在系列3防御中心上配置高可用性

目录

简介

本文档介绍用于系列3防御中心(DC)的高可用性(HA)的配置。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower技术
- 基本高可用性概念

使用的组件

本文档中的信息基于从软件版本5.3到软件版本5.4.1.6运行的Firepower防御中心系列3设备(DC1500、DC2000、DC3500、DC4000)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

为确保操作的连续性，高可用性功能允许您指定冗余防御中心来管理设备。防御中心维护来自受管设备的事件数据流和这些设备的某些配置元素。如果一个防御中心发生故障，您可以通过另一个防御中心监控您的网络，而不会中断。

高可用性功能

- HA同步是双向的，这意味着即使存在指定的主设备和辅助设备，在任一设备上添加的更改也会复制到另一设备。
- HA不要求设备直接连接。HA连接可以通过交换机完成，但此连接需要位于同一广播域中。
- HA设备通过其管理IP在端口8305进行通信。
- 设备的HA同步时间为五分钟，这意味着每五分钟设备就会尝试将其配置与其对等设备同步。由于同步所需的时间是特定于设备的，因此累计同步时间可以最大化到十分钟。
- 如果特定HA对等体需要重新映像，则建议中断HA，然后重新映像。
- 如果计划升级HA集群，则无需中断HA。从5.3.0版升级到5.4.0版时，逐个升级设备，升级后在主防御中心上执行同步任务。
- 两个DC上存在具有相同名称的访问策略会创建两个同名的访问控制策略。一个策略在本地配置，另一个策略从对等DC同步。

  注意：无法添加目标或应用此策略，因为它会引发错误，表明已存在同名策略。
- 许可证在DC对等体之间不同步，因此，它们需要单独添加到DC。
- 所有受管设备仅添加到一个DC。配置在对等DC之间同步。
- 受管设备将日志发送到两个DC。
- DC同步最新操作。例如，如果从DC-1删除用户，则另一个对等体DC-2不将用户配置同步到DC-1。它会同**步删**除操作，并且用户会从DC-1和DC-2中丢失。

对等体之间双向共享的配置

HA DC双向同步策略。这些配置在对等体之间双向同步。您还可以查看其中大多数配置，且路径在其旁边定义：

身份和身份验证

- 外部LDAP配置 — 导航至System > Local > User Management > External Authentication
- 用户（内部和外部） — 导航至System > Local> User Management> Users
- 自定义用户角色 — 导航至System > Local > User Management > User Roles

报告

- 报告模板 — 导航至“概述”>“报告”>“报告模板”

可配置策略（在“策略”部分下）

- 访问控制策略、入侵策略、文件策略、SSL策略、网络访问策略、关联策略和规则、合规性白名单和流量量变曲线。

- 入侵规则（本地和SRU） — 导航**到Policies > Intrusion> Rule Editor > Local Rules。**
- 网络发现、主机属性、网络发现用户反馈，包括注释和主机重要性、从网络映射中删除主机、应用和网络以及停用或修改漏洞。
- 自定义应用检测器
- 用户策略中的LDAP连接 — 导航**到策略>用户**
- 警报 — 导航到策**略>操作>警报**（在响应下）

设备信息

- NAT规则 — 导航**到Devices> NAT**
- VPN规则 — 导航**到Devices > VPN**
- 所有设备信息（包括名称及其组）都双向同步。每个设备的日志存储位置也会在对等体之间同步 — 导航**到Devices > Device Management**
- 自定义入侵规则分类
- 已激活自定义指纹
- 系统策略和运行状况策略
- 自定义控制面板、自定义工作流程和自定义表
- 更改协调、快照和报告设置
- Sourcefire规则更新(SRU)、地理定位数据库(GeoDB)和漏洞数据库(VDB)更新

配置未在DC之间同步

- 用户策略中的用户代理信息
- NMAP扫描
- 响应组
- 补救模块
- 补救实例
- Estreamer和主机输入客户端
- 备份配置文件
- 计划
- 许可证
- 更新
- 运行状况警报

