集群维护

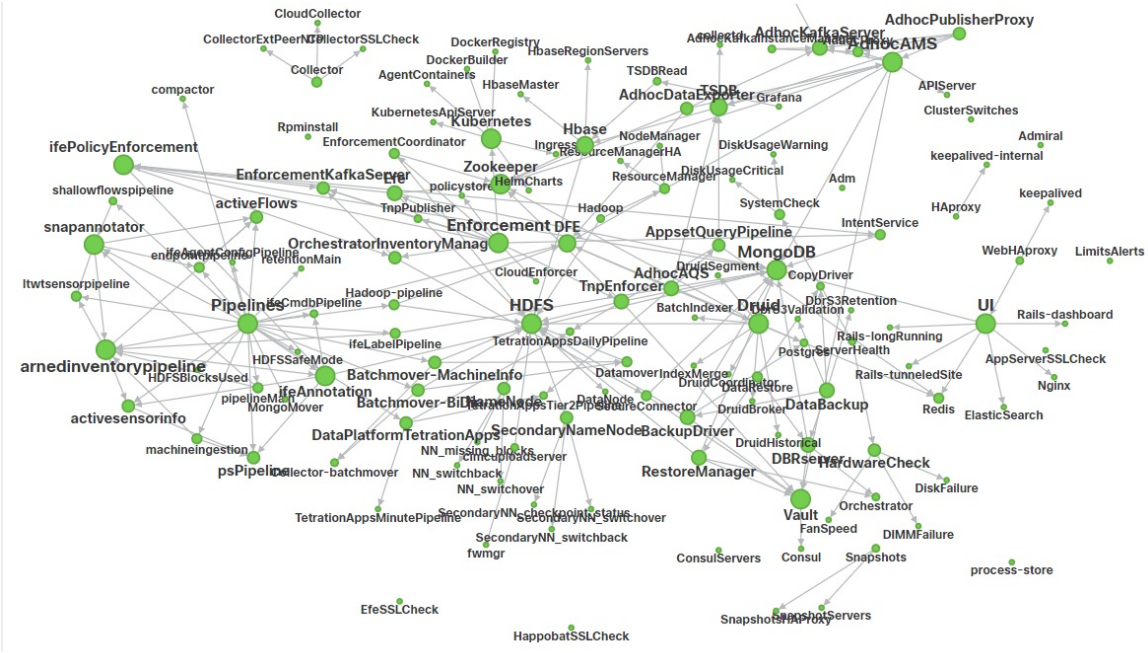
本章提供有关可以执行的各种集群维护操作的详细信息，例如升级、重启、计划数据备份和恢复数据。您还可以从**故障排除 (Troubleshoot)** 菜单下的可用选项查看服务和集群状态。

服务状态

在左侧导航窗格中，**故障排除 (Troubleshoot)** > **服务状态 (Service Status)** 页面会显示思科 Cisco Secure Workload 集群中使用的所有服务及其依赖关系的运行状况。

图形视图显示服务的运行状况，图中的每个节点显示服务的运行状况，边缘代表与其他服务的依赖关系。当服务不可用时，不正常的服务会别标记为红色，当服务降级但可用时，不正常服务会被标记为橙色。绿色节点表示服务正常。有关这些节点的更多调试信息，请使用树视图，其中包含**全部展开 (Expand All)** 按钮，以显示依赖关系树中的所有子节点。“关闭”(Down) 表示服务无法正常运行，“运行不正常”(Unhealthy) 表示服务无法完全正常运行。

Figure 1: “服务状态” *(Service Status)* 页面



Admiral 警报

Admiral 是一个集成的警报系统。它根据服务状态报告的服务运行状况来处理警报。因此，用户可以通过统一的方式来确定服务/集群的运行状况。服务状态显示服务的当前（时间点）的运行状况。当服务状态报告为红色时，服务被视为中断，否则被视为正常。正常运行时间是指服务被报告为正常运行的时间。Admiral 会评估一段时间内按服务状态报告的服务运行状况，并在服务正常运行时间百分比低于特定阈值时发出警报。这种持续时间的评估可确保我们减少误报，只对真正的服务中断发出警报。

由于服务的警报需求各不相同，因此不同服务的百分比和时间间隔也不同。

客户可以使用 Admiral 通知来接收这些事件的通知。它们还显示在**调查 (Investigate)** > **警报 (Alerts)** 页面上的平台类型下。

Note 只有选定的服务子集才具有关联的 Admiral 警报。如果服务不在上述子集中，则在服务关闭时不会发出 Admiral 警报。此具有 Admiral 警报的服务子集及其警报阈值百分比和时间间隔是固定的，用户不可配置。

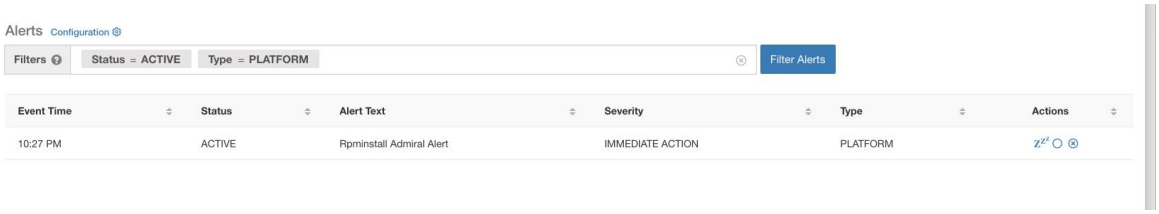
以下各节更详细地介绍了 Admiral 警报和通知。

Admiral 警报的生命周期

Admiral 会根据服务状态检查服务的正常运行时间。当正常运行时间低于预先设置的警报阈值时，它会发出警报。

例如，Rpminstall 是一项服务，用于在部署、升级、补丁等过程中安装 RPM。配置为在正常运行时间在一小时内低于 80% 时生成 Admiral 警报。如果 Rpminstall 服务关闭的持续时间超过上述指定的阈值，则会生成 Rpminstall Admiral 警报，状态为“活动”(ACTIVE)。

Figure 2: 活动 ***Admiral*** 警报



服务恢复后，正常运行时间百分比会开始增加。当正常运行时间超过阈值时，警报自动关闭，其状态将变为 CLOSED。在上述 Rpminstall 示例中，当 Rpminstall Admiral 警报的正常运行时间在一小时内超过 80% 时，它将自动关闭。

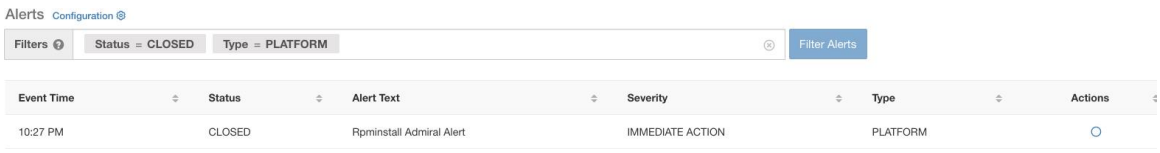
Note 警报关闭总是滞后于服务恢复正常。这是因为 Admiral 会查看一段时间内的服务运行状况。在上面的示例中，由于 Rpminstall 警报阈值设置为每小时正常运行时间的 80%，因此在警报关闭之前，它至少需要运行 48 分钟（一小时的 80%）。

无需执行任何操作即可关闭警报。这可确保所有活动 Admiral 警报均指明当前需要注意的潜在问题。

Note 警报关闭时，不会生成专用通知。

在警报变为 CLOSED 后，它将不再显示在 ACTIVE 警报下。使用过滤器 Status=CLOSED 仍可在 UI 上看到已关闭的警报，如下所示：

Figure 3: 服务恢复时自动关闭 ***Admiral*** 警报



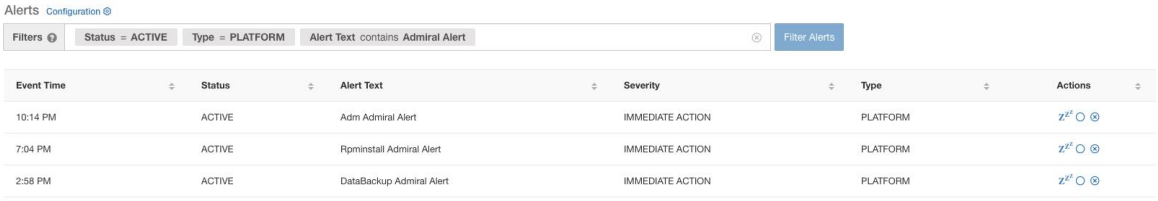
Admiral 警报有两种：

- 单个 Admiral 警报
- 摘要 Admiral 警报

单个 Admiral 警报

上一节中介绍的警报（针对单个服务发出的警报）属于“单个 Admiral 警报”类别。警报文本始终包含 <*Service Name*> Admiral Alert。这样就能轻松地按服务或按 **Admiral Alert** 后缀来过滤单个警报。

Figure 4: 用于单个 ***Admiral*** 警报的警报文本过滤器

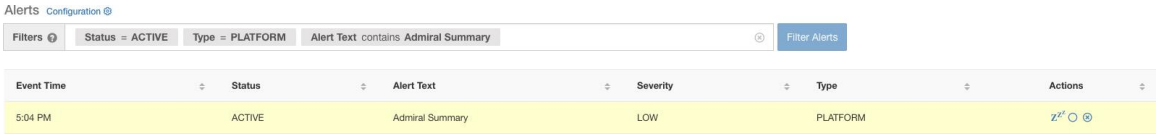


摘要 Admiral 警报

Admiral 会在 UTC 午夜生成每日摘要警报。它们包含当前活动警报和在过去一天内关闭的所有警报的列表。这使用户可以在一个位置查看 Admiral 报告的整体集群运行状况。这对于查看未生成专门通知的已关闭警报也很有用。如果集群运行状况正常，并且在过去一天内未关闭任何警报，则不会生成当天的摘要通知。这样做是为了减少不必要的通知和噪音。

