Cisco Secure Workload 中的外部协调器

外部协调器用于从网络系统中收集描述工作负载的现有元数据。某些外部协调器还可以执行分段策略。

对于授权记录系统中存在工作负载标签的部署，我们提供了一种通过外部协调器集成自动导入标签的方法。Cisco Secure Workload 将自动获知记录系统中的任何修改，并将其用于更新资产中的标签。

有关标签的功能和用途的详细信息，请参阅工作负载标签。

由于最近的 *GUI* 更新，用户指南中使用的某些图像或屏幕截图可能无法完全反映产品的当前设计。建议将本指南与最新版本的软件结合使用，以获得最准确的直观参考。

导航至“外部协调器”(External Orchestrators) 页面

通过从左侧菜单栏中选择**管理 (Manage)** > **工作负载 (Workloads)** > **外部协调器 (External Orchestrators)**，可以访问外部协调器的主页。

外部协调器列表

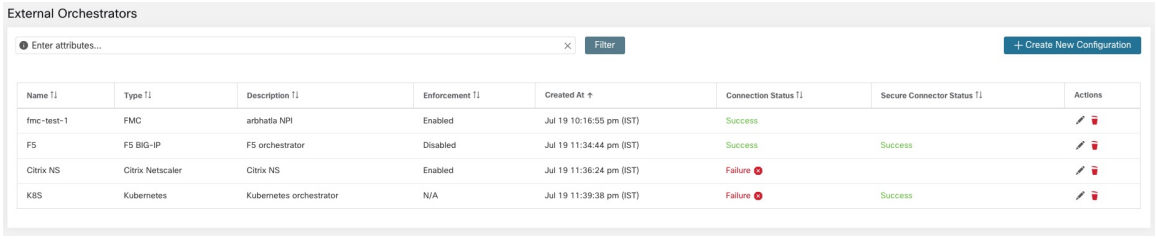
外部协调器页面显示现有外部协调器，并提供修改、删除和创建新外部协调器的功能：

Table 1: 外部协调器

类型	说明/何时使用
VMware vCenter	要将虚拟机数据（例如，主机名、IP 地址和标签）从 vCenter 服务器导入 Cisco Secure Workload。生成的标签可用于创建 Cisco Secure Workload 范围和执行策略。
Amazon Web Services	（您无法创建新的 AWS 协调器；而只能创建 AWS 连接器。请参阅 AWS 连接器。任何现有的 AWS 协调器均为只读）。要将 EC2 服务器实例的数据（例如主机名、IP 地址和标签）从给定 AWS 帐户导入 Cisco Secure Workload。生成的标签可用于创建 Cisco Secure Workload 范围和策略。
Kubernetes/OpenShift	导入 Kubernetes 的实体，例如节点、Pod、服务和标签。这些标签可在 Cisco Secure Workload 中用于定义范围和策略。
DNS	通过区域传输从 DNS 服务器导入 A/AAAA 和 CNAME 记录。这样会将 DNS 名称作为标签生成，在定义 Cisco Secure Workload 范围和策略时非常有用。
Infoblox	从启用 IPAM/DNS 的 Infoblox 设备导入具有可扩展属性的网络、主机和 A/AAAA 记录。导入的可扩展属性可被用作 Cisco Secure Workload 范围和策略中的标签。
F5 BIG-IP	从给定的 F5 负载均衡器读取虚拟服务器配置并为提供的服务生成标签，这些标签可用于在 Cisco Secure Workload 中定义执行策略。策略执行功能将通过 F5 REST API 将其转换为 F5 策略规则。
Citrix Netscaler	从给定的 Netscaler 负载均衡器读取虚拟服务器配置并为提供的服务生成标签，这些标签可用于在 Cisco Secure Workload 中定义执行策略。策略执行功能将通过其 REST API 将其转换为 Netscaler ACL。

类型	说明/何时使用
Secure Firewall Management Center	将策略部署到使用 REST API 注册到给定 Cisco Secure Firewall Management Center 的所有 Cisco Secure Firewall Threat Defense（以前称为 Firepower Threat Defense 或 FTD）设备。

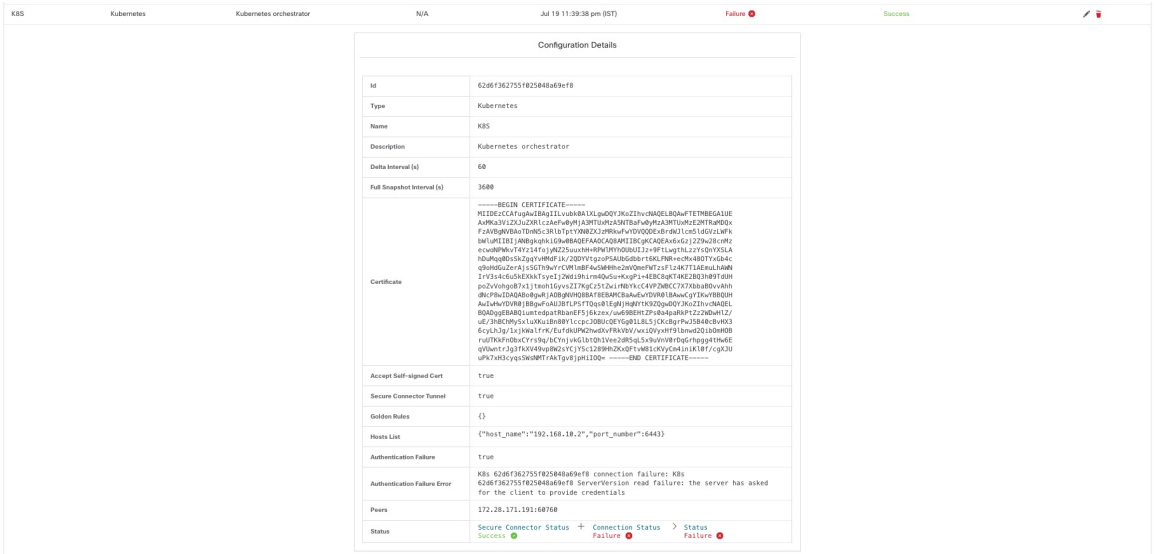
Figure 1: 外部协调器



每行显示外部协调器的简短版本，包括名称 *(Name)*、类型 *(Type)*、说明 *(Description)*、执行 *(Enforcement)*、创建时间 *(Created at)*、连接状态 *(Connection Status)* 和安全连接器状态 *(Secure Connector Status)*。连接状态会显示与给定外部数据源的连接是否成功。 安全连接器状态 *(Secure Connector Status)* 显示安全连接器隧道的状态：“成功”(Success) 或“失败”(Failure)。如果隧道未启用，则会显示 N/A。

在创建外部协调器配置时启用安全连接器隧道。如果启用了安全连接器隧道，则外部协调器的“连接状态”将取决于身份验证状态和安全连接器状态。如果未启用安全连接器隧道，则外部协调器的“连接状态”仅取决于身份验证状态。无论状态如何（成功或失败），您都可以点击相应的行以获取更多详细信息。有关安全连接器客户端指标的更多详细信息，请点击**状态 (Status)** 行，或在左侧窗格中导航至**管理 (Manage)** > **工作负载 (Workloads)** > **安全连接器 (Secure Connector)**。

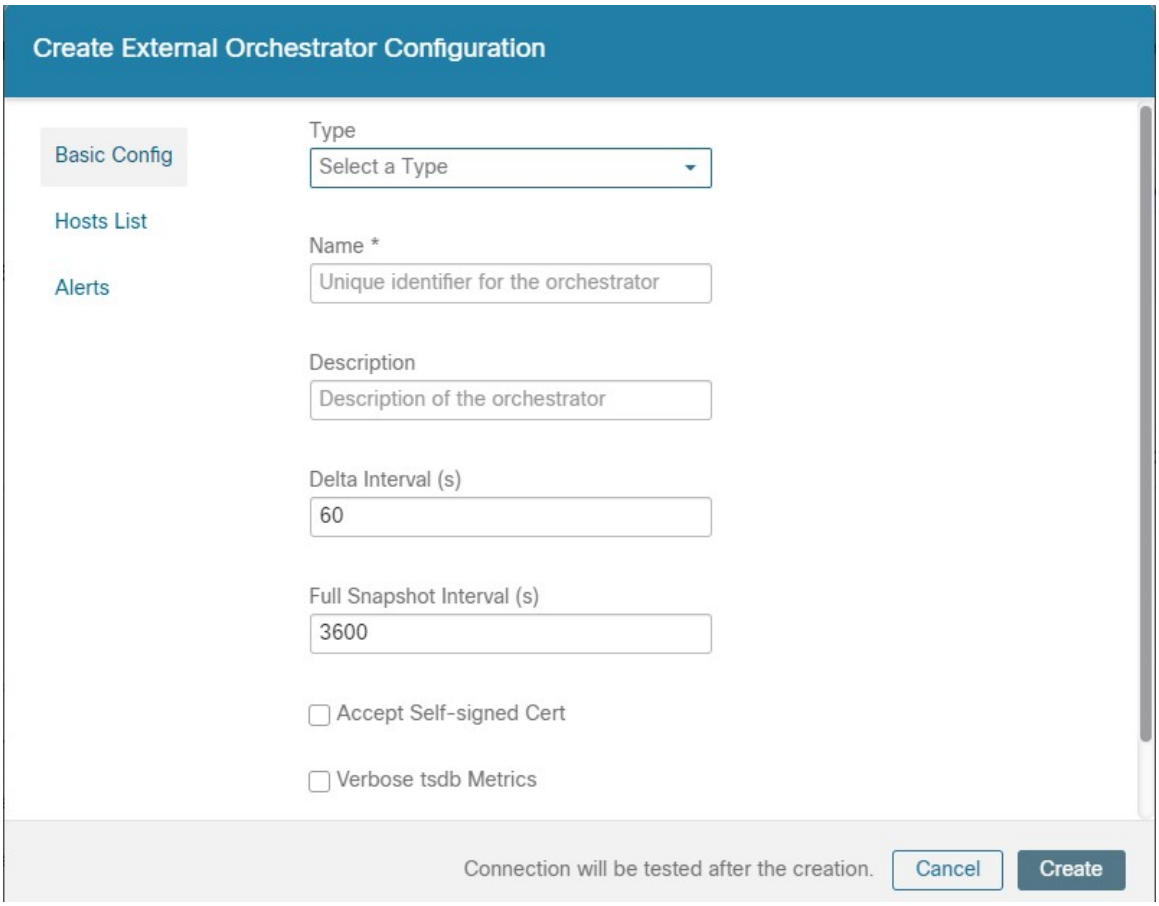
Figure 2: 外部协调器身份验证失败



创建外部协调器

可以通过点击外部协调器主页中的**创建新配置 (Create New Configuration)** 按钮来创建新的外部协调器。这将导致出现一个模式对话框，您可以在其中输入名称并选择外部协调器类型。下图显示基本配置页面：