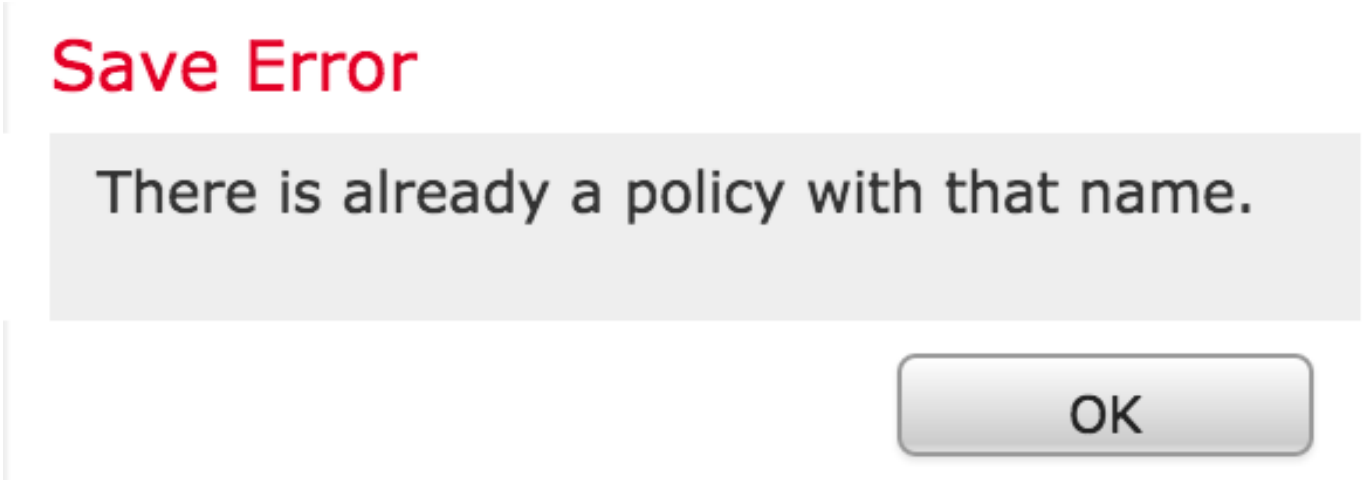
配置

配置高可用性的前提条件

- 设备的软件和硬件版本必须相同。
- 设备必须安装相同的VDB。
- 设备必须具有相同的SRU。
- 确保两个防御中心都具有名为admin的具有管理员权限的用户帐户。这些帐户必须使用相同的密码。
- 确保除管理员帐户外，两个防御中心没有具有相同用户名的用户帐户。在建立高可用性之前

，删除或重命名其中一个重复的用户帐户。

- 确保两台设备没有具有相同名称的任何访问控制策略。如果有两个名称相同的访问控制策略，它们在DC上共存。但是，它们无法与任何设备关联。添加目标设备后保存此策略后，此配置将被拒绝，并显示错误如图所示：