在这种情况下，警报文本始终为 **Admiral 摘要**。这样可以轻松过滤摘要警报，如下图所示。

Figure 5: Admiral 摘要文本过滤器



警报详细信息

单个警报

点击单个 Admiral 警报的警报时，它会展开以显示可用于调试和分析警报的字段。

Figure 6: 警报详细信息

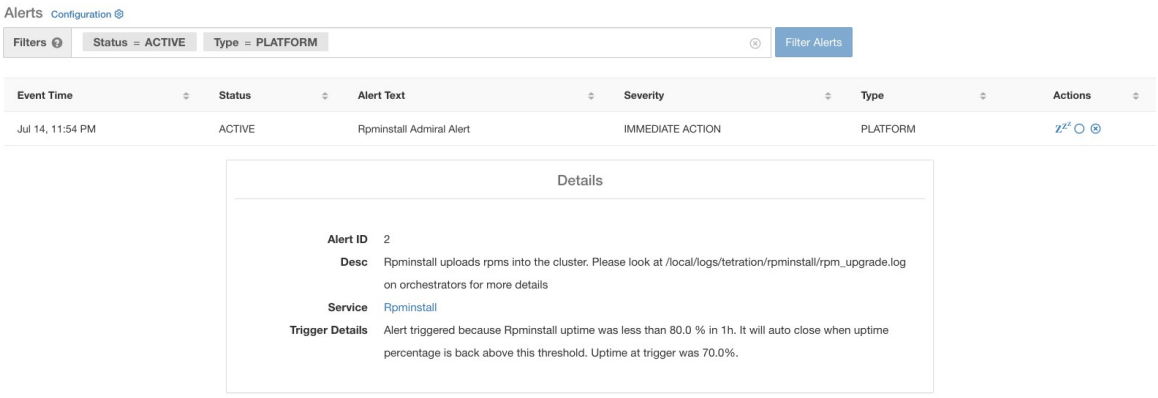


Table 1: “警报详细信息” ***(Alert Details)*** 字段说明

字段	说明
警报 ID (Alert ID)	警报的唯一ID。这有助于确定服务停用的特定事件。如前所述，当警报所报告的服务的基本正常运行时间变得正常时，警报会自动关闭。如果下一次同一服务再次出现故障，则会生成具有不同警报 ID 的新警报。因此，警报 ID 有助于对警报发出的每个事件进行唯一标识。
说明 (Desc)	说明字段包含有关导致警报的服务问题的其他信息。
服务 (Service)	其中包含一个链接，用户可通过该链接进入服务状态页面，以查看服务状态。用户还可以在服务状态页面获得更多详细信息，了解服务被标记为停用的原因。
触发器详细信息 (Trigger Details)	其中包含服务触发阈值的详细信息。通过查看这些阈值，用户可以了解警报在其基础服务恢复后何时关闭。例如，Rpminstall 阈值表示为 80% 的正常运行时间超过一小时。因此，Rpminstall 服务必须启动至少 48 分钟（一小时的 80%），警报才会自动关闭。它还会显示在触发警报时看到的服务的正常运行时间值。

下面是一个 JSON Kafka 输出示例：

```
{
"severity": "IMMEDIATE_ACTION",
"tenant_id": 0,
"alert_time": 1595630519423,
"alert_text": "Rpminstall Admiral Alert",
"key_id": "ADMIRAL_ALERT_5",
```

```
  "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
location_name='platform', location_grain='MIN',
root_scope_id='5efcfdf5497d4f474f1707c2'}/66eb975f5f987fe9eaefa81cee757c8b6dac5facc26554182d8112a98b35c4ab",

  "root_scope_id": "5efcfdf5497d4f474f1707c2",
  "type": "PLATFORM",
  "event_time": 1595630511858,
  "Check  /local/logs/tetration/rpminstall/rpm_upgrade.log on
orchestrators for more details\",\"Trigger Details\":\"Alert triggered because Rpminstall
uptime was less than 80.0 % in 1h. It will auto close when uptime percentage is back above
this threshold. Uptime at trigger was 65.0%. \"}"
  }
```


所有单个警报都遵循 JSON Kafka 格式。下表列出了 Admiral 监控涵盖的服务（来自服务状态）：

***Table 2: Admiral* 监控涵盖的服务**

服务	触发条件	严重性
KubernetesApiServer	服务正常运行时间在过去 15 分钟内降至 90% 以下。	IMMEDIATE ACTION
Adm	服务正常运行时间在过去一小时内降至 90% 以下。	IMMEDIATE ACTION
DataBackup	服务正常运行时间在过去 6 小时内降至 90% 以下。	IMMEDIATE ACTION
DiskUsageCritical	服务正常运行时间在过去一小时内降至 80% 以下。	IMMEDIATE ACTION
RebootRequired	服务正常运行时间在过去一小时内降至 90% 以下。	IMMEDIATE ACTION
Rpminstall	服务正常运行时间在过去一小时内降至 80% 以下。	IMMEDIATE ACTION
SecondaryNN_checkpoint_status	服务正常运行时间在过去一小时内降至 90% 以下。	IMMEDIATE ACTION

对于 8 或 39 RU 物理集群，还会监控以下服务：

***Table 3: Admiral* 监控涵盖的 *8* 或 *39 RU* 集群服务**

服务	触发条件	严重性
DIMMFailure	服务正常运行时间在过去一小时内降至 80% 以下。	IMMEDIATE ACTION
DiskFailure	服务正常运行时间在过去一小时内降至 80% 以下。	IMMEDIATE ACTION
FanSpeed	服务正常运行时间在过去一小时内降至 80% 以下。	IMMEDIATE ACTION

服务	触发条件	严重性
ClusterSwitches	服务正常运行时间在过去一小时内降至 80% 以下。	IMMEDIATE ACTION

Note Admiral 依靠服务状态生成的处理指标来生成警报。如果长时间无法进行指标检索（例如：服务状态为关闭），则会发出警报 (TSDBOracleConnectivity)，通知集群上基于服务的警报处理已关闭。

摘要警报

摘要警报属于信息性质，并且始终被设置为低优先级。点击 Admiral 摘要警报后，它会展开以显示包含 Admiral 警报摘要信息的各个字段。

Figure 7: Admiral 摘要警报的详细信息

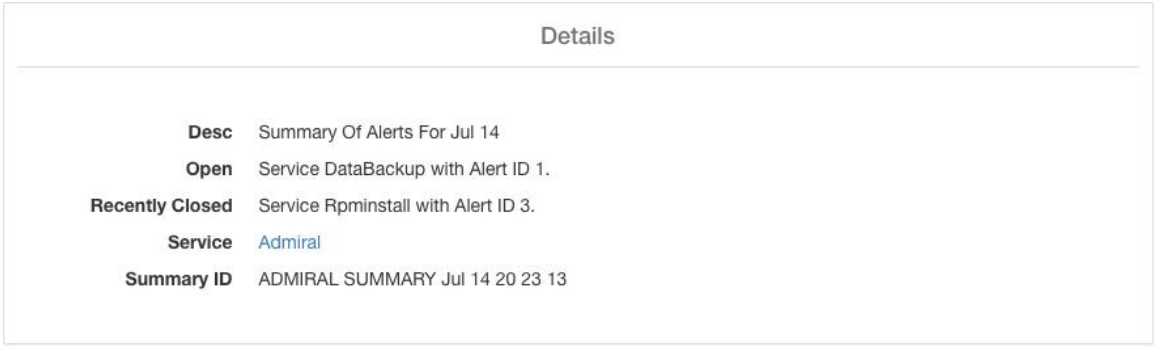


Table 4: Admiral 警报摘要字段说明

字段	说明
说明 (Desc)	说明字段包含每日摘要的日期。
待解决 (Open)	待处理警报指明生成摘要时哪些警报处于活动状态。
最近关闭 (Recently Closed)	这包含在过去 24 小时内（即生成摘要的当天）关闭的警报。其中还包括每个警报的ID。由于警报会自动关闭，因此某项服务可能会出现故障并产生警报，然后恢复正常，警报也会自动关闭。在这种情况下，最近关闭将列出每个事件及其唯一的警报ID。但是，鉴于每项服务在关闭警报前都必须达到一定的运行时间，因此预计这种情况不会经常发生。用户可以使用“Status = CLOSED”进行过滤，以获取有关每个事件的更多信息。

字段	说明
服务 (Service)	Admiral 的服务状态链接，用于处理和生成每日摘要。
摘要 ID (Summary ID)	摘要警报的 ID。

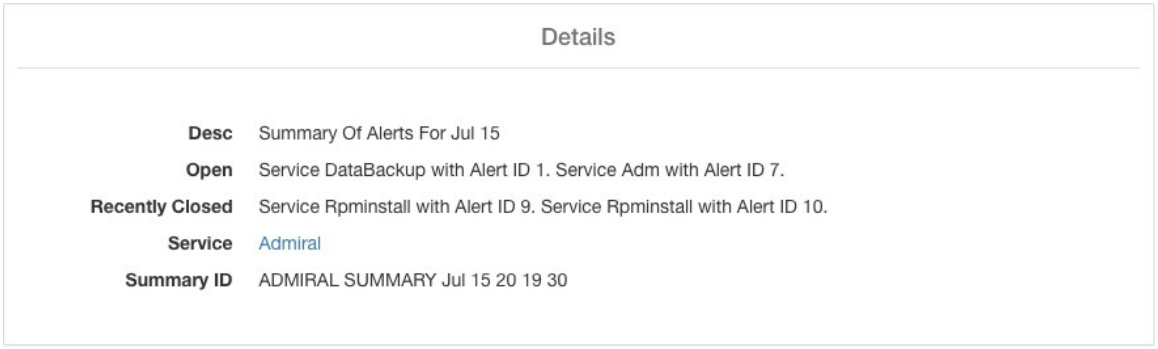
下面是一个 JSON Kafka 输出示例：

```
  {
    "severity": "LOW",
    "tenant_id": 0,
    "alert_time": 1595721914808,
    "alert_text": "Admiral Summary",
    "key_id": "ADMIRAL_SUMMARY_Jul-26-20-00-04",
    "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
location_name='platform', location_grain='MIN',
root_scope_id='5efcfdf5497d4f474f1707c2'}/e95da4521012a4789048f72a791fb58ab233bbff63e6cbc421525d4272d469aa",

    "root_scope_id": "5efcfdf5497d4f474f1707c2",
    "type": "PLATFORM",
    "event_time": 1595721856303,
    "alert_details": "{\"Desc\":\"Summary of alerts for Jul-26\",\"Recently
Closed\":\"None\",\"Open\":\" Service Rpminstall with Alert ID
5.\",\"Service\":\"Admiral\",\"Summary ID\":\"ADMIRAL_SUMMARY_Jul-26-20-00-04\"}"
  }
```

包含在一天内引发多个警报的服务的摘要警报示例如下所示：

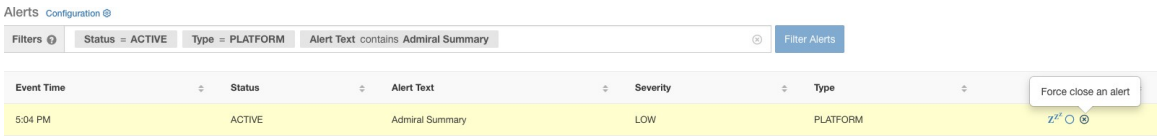
Figure 8: 多个警报



用户操作

由于 Admiral 警报每个警报仅生成一次单独的通知，因此不需要包括/排除或暂停特定警报。如上所述，当服务正常达到正常运行时间阈值时，警报会自动关闭。有一个强制关闭选项可用于强制关闭警报。它通常只用于从用户界面删除摘要警报，因为单个警报会自动关闭。

