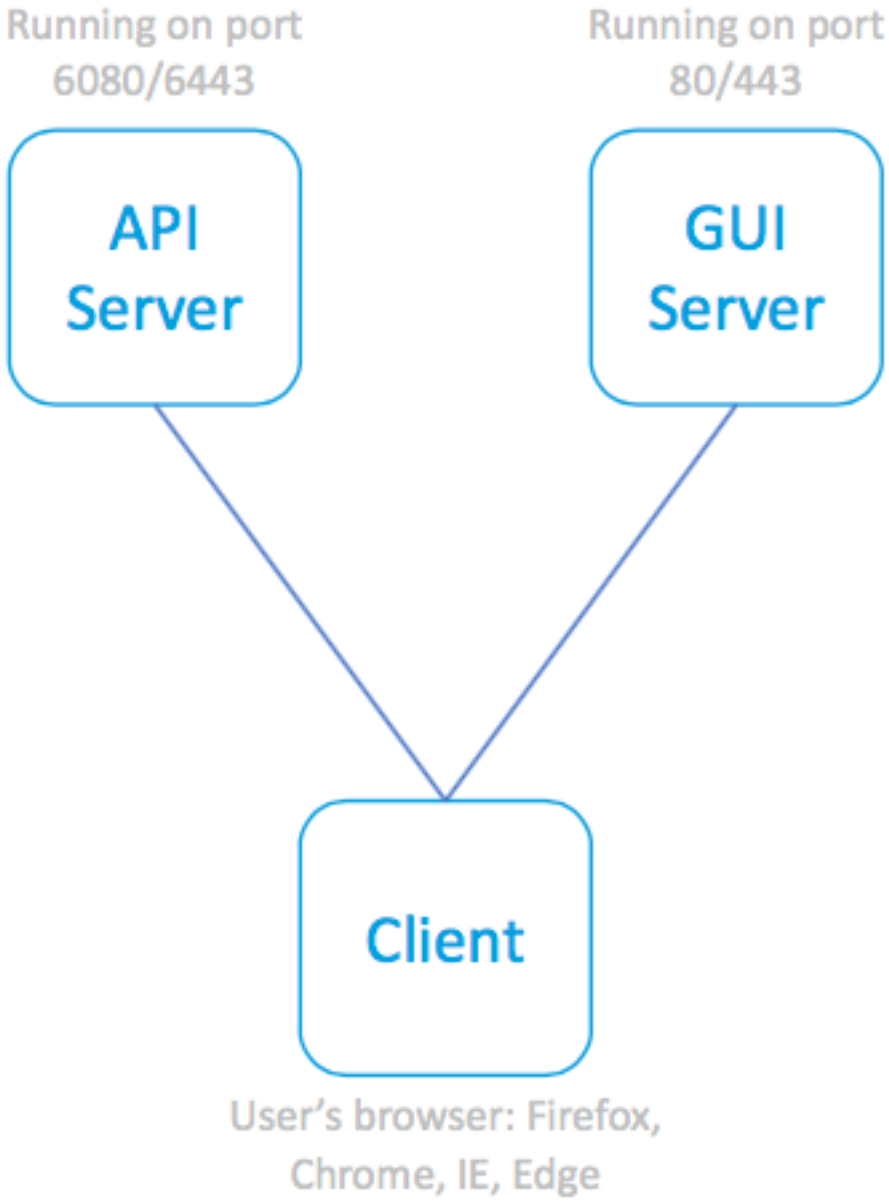
這將通訊濃縮為單個通訊流和證書接受。

Cisco已將CLI命令標籤為以**trailblazerconfig**啟用此功能。

第一個圖顯示兩個當前伺服器的示例：

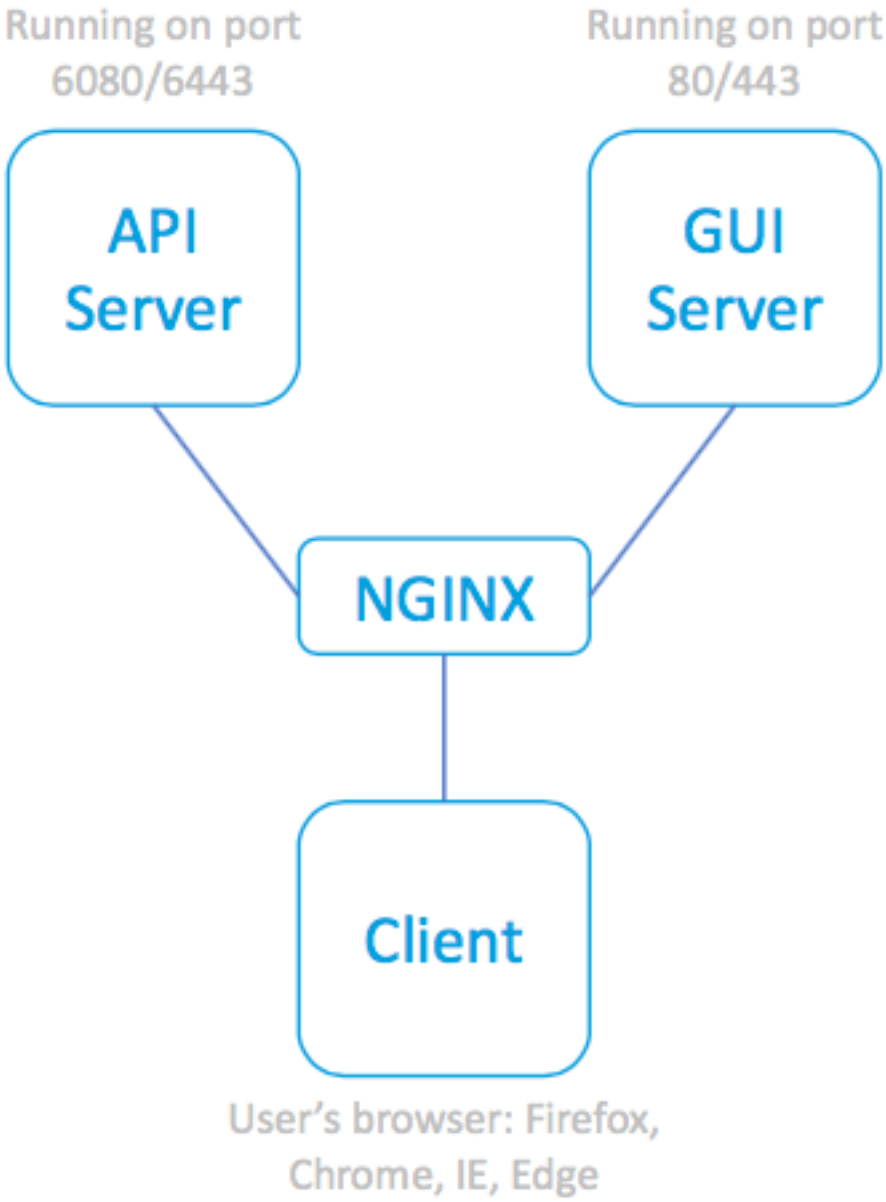
- API伺服器HTTP:6080和HTTPS:6443
- GUI伺服器HTTP:80和HTTPS:443

批准從GUI到API的通訊需要批准和埠訪問。



SPA和相關伺服器

下一個示例在API和GUI流程前面包含Nginx代理，從而消除了通訊受限的問題。



SPA，利用NGINX代理訪問關聯的伺服器

命令列示例

全面幫助：

```
sma.local> help trailblazerconfig

trailblazerconfig

   Configure and check the trailblazer.
(Please make sure existing UI is functioning on https)
   trailblazerconfig enable <https_port> <http_port>
   trailblazerconfig disable
   trailblazerconfig status

   Sub-commands:
       enable          - Runs the trailblazer either on
                         default ports (https_port: 4431 and http_port: 801)
```

```
                    or optionally specified https_port and http_port
      disable        - Disable the trailblazer
      status         - Check the status of trailblazer

   Options:
      https_port     - HTTPS port number, Optional
      http_port      - HTTP port number, Optional
```

檢查狀態：

```
sma.local> trailblazerconfig status