Figure 3: 创建外部协调器配置



下表介绍外部协调器的常见字段。根据所选的类型，基本配置 *(Basic Config)* 页面需要提供其他参数。这些内容将在下面各个外部协调器的相应部分中介绍。

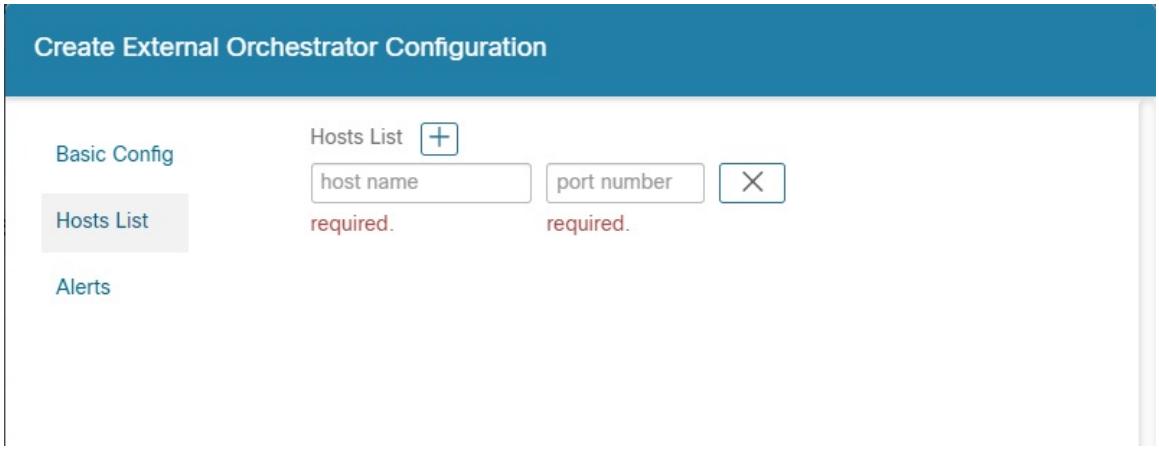
通用字段	必填	说明
类型 (Type)	是	从列表中选择外部协调器。
名称 (Name)	是	外部协调器的名称，对于活动租户必须是唯一的。
说明 (Description)	否	外部协调器的说明。

通用字段	必填	说明
完整快照间隔 (Full Snapshot Interval)	是	外部协调器尝试从所选类型导入配置的完整快照的间隔（秒）。
接受自签证书 (Accept Self-signed Cert)	否	选中此选项可接受 Cisco Secure Workload 用于从所选类型检索配置数据的 HTTPS 连接的自签名服务器证书。默认为不允许自签名服务器证书。
安全连接器隧道 (Secure Connector Tunnel)	否	选中此选项可将与 Cisco Secure Workload 集群的连接设置为通过安全连接器隧道建立隧道。

Note 上图所示的字段增量间隔 *(Delta interval)* 和详细 *TSDB* 指标 *(Verbose TSDB Metrics)* 为可选，仅适用于某些外部协调器，在下面的相应说明中进行了说明。

除外部协调器类型 *AWS* 外，必须提供主机列表。它指定外了部数据源的网络地址，外部协调器将从中获取数据并生成标签。这可以通过点击左侧的主机列表 *(Hosts List)* 选项卡来完成，如下图所示：

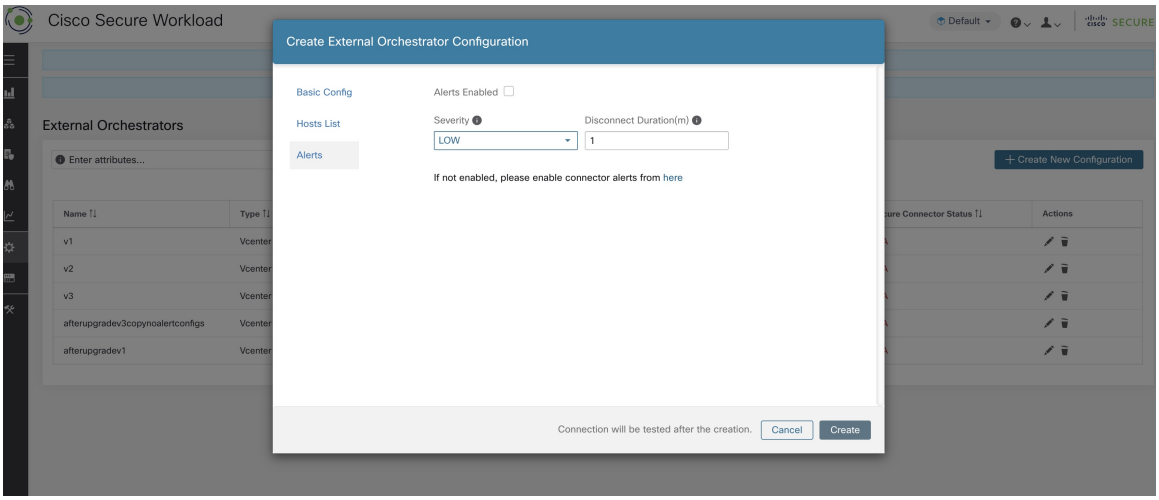
Figure 4: 外部协调器的主机列表



要添加新的主机列表条目，请点击加号。每一行都必须包含一个有效的 DNS 主机名、IPv4 或 IPv6 地址和端口号。根据所选的外部协调器类型，您可以输入多个主机以实现高可用性或冗余。有关详细信息，请参阅所选外部协调器的说明。

要为外部协调器设置警报，可以通过点击左侧的警报 *(Alert)* 选项卡来完成此操作，如下图所示：

Figure 5: 外部协调器的警报



对于每个外部协调器，配置警报需要提供其他参数。这些内容将在下面各个外部协调器的相应部分中介绍。

要为此外部协调器启用警报，请选中警报已启用 *(Alert enabled)* 复选框。

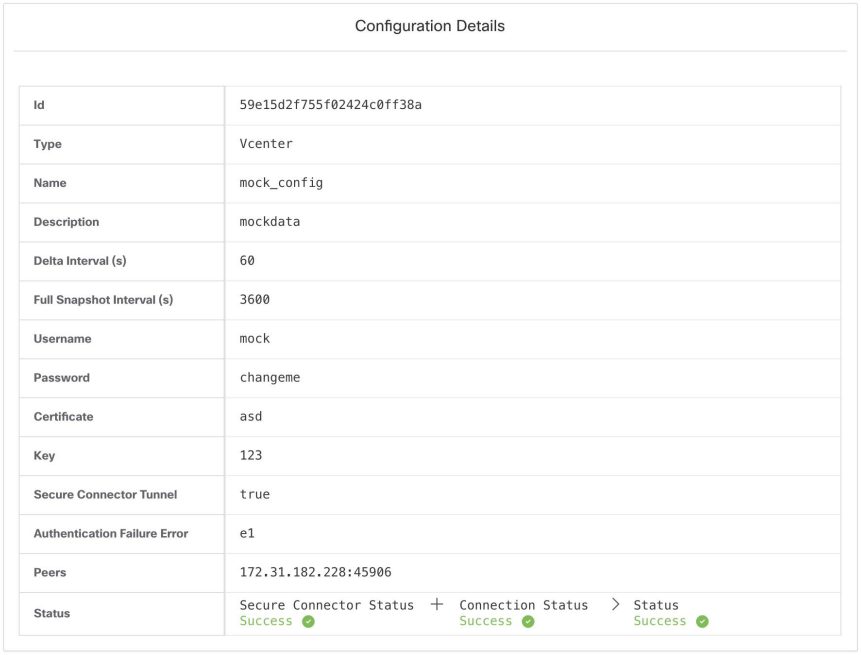
Note 确保还从**管理 (Manage)** > **工作负载 (Workloads)** > **警报配置 (Alert Configs)** 页面启用了连接器警报。

选择警报严重性级别和断开连接持续时间（以分钟为单位），以配置外部协调器警报。

字段	说明
严重性 (Severity)	选择此规则的严重性级别：**LOW**、**MEDIUM**、**HIGH**、**CRITICAL** 或 **IMMEDIATE ACTION**
断开连接持续时间（分钟）(Disconnect Duration[m])	连接断开的时间。

点击**创建 (Create)** 按钮以创建新的外部协调器，可以通过点击列表视图中的相应行来查看其配置详细信息：

Figure 6: 外部协调器的配置详细信息

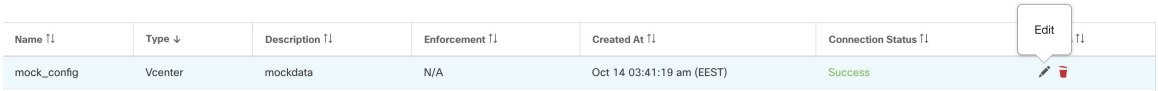


Note 由于从外部协调器提取第一个完整快照是异步操作，因此连接状态字段的更新时间大约为一分钟。

编辑外部协调器

点击外部协调器行右侧的铅笔按钮（如下所示），打开一个与创建外部协调器的模式对话框类似的模式对话框，然后您可以在其中修改配置。

Figure 7: 编辑外部协调器



Note

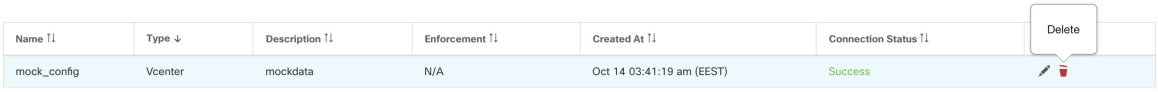
- **类型 (Type)** 字段不可编辑。
- 如果配置使用密钥/证书来进行身份验证，则每次更新配置时都必须提供密钥和证书。
- 由于外部协调器的配置更改是一项异步操作，因此连接状态字段的更新和输入更改的正确性确认需要大约一分钟的时间。

点击**更新 (Update)** 按钮以保存对配置所做的更改。

删除外部协调器

Caution 删除外部协调器也会删除该协调器提供的标签，而这将影响策略。要删除外部协调器，请点击垃圾桶按钮，如下所示：

Figure 8: 删除外部协调器



协调器生成的标签

Cisco Secure Workload 会将以下标签添加到所有 AWS 实例。

键	值
orchestrator_system/orch_type	AWS
orchestrator_system/cluster_name	<*kubernetes* 集群的名称>
orchestrator_system/name	<连接器的名称>
orchestrator_system/cluster_id	<*UUID of the orchestrator’s configuration in |product|*>