Figure 9: 强制关闭警报

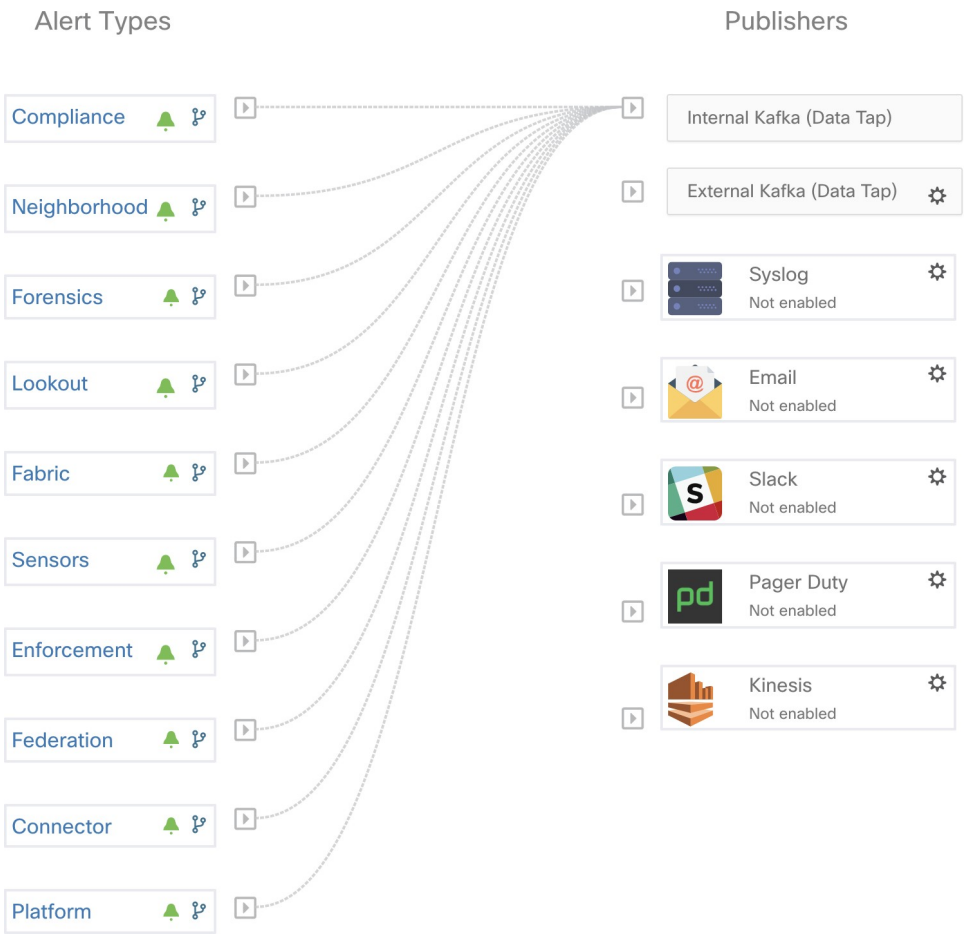


Warning 不应强行关闭单个警报。如果在基础服务仍然关闭或其正常运行时间低于其预期阈值时执行此操作，将导致在下一次 Admiral 处理迭代中针对同一服务发出另一个警报。

Admiral 通知

Admiral 警报的类型为 PLATFORM。因此，可以通过配置页面 ./configuration 将这些警报配置为通过平台警报的适当连接发送到各种发布服务器。为方便起见，平台警报和内部 Kafka 之间的连接默认处于打开状态，这使得无需任何手动配置即可在“当前警报”(Current Alerts) 页面上查看 Admiral 警报（转到**调查 (Investigate)** > **警报 (Alerts)**）。

Figure 10: 平台警报配置



Admiral 警报也会发送到**平台 (Platform)** > **集群配置 (Cluster Configuration)** > **Admiral 警报邮件 (Admiral Alert Email)** 下配置的邮件地址。

Figure 11: Admiral 邮件示例

There is a new admiral platform alert on your tetration cluster.
Service: Rpminstall
Start Time: 2020-07-14 23:09 UTC
Alert ID: 3
Description: Rpminstall uploads rpms into the cluster. Please look at /local/logs/tetration/rpminstall/rpm_upgrade.log for more details

This is an auto generated message about platform alerts on your cluster.
For more details, please go to Alerts On Cluster
Please make sure that you are on **Default Scope** to view the alerts.

这样，即使用户没有设置 TAN 边缘设备，也能收到 Admiral 通知。这类似于之前版本中的 Bosun 行为。

Figure 12: Admiral 邮箱

这些邮件通知是根据与“当前警报”(Current Alerts) 页面相同的触发器生成的。因此，系统会在创建警报时发送它们，并在 UTC 午夜发送每日摘要邮件。每日摘要邮件会列出所有活动警报以及过去 24 小时内关闭的警报。

Figure 13: Admiral 邮件摘要示例

Daily summary of admiral platform alerts:

State:Active

Service: DataBackup
Start Time: 2020-07-14 21:58 UTC
Alert ID: 1
Description: The last successful checkpoint was over 48 hours ago.

State:Closed

Service: Rpminstall
Start Time: 2020-07-14 22:41 UTC
Alert ID: 2
Description: Rpminstall uploads rpms into the cluster. Please look at /local/logs/tetration/rpminstall/rpm_upgrade.log for more details

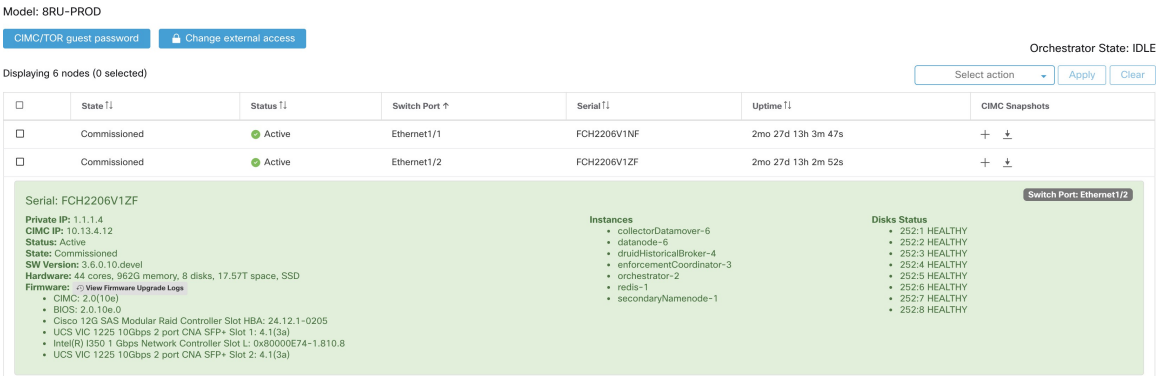
This is an auto generated message about platform alerts on your cluster.
For more details, please go to Alerts On Cluster
Please make sure that you are on **Default Scope** to view the alerts.

如果在过去 24 小时内没有活动警报，也没有关闭警报，则会跳过摘要邮件，以减少邮件干扰。

集群状态

站点管理员用户可以访问左侧导航栏中**故障排除 (Troubleshoot)** 菜单下的**集群状态 (Cluster Status)** 页面，但这些操作只能由**客户支持**用户来执行。它显示思科 Cisco Secure Workload 机架中所有物理服务器的状态。表中的每一行都代表一个物理节点，包含其硬件和固件配置以及 CIMC IP 地址（如果已分配）等详细信息。点击相应的行即可查看节点的详细信息视图。在此页面中，我们还可以更改节点的 CIMC 密码，并启用或禁用节点的外部访问。协调器状态也会显示在集群状态页面上，以便为客户支持提供上下文信息。

Figure 14: 集群状态



影响所有节点的操作

可以使用 **CIMC/TOR 访客密码 (CIMC/TOR guest password)** 和**更改外部访问 (Change external access)** 选项来更改 CIMC 密码以及启用或禁用外部 CIMC 访问。这些操作会对集群中的所有节点产生影响。

外部 CIMC 接入节点详细信息

点击**更改外部访问 (Change external access)** 将打开一个对话框，其中提供外部 CIMC 访问的状态，并允许启用、续约或禁用对 CIMC 的外部访问。

点击**启用 (Enable)** 可在后台配置集群，以启用外部 CIMC 访问。最多可能需要 60 秒才能完成任务并完全启用外部 CIMC 访问。启用外部 CIMC 访问后，当访问设置为自动到期时，系统会显示一个对话框，并将**启用 (Enable)** 更改为**续约 (Renew)** 以反映您可以续约外部 CIMC 访问。续约外部 CIMC 访问权限会使到期时间从当前时间延长两小时。

如果启用了外部 CIMC 访问，节点详细信息中的 CIMC IP 地址（可通过点击节点的行查看）就会变成一个可点击的链接，允许您直接访问 CIMC UI。您可能需要重新加载集群状态页面才能查看相关链接。

Figure 15: 外部 ***CIMC*** 接入节点详细信息

CIMC UI 通常使用自签名证书，访问 CIMC UI 可能会在浏览器中出现错误，提示证书无效。如果您使用的是 Google Chrome，当 Google Chrome 中显示无效证书错误时，您可能需要键入不带引号的 **`thisisunsafe`**，以绕过证书检查并访问 CIMC UI。

在 CIMC UI 中，仅当 CIMC 版本为 4.1(1g) 或更高版本时，KVM 访问才会发挥作用。启用外部 CIMC 访问后，除非续约或禁用访问，否则系统会在两小时后自动将其禁用。

禁用外部 CIMC 访问会在后台将集群配置为禁用外部 CIMC 访问。完成任务并完全禁用外部 CIMC 访问最多可能需要 60 秒。

Table 5: 物理节点详细信息

字段	说明
状态 (Status)	**状态 (Status)** 字段指明节点的电源状态。可能的值包括： • **活动 (Active)**：节点已打开电源。 • **非活动 (Inactive)**：节点未通电或未连接。
状态 (State)	**状态 (State)** 字段指明节点的集群成员身份状态。可能的值包括： • **新 (New)**：节点还不是集群的一部分。 • **已初始化 (Initialized)**：节点是集群的一部分。但是，Cisco Secure Workload 未部署在节点上。 • **已调试 (Commissioned)**：节点已启动并正在运行，其中部署了 Cisco Secure Workload。 软件版本字段也会显示，如果单个节点的版本与整个集群的版本不一致，该字段会变为红色。 • **已下线 (Decommissioned)**：出于故障排除目的，已从集群中删除节点。节点必须更换为新的硬件。可以使用下线操作下线节点，请参阅以下操作。

字段	说明
交换机端口 **(Switch Port)**	指物理节点所连接的两个交换机的交换机端口。
正常运行时间 **(Uptime)**	指明节点在未重启或关闭的情况下一直运行的时间。
CIMC 快照 **(CIMC Snapshots)**	可用于发起 CIMC 技术支持收集并下载 CIMC 技术支持。

Table 6: 集群补救操作

操作	说明
调试	选择此操作可将新节点集成到集群中。对于此操作，只能选择状态为“新”的节点。
下线	选择此操作可删除属于集群的节点。此操作只能选择状态为**已调试 (Commissioned)** 或**已初始化 (Initialized)** 的节点。
重新映像	选择此操作可重新部署 Cisco Secure Workload。这样可能会擦除所有集群数据，并且对于将裸机操作系统从旧版本升级到新版本特别有用。需要在下线裸机时执行此步骤。
固件升级	固件信息可用于可访问 CIMC IP 的节点。此操作有助于使用旧版本升级节点上的固件。
关闭电源	选择此操作可关闭节点。 **Note** 无法关闭处于**非活动 (Inactive)** 和**正在关闭 (Shutdown in progress)** 状态的节点。

固件升级详细信息

Cisco Secure Workload 本地集群捆绑了统一计算系统 (UCS) 思科集成管理控制器 (CIMC) 主机升级实用程序 (HUU) ISO。集群状态页面上的固件升级选项可用于将物理裸机更新为捆绑在 Cisco Secure Workload RPM 中的 HUU ISO 所包含的 UCS 固件版本。