- 两个防御中心必须都能访问互联网。

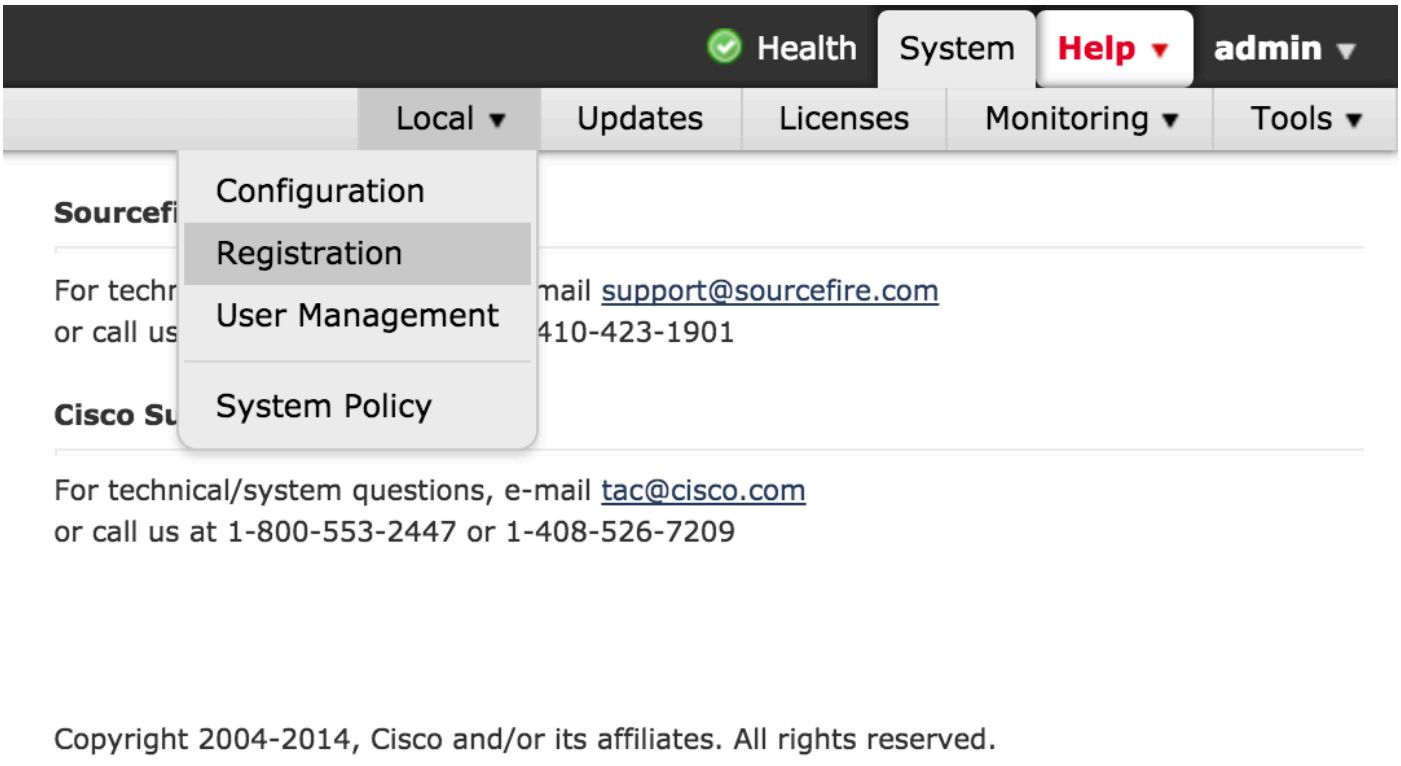
配置高可用性

以下是配置高可用性的8个步骤。

步骤1.确认软件和硬件版本以及VDB版本和规则更新版本相同。

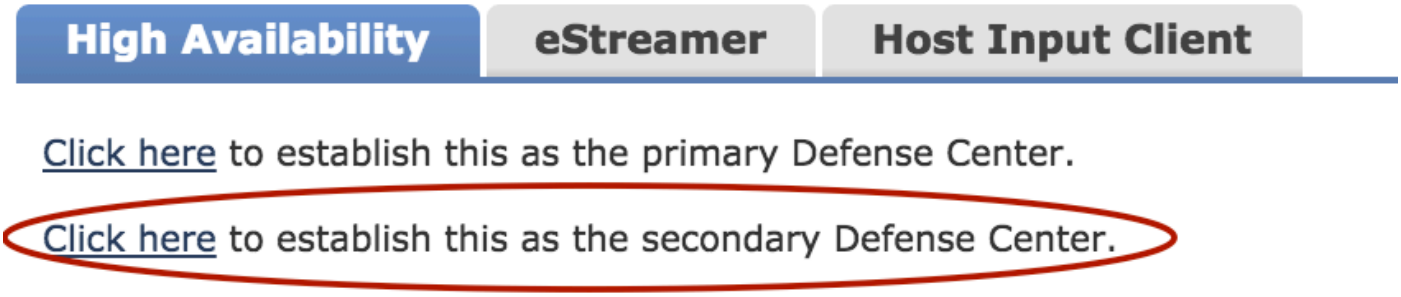
Model	Defense Center 1500
Serial Number	BZDW14300158
Software Version	5.4.1.2 (build 38)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 262)
Rule Update Version	2015-11-16-001-vrt
Rulepack Version	1606
Module Pack Version	1837
Geolocation Update Version	None
VDB Version	build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

