

在Cisco NAC中实现策略导入导出(PIE)的最佳实践

目录

- [简介](#)
- [先决条件](#)
- [要求](#)
- [使用的组件](#)
- [规则](#)
- [配置](#)
- [饼最佳实践推荐](#)
- [配置](#)
- [验证](#)
- [相关信息](#)

简介

本文目的将突出显示最佳实践指南保证策略进出口(饼)功能的成功实施在思科美洲台中。

先决条件

要求

熟悉要求与典型地配置的思科美洲台管理器(Clean Access管理器) Web接口和策略。参考思科美洲台版本的4.5版本注释什么的是和不支持饼。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科美洲台软件4.5.0

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。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置

饼最佳实践推荐

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用 [命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

配置

遵从如下所示的建议保证CAM策略进出口(饼)功能成功实施。

1. 思科建议您配置在两主控和接收方NACMs的同样自动更新设置(在**设备管理> Clean Access >更新>更新下**)保证所有NACMs有同样思科更新，在您执行一策略同步前。这是因为在重要的覆盖的当前检查在接收方的所有检查，如果执行在接收方NACM的思科更新用不同的自动更新设置然后执行策略同步。
2. 如果有一OOB NACM和与一个IB许可证的任何传统NACM，请确保您使用OOB NACM作为主控NACM和传统NACM作为接收方。
3. 一旦饼为在可控和接收方之间的一个特定的组件启用，接收器表/信息完全用从主控推送的信息替换。它不是渐增的在接收方。例如，如果接收方有允许对mcafee.com的访问，并且主控有交通规则对cisco.com和abc.com的允许的一个交通规则，但是mcafee.com的规则，接收方和主控不会有相同的规则，一旦同步被执行：cisco.com和abc.com。注意mcafee.com的交通规则在接收方不存在同步以后，因为主控没有该规则。最佳实践是如期望的一样配置主控NACM，但是不修改在接收方的策略设置。
4. 支持的接收方最大是10。虽然没有技术限制到接收方数量，最佳实践推荐是保持此对支持的编号(少于或等于到10)。**注意：** 对于NACM HA对，策略同步设置为待机NACM禁用。
5. 主控和接收方必须运行思科美洲台(4.5或更加高)版本同一个版本。
6. 保证两个美洲台管理器安排Certificate Authority (CA)签名证书和两主控和接收方委托证书彼此。证书是关键获取在可控和接收方之间的同步。主控必须委托接收方提交的证书和反过来也是一样地。对于此，保证是必要的每一个有他们的对等项证书(全双工一系列根CA，如果中间是包含的)在委托CA列表。在生产部署，最佳实践是替换在美洲台管理器的自签名证书用CA签名证书。简而言之，请确保美洲台管理器SSL证书最佳实践满足，在您实现饼前。
7. 确保您登陆，重要的美洲台管理器的一个完全控制管理员用户为了执行自动或手工的策略同步。
8. 自动同步允许您安排一自动策略同步，一旦几天每个X编号(最低是1天)。如果希望使用自动同步饼，思科强烈建议您执行一手工的同步和验证同步顺利地运作，在您启用在您的美洲台管理器之间前的自动同步。

验证

当前没有可用于此配置的验证过程。

相关信息

- [技术支持和文档 - Cisco Systems](#)