目录

简介

本文描述High Availability(HA)的配置系列3防御的Centers(DC)。

先决条件

要求

Cisco 建议您了解以下主题：

- 火力技术
- 基本高性能的概念

使用的组件

本文档中的信息根据火力防御中心系列运行从软件版本5.3到软件版本5.4.1.6的3个设备(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

要保证操作连续性，高性能的功能允许您选定冗余防御中心管理设备。防御中心维护从受管理设备和这些设备某些配置元素的事件数据数据流。如果中心一的防御发生故障，您能监控您的网络，不用中断通过另一防御中心。

高性能的功能

- 含义的HA同步是双向的，即使有一个指定主要的和辅助设备，在任何一个添加的更改设备复制对其他。
- HA不要求直接地连接的设备。HA连接可以在交换机完成，但是此连接需要在同一广播域。
- HA设备在他们的管理IP连通在端口8305。
- 设备的HA同步时间是五分钟，因此意味着在每五分钟之后设备尝试同步其与其对等体的配置。因为同步的所需的时间是特定对设备，累积，同步时间可以最大化到十分钟。
- 如果重新镜像为特定HA对等体要求推荐中断HA然后再镜像。
- 如果计划升级HA集群中断HA是不必要的。当您从版本5.3.0到5.4.0时升级，逐个请升级设备和，一旦他们升级执行在主要防御中心的一同步任务。
- 一个访问策略的出现与同一名称的在两DC创建同一名称的两项访问控制策略。一项策略配置本地，并且其他从对等体DC同步。

  注意：您不能添加目标或运用此策略，因为投掷错误，阐明，已经有与同一名称的一项策略。
- 许可证没有同步在DC对等体之间，因此，他们要求分开被添加到DC。
- 所有受管理设备仅被添加到一个DC。配置同步在对等体DC之间。
- 受管理设备对两DC的发送日志。
- DC同步最新的操作。例如，如果删除从DC-1的一个用户，另一对等体DC-2不同步用户配置对DC-1。它**删除操作，**并且用户从DC-1 & DC-2失去。

配置共享双向在对等体之间

HA DC同步策略双向。这些配置被同步双向在对等体之间。您能在它旁边也查看大多与路径定义的权利的这些配置：

标识和验证

- 外部IDAP配置导航对**系统>本地>用户管理>外部验证**
- 用户(内部和外部) -导航toSystem **> Local>用户Management>用户**
- 自定义用户角色 **>本地>用户管理>用户角色**

报告

- 报告模板**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、相关性策略和规则、法规遵从性whitelist和数据流配置文件。

- 入侵规则(本地和SRU) -请导航toPolicies **> Intrusion>规则编辑器>本地规则。**
- 网络发现，主机属性，网络发现用户反馈，包括笔记和主机重要性、主机的删除，应用程序和网络从网络图和漏洞的去活或者修改。
- 定制应用探测器
- 在用户策略的LDAP连接导航toPolicies **> Users**
- 戒备**Policies>操作>警报**(在答复下)

设备信息

- NAT规则导航toDevices **> NAT**
- VPN规则 **> VPN**
- 所有设备信息包括名称和其组被同步双向。日志存储设备的位置每个设备的也被同步在对等体之间 **>设备管理**
- 自定义入侵规则分类
- 激活的自定义指纹
- 系统策略和卫生政策
- 自定义显示板、自定义工作流和自定义表
- 崔凡吉莱调节、快照和报告设置
- Sourcefire规则更新(SRU)， Geolocation数据库(GeoDB)和漏洞数据库(VDB)更新