Amazon Web Services

Note AWS 外部协调器功能现在已成为新 AWS 云连接器功能的一部分。如果您已升级到此版本，则现有 AWS 外部协调器现在是只读的；如果需要进行更改，请创建新的 AWS 连接器。有关完整信息，请参阅 AWS 连接器。

Cisco Secure Workload 支持从 AWS 区域自动实时注入资产。在为“aws”类型添加外部协调器配置时，Cisco Secure Workload 设备将连接到 AWS 终端，并获取处于运行/停止状态的所有实例的元数据。

前提条件

- 使用的安全令牌（访问密钥和秘密）应具有正确类型的 IAM 权限，以允许获取协调器信息。

配置字段

属性	说明
ID	协调器的唯一标识符。
名称	用户指定的协调器名称。
类型	协调器类型 -（在本例中为 *aws*）
说明	协调器的简短说明。
AWS 访问密钥 ID	与创建协调器配置的帐户相关联的 ACCESS KEY。
AWS 密钥访问密钥	与您为协调器配置创建的帐户关联的密钥。 **Note** 如果修改协调器配置，请重新输入密钥。
AWS 区域	已部署工作负载的区域。如果工作负载分布在多个区域，则每个区域都需要单独的配置。有关正确的区域值，请参阅下面的链接。:ref:https://docs.aws.amazon.com/general/latest/gr/rande.html。
接受自签证书	为 AWS 自动标记为 true。用户无法对其进行编辑。
完整快照间隔	以秒为单位的完整快照间隔。协调器资产管理器将从协调器执行全面刷新轮询。
增量快照间隔	以秒为单位的增量快照间隔。协调器资产管理器将只从协调器获取增量更新。
主机列表	AWS 协调器类型不需要主机列表。AWS 的终端将源自上面的 *AWS* 区域 *(AWS Region)* 字段。此字段应留空。
详细 TSDB 指标	如果启用，系统将报告每个协调器的 tsdb 指标。否则，将报告所有协调器指标的汇聚。
安全连接器隧道	通过安全连接器隧道建立到此协调器主机的隧道连接。

工作流程

- 使用上述配置字段来配置 AWS 协调器。

协调器生成的标签

Cisco Secure Workload 会将以下标签添加到所有 AWS 实例。

键	值
orchestrator_system/orch_type	AWS
orchestrator_system/cluster_name	<*kubernetes* 集群的名称>
orchestrator_system/name	<连接器的名称>
orchestrator_system/cluster_id	<*UUID of the orchestrator’s configuration in |product|*>

实例特定标签

以下标签是实例特定的。

键	值
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	<由 *AWS* 分配的 *InstanceID*>
orchestrator_system/machine_name	<由 *AWS* 赋予此节点的 *PublicDNS(FQDN)*>
orchestrator_‘<AWS Tag Key>‘	<*AWS* 标记值>

故障排除

- AWS 区域和可用区域之间存在混淆。

  这两个值相互关联，不应被混淆。例如，us-west-1 可能是区域，可用性区域可以是 us-west-1a 或 us-west-1b 等。在配置协调器时，应使用区域 *(Region)*。有关所有区域，请参阅 https://docs.aws.amazon.com/general/latest/gr/rande.html。

- 更新协调器配置后出现连接/凭证问题。

  每次配置更新时，客户都必须重新提交 *AWS* 密钥。

Kubernetes/OpenShift

Note EKS 和 AKS 外部协调器功能现已分别成为 AWS 和 Azure 云连接器新功能的一部分。如果升级到此版本，现有的 EKS 和 AKS 外部协调器现在为只读；如果需要更改，请创建新的 AWS 或 Azure 连接器。有关完整信息，请参阅云连接器下的相关主题。

用于普通 Kubernetes 和 OpenShift 的外部协调器没有变化。

Cisco Secure Workload 支持从 Kubernetes 集群实时自动注入资产。当为 Kubernetes/OpenShift 集群添加外部协调器配置时，Cisco Secure Workload 会连接到集群的 API 服务器并跟踪该集群中节点、Pod 和服务的状态。对于每种对象类型，Cisco Secure Workload 会导入所有 Kubernetes 标签和与对象关联的标签。所有值均按原样导入。

除了导入为 Kubernetes/OpenShift 对象定义的标签之外，Cisco Secure Workload 还会生成便于在资产过滤器中使用这些对象的标签。这些附加标签在定义范围和策略时特别有用。

有关所有这些标签的详细信息，请参阅与 Kubernetes 集群相关的标签。

如果在Kubernetes节点上启用了执行（安装了执行代理，并且配置文件在这些代理上启用了执行），则将使用通过此集成。

关于云平台上的 Kubernetes

对于在支持的云平台上运行的以下托管 Kubernetes 服务，此协调器的功能可通过云连接器提供：

- 在 Amazon Web 服务 (AWS) 上运行的弹性 Kubernetes 服务 (EKS)
- 在 Microsoft Azure 上运行的 Azure Kubernetes 服务 (AKS)
- 在 Google Cloud 平台 (GCP) 上运行的 Google Kubernetes Engine (GKE)

有关从云平台上的 Kubernetes 集群获取数据的详细信息，请参阅云连接器下的主题。

要求和前提条件

- 有关支持的 Kubernetes 和 OpenShift 版本，请参阅https://www.cisco.com/go/secure-workload/requirements/integrations
- 安全连接器隧道，如果需要可用于实现连接。

配置字段

以下配置字段与协调器对象中的 Kubernetes 协调器配置有关。

字段	说明
名称	用户指定的协调器名称。

字段	说明
说明	用户指定的协调器说明。
增量间隔	检查 Kubernetes 终端是否有更改的时间间隔（以秒为单位）
完整快照间隔	对 Kubernetes 数据执行完整快照的时间间隔（以秒为单位）
用户名	协调终端的用户名。
密码	协调终端的密码。
证书	用于身份验证的客户端证书
键	与客户端证书对应的密钥。
身份验证令牌	不透明身份验证令牌（持有者令牌）。
CA 证书	用于验证协调终端的 CA 证书。
Accept Self-Signed Cert	用于禁用 Kubernetes API 服务器证书的 strictSSL 检查的复选框
详细 TSDB 指标	维护每个 Kubernetesorchestrator 指标 - 如果设置为 False，则仅维护 Cisco Secure Workload 集群范围的指标。
安全连接器隧道	通过安全连接器隧道建立到此协调器主机的隧道连接
主机列表	{“host_name”, port_number} 对的数组，指定 Cisco Secure Workload 必须如何连接到协调器
K8s 管理器类型	kubernetes 集群的管理器类型（Vanilla/Openshift kubernetes 部署无此类型）
AWS 集群名称	创建集群时指定的协调器名称（预先存在的 EKS）
AWS 访问 ID	与创建协调器配置的帐户相关联的 ACCESS KEY（预先存在的 EKS）
AWS 秘密访问密钥	与创建协调器配置的帐户关联的 SECRET KEY。每次编辑配置时，请重新输入密钥。（预先存在的 EKS）

字段	说明
AWS 区域	已部署工作负载的区域。如果工作负载分布在多个区域，则每个区域都需要单独的配置。有关正确的区域值，请参阅下面的链接。:ref: https://docs.aws.amazon.com/general/latest/gr/rande.html。（预先存在的 EKS）
AWS 承担角色 ARN	连接到协调器时要代入的角色的 Amazon 资源编号参考：https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html（预先存在的 EKS） 。
Azure 租户 ID	与 Azure 订用关联的租户 ID。（仅限预先存在的 AKS）
Azure 客户端 ID	与需要使用 Azure AD 进行身份验证的应用相关联的全局唯一 ID。（仅限预先存在的 AKS）
Azure 客户端秘密	与需要使用 Azure AD 进行身份验证的应用的服务主体相关联的密码。（仅限预先存在的 AKS）

协调器黄金规则

黄金规则对象属性如下所述。在 Kubernetes 集群节点上启用执行后，这些黄金规则允许对 Kubernetes 集群保持正常运行所需的规则进行简明规范。

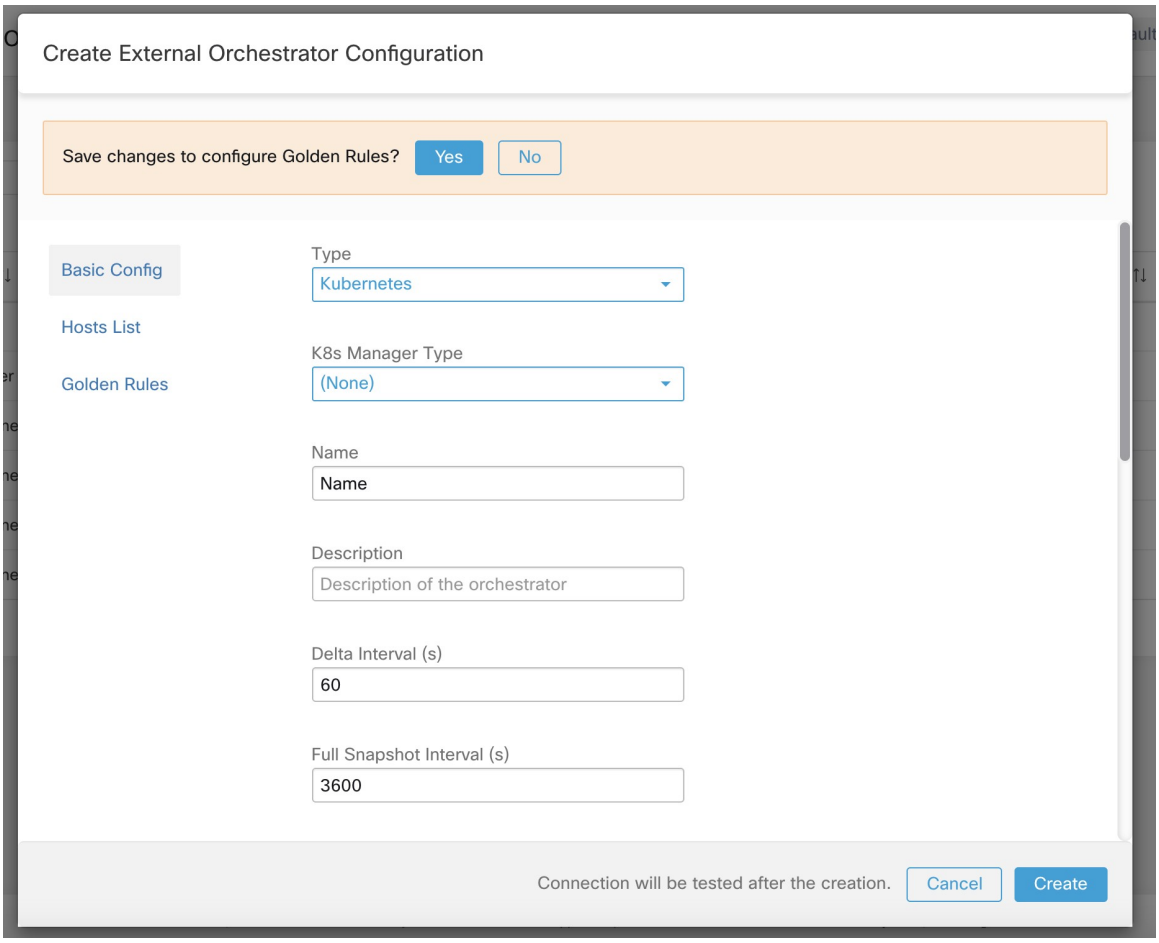
属性	说明
Kubelet 端口	Kubelet 节点本地 API 端口
服务	Kubernetes 服务对象数组