trailblazer is not running
```

啟用：

```
sma.local> trailblazerconfig enable

trailblazer is enabled.
To access the Next Generation web interface, use the port 4431 for HTTPS.
```

啟用後，檢查狀態：

```
sma.local> trailblazerconfig status

trailblazer is running with https on port 4431.
```

命名語法示例

啟用trailblazer的Web訪問將包括URL地址中的trailblazer埠：

- NGSMA管理門戶將顯示為：https://hostname:4431/ng-login
- NGSMA終端使用者隔離（或ISQ）門戶將顯示為：https://hostname:4431/euq-login

疑難排解

一些實施側重於垃圾郵件通知的輔助介面。如果管理介面「hostname」在DNS中不可解析(即 **nslookup** 主機名)，則跟蹤程式將無法初始化。

要立即確認和還原服務，可以將可解析的主機名新增到管理介面。（然後建立A記錄以正確解析指定的主機名。）

使用者端安全限制阻止使用者環境訪問SMA 4431 TCP埠：

1. 測試以確保該埠對瀏覽器可用
2. 輸入主機名和埠為：
   https://hostname:4431

TCP埠443未開啟

- **IE11:無法顯示此頁面**
- **Chrome:無法訪問此站點。拒絕連線**
- **Firefox:無法連線**

TCP埠4431開啟且證書被接受

- **IE:HTTP 406**
- **Chrome:{"error":{"消息":「未授權」，「代碼」：「401」、「解釋」："401 =無許可權 — 請**

授權方案。"}}

- **Firefox:證書提示（接受）。 Firefox:過帳證書 >「未授權」。 401**

正確的URL語法：

- 啟用非先行器的系統將不會使用名稱中的埠4431: https://hostname/ng-login

  — 或 — https://*hostname*/euq-login

- 支援開拓者的系統將在名稱中包含埠號4431: https://hostname:4431/ng-login

  — 或 — https://*hostname*:4431/euq-login