配置没有同步了在DC之间

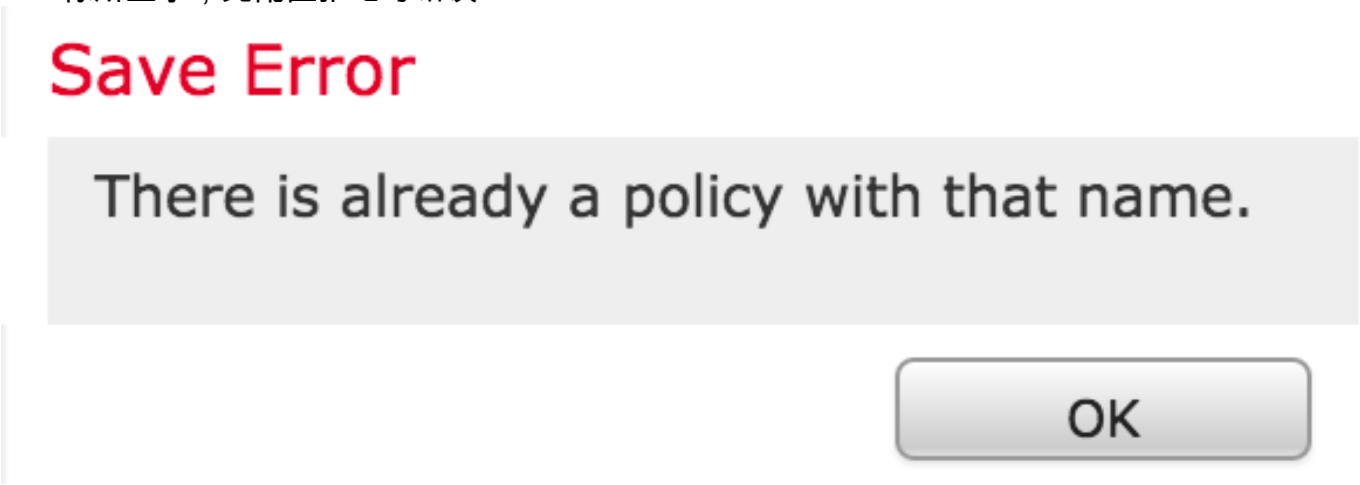
- 在用户策略的用户代理信息
- NMAP扫瞄
- 答复组
- 修正模块
- 修正实例
- Estreamer和主机输入客户端
- 备份配置文件
- 日程
- 许可证
- 更新
- 健康警报

配置

配置高可用性的前提

- 设备必须是同样软件和硬件版本。
- 设备必须有安装的同样VDB。
- 设备必须有同样SRU。
- 保证两防御中心有名为与管理员权限的admin的用户帐户。这些帐户必须使用同一个密码。
- 保证除管理帐户之外，两防御中心没有与相同的用户名的用户帐户。在您设立高可用性前，请删除或重命名一重复的用户帐户。

- 保证两个设备没有与同一名称的任何访问控制策略。如果有与同一名称的两项访问控制策略他们在DC共存。然而，他们不能与任何设备有关联。一旦在添加目标设备以后保存此策略，如镜像所显示，此配置拒绝与错误：