要创建允许从 Kubernetes 管理后台守护程序向 kubelet 传输流量（如实时日志、交互模式下的 Pod 执行等）的策略，就必须使用 kubelet 端口。各种 kubernetes 服务和后台守护程序之间的重要连接被指定为一系列服务--服务数组中的每个条目都具有以下结构

- 说明：描述服务的字符串
- 地址：服务终端地址的列表，格式为 <IP>:<port>/<protocol>。
- 使用者：终端的使用者列表（允许的值为 Pod 或节点）

Note 如果选择 **kubernetes** 作为类型，则允许黄金规则配置。

Figure 9: 为 ***Kubernetes*** 类型创建黄金规则配置



工作流程

- 如有需要，请配置安全连接器隧道，以建立从 Cisco Secure Workload 集群到一个或多个 Kubernetes API 服务器的连接。
- 配置 Kubernetes 协调器，并填写上述配置字段。
- 为 Kubernetes 协调器配置黄金规则。

Kubernetes 基于角色的访问控制 (RBAC) 资源注意事项

Kubernetes 客户端尝试 GET/LIST/WATCH 以下资源。强烈建议不要配置管理员密钥/证书或管理员服务帐户。

提供的 Kubernetes 身份验证凭证应具有对以下资源的最低权限集：

资源	Kubernetes 动词
endpoints	[get list watch]
namespaces	[get list watch]
nodes	[get list watch]
pods	[get list watch]
services	[get list watch]
ingresses	[get list watch]
replicationcontrollers	[get list watch]
replicasets	[get list watch]
deployments	[get list watch]
daemonsets	[get list watch]
statefulsets	[get list watch]
jobs	[get list watch]
cronjobs	[get list watch]

从根本上说，您可以在 Kubernetes 服务器上创建一个拥有这些最低权限的特殊服务帐户。下面是一个 kubectl 命令的示例序列，可帮助创建此服务帐户。请注意 clusterrole（非角色）和 clusterrolebindings（非角色绑定）的使用 - 这些是集群范围的角色，而非每个命名空间。使用角色/角色绑定将不起作用，因为 Cisco Secure Workload 会尝试从所有命名空间检索数据。

```
$ kubectl create serviceaccount csw.read.only
```

创建集群角色。

下面提供了具有最低权限的示例 clusterrole.yaml

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: csw.read.only
rules:
  - apiGroups:
    - ""
    resources:
      - nodes
      - services
      - endpoints
      - namespaces
      - pods
      - replicationcontrollers
      - ingresses
    verbs:
      - get
      - list
```

```
      - watch
  - apiGroups:
    - extensions
    - networking.k8s.io
    resources:
      - ingresses
    verbs:
      - get
      - list
      - watch
  - apiGroups:
    - apps
    resources:
      - replicasets
      - deployments
      - statefulsets
      - daemonsets
    verbs:
      - get
      - list
      - watch
  - apiGroups:
    - batch
    resources:
      - jobs
      - cronjobs
    verbs:
      - get
      - list
      - watch

$ kubectl create -f clusterrole.yaml
```

Note 这些不同资源的API组很容易在Kubernetes版本之间发生变化。上述示例应适用于Kubernetes 1.20-1.24版本，其他版本可能需要做一些调整。

创建集群角色绑定

```
$ kubectl create clusterrolebinding csw.read.only --clusterrole=csw.read.
  →only --serviceaccount=default:csw.read.only
```

要从服务帐户（在 GUI 的“身份验证令牌”(Auth Token) 字段中使用）检索身份验证令牌密钥并从 base64 解码，您可以通过使用 yaml 输出列出服务帐户来检索密钥的名称。

```
$ kubectl get serviceaccount -o yaml csw.read.only
apiVersion: v1
kind: ServiceAccount
metadata:
  creationTimestamp: 2020-xx-xxT19:59:57Z
  name: csw.read.only
  namespace: default
  resourceVersion: "991"
  selfLink: /api/v1/namespaces/default/serviceaccounts/e2e.minimal
  uid: ce23da52-a11d-11ea-a990-525400d58002
secrets:
- name: csw.read.only-token-vmvmz
```

在 yaml 输出模式下列出密钥将生成令牌，但采用 Base64 格式（这是密钥数据的标准 Kubernetes 程序）。Cisco Secure Workload 不接受此格式的令牌，您必须通过 Base64 对其进行解码。

```
$ kubectl get secret -o yaml csw.read.only-token-vmvmz
apiVersion: v1
data:
  ca.crt: ...
  namespace: ZGVmYXVsdA==
  token: ZXlKaGJHY2lPaUpTVX....HRfZ2JwMVZR
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: csw.read.only
    kubernetes.io/service-account.uid: ce23da52-a11d-11ea-a990-525400d58002
  creationTimestamp: 2020-05-28T19:59:57Z
  name: csw.read.only-token-vmvmz
  namespace: default
  resourceVersion: "990"
  selfLink: /api/v1/namespaces/default/secrets/csw.read.only-token-vmvmz
  uid: ce24f40c-a11d-11ea-a990-525400d58002
type: kubernetes.io/service-account-token
```

要在一个命令中列出密钥并仅输出 `.data.token` 字段并从 base 64 编码进行解码，以下使用 `--template` 选项的命令会有所帮助。

