配置系列3防禦中心的高可用性

目錄

簡介

本檔案介紹系列3防禦中心(DC)的高可用性(HA)配置。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower技術
- 基本的高可用性概念

採用元件

本文檔中的資訊基於從軟體版本5.3到軟體版本5.4.1.6運行的Firepower防禦中心系列3裝置(DC1500、DC2000、DC3500、DC400)

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

為確保操作的連續性，高可用性功能允許您指定冗餘防禦中心來管理裝置。防禦中心維護來自受管裝置和這些裝置的特定配置元素的事件資料流。如果一個防禦中心發生故障，您可以通過另一個防禦中心監控您的網路而不會中斷。

高可用性功能

- HA同步是雙向的，這意味著即使存在指定的主裝置和輔助裝置，在任何一個裝置上新增的更改也會複製到另一個裝置。
- HA不需要直接連線裝置。HA連線可以通過交換機完成，但此連線需要位於同一個廣播域中。
- HA裝置通過其管理IP在埠8305進行通訊。
- 裝置的HA同步時間是五分鐘，這表示裝置每五分鐘會嘗試與其對等裝置同步其配置。由於同步所需的時間特定於裝置，因此累計起來，同步時間可以最大為10分鐘。
- 如果特定HA對等點需要重新映像，建議先中斷HA，然後重新映像。
- 如果您計畫升級HA群集，則無需中斷HA。當您從5.3.0版升級到5.4.0版時，請逐個升級裝置，升級裝置後，在主Defense Center上執行同步任務。
- 兩個DC上存在同名的訪問策略會建立兩個同名的訪問控制策略。一個策略在本地配置，另一個策略從對等DC同步。

  附註：無法新增目標或應用此策略，因為它引發了一個錯誤，表明已存在同名的策略。
- 許可證不會在DC對等體之間同步，因此，需要將它們單獨新增到DC。
- 所有受管裝置僅新增到一個DC。在對等DC之間同步配置。
- 受管裝置向兩個DC傳送日誌。
- DC同步最新操作。例如，如果從DC-1中刪除使用者，則另一個對等DC-2不會將使用者配置同步到DC-1。它將同步刪除**操作，並且使用者會從DC-1和DC-2中丟失。**

對等體之間雙向共用配置

HA DC雙向同步策略。這些配置在對等體之間雙向同步。您還可以檢視大部分設定，並在路徑旁邊定義路徑：

標識和身份驗證

- 外部LDAP配置 — 導航到System > Local > User Management > External Authentication
- 使用者（內部和外部） — 導航至**系統>本地>使用者管理>使用者**
- 自定義使用者角色 — 導航到**系統(System)>本地(Local)>使用者管理(User Management)>使用者角色(User Roles)**

報告

- 報告模板 — 導航至**概覽>報告>報告模板**

可配置的策略（在「策略」部分下）

- 訪問控制策略、入侵策略、檔案策略、SSL策略、網路訪問策略、關聯策略和規則、合規性白

名單和流量配置檔案。
- 入侵規則（本地和SRU） — 導航至**Policies > Intrusion> Rule Editor > Local Rules**。
- 網路發現、主機屬性、網路發現使用者反饋（包括註釋和主機重要性）、從網路對映中刪除主機、應用程式和網路，以及停用或修改漏洞。
- 自定義應用檢測器
- 使用者策略中的LDAP連線 — 導航到**策略>使用者**
- 警報 — 導航到**策略>操作>警報**（在「響應」下）

裝置資訊

- NAT規則 — 導**寰至Devices> NAT**
- VPN規則 — 導航**至Devices > VPN**
- 所有裝置資訊（包括名稱及其組）都以雙向方式同步。每個裝置的日誌儲存位置也是在對等裝置之間同步的 — 導航到**裝置>裝置管理**
- 自定義入侵規則分類
- 啟用的自定義指紋
- 系統策略和運行狀況策略
- 自定義儀表板、自定義工作流程和自定義表
- 更改協調、快照和報告設定
- Sourcefire規則更新(SRU)、地理定位資料庫(GeoDB)和漏洞資料庫(VDB)更新