- 两防御中心必须访问互联网。

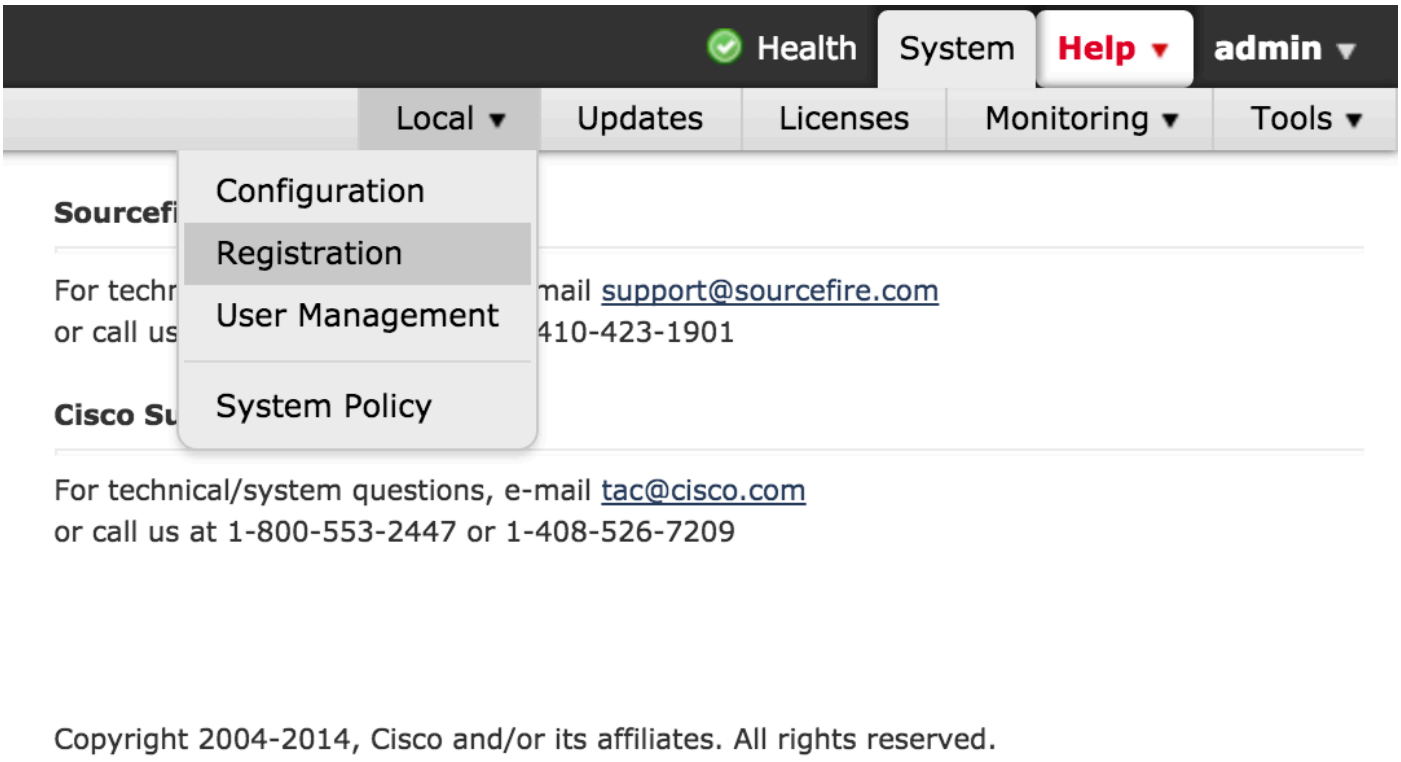
配置高可用性

这些是配置高可用性的8个步骤。

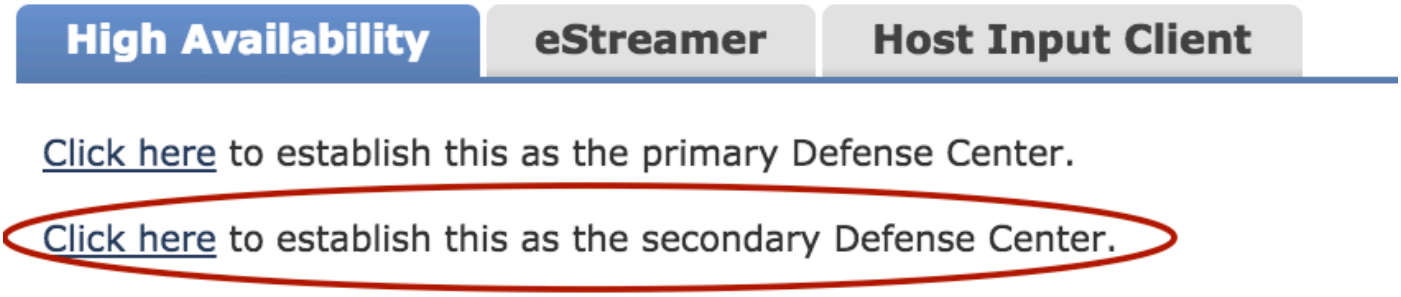
步骤1.确认与VDB版本一起的软件和硬件版本和规则更新版本是相同的。

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)

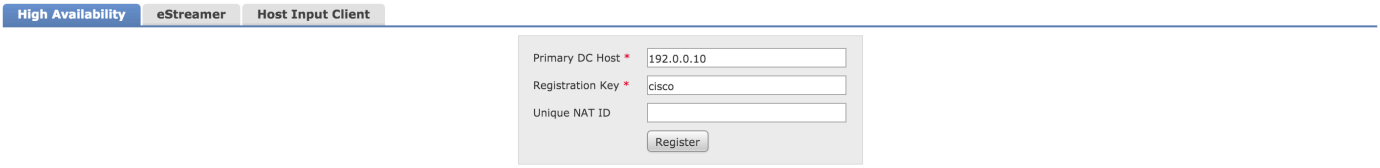
步骤2.如镜像所显示，为了做您的设备第二，请导航对**系统>本地>注册**。保证您没有在此DC的配置。