```
$ kubectl get secret csw.read.only-token-vmvmz --template "{{ .data.token }}" | base64
-d
```

此身份验证令牌可用于在 Cisco Secure Workload UI 中配置 Kubernetes 协调器，而不是用户名/密码或密钥/证书。

请参阅“EKS 特定的 RBAC 注意事项”。

协调器生成的标签

请参阅与 Kubernetes 集群相关的标签。

故障排除

- 客户端密钥或证书凭证正在解析或不匹配

  这些必须以 PEM 格式提供，并且是 kubectl.conf 文件中的正确条目。我们遇到过客户将 CA 证书粘贴到客户端证书字段，以及密钥和证书不匹配的情况。

- Gcloud 凭证而不是 GKE 凭证

  在 gcloud CLI 下使用 GKE 的客户在需要 GKE 集群凭证时错误地提供了 gcloud 凭证。

- Kubernetes 集群版本不受支持

  使用不兼容的 Kubernetes 版本可能会导致失败。验证 Kubernetes 版本是否在支持的版本列表中。

- 凭证权限不足

  验证所使用的身份验证令牌或用户或客户端密钥或证书是否拥有上表中列出的所有权限。

- Kubernetes 资产不断切换

hosts_list 字段为同一 Kubernetes 集群指定 API 服务器池 - 您不能使用此池配置多个 Kubernetes 集群。Cisco Secure Workload 将探测活动性，随机选择其中一个终端进行连接并检索 Kubernetes 资产信息。这里不执行负载均衡，也不保证在这些终端之间均匀分配负载。如果是不同的集群，Kubernetes 资产会根据我们连接到哪个集群的 API 服务器，在它们之间不断切换。

- 多种授权方法

  在配置过程中可填写多种授权方法（用户名或密码、自动令牌、客户端密钥或证书），并将在与 API 服务器建立的客户端连接中使用。适用于有效同步授权方法的标准 Kubernetes 规则在此处也适用。

- SSL 证书验证失败

  如果 Kubernetes API 终端位于 NAT 或负载均衡器之后，则 kube 控制平面节点上生成的 SSL 证书中的 DN 可能与 Cisco Secure Workload 中配置的 IP 地址不匹配。即使提供了有效的 CA 证书，也会导致 SSL 验证失败。“不安全”(Insecure) 旋钮可绕过严格的服务器 SSL 证书验证，有助于解决这一问题，但可能导致 MITM 问题。正确的解决方法是更改 CA 证书，为可用于连接 Kubernetes 集群的所有 DNS 或 IP 条目提供 SAN（主题备用名称）条目。

VMware vCenter

vCenter 集成允许用户从配置的 vCenter 获取裸机和虚拟机属性。

当为“vCenter”类型添加外部协调器配置时，Cisco Secure Workload 会获取该 vCenter 实例控制的所有裸机和虚拟机的裸机和虚拟机属性。Cisco Secure Workload 将导入裸机/VM 的以下属性：a) 主机名 b) IP 地址 c) BIOS UUID d) 类别/标签。

如果设备中不存在资产，则将在 Cisco Secure Workload 中使用上述裸机/VM 属性来创建新资产。如果设备中已存在资产（由在裸机/VM 上运行的 Cisco Secure Workload 可视性传感器创建），则现有资产将使用获取的裸机/VM 类别/标签列表进行标记。

前提条件

- 安全连接器隧道，如果需要可用于实现连接
- 支持的 vCenter 版本为 6.5+

配置字段

除创建外部协调器中所述的通用配置字段外，还可以配置以下字段：

- **主机列表**是一个主机名/IP 和端口对数组，指向将从中获取裸机/虚拟机属性的 vCenter 服务器。

工作流程

- 首先，用户必须验证是否可从 Cisco Secure Workload 集群在该 IP/端口上访问 vCenter 服务器。

- 对于 TaaS 或无法直接访问 vCenter 服务器的情况，用户必须通过配置安全连接器隧道来提供连接。

协调器生成的标签

Cisco Secure Workload 向从 vCenter 服务器获知的所有虚拟机添加以下标签。

键	值
orchestrator_system/orch_type	vCenter
orchestrator_system/cluster_name	<此集群配置的名称>
orchestrator_system/cluster_id	<|产品| 中集群配置的 *UUID*>

实例特定标签

以下标签是实例特定的。

Table 2: 以下标签是实例特定的。

键	值
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	裸机/虚拟机的 *BIOS UUID*
orchestrator_system/machine_name	裸机/*VM* 的主机名
orchestrator_‘<Category Name>‘	<标签值>

警告

- 当为 vCenter 添加外部协调器配置时，Cisco Secure Workload 软件将连接到主机列表中指定的 vCenter 服务器。成功连接到服务器后，Cisco Secure Workload 软件将为 vCenter 服务器中存在的所有裸机和虚拟机导入主机名、IP地址和类别/标签。要导入裸机和VM的主机名和IP地址，必须在所有裸机和VM上安装VM工具。如果没有为给定的裸机/虚拟机安装VM工具，则Cisco Secure Workload 软件将不会显示该特定裸机/VM 的类别/标签。
- Cisco Secure Workload 软件不会导入裸机/VM 的自定义属性。
- 建议将 **Delta** 间隔计时器设置为 10 分钟以上，以减少 vCenter 服务器上的负载。在修改上述计时器后，vCenter 服务器上资产/标签的任何更改都将具有至少 10 分钟的传播延迟。

故障排除

- 连接问题

  如果 Cisco Secure Workload 设备无法连接/访问 vCenter 服务器，外部协调器的**连接状态 (Connection Status)** 选项卡将显示故障状态以及相应的错误（如有）。

- Cisco Secure Workload 软件运行状况检查。

  检查**维护/服务状态 (MAINTENANCE/Service Status)** 页面，查看是否有任何服务已关闭。检查 **OrchestratorInventoryManager** 是否已启动并正在运行。

DNS

DNS 集成允许 Cisco Secure Workload 使用 DNS 信息（如 CNAME 和 A/AAAA 记录中的主机名）对已知资产进行注释。

当为类型“dns”添加外部协调器配置时，Cisco Secure Workload 设备将尝试连接到 DNS 服务器并执行 DNS 记录的区域传输下载。这些记录（仅 A/AAAA 和 CNAME 记录）将被解析并用于丰富 Cisco Secure Workload 管道（属于配置了协调器的租户）中的资产，其中包含一个名为“orchestrator_system/dns_name”的单个多值标签，而其值将是指向（直接或间接）该 IP 地址的 DNS 条目。

前提条件

- 安全连接器隧道，如果需要可用于实现连接
- 支持的 DNS 服务器：BIND9、支持 AXFR 的服务器 (RFC 5936)、Microsoft Windows Server 2016

配置字段

- **DNS 区域**是一个字符串数组，每个字符串表示要从 DNS 服务器传输的 DNS 区域。所有 DNS 区域都必须以句点（“.”）字符结尾。
- **主机列表**是指向要从中获取 DNS 记录的 DNS 服务器的主机名/IP 和端口对数组。仅可出于高可用性目的，在此处配置多个 DNS 服务器。hosts_list 中指定的多个 DNS 服务器上的高可用性行为是“第一个正常运行的服务器”，并且会优先使用 hosts_list 中较早的条目。不能跨 DNS 服务器拆分区域。

工作流程

- 首先，用户必须验证是否可从 Cisco Secure Workload 集群在该 IP/端口上访问 DNS 服务器。
- 对于 TaaS 或 DNS 服务器无法直接连接的情况，用户必须配置安全连接器隧道来提供连接。

- 在 DNS 服务器上配置正确的 DNS 区域传输 ACL/配置。有关详细信息，请参阅特定 DNS 服务器软件的文档。

生成的标签

orchestrator_system/dns_name -> 一个多值字段，其值是指向该 IP 的所有 CNAME 和 A/AAAA 主机名。

警告

- DNS 协调器源是一个元数据源 - 从 DNS 区域传输获知的 IP 地址不会在 Cisco Secure Workload 中创建资产项目，而是使用新的 DNS 元数据更新现有 IP 地址的标签。系统会以静默方式丢弃未知 IP 的 DNS 数据。要向未从任何传感器或通过任何其他协调器集成了解到的 IP 注释 DNS 元数据，必须通过 CMDB 批量上传机制上传 IP，以便为其创建资产条目。从 CMDB 上传获知的子网不会创建资产条目。
- 仅处理来自 DNS 服务器的 CNAME 和 A/AAA 记录。CNAME 记录将通过其指向的 A/AAAA 记录处理为最终 IPv4/IPv6 记录。只要 CNAME 指向来自同一协调器的 A/AAAA 记录，就只支持单级延迟（即，不延迟 CNAME -> CNAME -> A/AAAA 或更长链）。不支持跨不同 DNS 协调器的 CNAME 延迟。

故障排除

- 连接问题

  Cisco Secure Workload 将尝试使用来自以下任一 Cisco Secure Workload 设备服务器的 TCP 连接或来自云（如果是 TaaS）或来自托管 Cisco Secure Workload 安全连接器 VPN 隧道服务的 VM 的 TCP 连接连接到提供的 IP/主机名和端口号。为了正确建立此连接，防火墙必须配置为允许该流量。

- DNS AXFR 权限问题

  此外，大多数 DNS 服务器（BIND9 或 Windows DNS 或 Infoblox）在客户端 IP 尝试 DNS 区域传输（根据 DNS 协议操作码的 AXFR 请求）时都需要额外配置，因为与解析单个 DNS 记录的简单 DNS 请求相比，这些请求需要更多资源，权限也更高。这些错误通常显示为 AXFR 被拒绝，原因代码为 5 (REFUSED)。

  因此，任何旨在确定DNS服务器配置正确的手动测试都不能依赖于成功的主机名查询，而必须专门测试 AXFR 请求（使用 dig 等工具）。

  Cisco Secure Workload 设备将在“authentication_failure_error”字段中报告任何从 DNS 服务器执行 AXFR 区域传输的失败。

  另请注意，Cisco Secure Workload 将尝试从所有已配置的 DNS 区域进行区域传输，并且所有 DNS 区域必须成功，才能将 DNS 数据注入 Cisco Secure Workload 标签数据库。

- 资产主机名字段不是由 DNS 填充字段“主机名”始终从 Cisco Secure Workload 传感器获知。如果资产是通过 CMDB 上传而不是从传感器上传的，则可能缺少主机名。来自 DNS 协调器工作流程的所有数据仅显示在“orchestrator_system/dns_name”标签下，永远不会填充主机名字段。

DNS 协调器的完全/Delta 轮询行为

默认完整快照间隔为 24 小时

默认增量快照间隔为 60 分钟

这些也是计时器允许的最小值。

DNS 记录可能很少更改。因此，为了实现最佳获取行为，在每个增量快照间隔时，Cisco Secure Workload 将检查是否有任何 DNS 区域的序列号与上一个间隔相比已发生变化。如果任何区域均无变化，则无需执行任何操作。

如果有任何区段发生变化，则会从所有已配置的DNS区段（而不仅仅是发生变化的单个区段）执行区段传输。

在每个完整快照间隔时，Cisco Secure Workload 将从所有区域执行区域传输下载，并注入标签数据库，无论区域序列号是否已更改。

不支持的功能

Warning

- 不支持 DNAME 别名和查找。
- 不支持增量区域传输 (IXFR)。

Infoblox

Infoblox 集成允许 Cisco Secure Workload 将 Infoblox 子网、主机 (*record:host*) 和 A/AAAA 记录导入 Cisco Secure Workload 资产数据库。可扩展属性名称和值按原样导入，可用作 Cisco Secure Workload 标签来定义范围和执行策略。

Note 仅考虑具有可扩展属性的 Infoblox 对象，也就是将从导入中排除未附加任何可扩展属性的对象。

下图显示了为从 Infoblox 导入的具有可扩展属性 *Department* 的主机对象生成的标签示例：

Figure 10: Infoblox 标签示例