只要裸机状态不是已初始化或 *SKU* 不匹配，裸机主机就可以在状态为活动或非活动时启动固件更新。每次只能更新一个裸机的 UCS 固件。要启动固件更新，Cisco Secure Workload 协调程序的状态必须为空闲 *(Idle)*。启动 UCS 固件更新时，如果必须将 Consul 领导者、活动协调器或活动固件管理器 (fwmgr) 切换到其他主机，则集群状态页面特有的某些用户界面功能可能会暂时受到影响 - 这些切换应自动进行。在固件更新过程中，不会显示正在更新的裸机的固件详细信息，更新后可能需要 15 分钟才能在“集群状态”(Cluster Status) 页面中再次显示固件详细信息。在开始固件更新之前，请检查“服务状态”(Service Status) 页面以验证所有服务是否正常。

当您在裸机上启动固件更新时，fwmgr会验证更新是否可以继续，如果需要，请平稳关闭裸机电源，然后登录裸机上的 CIMC 并启动基于 HUU 的固件更新。基于 HUU 的固件更新过程涉及将裸机启动到 HUU ISO 中，执行更新，重启 CIMC 以激活新固件，然后将裸机启动回 HUU ISO 以验证更新是否已完成。G1 裸机的整个更新过程需要 2 个多小时，G2 裸机则需要 1 个多小时。启动固件更新过程时，“服务状态”(Service Status) 页面可能会显示某些服务不正常，因为裸机和在该裸机上运行的所有虚拟机在集群中都不再处于活动状态。固件更新完成后，裸机可能需要额外的30分钟才能再次在集群中激活，所有服务也可能需要更多时间才能恢复正常状态。如果固件更新后两小时内服务仍未恢复，请联系客户服务代表。

您可以点击集群“状态页面”(Cluster Status) 中的裸机节点，以展开有关裸机的详细信息。一旦启动固件更新，您可以点击查看固件升级日志 *(View Firmware Upgrade Logs)* 按钮以查看固件更新的状态。日志包含固件更新的整体状态，而状态可以是以下其中之一：

- **已触发固件更新**：已请求固件更新，但尚未开始。在此过程中，fwmgr 将检查以确保固件更新所需的服务正常运行，并且 CIMC 可以访问这些服务。
- **固件更新正在运行**：已开始固件更新。当固件更新达到此状态时，CIMC 和 HUU 会控制更新，并且 Cisco Secure Workload 集群将报告从 CIMC 获得的有关更新的状态。
- **固件更新已超时**：这表示固件更新中的某些进程已超出了预期的完成时间。一旦进入固件更新正在运行阶段，整个固件更新过程的时间限制为 240 分钟。在固件更新期间，CIMC 在重启到新版本时可能无法访问；在固件更新被声明为超时之前，此不可达状态的超时时间为40分钟。一旦开始固件更新，对该更新的监控将在 120 分钟后超时。
- **固件更新失败并显示错误**：这表示发生了错误，并且固件更新失败。CIMC 通常不提供成功或失败的指示，因此该状态通常表示在固件更新实际运行之前发生的错误。
- **固件更新已完成**：固件更新已完成，未遇到任何错误或超时。CIMC 通常不会给出成功或失败的提示，最好在“集群状态”(Cluster Status) 页面提供详细信息时验证 UCS 固件版本是否已更新 - 这些详细信息可能需要 15 分钟才会提供。

在查看固件升级日志 *(View Firmware Upgrade Logs)* 弹出窗口的整体状态下方，更新进度 *(Update progress)* 部分将提供带有时间戳的日志信息，表示固件的更新进度。在这些日志消息中显示正在重启主机 *(Rebooting Host In Progress)* 状态后，CIMC 将控制更新，集群将监控该更新 - 大多数后续日志消息直接来自 CIMC，仅在更新状态发生变化时才会添加到日志消息列表中。

当 CIMC 开始提供各个组件更新时，查看固件升级日志 *(View Firmware Upgrade Logs)* 弹出窗口的更新进度 *(Update progress)* 部分下方将显示组件更新状态 *(Component update status)* 部分。本部分总结了裸机上各种 UCS 组件的更新情况。

数据备份和恢复

数据备份和恢复是一种灾难恢复机制，用于将数据从 Cisco Secure Workload 集群、连接器和外部协调器复制到异地存储。如果发生灾难，数据可从异地存储恢复到相同形式的集群。您还可以在不同的备份站点之间切换。

- 物理集群-8 和 39 RU 支持数据备份和恢复。

- 数据可备份到任何与 S3V4 API 兼容的外部对象存储。
- Cisco Secure Workload 需要足够的带宽和存储来备份数据。较慢的网络速度和高延迟可能会导致备份失败。
- 数据存储限制基于所选的备份类型。
  - 对于使用连续模式的数据备份，建议为完整备份（包括流数据）提供 200 TB 的存储。要确定所需的实际存储空间，请使用“数据备份”(Data Backup) 页面上的**容量规划器 (Capacity Planner)** 选项。有关详细信息，请参阅使用容量规划器, on page 20。多个备份的存储空间不足会导致频繁删除旧备份，以便能够管理存储限制内的备份。必须有足够的存储空间至少进行一个备份。
  - 对于精简模式备份，1 TB 的存储空间已经足够，因为构成大部分备份数据的流数据并不会包含在备份中。
- 数据只能被恢复到外形规格兼容且与主设备运行相同版本的集群。例如，您只能将数据从 8 RU 集群恢复到另一个 8 RU 集群。

数据备份

可以使用 UI 上的“数据备份”(Data Backup) 部分配置数据备份计划。备份可根据配置设置在计划时间每天触发一次，也可配置为连续运行。成功的备份称为检查点。检查点是集群主数据存储的时间点快照。

成功的检查点可用于将数据恢复到另一个集群或同一集群上。

每次检查点都会备份集群配置数据。流和其他数据是备份数据的主体。因此，如果配置得当，则只会备份增量更改。增量备份有助于减少推送到外部存储的数据量，从而避免网络过载。如果配置了增量备份，还可选择按计划触发所有数据源的完整备份。完整备份会复制检查点中的每个对象，即使该对象已被复制且未发生变化。这可能会显著增加集群、集群与对象存储库之间的网络以及对象存储库本身的负载。如果对象出现损坏或对象存储区出现任何无法恢复的硬件故障，则可能需要进行完整备份。此外，如果所提供的备份存储桶发生变化，则会自动执行完整备份，因为在增量备份发挥作用之前，必须先进行完整备份。

Table 7: 在不同模式下备份的集群数据

Cisco Secure Workload 集群数据	数据是在完整备份模式下备份的吗？	数据是在精简备份模式下备份的吗？
集群配置	是	是
用于集群映像的 RPM	是	是
软件代理部署映像	是	是
流数据库	是	否
自动策略发现所需的数据	是	否

Cisco Secure Workload 集群数据	数据是在完整备份模式下备份的吗？	数据是在精简备份模式下备份的吗？
用于帮助取证的数据，例如文件散列、数据泄漏模型	是	否
用于帮助进行攻击面分析的数据	是	否
CVE 数据库	是	否

Note

- 安全连接器信息不会在 Cisco Secure Workload 的内部部署版本中备份或恢复，但在 Cisco Secure Workload 的 SaaS 版本中会备份和恢复。
- 恢复备份数据后，无法恢复 FMC 连接器的虚拟补丁信息。

数据备份的前提条件

- 请联系思科技术支持中心，在集群上启用数据备份和恢复选项。
- 需要对象存储库的访问密钥和秘密。数据备份和恢复选项不适用于对象存储的预身份验证链接。
- 配置任何管制，以限制 Cisco Secure Workload 设备用于对象存储的带宽。如果需要备份的数据量很大，则使用低带宽进行 Policing 会导致备份失败。
- 配置集群 FQDN 并确保软件代理可以解析 FQDN。

Note 启用数据备份和还原后，只有当前和以后的软件代理版本可用于安装和升级。由于不兼容，当前集群版本之前的版本仍会保持隐藏状态。

软件代理或 Kafka FQDN 要求

软件代理会使用 IP 地址从 Cisco Secure Workload 设备获取控制信息。要启用数据备份和恢复并允许在灾难后进行无缝确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移，代理必须切换为使用 FQDN。对于此交换机，升级 Cisco Secure Workload 集群还不够。从 Cisco Secure Workload 版本 3.3 及更高版本开始，软件代理支持使用 FQDN。因此，要启用代理确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移并确保代理已准备好进行数据备份和恢复，请将代理升级到版本 3.3 或更高版本。

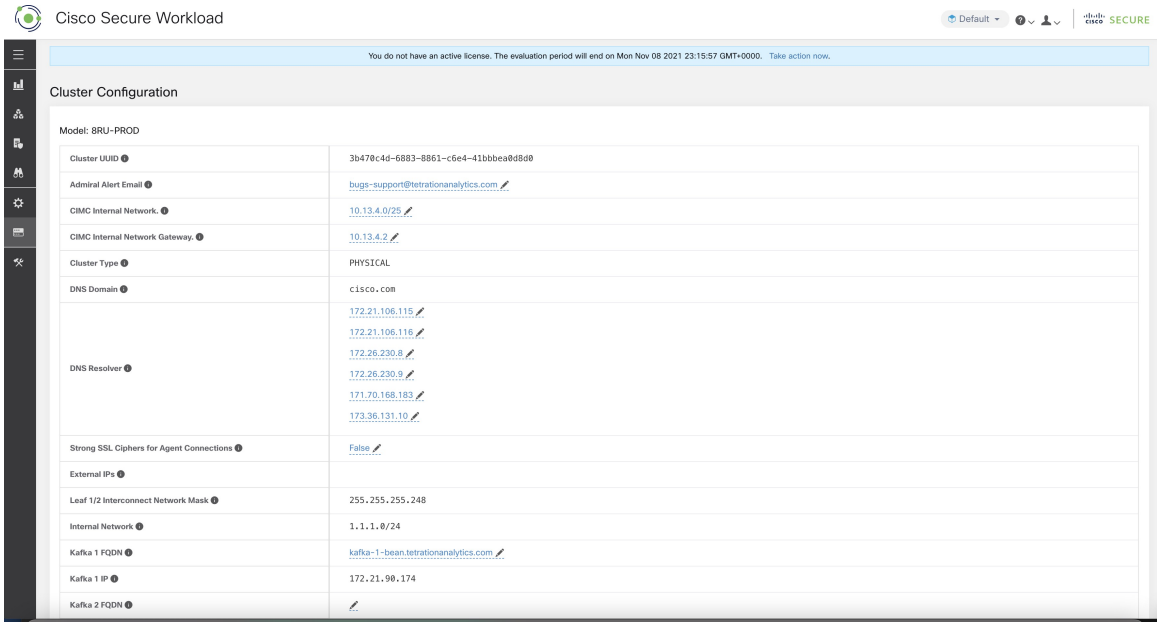
如果未配置 FQDN，则默认 FQDN 为：

IP 类型	默认 FQDN
传感器 VIP	wss{{cluster_ui_fqdn}}
Kafka 1	kafka-1-{{cluster_ui_fqdn}}

IP 类型	默认 FQDN
Kafka 2	kafka-2-{{cluster_ui_fqdn}}
Kafka 3	kafka-3-{{cluster_ui_fqdn}}

