监控 Cisco Secure Workload 中的配置

可用的**监控 (Monitoring)** 选项会因您的角色而异。

代理监控

该页面会根据当前选定的根范围来显示集群中所有受监控代理的计数。

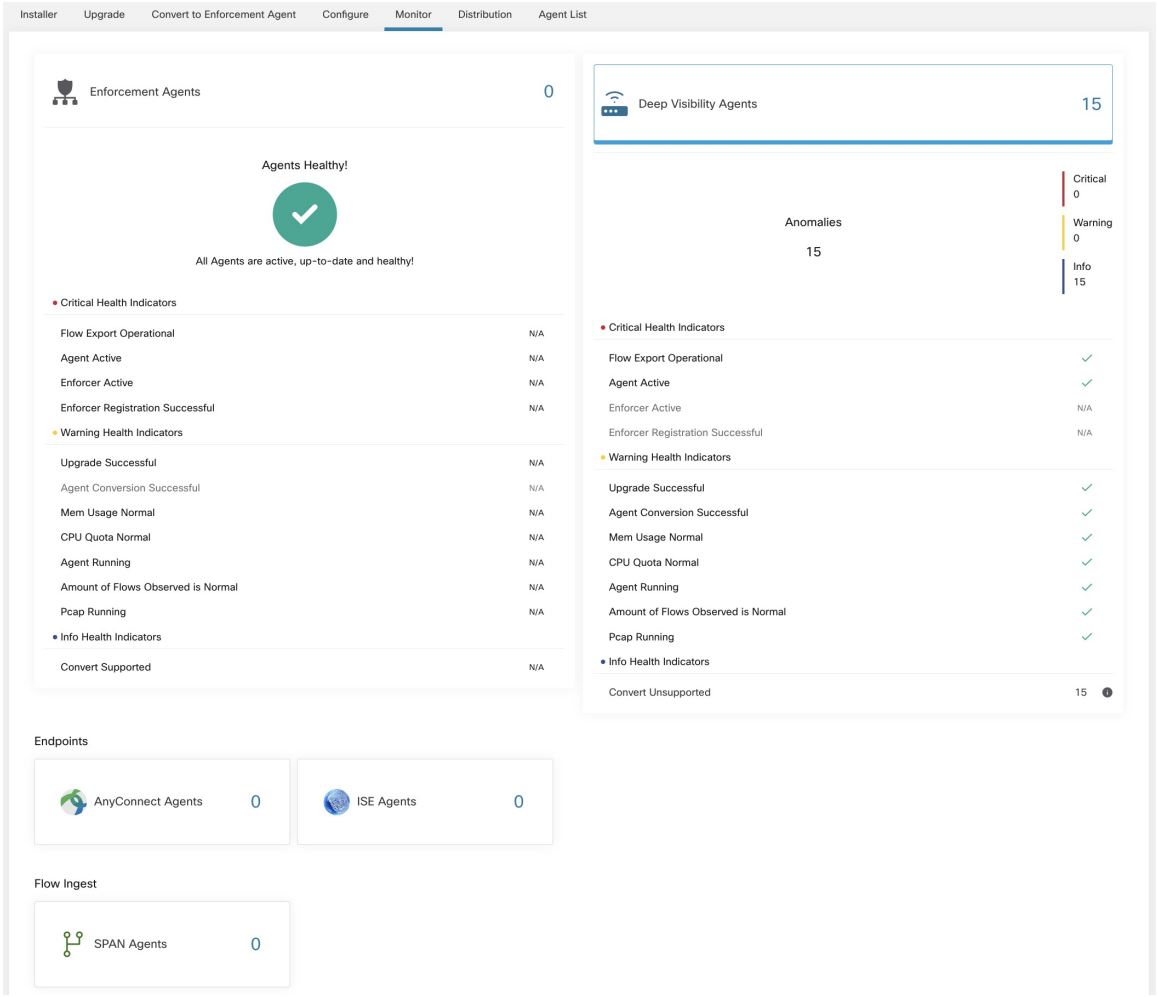
Note 资产总数是应用收集规则后在网络上观察到的所有资产的总和。

代理监控类型

要监控代理，请点击左侧导航栏中的**管理 (Manage)** > **代理 (Agents)**，然后点击**监控 (Monitor)** 选项卡。

此页面仅适用于具有**站点管理员 (Site Admin)** 和**客户支持 (Customer Support)** 角色的用户。**范围所有者**可以查看资产、深度可视性代理和执行代理。