```
1. orchestrator_Department = AES789
2. orchestrator_system/cluster_id = [redacted]
3. orchestrator_system/cluster_name = scale13-ib
4. orchestrator_system/machine_id =
   record:host/[redacted]:client8/%20
5. orchestrator_system/machine_name = client8
6. orchestrator_system/orch_type = infoblox
```

前提条件

- 支持 WAPI 版本 2.6、2.6.1、2.7、2.7.1 的 Infoblox REST API 终端（推荐）

配置字段

除创建外部协调器中所述的通用配置字段外，还可以配置以下字段：

通用字段	必填	说明
主机列表	是	主机列表表示一个 Infoblox 网格，即可以添加多个具有 REST API 访问权限的网格成员，如果出现连接错误，外部协调器将切换到列表中的下一个。如果要从另一个 Infoblox 网格导入标签，请为其创建一个新的外部协调器。

Note 对于 Infoblox 外部协调器，支持 IPv4 和 IPv6（双堆栈模式）地址。但请注意，双堆栈支持是一项测试功能。

工作流程

- 首先，用户必须验证是否可从 Cisco Secure Workload 集群访问 Infoblox REST API 终端。
- 对于 TaaS 或无法直接访问 Infoblox 服务器的情况，用户必须配置安全连接器隧道以提供连接。
- 创建类型为 *Infoblox* 的外部协调器。根据 Infoblox 数据量（即子网、主机和 A/AAA 记录的数量）的不同，在 Cisco Secure Workload 中提供第一个完整快照可能需要长达一小时的时间。
- 在创建 infoblox 配置时，用户可以选择取消选择任何记录类型（子网、主机、A/AAAA 记录）。

协调器生成的标签

Cisco Secure Workload 向从 Infoblox 检索的所有对象添加以下系统标签。

键	值
orchestrator_system/orch_type	infoblox
orchestrator_system/cluster_id	Cisco Secure Workload 中外部协调器的 <UUID>
orchestrator_system/cluster_name	<此外部协调器的名称>
orchestrator_system/machine_id	<Infoblox 对象引用/标识符>
orchestrator_system/machine_name	<Infoblox 主机 (DNS) 名称>

生成的标签

所有 Infoblox 可扩展属性都将作为带有前缀 *orchestrator_* 的 Cisco Secure Workload 标签导入。例如，具有名为 *Department* 的可扩展属性的主机可以在 Cisco Secure Workload 资产搜索中作为 *orchestrator_Department* 进行寻址。

键	值
orchestrator_<extensible attribute>	<从 Infoblox 获取的可扩展属性的值>

警告

- 可从 Infoblox 导入的最大子网数为 50000。
- 可从 Infoblox 导入的最大主机数和 A/AAAA 记录总数为 400000。

故障排除

- 连接问题 Cisco Secure Workload 将尝试使用来自以下任一 Cisco Secure Workload 设备服务器的 HTTPS 连接或来自云（如果是 TaaS）或来自托管 Cisco Secure Workload 安全连接器隧道的 VM 的 HTTPS 连接来连接到提供的 IP/主机名和端口号服务。为了正确建立此连接，防火墙必须配置为允许该流量。此外，请确保给定凭证正确无误，并且有权将 REST API 请求发送到 Infoblox 设备。
- 并非所有预期对象都已导入，Cisco Secure Workload 只会导入具有附加可扩展属性的子网、主机和 A/AAAA 记录。请注意，可以从 Infoblox 导入的对象数量有限制，请参阅警告。
- 无法在资产中找到子网无法使用资产搜索来查找 Infoblox 子网，因为 Cisco Secure Workload 资产仅包含 IP 地址，即主机和 A/AAAA 记录。

- 找不到主机或 A/AAAA 记录，Cisco Secure Workload 会导入从 Infoblox 检索到的所有可扩展属性。请记住将前缀 *orchestrator_* 添加到资产搜索等中的可扩展属性名称。请注意，子网可扩展属性如果未在 Infoblox 中标记为继承，就不是主机的一部分，因此无法在 Cisco Secure Workload 中搜索。

F5 BIG-IP

F5 BIG-IP 集成允许 Cisco Secure Workload 从 F5 BIG-IP 负载均衡器设备导入虚拟服务器并派生服务资产。服务资产对应于 F5 BIG-IP 虚拟服务器，其服务通过 *VIP*（虚拟 IP 地址）、协议和端口进行表征。导入到 Cisco Secure Workload 中后，此服务资产将具有 *service_name* 等标签，这些标签可用于资产搜索以及创建 Cisco Secure Workload 范围和策略。

此功能的一大优势在于策略的执行，因为 *F5 BIG-IP* 外部协调器将 Cisco Secure Workload 策略转换为分配给虚拟服务器的安全规则，并通过其 REST API 将其部署到 F5 BIG-IP 负载均衡器。

前提条件

- 安全连接器隧道，如果需要可用于实现连接
- F5 BIG-IP REST API 终端版本 12.1.1

配置字段

除创建外部协调器中所述的通用配置字段外，还可以配置以下字段：

字段	必填	说明
主机列表	是	这将为 F5 BIG-IP 负载均衡器指定 REST API 终端。如果为 F5 BIG-IP配置了高可用性，请输入备用成员节点，以便外部协调器在发生故障转移时切换到当前节点。如果要从其他 F5 BIG-IP 负载均衡器导入标签，则需要创建一个新的外部协调器。
启用执行	不兼容	默认设置为 false（未选中）。如果选中，这将允许 Cisco Secure Workload 策略执行将安全策略规则部署到相应的 F5 BIG-IP 负载均衡器。请注意，给定凭证必须对 F5 BIG-IP REST API 具有写入访问权限。

字段	必填	说明
路由域	不兼容	默认值为 0（零）。路由域指定外部协调器将考虑哪些虚拟服务器。这取决于分配给给定路由域的分区列表，并且只有在这些分区中定义的虚拟服务器才会被导入到 Cisco Secure Workload 中。

工作流程

- 首先，用户必须验证是否可从 Cisco Secure Workload 访问 F5 BIG-IP REST API 终端。
- 对于 TaaS 或 F5 BIG-IP 设备无法直接访问的情况，用户必须配置安全连接器隧道以提供连接。
- 创建类型为 *F5 BIG-IP* 的外部协调器。
- 根据增量间隔值，F5 BIG-IP 虚拟服务器的第一个完整快照可能需要长达 60 秒（默认增量间隔）才能完成。此后，生成的标签可用于创建 Cisco Secure Workload 范围和执行策略。

协调器生成的标签

Cisco Secure Workload 会为 *F5 BIG-IP* 的外部协调器添加以下系统标签：

键	值
orchestrator_system/orch_type	F5
orchestrator_system/cluster_id	<外部协调器的 UUID>
orchestrator_system/cluster_name	<此外部协调器的名称>
orchestrator_system/workload_type	service
orchestrator_system/namespace	<虚拟服务器所属的分区>
orchestrator_system/service_name	<F5 BIG-IP 虚拟服务器的名称>

生成的标签

外部协调器将为每个虚拟服务器生成以下标签：

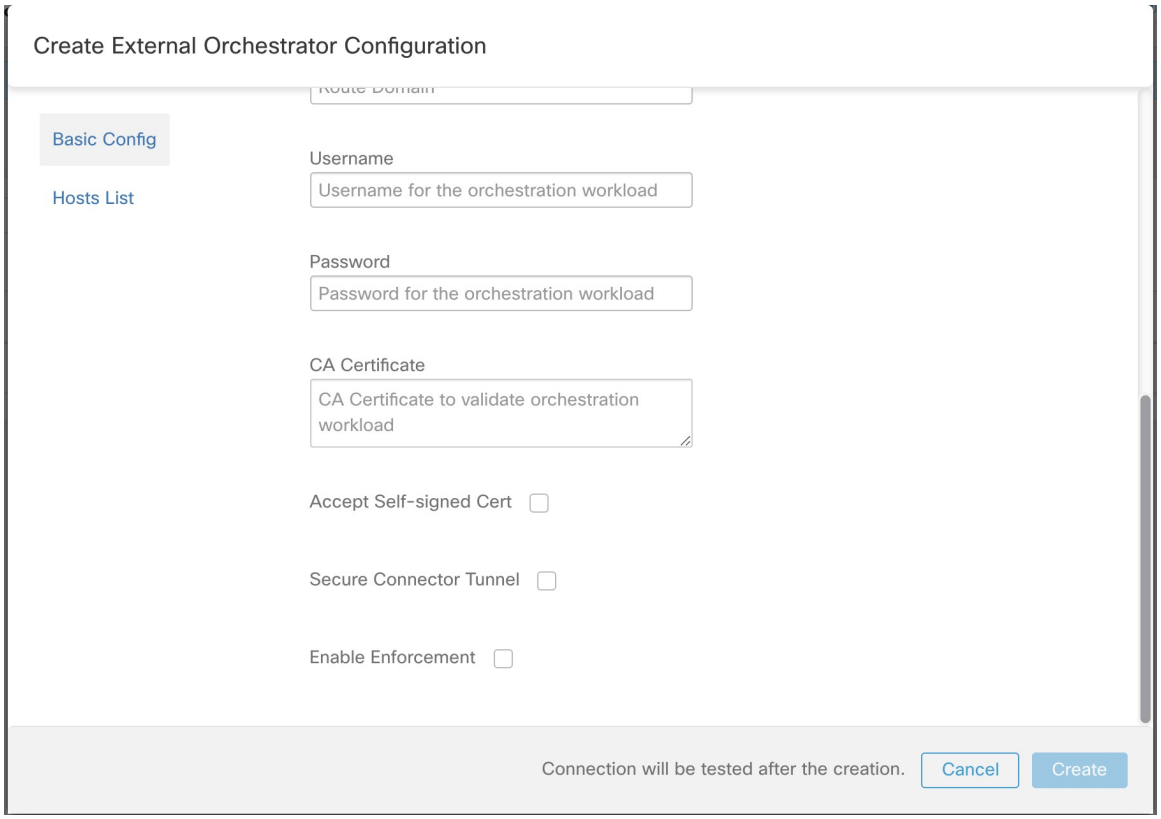
键	值
orchestrator_annotation/snat_address	<虚拟服务器 SNAT 地址>

F5 BIG-IP 的策略执行

此功能使 Cisco Secure Workload 能够将具有提供者组（匹配标记为 *F5 BIG-IP* 虚拟服务器）的逻辑策略转换为 *F5 BIG-IP* 安全策略规则，并使用其 REST API 将它们部署到负载均衡器设备。如上所述，现有安全策略到相应 *F5 BIG-IP* 虚拟服务器的任何分配都将被替换为指向 Cisco Secure Workload 生成的安全策略的新分配。现有安全策略不会更改或从 *F5 BIG-IP* 策略列表中删除。

默认情况下，外部协调器配置中未启用执行：

Figure 11: 配置选项“启用执行”***(Enable Enforcement)***

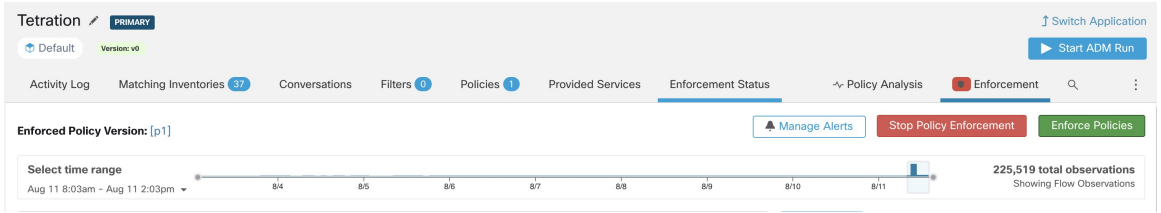


此选项可以根据需要随时修改。

启用执行不会将策略部署到负载均衡器设备，除非您在包含至少一个适用于负载均衡器的策略的工作空间中启用执行，或者由于资产有任何更新。

但是，禁用协调器的执行将导致立即从 *F5 BIG-IP* 负载均衡器中删除所有已部署的安全策略规则。

Figure 12: 工作空间策略执行



Note

- *F5 BIG-IP* 协调器还会检测安全策略规则的任何偏差，并将其替换为 Cisco Secure Workload 策略，即表示对虚拟服务器的任何策略更改应仅使用 Cisco Secure Workload 完成。
- 当策略执行停止或外部协调器被删除时，虚拟服务器的安全策略将变为空，因为将从 *F5 BIG-IP* 负载均衡器中删除所有 Cisco Secure Workload 策略。

外部协调器的 OpenAPI 策略执行状态可用于检索与外部协调器关联的负载均衡器设备的 Cisco Secure Workload 策略执行状态。这样有助于验证将安全策略规则部署到 *F5 BIG-IP* 设备是成功还是失败。

F5 入口控制器的策略执行

当 Pod 使用 Kubernetes 入口对象向外部客户端公开时，Cisco Secure Workload 会在 *F5 BIG-IP* 负载均衡器和后端 Pod 上执行策略。

以下是使用 F5 入口控制器执行策略的步骤。

Procedure

步骤 1 如前所述，为 *F5 BIG-IP* 负载均衡器创建外部协调器。

步骤 2 如此处所述，为 Kubernetes/OpenShift 创建外部协调器。

```
→  ~
→  ~ k8s get ingress
NAME           HOSTS   ADDRESS          PORTS   AGE
test-ingress   *       192.168.60.100   80      7s
→  ~
```

步骤 3 在 Kubernetes 集群中创建入口对象。下图提供了用于创建入口对象的 yaml 文件的快照。