可以在**平台 (Platform)** > **集群配置 (Cluster Configuration)** 页面上更改 FQDN。

Figure 16: 集群配置页面上用于数据备份和恢复的 ***FQDN*** 或 ***IP***



使用同一页面上提供的 IP 更新 FQDN 的 DNS 记录。下表列出了 IP 和 FQDN 的映射。

字段名称	对应的 IP 字段	说明
传感器 VIP FQDN (Sensor VIP FQDN)	传感器 VIP (Sensor VIP)	更新 FQDN 以连接到集群控制平面
Kafka 1 FQDN	Kafka 1 IP	Kafka 节点 1 IP
Kafka 2 FQDN	Kafka 2 IP	Kafka 节点 2 IP
Kafka 3 FQDN	Kafka 3 IP	Kafka 节点 3 IP

Note 传感器 VIP 和 Kafka 主机的 FQDN 只能在配置数据备份和恢复之前更改。在配置后，FQDN 将无法更改。

对象存储要求

对象库必须提供 S3V4 兼容接口。

Note 一些符合 S3V4 标准的对象存储不支持 DeleteObjects 功能。删除过时的检查点信息需要使用 DeleteObjects 功能。缺少此功能可能会导致尝试从存储中删除过期检查点时失败，并可能导致存储空间不足。

- **位置**

  对象存储空间的位置对备份和恢复存储空间的延迟至关重要。要缩短恢复时间，请请确保对象存储的位置更靠近备用集群。

- **存储段**

  在对象存储库中为 Cisco Secure Workload 创建新的专用存储桶。只有集群才应对此存储桶进行写入访问。集群将写入对象并管理存储桶的保留。为存储桶调配至少 200 TB 的存储，并为存储桶获取访问密钥和秘密密钥。Cisco Secure Workload 中的数据备份和恢复不适用于预先进行身份验证的链接。

Note 如果将 Cohesity 用作对象存储库，请在计划时禁用分段上传。

- **HTTPS**

  数据备份选项仅支持与对象存储库的 HTTPS 接口。这是为了确保传输到对象存储库的数据已经过加密且安全。如果存储 SSL/TLS 证书由受信任的第三方 CA 签名，集群将使用它们来验证对象存储。如果对象存储库使用自签名证书，则可以通过选择**使用服务器 CA 证书 (Use Server CA Certificate)** 选项来上传公钥或 CA。

- **服务器端加密**

  强烈建议为分配给 Cisco Secure Workload 集群的存储桶打开服务器端加密。集群将使用 HTTPS 将数据传输到对象存储。但是，对象存储库应为对象进行加密，以确保静态数据的安全。

数据备份的配置

Note

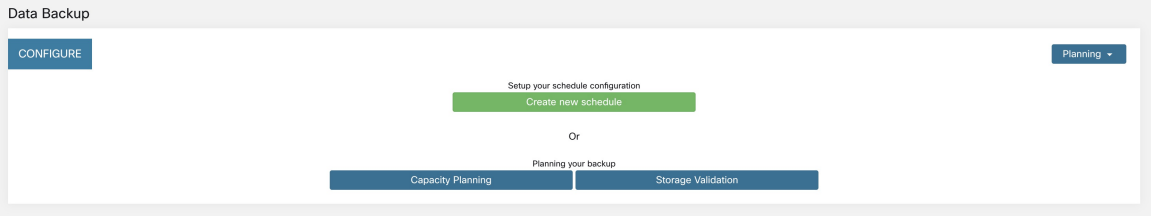
- 如果**平台 (Platform)** 下的**数据备份 (Data Backup)** 链接不可用，请联系思科技术支持中心以启用数据备份和恢复选项。
- 如果集群处于备用模式，您将无法查看**数据备份 (Data Backup)** 链接。

要在 Cisco Secure Workload 中配置数据备份，请执行以下操作：

1. **规划**：数据备份选项提供计划器来测试对对象存储的访问，确定存储要求以及每天所需的备份持续时间。这可用于在配置计划之前进行试验。

   要使用数据备份和恢复计算器，请导航至**平台 (Platform)** > **数据备份 (Data Backup)**。如果未配置数据备份和恢复，这将导航至“数据备份”(Data Backup) 登录页面。

   Figure 17: 备份登录页面

   要计划数据备份，请使用以下选项：

   - 使用存储规划器, on page 19
   - 使用容量规划器, on page 20

Note 如果无法在平台下查看数据备份选项，请确保您拥有启用数据备份和恢复的许可证。

2. **配置和计划数据备份**：Cisco Secure Workload 仅在配置的时间窗口内将数据复制到对象存储。首次配置备份时，系统会运行预先检查，以确保FQDN可解析并解析为正确的IP。在初始验证后，系统会将更新推送到已注册的软件代理，以切换为使用FQDN。如果没有FQDN，代理将无法在灾难事件后故障转移到其他集群。要支持此功能，必须将代理升级到集群支持的最新版本，并且所有代理都应能够解析传感器 VIP FQDN。从 Cisco Secure Workload 版本 3.3 及更高版本开始，只有深度可视性和执行代理支持数据备份和恢复，并将改用 FQDN。

   要创建计划和配置数据备份，请参阅配置数据备份, on page 21。

使用存储规划器

Procedure

步骤 1 要确保存储与 Cisco Secure Workload 兼容，请执行以下操作之一：

- 在**数据备份 (Data Backup)** 登录页面上，点击**存储规划 (Storage Planning)**。
- 从**规划 (Planning)** 下拉菜单中，选择**存储 (Storage)**。

系统将显示**存储规划 (Storage Planning)** 页面。

步骤 2 输入下列详细信息：

- 存储的名称。

- 符合 S3 标准的存储终端的 URL。
- 在存储上配置的符合 S3 的存储桶名称。
- （对于某些存储为可选）S3 兼容存储的区域。
- 存储的访问密钥。
- 存储的密钥。

步骤 3 （可选）如有需要，您可以启用 HTTP 代理。

步骤 4 （可选）要对支持的数据使用分段上传，请启用**使用分段上传 (Use Multipart Upload)**。

步骤 5 （可选）如果需要 CA 证书对存储服务器进行身份验证，请启用**使用服务器 CA 证书 (Use Server CA Certificate)** 并输入证书详细信息。

步骤 6 点击**测试 (Test)**。

存储验证将测试：

- 对象存储和存储桶的身份验证和访问。
- 在配置的存储桶中上传和下载。
- 带宽检查。

存储规划过程大约需要五分钟即可完成。

使用容量规划器

Procedure

步骤 1 要规划存储大小和备份窗口估计值，请执行以下操作之一：

- 在**数据备份 (Data Backup)** 登录页面上，点击**容量规划 (Capacity Planning)**。
- 从**规划 (Planning)** 下拉菜单中，选择**容量 (Capacity)**。

系统将显示**容量规划 (Capacity Planning)** 页面。

步骤 2 输入备份数据的最大带宽限制。

此带宽最多只能是限制传输到对象存储库的数据的流量监管器配置。

步骤 3 系统会自动填充已注册的软件代理计数。根据预测，您可以更改座席计数。

步骤 4 （可选）启用**精益数据模式 (Lean Data Mode)**，以从备份中排除非配置数据。使用此选项可将存储限制降低 75%。

步骤 5 为存储桶配置的最大存储空间。这将自动设置备份的保留期。

输入所需详细信息后，“预计备份持续时间”(Estimated Backup Duration) 将显示备份一天数据所需的时间。这是根据典型的代理负载、估计的代理数量和配置的最大带宽得出的估计值。估计的最大存储空间会显示 Cisco Secure Workload 为支持指定的保留和估计的代理计数所需的估计最大存储空间。

配置数据备份

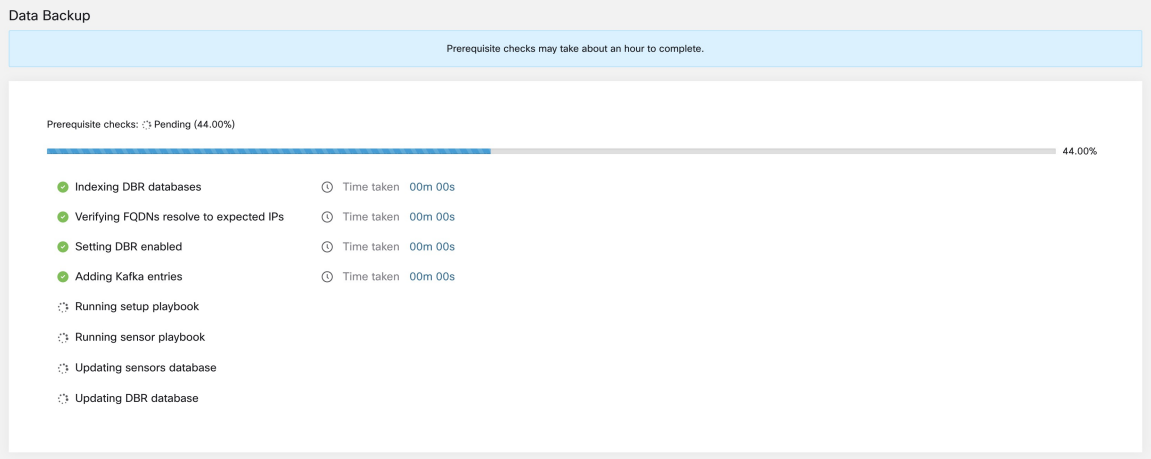
Procedure

步骤 1 在数据备份登录页面上，点击**创建新计划 (Create new schedule)**。

步骤 2 要确认运行前提条件检查，请选中**批准 (Approve)** 按钮，然后点击**继续 (Proceed)**。

前提条件检查大约需要 30 分钟才能完成，并且只在首次配置计划时运行。

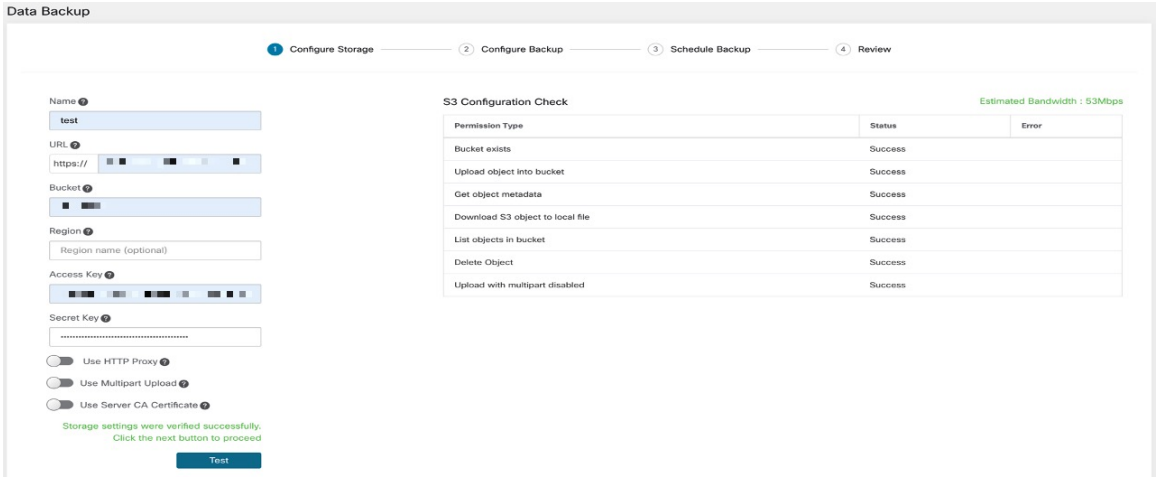
Figure 18: **备份前提条件运行**



步骤 3 要配置存储，请输入以下详细信息，然后点击**测试 (Test)**。

- 存储的名称。
- 符合 S3 标准的存储终端的 URL。
- 在存储上配置的符合 S3 的存储桶名称。
- （对于某些存储为可选）S3 兼容存储的区域。
- 存储的访问密钥。
- 存储的密钥。
- （可选）如有需要，请启用 HTTP 代理。
- （可选）要对支持的数据使用分段上传，请启用**使用分段上传 (Use Multipart Upload)**。
- （可选）如果需要CA 证书对存储服务器进行身份验证，请启用**使用服务器 CA 证书 (Use Server CA Certificate)** 并输入证书详细信息。