Figure 1: 已安装的代理总数



下表显示了每种代理类型之间的差异。

代理类型	说明
深入可视性	就时序流数据、主机上运行的进程提供最高精确度。支持大多数 Linux 和 Windows 平台。请参阅 sw_agents_deployment-label
执行	提供深度可视性代理中的所有可用功能。此外，执行代理能够在已安装的主机上设置防火墙规则。

AnyConnect	在运行具有网络可视性模块 (NVM) 的 AnyConnect 安全移动代理的终端上提供时序流数据，而无需安装任何思科 Cisco Secure Workload 代理。NVM 生成的 IPFIX 记录会被发送到 Cisco Secure Workload AnyConnect 代理连接器。支持 Windows、Mac 和某些智能手机平台。
ISE	提供有关向思科 ISE 注册的终端的元数据。通过 ISE pxGrid，ISE 连接器会收集元数据，在 Cisco Secure Workload 上注册 ISE 终端，因为 ISE 代理会根据从 ISE 设备获取的属性和登录到终端的用户的 LDAP 属性推送标签。
下表简要总结了思科 Cisco Secure Workload 提供的各种设备代理。	
设备代理	说明
SPAN	提供流分析，而无需安装任何每主机代理。它在 Cisco Secure Workload ERSPAN VM 设备中运行。它会使用任何思科交换机获取的 ERSPAN 数据包。

Note 现在支持 NetFlow、NetScaler、F5、AWS 和 AnyConnect Proxy 等设备代理作为连接器。有关连接器的详细信息，请参阅什么是连接器。