```
→  ~
→  ~ k8s get ingress test-ingress -o yaml
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  annotations:
    virtual-server.f5.com/ip: 192.168.60.100
    virtual-server.f5.com/partition: k8scluster
  creationTimestamp: "2019-07-26T18:34:39Z"
  generation: 1
  name: test-ingress
  namespace: default
  resourceVersion: "8310"
  selfLink: /apis/extensions/v1beta1/namespaces/default/ingresses/test-ingress
  uid: 06f8a705-afd4-11e9-97fb-525400d58002
spec:
  backend:
    serviceName: nginx
    servicePort: 80
status:
  loadBalancer:
    ingress:
    - ip: 192.168.60.100
→  ~
```

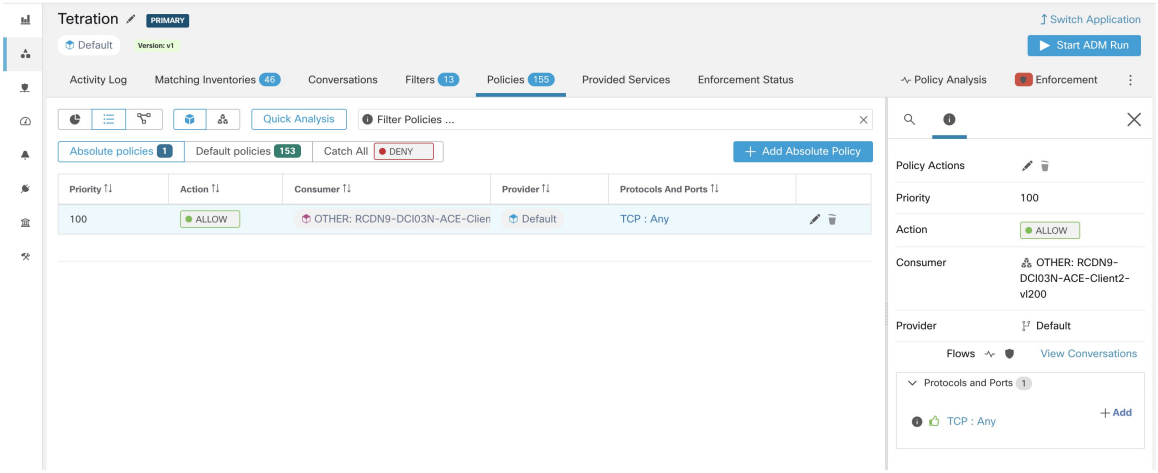
步骤 4 在 Kubernetes 集群中部署 F5 入口控制器 Pod。

```
→  ~ k8s get deploy -n kube-system
NAME                     DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE
coredns                  2         2         2            2           31m
k8s-bigip-ctlr-cluster   1         1         1            1           5m20s
→  ~
```

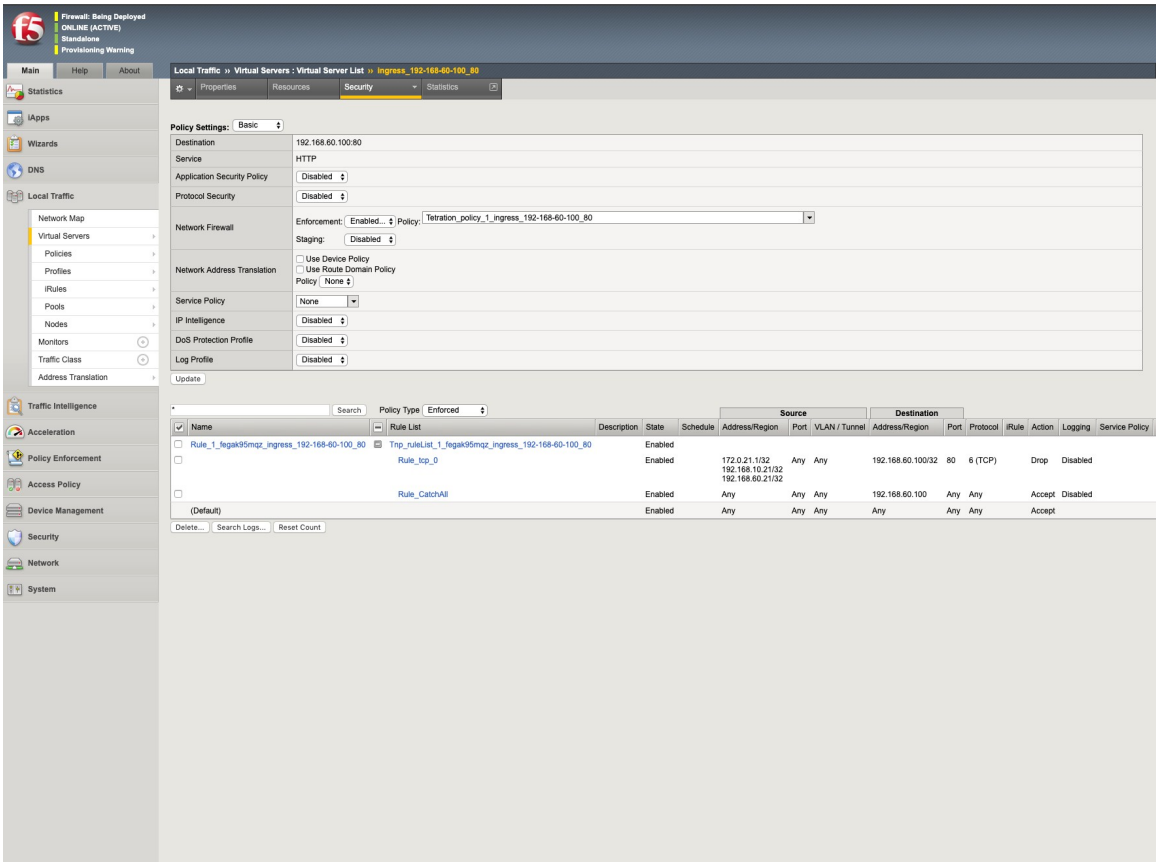
步骤 5 创建后端服务，该服务可供集群外部的使用者访问。在下面提供的示例中，我们创建了一个 *Nginx* 服务。