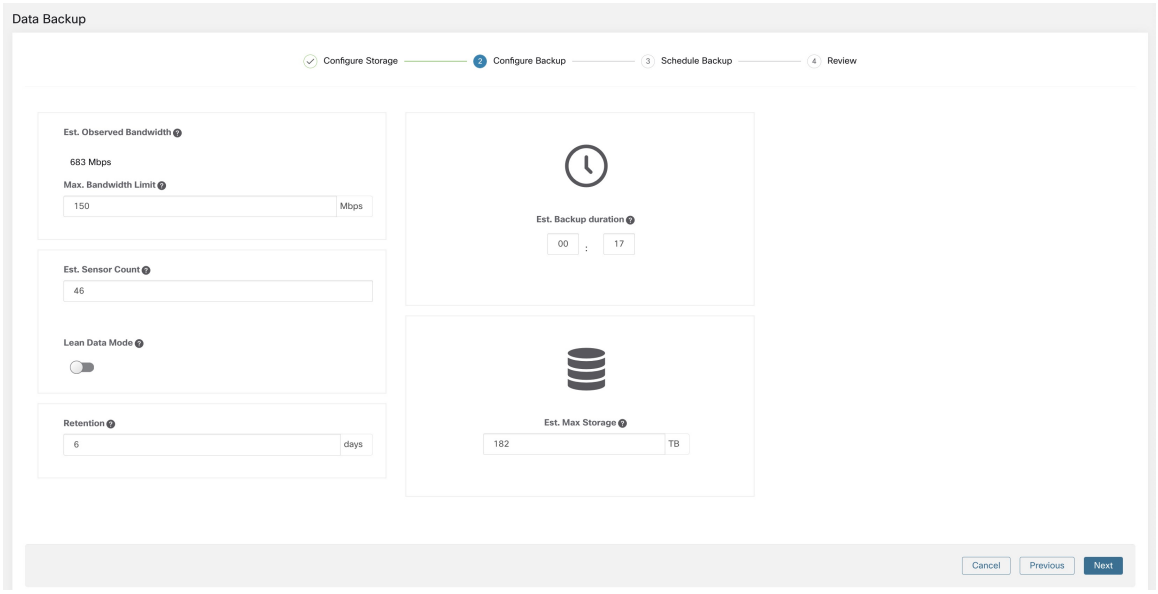
Figure 19: 存储配置



步骤 4 要配置存储容量，请输入以下详细信息：

- 备份数据的最大带宽限制。此带宽最多只能是限制传输到对象存储库的数据的流量监管器配置。
- 系统会自动填充已注册的软件代理计数。根据预测，您可以更改座席计数。
- （可选）启用**精益数据模式 (Lean Data Mode)**，以从备份中排除非配置数据。使用此选项可将存储限制降低 75%。
- 为存储桶配置的最大存储空间。这将自动设置备份的保留期。

Figure 20: 容量规划



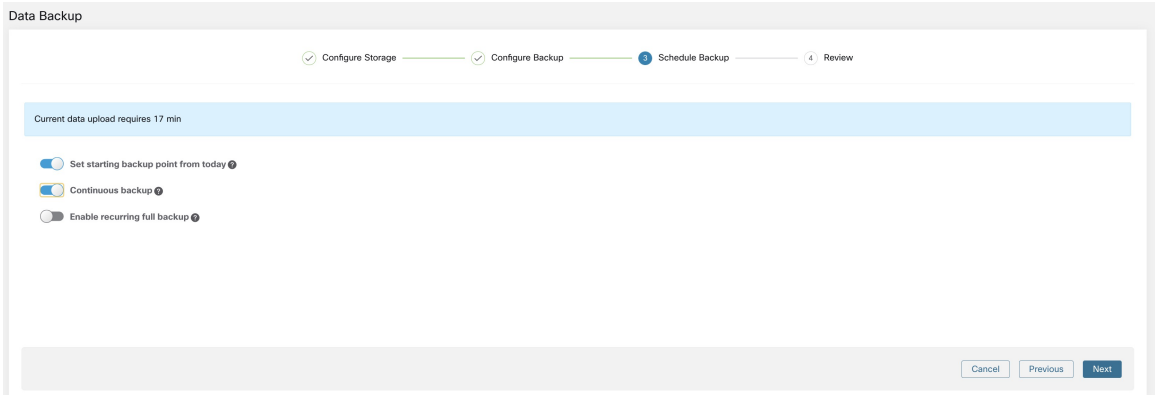
步骤 5 要计划备份，请启用以下选项：

- 默认情况下，**从今天起设置起始备份点 (Set starting backup point from today)** 已启用。此选项将忽略配置当天午夜（世界协调时）之前创建的所有文件。在工作集群中，第一天可能有大量数据需要备份，集群、网络和对象存储可能不堪重负。如果要备份所有现有数据，请禁用此复选框，但要注意对网络、对象存储和集群的影响。

  Note 无论是否选择此选项，所有配置数据都将被备份。

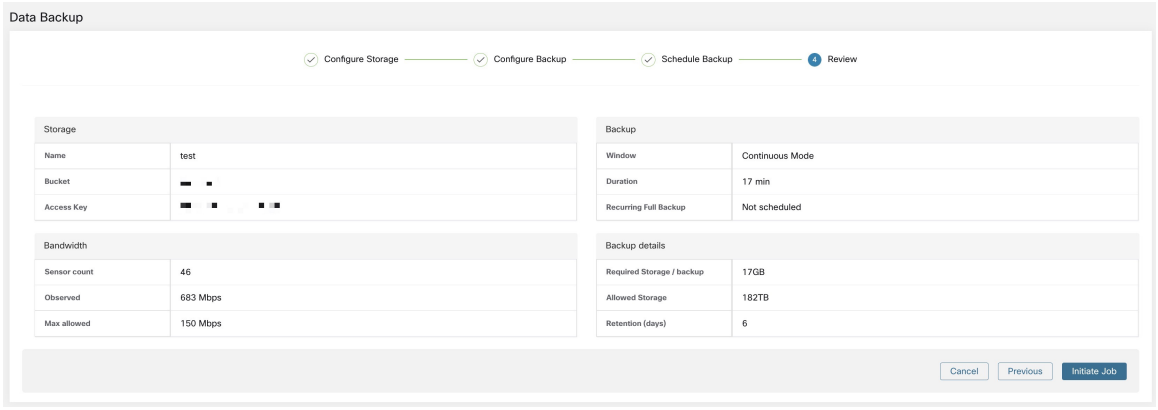
- 连续备份 - 如果启用，数据将在上一次备份完成后 15 分钟进行备份。此选项允许持续运行备份，而不是安排在特定时间进行备份。启用连续备份时，**时区 (Time zone)** 和**允许的开始备份窗口 (Allowed Start backup window)** 选项将不可用。
- 如果不使用连续备份，接下来的两个选项用于配置备份计划。
  - 时区：默认为 Web 浏览器时区
  - 允许的开始备份窗口：开始备份的时间（小时或分钟）。时间必须以 24 小时格式输入
  - 启用周期性完整备份（默认未选择）： 如果启用，则可配置完整备份计划。默认情况下，第一次完整备份后，所有备份都是增量备份。启用此配置后，将强制按照指定的时间表进行完整备份。

Figure 21: 安排备份



步骤 6 查看配置的备份计划和设置，然后点击**启动作业 (Initiate Job)**。

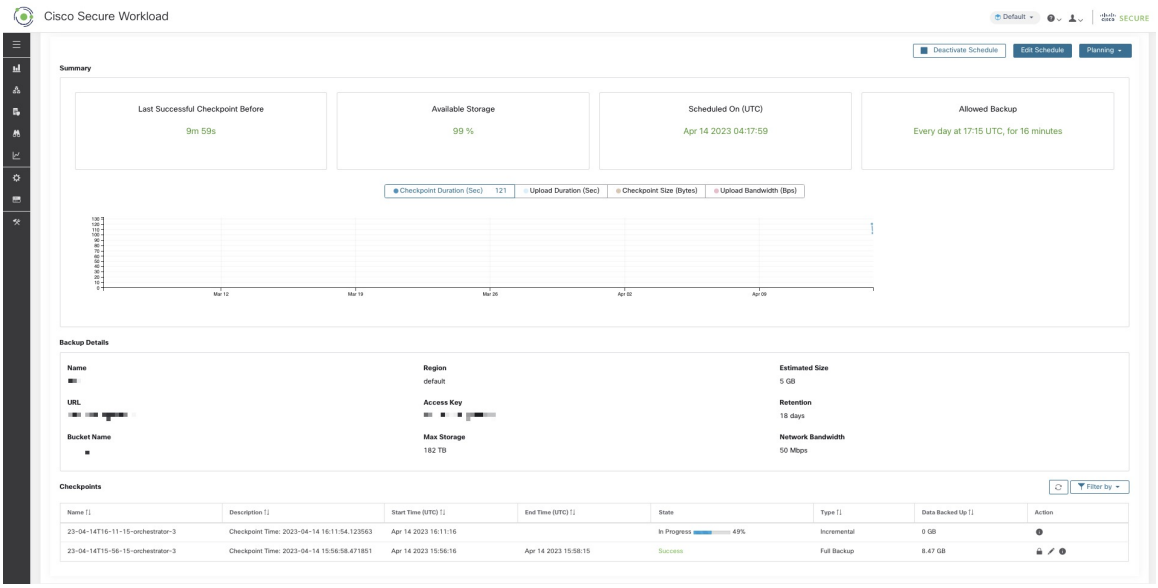
Figure 22: 备份配置审核



备份状态

配置数据备份后，除非启用连续模式，否则每天都会在预定时间触发备份。通过导航至**平台 (Platform)** > **数据备份 (Data Backup)**，可以在“数据备份”(Data Backup) 控制面板上查看备份状态。

Figure 23: 备份状态



距离上次成功检查点的时间应少于 24 小时加上到达检查点所需的时间。例如，如果检查点 + 备份大约需要 6 小时，则自上次成功执行检查点以来的时间应少于 30 小时。