步骤2.要使设备成为辅助设备，请导航至**System > Local > Registration**，如图所示。确保此DC上没有配置。

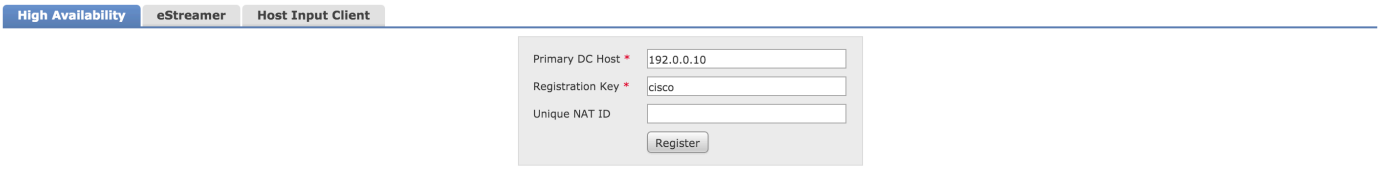


步骤3.在High Availability选**项卡**下，单击**Click here（单击此处）将其建立为辅助防御中**心，如图所

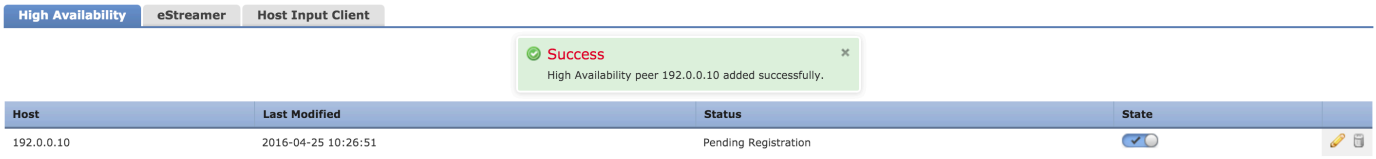
示：



步骤4.完成步骤3后，将显示一个页面，如图所示。添加主DC的IP和密钥。 确保为网络地址转换后的设备添加唯一的NAT ID。



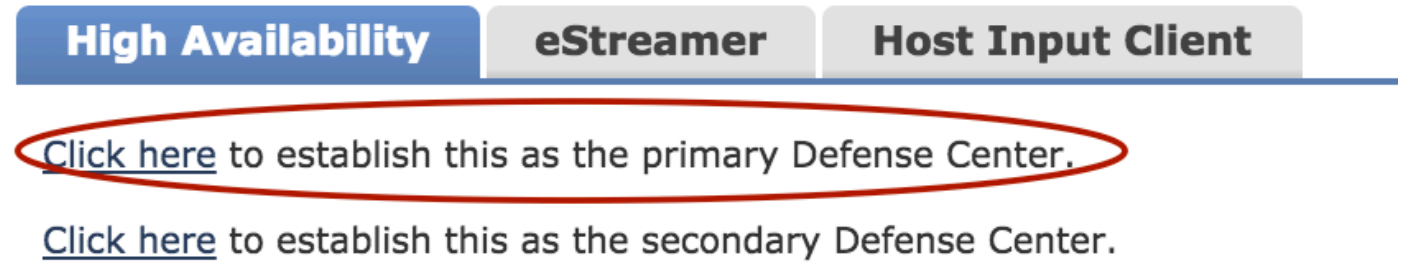
步骤5.在验证IP地址后，如果正确，请单击**Register**。您会看到如图所示的页面：