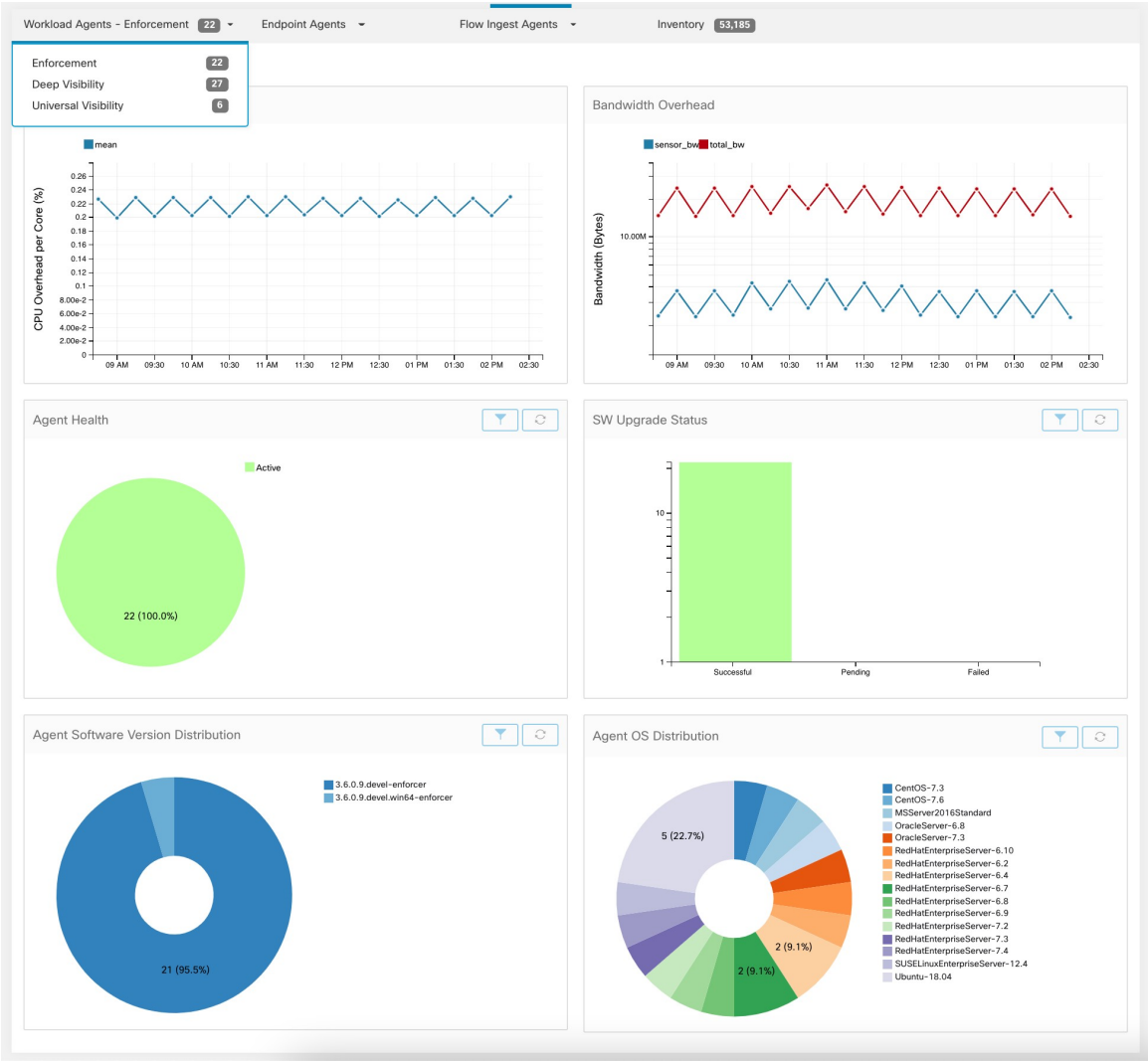
任何非零代理类型按钮都可进一步深入了解每种代理类型的分布情况。

代理状态和统计信息

要查看本主题中介绍的图表，请依次选择**管理 (Manage) > 代理 (Agents)**，然后点击**分布 (Distribution)** 选项卡。

以下图表适用于深度可视性和执行代理类型。

Figure 2: 代理分布



对于每种代理类型，该页面都会提供注册代理的概述和运行状况，包括总体CPU开销、带宽开销、错过的数据包、操作系统/版本分布和代理升级状态。

CPU 开销图表

“CPU 开销”图表提供所有代理每个核心的 CPU 开销的汇聚视图。每个代理的 CPU 开销作为工作负载配置文件的一部分提供。此图表仅适用于深度可视性和执行代理类型。

带宽开销图表

“带宽开销”图表提供总带宽和代理使用的带宽的汇总统计信息。每代理带宽开销作为工作负载配置文件的一部分提供。此图表仅适用于深度可视性和执行代理类型。

代理运行状况图表

“代理运行状况”图表提供活动或非活动代理的数量。活动代理会定期向配置服务器报告升级情况。检查间隔为30分钟。如果看到某个代理错过了来自代理的两个以上的签入期，则它将被声明为非活动代理。

软件代理更新到最新版本图表

每次代理向配置服务器报到时，代理也会提供其当前的RPM版本。如果代理配置为特定版本，并且在 2 个签入期后无法更新，则该代理将被声明为无法升级到最新版本。

错过的代理数据包图表

在极少数情况下，当穿越主机的流量大于代理的检测速度时，系统会跳过一些数据包进行分析。错过的数据包数和相应的代理名称显示在此图表中。

代理软件版本和操作系统分布图

这些图表将显示向 Cisco Secure Workload 集群注册的所有代理的代理版本分布和父操作系统平台。

执行状态

要查看执行状态，请点击窗口左侧导航栏中的**防御 (Defend)** > **执行状态 (Enforcement Status)**。

此页面可供站点管理员/客户支持用户和范围所有者大致了解所有执行代理的当前状态，包括正在执行策略的云连接器。

如果任何图表显示红色或橙色，请参阅相应主题：

Table 1: *“执行状态”(Enforcement Status)* 图表

图表	结果	采取行动
已启用代理执行 (Agent Enforcement Enabled)	未启用	确保在代理配置中启用执行。请参阅创建代理配置文件。
代理策略配置 (Agent Policy Config)	过期策略	这种情况一般是暂时的，通常不需要采取任何行动。这是因为基于标签的 Cisco Secure Workload 部署会动态地更新资产和策略。 但是，如果任何个别工作负载仍然存在这种情况，请联系思科技术支持中心。
代理具体策略 (Agent Concrete Policies)	已跳过	这表示策略未被推送到某些代理。