下图提供了更多额外信息：

- 检查点持续时间：此图显示了检查点所用时间的趋势线。
- 上传持续时间：此图显示了将检查点上传到备份所需的时间的趋势线。

- 检查点大小：此图显示了检查点大小的趋势线。
- 上传带宽：此图显示了上传带宽的趋势线。

下表显示了所有检查点。可以编辑检查点标签，在选择检查点恢复备用集群上的数据时，这些标签将可供使用。

一个检查点会转换多个状态，以下是可能的状态：

- 已创建/待处理：检查点刚刚创建，正在等待复制
- 正在运行：正在将数据主动备份到外部存储
- 成功：检查点已完成且已成功；可用于数据恢复
- 失败：检查点已完成且已失败；无法用于数据恢复
- 正在删除/已删除：正在删除或已删除过期的检查点

要更改计划或存储桶，请点击**编辑计划 (Edit Schedule)**。要完成该向导，请参阅“配置数据备份”部分。

要对创建检查点期间的任何错误进行故障排除，请参阅故障排除：数据备份和恢复, on page 32。

停用备份计划

可以通过点击**停用计划 (Deactivate Schedule)** 按钮来停用备份。建议在更改计划之前停用备份计划。只有当没有正在进行的检查点时才停用计划。在检查点进行时运行测试或禁用计划可能会导致正在进行的检查点失败，并使上传处于未定义的状态。

对象存储保留

Cisco Secure Workload 集群管理存储桶中对象的生命周期。您不得在存储桶中删除对象或添加对象，否则可能会导致不一致并损坏成功的检查点。在配置向导中，必须指定要使用的最大存储空间。Cisco Secure Workload 将确保存储桶的使用率保持在配置的限制范围内。存储保留服务会使对象过期，并将其从存储桶中删除。在存储使用量达到根据配置的最大存储和传入数据速率计算的阈值（存储桶容量的 80%）后，保留将尝试删除未保留的检查点，以将使用量降低到阈值以下。在任何时候，保留功能还将至少保留两个成功的检查点和所有保留的检查点，以数量多者为准。如果保留无法删除任何检查点以腾出空间，则**检查点将开始失败**。

保留检查点

随着新检查点的创建，旧检查点将过期并被删除。但是，检查点可以保留，从而防止因保留而被删除。系统不会删除保留的检查点。如果有多个保留的检查点，有时存储将不足以容纳新的对象，并且过期的检查点无法删除，因为它们已被保留。最佳实践是根据需要保留检查点，并将原因和有效性用作参考来更新检查点的标签。要保留检查点，请点击所需检查点的锁形图标。

恢复数据

- 要使用备份数据进行恢复，集群必须处于**DBR 备用模式**。目前，您**只能在初始设置期间**将集群设置为备用模式。
- 在集群进入备用模式后，从导航窗格中选择**平台**以访问数据恢复选项。

Cisco Secure Workload 支持以下组合：

主集群 SKU	备用集群 SKU
8RU-PROD	8RU-PROD、8RU-M5
8RU-M5	8RU-PROD、8RU-M5
39RU-GEN1	39RU-GEN1、39RU-M5
39RU-M5	39RU-GEN1、39RU-M5

在备用模式下部署集群

Note 联系思科技术支持中心以启动数据恢复。

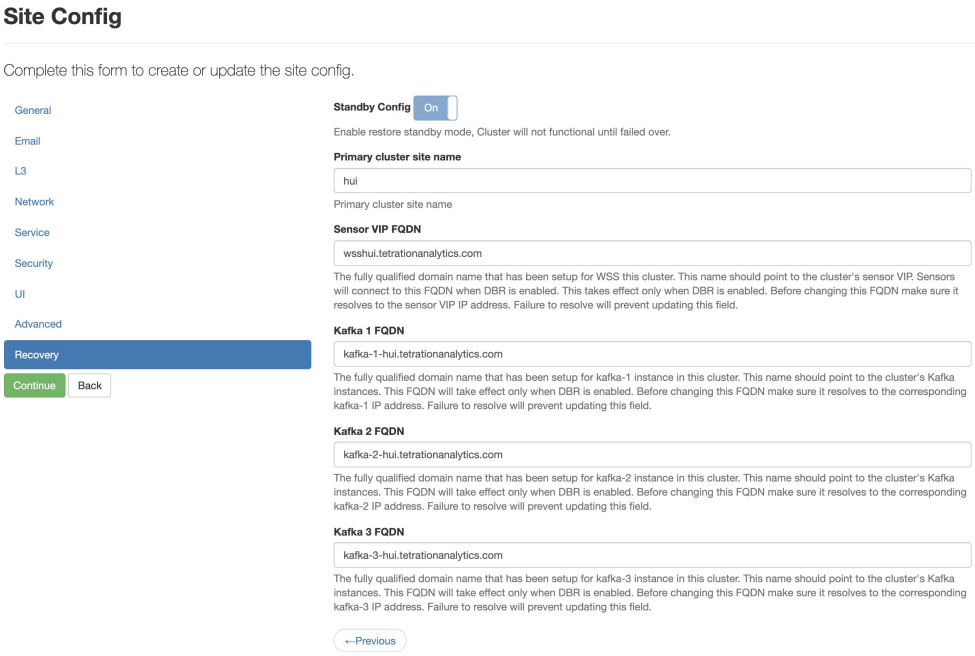
通过在站点信息中配置恢复选项，您可以在备用模式下部署集群。在部署期间配置站点信息时，请在部署期间在设置 UI 的**恢复 (Recovery)** 选项卡下配置恢复详细信息。

共有三种模式（请参阅备用部署模式部分）可用于部署备用集群，对于所有这三种模式，请配置以下设置：

- 将**备用配置 (Standby Config)** 设置为**开 (On)**。此配置一经设置便无法更改，直到重新部署集群为止。
- 配置主集群名称和 FQDN。您可以稍后更改此配置。

Note Kafka 和传感器 FQDN 必须与主集群匹配，否则恢复过程将失败。

Figure 24: 启用备用模式



- 部署的其余部分与 Cisco Secure Workload 集群的常规部署相同。
- 集群进入备用模式后，Cisco Secure Workload UI 上会显示一个横幅。
- 部署后可以重新配置主集群名称和 FQDN，以便让备用集群能够跟踪另一个集群。这可以稍后在从**集群配置 (Cluster Configuration)** 页面触发确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移之前重新配置。

备用部署模式

- **冷备用**：没有备用集群。但是，主集群会将数据备份到 S3。在发生灾难期间，必须调配新集群（或与主集群相同的集群），在备用模式下部署并恢复。
- **热备用**：备用集群可运行并在备用模式下部署。它会定期从 S3 集群获取状态，并将其置于就绪状态，以便在发生灾难时运行。在发生灾难期间，登录到此新集群并触发确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移。
- **Luke 热备用**：多个主集群由较少的备用集群提供支持。备用集群在备用模式下部署。只有在灾难发生后，才会配置存储桶信息，预取数据并恢复集群。

将数据恢复到 Cisco Secure Workload 集群

Before you begin

确保以备用模式部署集群。有关详细信息，请参阅在备用模式下部署集群。

Procedure

步骤 1 （可选）如果已配置存储详细信息，请转至步骤 2。要配置 S3 存储，请输入以下详细信息：

- 存储的名称。
- 符合 S3 标准的存储终端的 URL。
- 在终端存储上配置的符合 S3 的存储桶名称。
- （对于某些存储为可选项）S3 兼容存储的区域。
- 存储的访问密钥。
- 存储的密钥。
- （可选）如有必要，请启用 HTTP 代理。
- （可选）如果需要CA证书对存储服务器进行身份验证，请启用**使用服务器 CA 证书 (Use Server CA Certificate)** 并输入证书详细信息。

步骤 2 点击**测试 (Test)** 以检查是否可从 Cisco Secure Workload 集群访问 S3 存储。

已执行测试的状态显示在表中。如果连接到存储时出现任何错误，请阅读说明并排除错误，以继续执行下一步。

步骤 3 点击**下一步 (Next)**。

步骤 4 在**预先检查 (Pre-checks)** 下，显示 Cisco Secure Workload 运行的预先检查的状态。要手动运行预先检查，请点击**执行检查 (Perform Check)**。

系统将显示所有检查的状态：

- 对于存在错误但不阻止您恢复数据的检查，请将光标悬停在警告图标上以获取详细信息，并将光标悬停在链接以导航至**服务状态 (Service Status)** 页面以获取有关服务的更多详细信息。
- 如果任何检查失败，则必须解决问题才能继续数据恢复。导航至**服务状态 (Service Status)** 页面，获取该服务的更多详细信息。

Note 确保要恢复到的检查点是最新的且没有错误。

步骤 5 点击**开始恢复过程 (Start restore process)**。

在**恢复 (Restore)**下，显示已运行的所有数据恢复作业、配置的 S3 存储详细信息以及数据恢复预先检查的状态。

步骤 6 点击**恢复 (Restore)**。

步骤 7 在确认对话框中，选中复选框以确认您同意在数据恢复过程中代理连接会丢失，数据也可能丢失。点击**确认 (Confirm)** 开始数据恢复过程。

系统将显示数据恢复过程的进度。

Caution 在**恢复前 Playbook**阶段，集群中的所有服务都将重新初始化，并且停机时间约为两小时。在此阶段，Cisco Secure Workload GUI 无法访问。有关数据恢复所涉及阶段的详细信息，请参阅集群恢复阶段。

如果 GUI 长时间无法访问，请联系思科技术支持中心以解决问题。

Note

在**恢复后 Playbook** 阶段之后，可以访问 GUI 并更新所有作业的状态。系统将显示一条确认消息，指明数据恢复成功。

What to do next

更新 DNS 服务器以将配置的 FQDN 重定向到集群 IP 地址，从而确保软件代理在集群确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移完成后与集群通信。