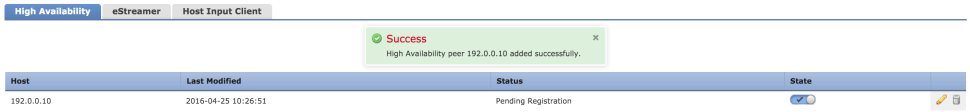
第三步：如镜像所显示，在**高性能的**选项卡下请单击**点击此处设立此作为一附属防御中心**，：



第四步：因为您完成步骤3，如镜像所显示，页显示。添加主要的DC和通行证密钥的IP。 保证您添加设备的唯一NAT ID，是在网络地址转换后。



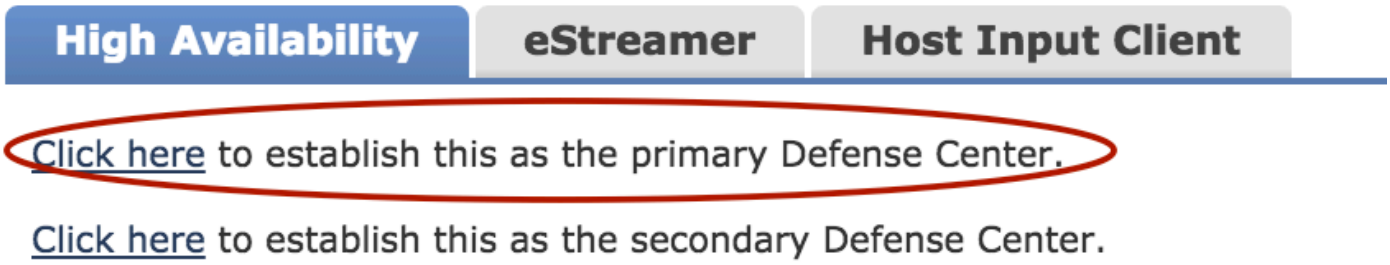
第五步：在IP地址验证后，如果正确请点击**寄存器**。如镜像所显示，您看到页：