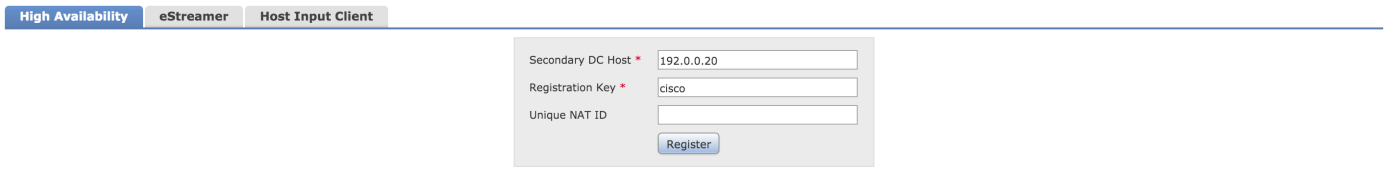
这意味着在辅助DC上配置了HA，您需要在主DC上配置它。

步骤6.登录要配置为主DC的设备。导航至**System > Local > Registration**。

在“高可**用性**”选项卡下，**单击此处添加为主防御中心**，如图所示：

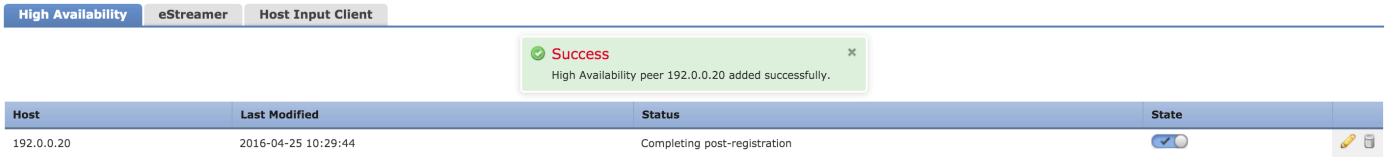


步骤7.完成步骤6后，将显示一个页面，如图所示：



添加辅助DC IP。提供配置辅助DC时提供的相同注册密钥和NAT ID。

步骤8.验证IP的详细信息后，单击“注册”。注册完成后，“成功”页将显示如图所示：



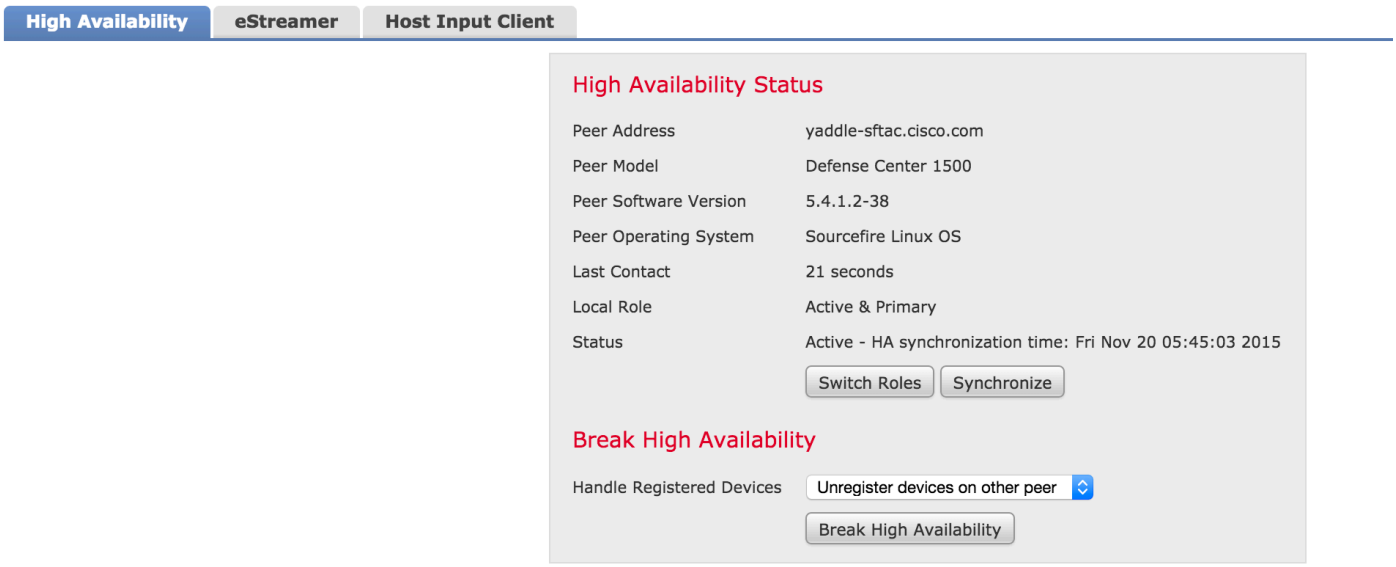
5-10分钟后，HA的配置和同步完成。

完成HA的配置和同步大约需要5到10分钟