DC之間未同步配置

- 使用者策略中的使用者代理資訊
- NMAP掃描
- 響應組
- 修正模組
- 補救例項
- Estreamer和主機輸入客戶端
- 備份配置檔案
- 計畫
- 授權
- 更新
- 運行狀況警報

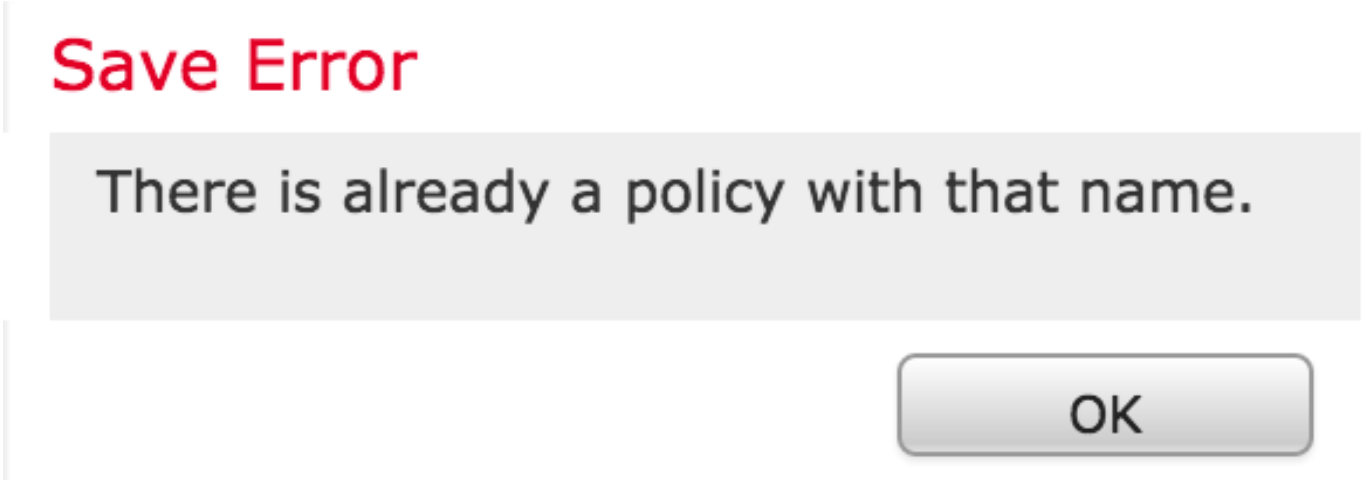
設定

配置高可用性的前提條件

- 裝置的軟體和硬體版本必須相同。
- 裝置必須安裝相同的VDB。
- 裝置必須具有相同的SRU。
- 確保兩個防禦中心都有一個名為admin且具有管理員許可權的使用者帳戶。這些帳戶必須使用相同的密碼。

- 請確保除管理員帳戶外，兩個防禦中心沒有具有相同使用者名稱的使用者帳戶。在建立高可用性之前，請刪除或重新命名其中一個重複使用者帳戶。

- 確保兩台裝置沒有具有相同名稱的任何訪問控制策略。如果有兩個名稱相同的訪問控制策略，則它們在DC上共存。但是，它們無法與任何裝置關聯。一旦在新增目標裝置後儲存此策略，此配置就會被拒絕，並出現錯誤，如圖所示：