Tip

- 要查看单个范围或整个租户的状态，请使用页面左上角的**按范围过滤 (Filter by Scope)** 选项。
- 如果图表指明了存在问题，请点击图表的相关部分，确定哪些工作负载存在问题。

  该表会显示受影响的工作负载。

  或者，要查看过滤选项，请点击图表下方**过滤器 (Filter)** 框中的 (i) 按钮。
- 要查看更多详细信息，请点击已过滤的工作负载列表中的 IP 地址链接，以便显示“工作负载配置文件”(Workload Profile) 页面。

下表介绍了执行状态表中显示的字段。

字段	说明
主机名 (Host Name)	工作负载的主机名。
地址 (Address)	工作负载上所有接口的 IP 地址。
已启用执行 (Enforcement Enabled)	指明是否已在代理上启用执行。
同步的具体策略 (Concrete Policies in Sync)	这表示当前是否在代理上执行了所需版本的具体策略。
具体策略 (Concrete Policies)	如果任何主机的此值显示为已**跳过 (Skipped)**，则表示该主机上的代理已达到策略限制。（请参阅与策略相关的限制。）
策略计数 (Policy Count)	代理上的具体策略数。
状态 (Status)	最新策略配置执行的状态。如果状态为 **CONFIG_SUCCESS**，则表示当前版本已执行且没有任何问题。

云连接器的执行状态

如果您已设置 AWS 或 Azure 云连接器：

所有接口的执行状态都显示在执行状态页面上。如果策略应用成功，则表示策略同步，否则会显示相应的错误消息。

执行状态页面中的策略计数是 Cisco Secure Workload 记帐，但不是 AWS 或 Azure 规则记帐。

（仅限 AWS）此页面上的主机名字段派生自公共 DNS。如果给定 VPC 上未启用公共 DNS，则主机名字段为空。

暂停策略更新

Caution 此选项会暂停所有范围中所有工作负载的策略更新。

此功能需要站点管理员或客户支持权限。

要为所有范围内的所有执行终端暂停规则更新，请执行以下操作：

1. 从导航窗格中，选择**防御 (Defend)** > **执行 (Enforcement)**。
2. 点击**策略更新 (Policy Updates)** 旁边的状态。
3. 阅读并接受 EULA。

Figure 3: 防火墙规则不断更新

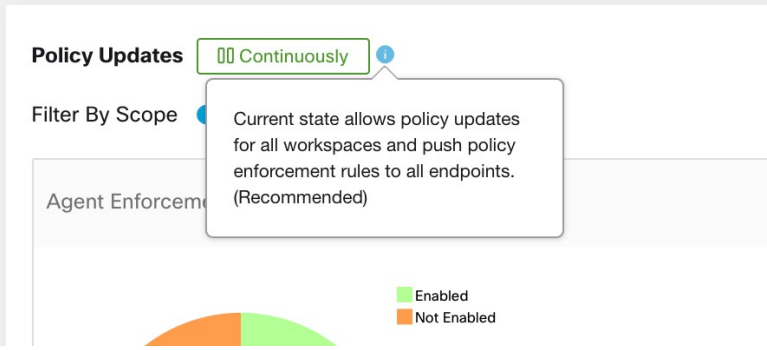
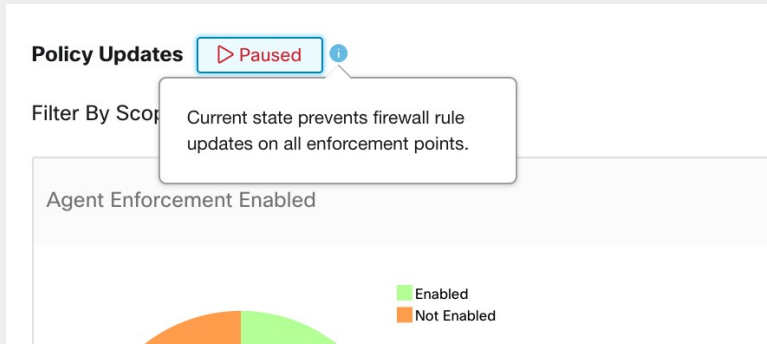


Figure 4: 防火墙规则更新已暂停



当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。