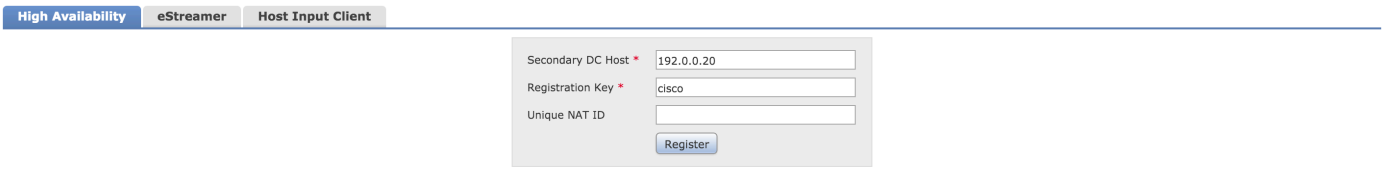
这意味着HA在第二DC配置，并且您在主要的DC需要配置它。

步骤6.您希望配置作为主要的DC的设备的洛金。导航对**系统>本地>注册。**

如镜像所显示，在**高性能的**选项卡下请单击**点击此处添加作为主要防御中心**， ：

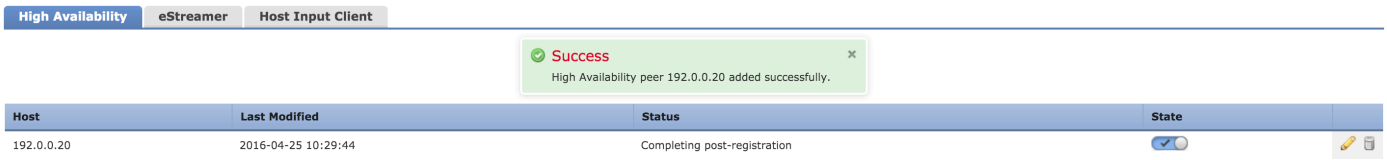


步骤 7.在您完成步骤6后，如镜像所显示，页显示：



添加第二DC IP。提供同一注册密钥和提供的NAT id，当您配置第二DC时。

步骤 8在IP的详细信息验证后请点击**寄存器。** 一旦注册完成，如镜像所显示，成功页被看到：



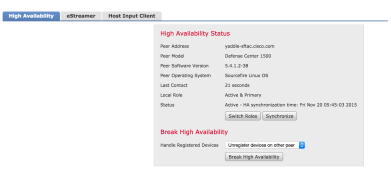
在5-10分钟之后HA的配置和同步完成。

需要差不多5-10分钟为了完成

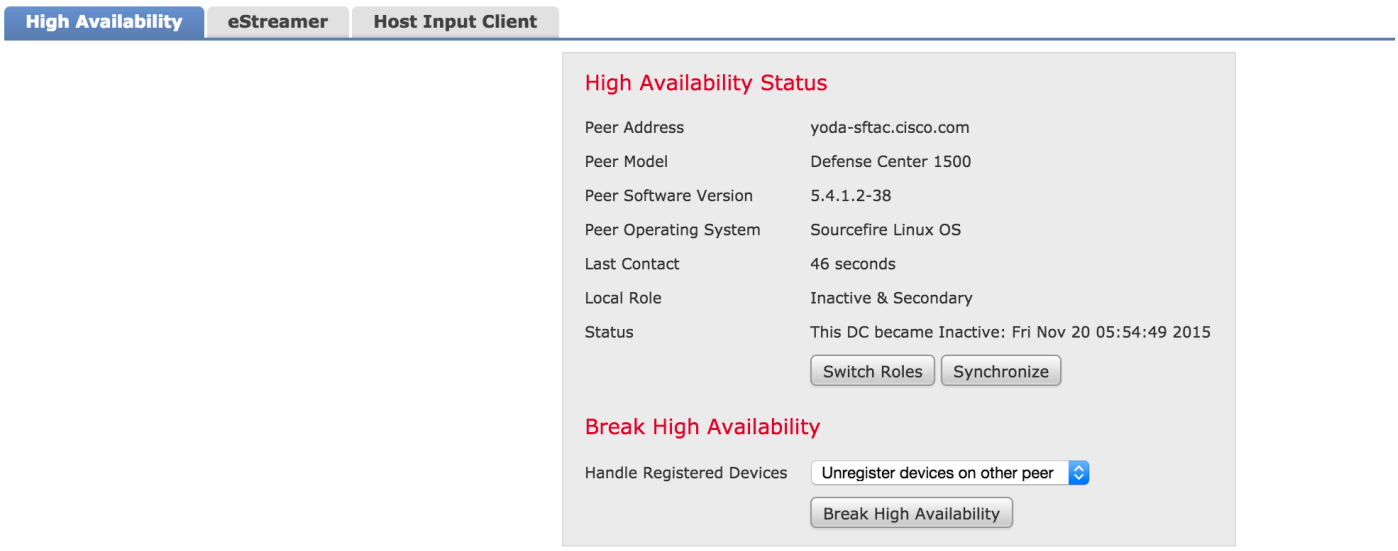
验证

验证逐步的配置您的DC为高可用性正确地配置。

步骤1.如镜像所显示，导航对在主要设备的**系统>Local >Registration** ：



步骤2.**系统>Local >Registration** ：



故障排除

此部分为高可用性提供基本故障排除步骤。

- 保证DC在TCP端口8305侦听的两个，因为HA使用此端口同步信息和检测信号。
- 保证TCP端口8305没有阻塞在网络或由所有中间设备。
- HA创建发生故障，如果有删除或替换一上一个对等设备的一个过时的条目。EM_Peers表在这样对等设备提供更多信息。

相关信息

- 堆叠的配置在Cisco火力8000系列设备的
- Firesight系统用户指南5.4.1
- 技术支持和文档 - Cisco Systems