- 兩個防禦中心都必須能夠訪問網際網路。

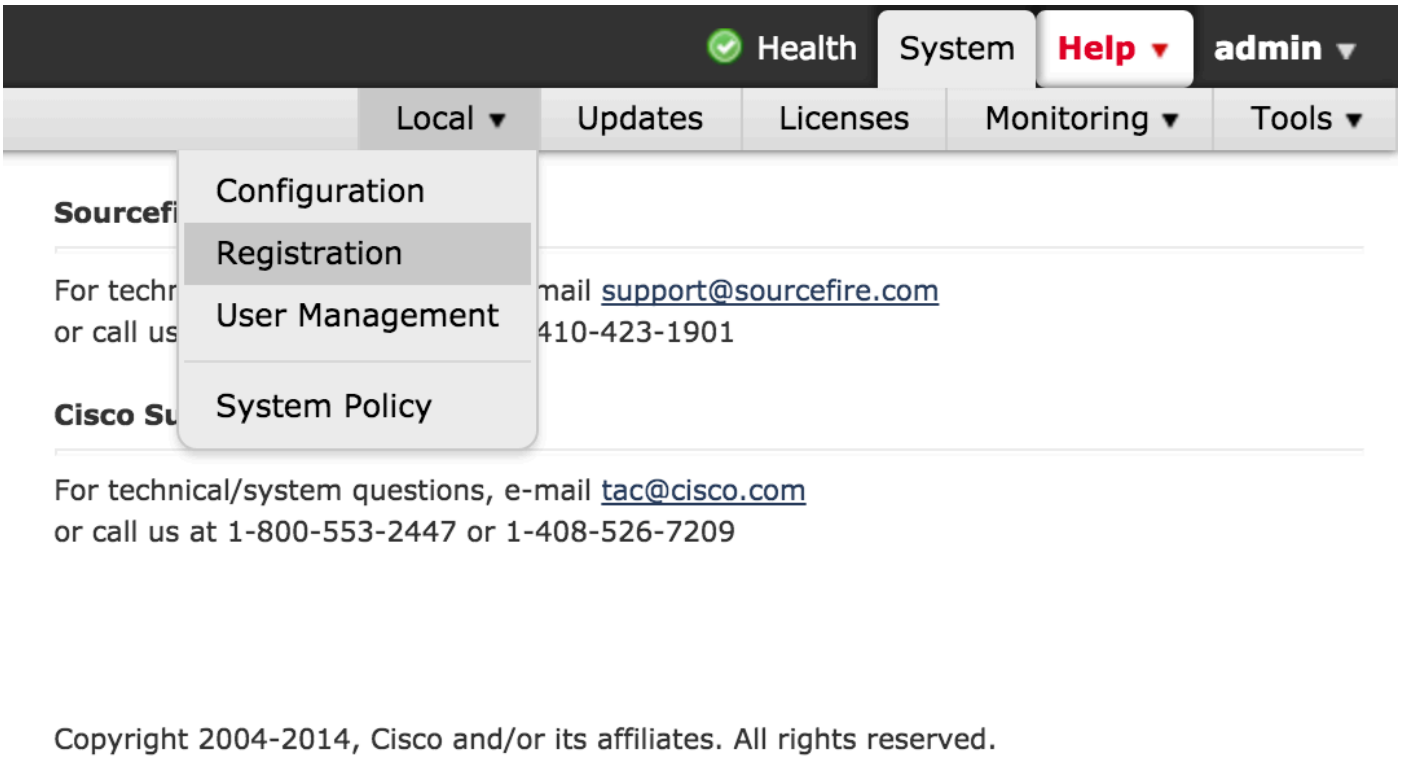
配置高可用性

以下是配置高可用性的8個步驟。

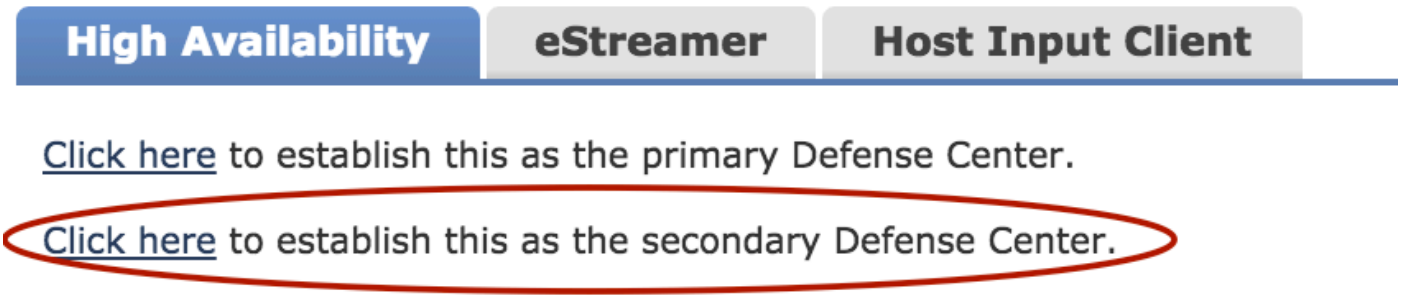
步驟1.確認軟體和硬體版本以及VDB版本和規則更新版本相同。

Model	Defense Center 1500
Serial Number	BZDW14300158
Software Version	5.4.1.2 (build 38)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 262)
Rule Update Version	2015-11-16-001-vrt
Rulepack Version	1606
Module Pack Version	1837
Geolocation Update Version	None