```
→  ~
→  ~ k8s get deploy
NAME    DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE
nginx   1         1         1            0           5s
→  ~
```

步骤 6 在外部使用者和后端服务之间创建策略。使用策略执行 *(Policy Enforcement)* 选项卡执行策略。



步骤 7 检查 *F5 BIG-IP* 负载均衡器和后端 Pod 上的策略。对于 F5，负载均衡器 Cisco Secure Workload 将应用适当的允许/丢弃规则，其中源为第 6 步中指定的使用者，而目标为 VIP [F5 的入口虚拟服务的 VIP]。对于后端 Pod，Cisco Secure Workload 将应用适当的允许/丢弃规则，其中源为 SNIP [如果启用 SNAT 池] 或 F5 IP [已启用自动映射]，目标为后端 Pod IP。



警告

- 在 *F5 BIG-IP* HA 模式的部署阶段，请启用配置同步选项。这样可确保外部协调器可以从当前连接的主机获取虚拟服务器的最新列表。
- 在 *F5 BIG-IP* HA 部署模式下，如果为地址转换配置了自动映射 *(Auto-Map)* 而不是 SNAT 池，请确保为主 *BIG-IP (Primary BIG-IP)* 配置了浮动自身 *IP (Self IP)* 地址。
- 仅支持指定为单个地址的 VIP，即不支持作为子网指定的 VIP。

故障排除

- 连接问题 Cisco Secure Workload 将尝试使用来自以下任一 Cisco Secure Workload 设备服务器的 HTTPS 连接或来自云（如果是 *TaaS*）或来自托管 Cisco Secure Workload 安全连接器隧道的 VM 的 HTTPS 连接来连接到提供的 IP/主机名和端口号服务。为了正确建立此连接，防火墙必须配置为允许该流量。此外，请确保给定的凭证正确且具有向 *F5 BIG-IP* 设备发送 REST API 请求的读写访问权限。
- 未找到安全规则 如果未找到已定义虚拟服务器的安全规则，则在执行策略执行后，请确保启用相应的虚拟服务器，即其可用性/状态必须为可用/已启用。

Citrix Netscaler

Citrix Netscaler 集成允许 Cisco Secure Workload 从 Netscaler 负载均衡器设备导入负载均衡虚拟服务器并派生服务资产。服务资产对应于虚拟服务器提供的 Netscaler 服务并具有 *service_name* 等标签，可用于资产搜索以及创建 Cisco Secure Workload 范围和策略。

此功能的一大优势是可以执行策略，因为 *Citrix Netscaler* 的外部协调器会将 Cisco Secure Workload 策略转换为 Netscaler ACL 规则，并通过其 REST API 将其部署到 Netscaler 负载均衡器。

前提条件

- 安全连接器隧道，如果需要可用于实现连接
- Netscaler REST API 终端版本 12.0.57.19

配置字段

除创建外部协调器中所述的通用配置字段外，还可以配置以下字段：

通用字段	必填	说明
主机列表	是	这将为 Citrix Netscaler 负载均衡器指定 REST API 终端。如果在 Citrix Netscaler 上配置了高可用性，请输入另一个成员节点，以便外部协调器在发生故障转移时切换到当前节点。如果要从其他 Citrix Netscaler 负载均衡器导入标签，请创建一个新的外部协调器。
启用执行	不兼容	默认设置为 false（未选中）。如果选中，这将允许 Cisco Secure Workload 策略执行将 ACL 规则部署到相应的 Citrix Netscaler 负载均衡器。请注意，给定凭证必须对 Citrix Netscaler REST API 具有写入访问权限。

工作流程

- 首先，用户必须验证是否可从 Cisco Secure Workload 集群访问 Netscaler REST API 终端。
- 对于 TaaS 或 Netscaler 设备无法直接访问的情况，用户必须配置安全连接器隧道以提供连接。
- 创建类型为 *Citrix Netscaler* 的外部协调器。
- 根据增量间隔值，Netscaler 虚拟服务器的第一个完整快照可能需要长达 60 秒（默认增量间隔）才能完成。此后，生成的标签可用于创建 Cisco Secure Workload 范围和执行策略。
- 从 Cisco Secure Workload 执行策略以部署 Netscaler ACL 规则。

协调器生成的标签

Cisco Secure Workload 为 *Citrix Netscaler*的外部协调器添加了以下系统标签：

键	值
orchestrator_system/orch_type	nsbalancer
orchestrator_system/cluster_id	<外部协调器的 UUID>
orchestrator_system/cluster_name	<此外部协调器的名称>
orchestrator_system/workload_type	service
orchestrator_system/service_name	<负载均衡虚拟服务器的名称>

生成的标签

外部协调器将为每个负载平衡虚拟服务器生成以下标签：

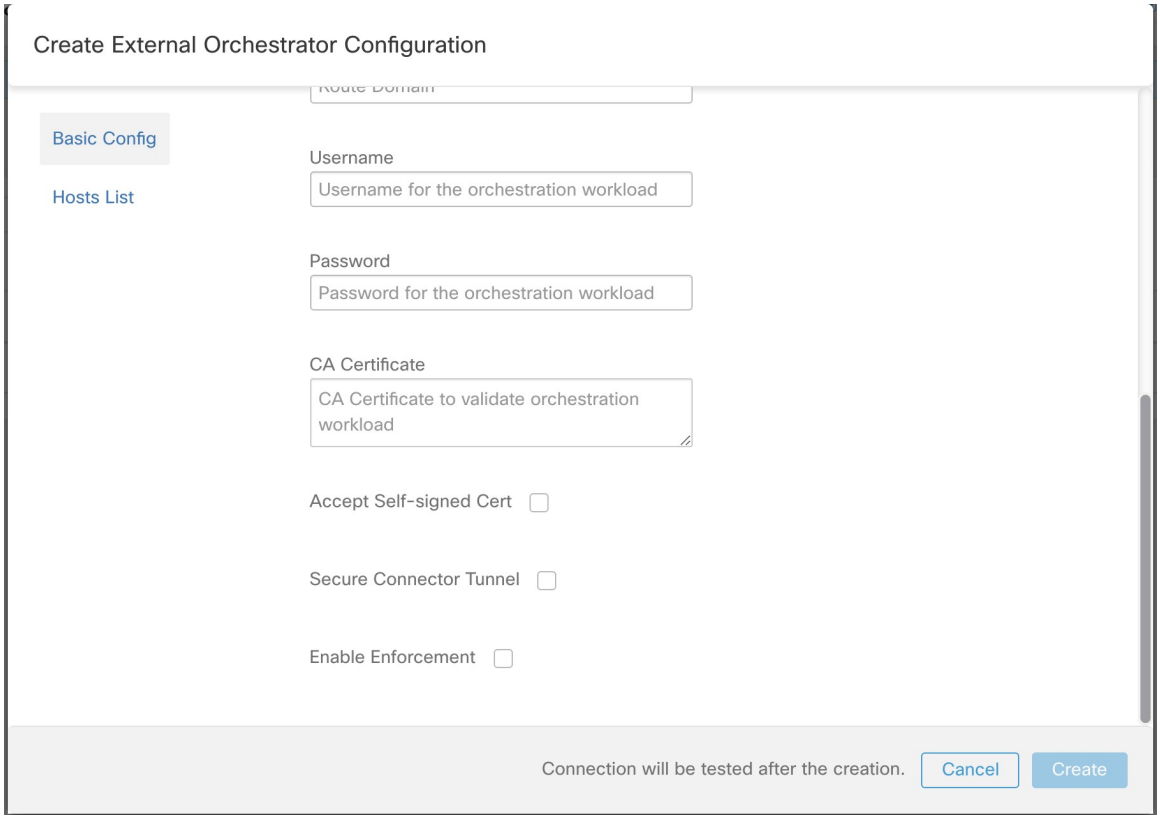
键	值
orchestrator_annotation/snat_address	<虚拟服务器 SNAT 地址>

Citrix Netscaler 的策略执行

此功能使 Cisco Secure Workload 能够将具有提供者组的逻辑策略转换为 *Citrix Netscaler* ACL 规则，并使用其 REST API 将其部署到负载均衡器设备。如上所述，所有现有 ACL 规则都将替换为 Cisco Secure Workload 生成的策略规则。

默认情况下，在创建协调器 *(Create Orchestrator)* 对话框中未选中字段启用强制 *(Enable Enforcement)*，即已禁用，如下图所示：

Figure 13: 配置选项“启用执行”***(Enable Enforcement)***

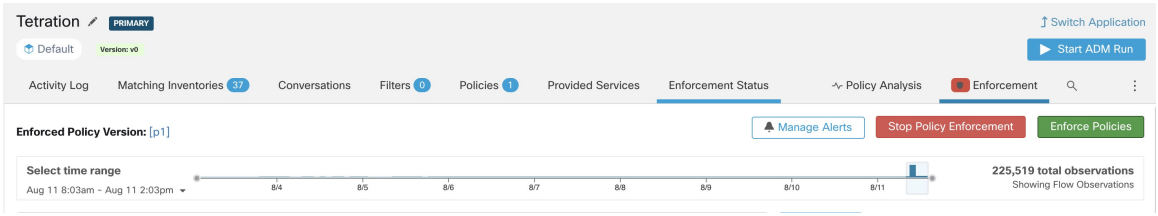


只需点击指定的复选框即可启用协调器的执行。此选项可以根据需要随时修改。

不管是通过创建还是编辑协调器配置，为协调器启用执行功能都不会立即将当前逻辑策略部署到负载均衡器设备。如下图所示，此任务是工作空间策略执行的一部分，由用户触发或由于资产更新而

触发。但是，禁用协调器的执行将导致立即从 *Citrix Netscaler* 负载均衡器中删除所有已部署的 ACL 规则。

Figure 14: 工作空间策略执行



Note

- *Citrix Netscaler* 协调器还会检测 ACL 规则的任何偏差，并将其替换为 Cisco Secure Workload 策略，即表示对负载均衡虚拟服务器的任何策略更改应仅使用 Cisco Secure Workload 完成。
- 当策略执行停止或外部协调器被删除时，ACL 将变为空，因为将从 *Citrix Netscaler* 负载均衡器中删除所有 Cisco Secure Workload 策略。

外部协调器的 OpenAPI 策略执行状态可用于检索与外部协调器关联的负载均衡器设备的 Cisco Secure Workload 策略执行状态。这有助于验证将 ACL 规则部署到 *Citrix Netscaler* 设备是成功还是失败。

警告

- 如果启用了执行，则 Cisco Secure Workload 策略将始终部署到 ACL 的全局列表，即分区默认。
- 仅支持指定为单个地址的 VIP，即不支持作为地址模式指定的 VIP。
- 不支持检测到的服务（*Citrix Netscaler* 虚拟服务器）的可视性。

故障排除

- 连接问题 Cisco Secure Workload 将尝试使用来自以下任一 Cisco Secure Workload 设备服务器的 HTTPS 连接或来自云（如果是 *TaaS*）或来自托管 Cisco Secure Workload 安全连接器隧道的 VM 的 HTTPS 连接来连接到提供的 IP/主机名和端口号服务。为了正确建立此连接，防火墙必须配置为允许该流量。此外，请确保给定的凭证正确，并具有向 *Citrix Netscaler* 设备发送 REST API 请求的读写访问权限。
- 未找到 ACL 规则 如果未找到 ACL 规则，则在执行策略执行后，请确保启用相应的虚拟服务器，即其状态必须为已启用。

TAXII

通过 TAXII（值得信赖的自动智能信息交换）集成，Cisco Secure Workload 可以提取来自安全供应商的威胁智能数据源，以使用 STIX（结构化威胁信息表达式）指标（例如恶意 IP、恶意散列）来注释网络流和处理散列。

在为类型“taxii”添加外部协调器配置时，Cisco Secure Workload 设备将尝试连接到 TAXII 服务器并轮询 STIX 数据源集合。STIX 数据源（仅 IP 和二进制散列指示符）将被解析并用于注释网络流并处理 Cisco Secure Workload 管道中的散列（属于配置协调器的租户）。

提供者或使用者地址与导入的恶意 IP 匹配的网络流将被标记为多值标签“orchestrator_malicious_ip_by_<vendor name>”，其中 <vendor name> 是用户协调器配置输入 TAXII 供应商，而标签值为“是”(Yes)。

注入的 STIX 二进制散列指标将用于注释工作负载进程散列，这些散列将显示（如果匹配）在安全控制面板/进程散列详细信息和工作负载配置文件/文件散列中。

前提条件

- 安全连接器隧道，如果需要可用于实现连接
- 支持的 TAXII 服务器：1.0
- STIX 版本支持的 TAXII 源：1.x

配置字段

除创建外部协调器中所述的通用配置字段外，还可以配置以下字段：

通用字段	必填	说明
名称	是	用户指定的协调器名称。
说明	是	用户指定的协调器说明。
供应商	是	供应商提供智能数据源。
完整快照间隔	是	对 TAXII 源执行完整快照的间隔（以秒为单位）。 （默认值：1 天）
轮询 Url	是	轮询数据的轮询完整 URL 路径。
集合	是	要轮询的 TAXII 源集合名称。

通用字段	必填	说明
轮询天数	是	要从 TAXII 源轮询的较早日期的威胁数据数。
用户名		用于身份验证的用户名。
密码		用于身份验证的密码。
证书		用于身份验证的客户端证书
键		与客户端证书对应的密钥。
CA 证书		用于验证协调终端的 CA 证书。
Accept Self-Signed Cert		用于禁用 TAXII API 服务器证书的严格 SSL 检查的 复选框
Secureconnector 隧道		通过安全连接器隧道建立到此协调器主机的 隧道连接。
主机列表	是	指向 TAXII 服务器的主机名/IP 和端口对。

工作流程

- 首先，用户必须验证是否可从 Cisco Secure Workload 集群在该 IP/端口上访问 TAXII 服务器。
- 使用轮询路径和 TAXII 源名称来配置正确的 TAXII 服务器。

生成的标签

键	值
orchestrator_system/orch_type	*TAXII*
orchestrator_system/cluster_id	Cisco Secure Workload 中集群配置的 UUID。
orchestrator_system/cluster_name	此集群配置的名称>。
orchestrator_malicious_ip_by_<vendor>	如果流提供者/使用者地址与导入的TAXII 恶意 IP 数据匹配，则为是 *(Yes)*。

警告

- 仅内部部署的 Cisco Secure Workload 支持 TAXII 集成。
- 仅注入来自 TAXII 源的 IP 和散列指示器。
- 每个 TAXII 源的最大注入 IP 数为 10 万个（最近更新）。
- 所有 TAXII 源的最大注入散列数为 50 万（最近更新）。
- 仅支持 STIX 版本 1.x 的 TAXII 源。

故障排除

- 连接问题

  Cisco Secure Workload 将尝试从 Cisco Secure Workload 设备服务器之一或从托管 Cisco Secure Workload 安全连接器 VPN 隧道服务的 VM 连接到提供的轮询 URL 路径。为了正确建立此连接，防火墙必须配置为允许该流量。

TAXII 协调器的完全轮询行为

默认完整快照间隔为 24 小时

每隔一个完整快照间隔，Cisco Secure Workload 将执行将 IP 和散列的 TAXII 源提取到标签数据库中，直至达到上述限制。

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。