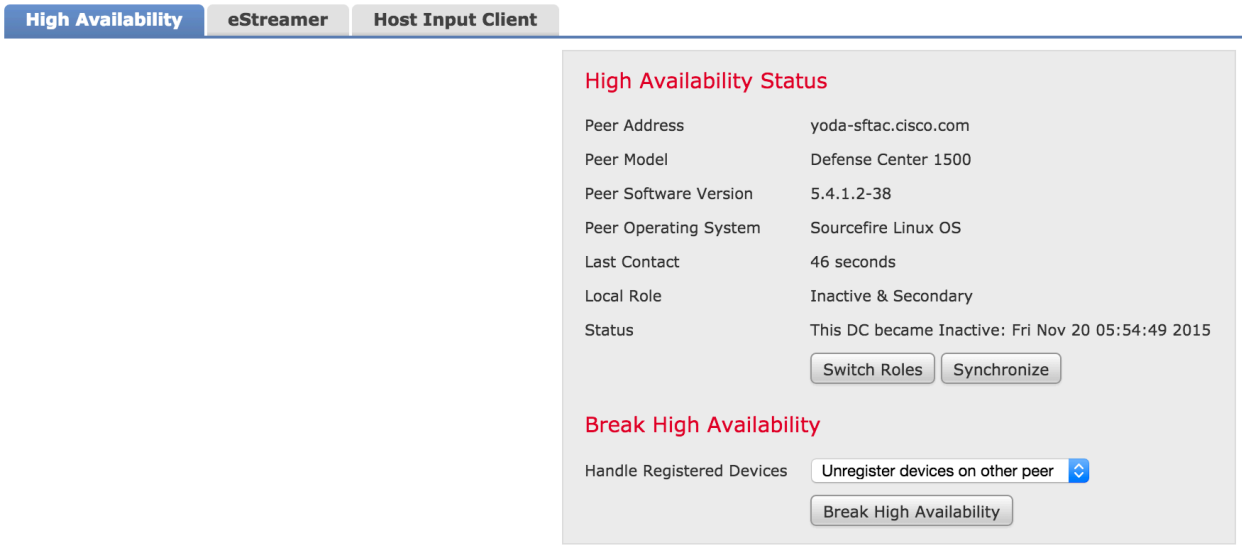
验证

逐步配置，以验证您的DC是否已正确配置以实现高可用性。

步骤1.导航至主设备上的System >Local >Registration，如图所示：



步骤2.导航至System >Local >Registration 如图所示：



故障排除

本节提供高可用性的基本故障排除步骤。

- 确保两个DC都在侦听TCP端口8305，因为HA使用此端口来同步信息和心跳。
- 确保TCP端口8305不会被网络或任何中间设备阻止。
- 如果删除或替换之前对等设备的过时条目，则HA创建失败。EM_Peers表提供有关此类对等设备的详细信息。

相关信息

- [在Cisco Firepower 8000系列设备上配置堆栈]
- [Firesight系统用户指南5.4.1]
- [技术支持和文档 - Cisco Systems]