VDB Version	build 258 (2015-11-10 22:58:57)

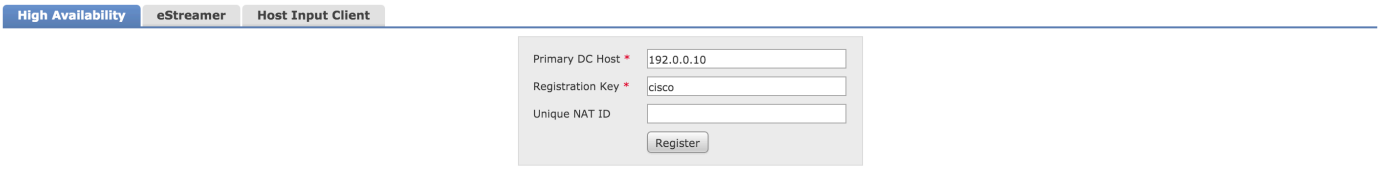
步驟2。若要使裝置成為輔助裝置，請導覽至**System > Local > Registration**，如下圖所示。確保此DC上沒有配置。



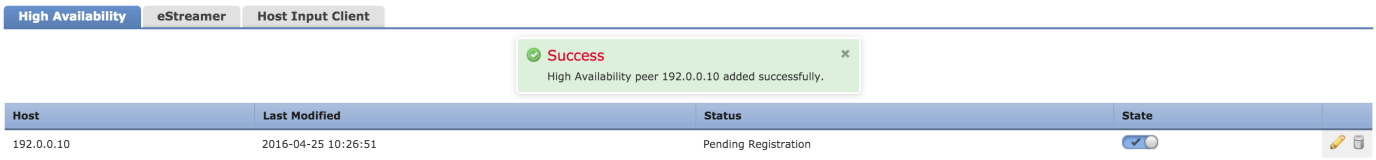
步驟3.在**High Availability**索引標籤下按一下**Click here**以將其建立為二級防禦中心，如下圖所示：



步驟4.完成步驟3後，系統會顯示頁面，如下圖所示。新增主DC的IP和傳遞金鑰。 確保為網路地址轉換後的裝置新增唯一的NAT ID。



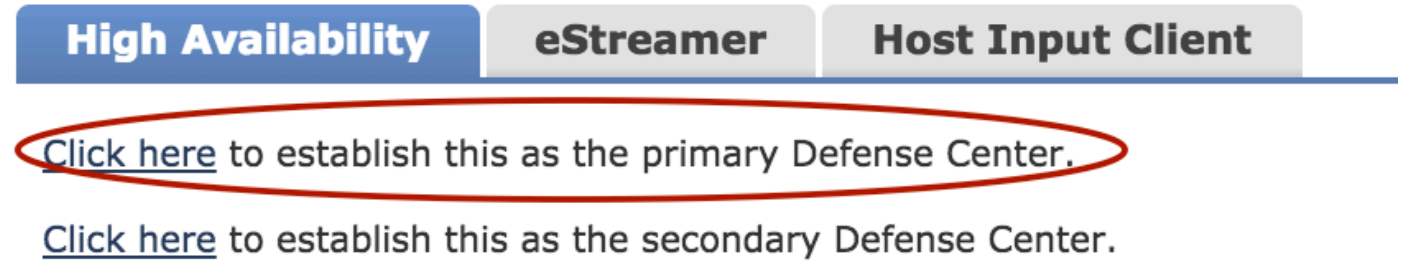
步驟5.驗證IP位址後，如果正確，請按一下**Register**。您可以看到如下圖所示的頁面：



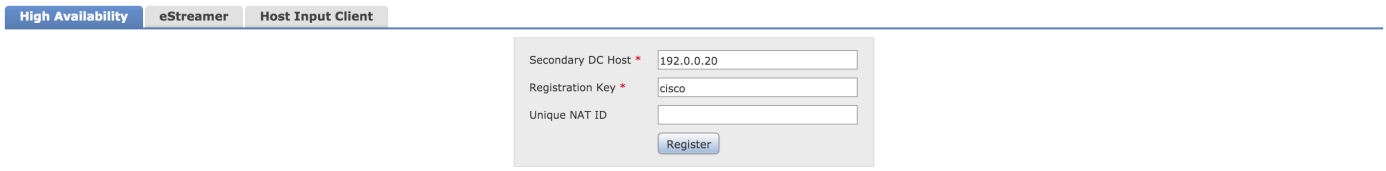
這表示在輔助DC上配置了HA，並且需要在主DC上配置它。

步驟6.登入到要配置為主DC的裝置。導航到**System > Local > Registration**。

在**High Availability**頁籤下，按一下**Click here to add as the primary Defense Center**，如下圖所示：

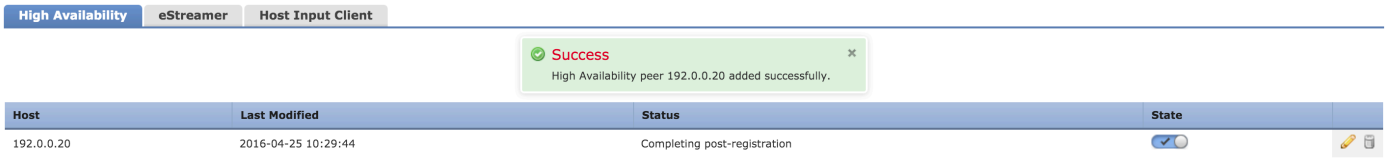


步驟7.完成步驟6後，系統會顯示頁面，如下圖所示：



新增輔助DC IP。提供配置輔助DC時提供的相同註冊金鑰和NAT ID。

步驟8.驗證IP的詳細資訊後，按一下**Register**。註冊完成後，將顯示「Success」頁面，如下圖所示：



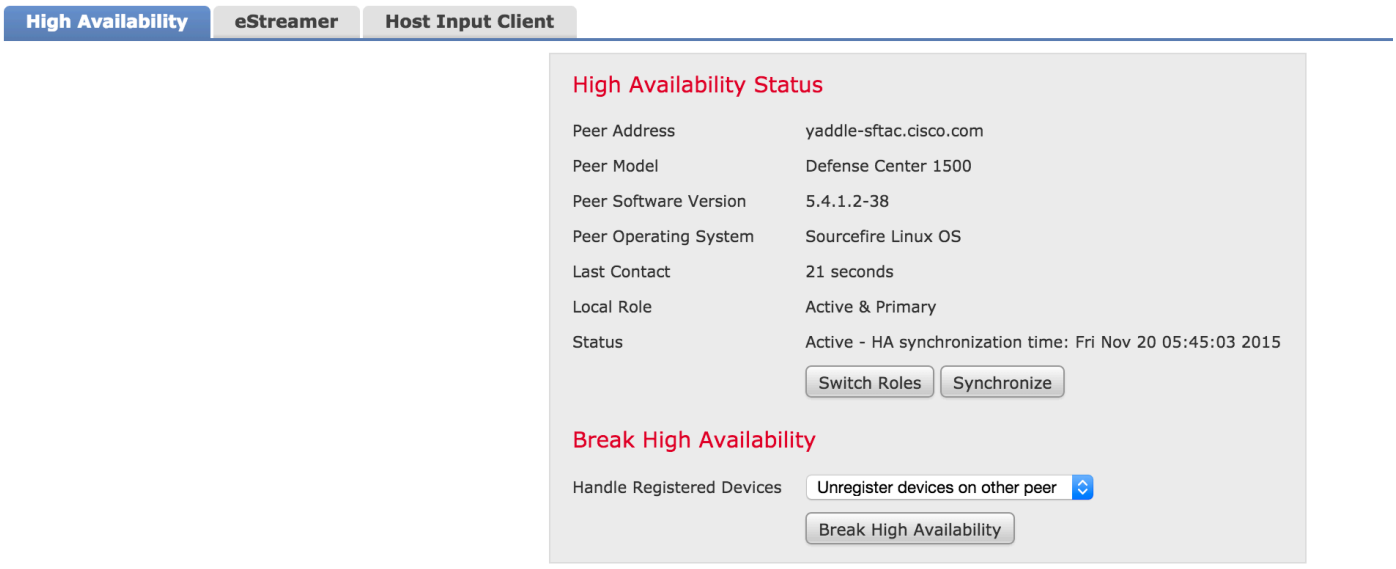
5-10分鐘後，HA的配置和同步完成。

完成HA的組態和同步大約需要5-10分鐘

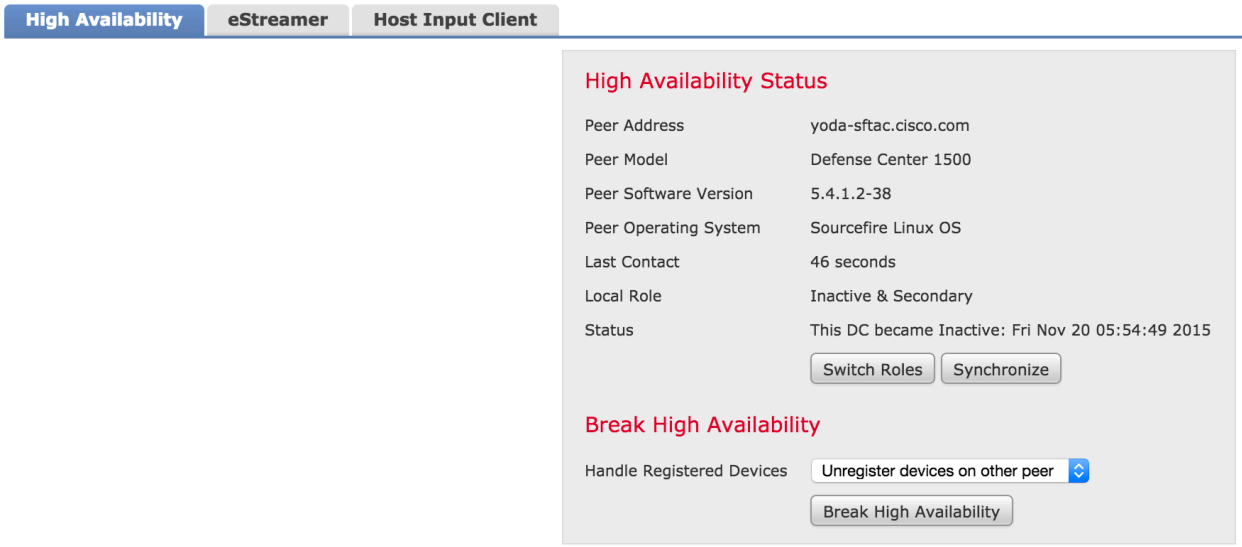
驗證

一步一步配置，驗證您的DC是否正確配置以實現高可用性。

步驟1。導覽至主要裝置上的**System >Local >Registration**，如下圖所示：



步驟2.導覽至**System >Local >Registration** 如圖所示：



疑難排解

本節提供高可用性的基本故障排除步驟。

- 確保兩個DC都在TCP埠8305上偵聽，因為HA使用此埠來同步資訊和心跳。
- 確保網路或任何中間裝置都沒有阻止TCP埠8305。
- 如果刪除或替換了先前對等裝置的過時條目，HA建立將失敗。EM_Peers表提供了有關此類對等裝置的詳細資訊。

相關資訊

- 在Cisco Firepower 8000系列裝置上配置堆疊
- Firesight系統使用手冊5.4.1
- 技術支援與文件 - Cisco Systems