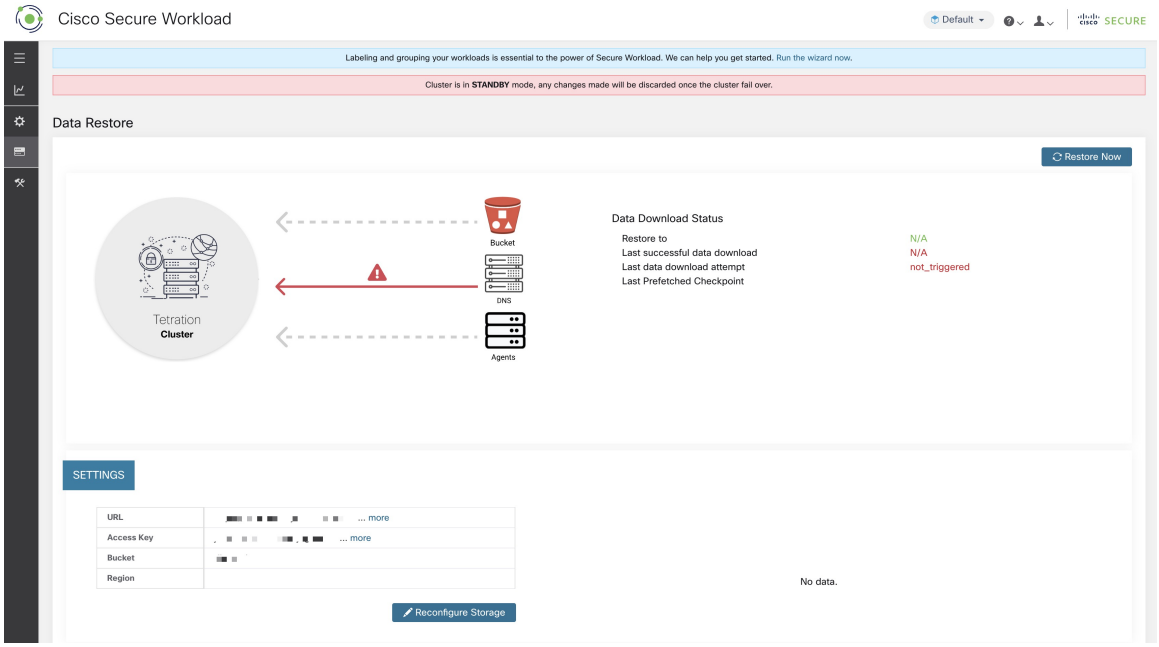
预提取集群数据

在恢复集群之前，必须先预取数据。检查点数据从用于备份数据的同一存储桶预取。必须提供凭证，备份服务才能从存储下载。如果存储未设置预取，则**数据恢复 (Data Restore)** 选项卡将启动设置向导。

Note 备用集群只会与 S3 存储交互。当主集群上的备份更新为使用不同的存储或存储桶时，必须更新备用集群上的存储。

验证信息后，存储会自动配置为预取。“恢复”(Restore) 选项卡将显示预取状态。

Figure 25: 预取状态



状态页面将显示以下信息：

- 左上部分有一个图形，指明各组件是否已准备好开始恢复。要查看数据，请将鼠标悬停在组件上。关联数据将显示在右上角部分。
  - **存储桶**：显示预取状态。如果最新数据的时间超过45分钟，则显示为红色。请注意，如果每个检查点在活动状态下的备份时间都超过 45 分钟，那么最新数据的时间超过 45 分钟就不是一个问题。
  - **DNS**：显示与备用集群 IP 地址相关的 Kafka 和 WSS FQDN 解析。在恢复过程中，如果 FQDN 没有更新为备用集群 IP 地址，则代理将无法连接。FQDN 开始解析到备用集群后，状态将变为绿色。
  - **代理**：显示已成功切换到备用集群的软件代理的数量。这仅在触发恢复后才相关。
- 右上部分显示与左侧部分中所选图形相关的信息。点击**立即恢复 (Restore Now)** 将启动恢复过程。
- 左下部分显示正在使用的预取存储设置。
- 右下部分显示预取延迟图。

数据预取会更新多个必要组件，以确保快速恢复。如果数据预取无法完成，则状态页面上会显示失败原因。

可能导致预取失败的常见错误：

S3 访问错误：在这种情况下，无法成功下载存储中的数据。这可能是由于凭证无效、存储策略更改或临时网络问题导致的。

集群版本不兼容：可以将数据恢复到与主集群运行相同版本（包括相同补丁版本）的 Cisco Secure Workload 的集群。当只升级其中一个集群时，升级过程中可能就会出现这种情况。或者在部署过程中使用不同的版本进行部署。将集群部署到一个通用版本就能解决此问题。

不兼容的SKU版本：记下允许用于主集群的备用集群的SKU。只允许恢复主集群SKU的特定SKU。

集群恢复阶段

集群数据分两个阶段恢复：

- **强制阶段**：首先恢复重启服务所需的数据。强制阶段所需的时间取决于配置、安装的软件代理数量、备份的数据量和流量元数据。在强制阶段，UI 不可访问。**在强制阶段，如有需要，任何支持都需要使用有效的 TA 访客密钥**。
- **延迟阶段**：集群数据（包括流数据）在后台恢复，并且不会阻止集群使用。可以访问集群 UI，并显示一条包含已完成恢复百分比的横幅。在此阶段，集群会正常运行，数据管道会正常运行，流搜索也将可用。

在恢复的强制阶段完成且 UI 可访问后，集群中的更改必须传达给软件代理。在代理使用的 DNS 服务器中，必须更新与集群 FQDN 相关联的 IP 地址，并且 DNS 条目应指向已恢复的集群。当与主集群的连接中断时，代理会触发 DNS 查找。根据更新的 DNS 条目，代理将连接到已恢复的集群。

恢复时间目标和恢复点目标

本部分介绍数据备份和恢复解决方案的恢复时间目标 (RTO) 和恢复点目标 (RPO)。

主集群上启动的备份需要一些时间才能完成，具体取决于备份的数据量和备份配置。不同的备份模式定义了解决方案的 RPO。

- 如果已计划，则使用非连续备份，每天启动一次备份。如果发生灾难，那么丢失数据的最长时间约为 24 小时，再加上将数据复制到备份存储器所需的时间。因此，RPO 至少为 24 小时。
- 如果使用连续备份模式，则在上一次备份15分钟后启动新的备份。创建每个备份需要一定的时间，然后将数据上传到备份存储器也需要一定的时间。第一次备份是完整备份，之后的备份是增量备份，增量备份不会花费太多时间。如果发生灾难，丢失的数据量将是创建备份所花时间与将备份上传到存储器所花时间的总和。通常情况下，这种情况下的 RPO 约为几分钟到一小时。

在恢复集群时，首先会从存储中预取强制数据，然后触发强制恢复阶段。UI 在强制恢复阶段不可用。强制恢复完成后，即可使用UI。其余数据会在延迟恢复阶段进行恢复。在这种情况下，RTO是指在强制阶段完成后，UI 恢复使用之前所需的时间。RTO 取决于备用部署模式。

- 冷备用模式：在此模式下，必须先部署集群，这大约需要几个小时。然后，必须使用备份存储凭证来配置集群。由于这是第一次将备份上传到备用集群，因此需要检索和处理大量的必需数据。预取时间约为10分钟（具体取决于备份的数据量）。必需恢复阶段大约需要30分钟完成。这些加在一起构成大约几个小时的 RTO 时间，主要是由于启动和部署集群所花费的时间。
- Luke 热备用模式：在此模式下，集群已部署，但未配置备份存储。必须使用备份存储凭证来配置集群。由于这是第一次将备份上传到备用集群，因此需要检索和处理大量的必需数据。预取

时间约为 10 分钟（具体取决于备份的数据量）。必需恢复阶段大约需要 30 分钟完成。根据备份的数据量和从备份存储中提取数据所需的时间，RTO 时间约为一小时至两小时。

- 热备用模式：在此模式下，集群已部署，备份存储已配置，并且预取正在从存储中检索数据。现在可以恢复集群，这将触发强制恢复阶段，大约需要 30 分钟完成。这就构成了大约 30 分钟的 RTO 时间。请注意，从主用设备备份上传到存储到备用设备提取备份之间会有一定的延迟。这大约需要几分钟。如果主用设备备份（发生灾难事件之前）的最新备份尚未预取到备用备份，则必须等待几分钟才能检索到。

使用数据备份和恢复进行升级

在集群上启用数据备份和恢复时，建议在开始升级之前停用计划。请参阅停用备份计划。这样可确保在升级开始之前存在成功的备份，并且不会上传新的备份。当检查点不在进行中时，必须停用计划，以避免创建失败的检查点。

故障排除：数据备份和恢复

S3 配置检查不成功

如果存储测试不成功，请确定右侧窗格中显示的故障情况，并确保：

- S3 兼容存储 URL 正确。
- 存储的访问密钥和秘密正确。
- 存储上存在存储桶，并授予了正确的访问（读/写）权限。
- 如果必须直接访问存储，则配置代理。
- 如果使用 Cohesity，则会禁用分段上传选项。

S3 配置检查的错误场景

下表列出了常见错误场景及解决方法，但并非详尽无遗。

***Table 8: S3* 配置检查期间的错误消息及解决方法**

错误消息	场景	解决方法
未找到	存储桶名称不正确	输入在存储设备上配置的存储桶的正确名称
SSL 连接错误	SSL 证书到期或验证错误	验证 SSL 证书
	无效的 HTTPS URL	• 重新输入存储的正确HTTPS URL。 • 解决SSL证书验证过程中出现的任何故障。

错误消息	场景	解决方法
连接超时	S3 服务器的 IP 地址无法访问	验证集群和 S3 服务器之间的网络连接
无法连接到 URL	存储桶区域不正确	输入正确的存储桶区域
	无效的 URL	重新输入 S3 存储终端的正确 URL
禁止	密码无效	输入正确的存储密钥
	访问密钥无效	输入正确的存储访问密钥
无法验证 S3 配置	其他异常或一般错误	稍后尝试配置 S3 存储

检查点的错误代码

下表列出了检查点的常见错误代码，但并非详尽无遗。

Table 9: 检查点的错误代码

错误代码	说明
E101：数据库检查点故障	无法为 MongoDB 操作日志创建快照
E102：流数据检查点故障	无法为 Druid 数据库创建快照
E103：数据库快照上传失败	无法上传 Mongo 数据库快照
E201：数据库复制失败	无法将 Mongo 快照上传到 HDFS
E202：配置复制失败	无法将 Consul-Vault 快照上传到 HDFS
E203：配置检查点故障	无法检查点 consul-vault 数据
E204：检查点期间配置数据不匹配	达到最大重试次数后无法生成 Consul/Vault 检查点
E301：备份数据上传失败	HDFS 检查点故障
E302：检查点上传失败	Copydriver 未能将数据上传到 S3
E401：检查点期间的系统升级	集群在此检查点期间升级；无法使用检查点
E402：在检查点期间重启服务	Bkpdriver 在创建状态下重启；无法使用检查点
E403：上一个检查点故障	上一次运行检查点失败
E404：另一个检查点进行中	正在执行另一个检查点

错误代码	说明
E405：无法创建检查点	检查点子进程出错
失败：已完成	前一个检查点失败；可能是多个检查点发生了重叠。

Cisco Secure Workload 中的高可用性

Cisco Secure Workload 可在服务、节点和虚拟机可能发生故障时提供高可用性。高可用性提供了恢复方法，确保停机时间最短，网站管理员的干预最少。

在 Cisco Secure Workload 中，服务会跨集群中的节点分布。多个服务实例在节点上同时运行。配置一个主实例和一个或多个辅助实例，以实现跨多个节点的高可用性。当服务的主实例发生故障时，该服务的辅助实例将作为主实例立即投入使用。

Cisco Secure Workload 集群设计

Cisco Secure Workload 集群的关键组件包括：

- 托管多个虚拟机的裸机服务器，而这些虚拟机又托管了许多服务。
- Cisco UCS C 系列机架式服务器配备 Cisco Nexus 9300 系列交换机，可为集成的高性能网络做出贡献。
- 基于硬件的设备模型，外形尺寸可大可小，可支持特定数量的工作负载：
  - 小型部署，配备六台服务器和两台 Cisco Nexus 9300 交换机。
  - 大型部署，配备 36 台服务器和 3 台 Cisco Nexus 9300 交换机。

Figure 26: Cisco Secure Workload 集群设计设计

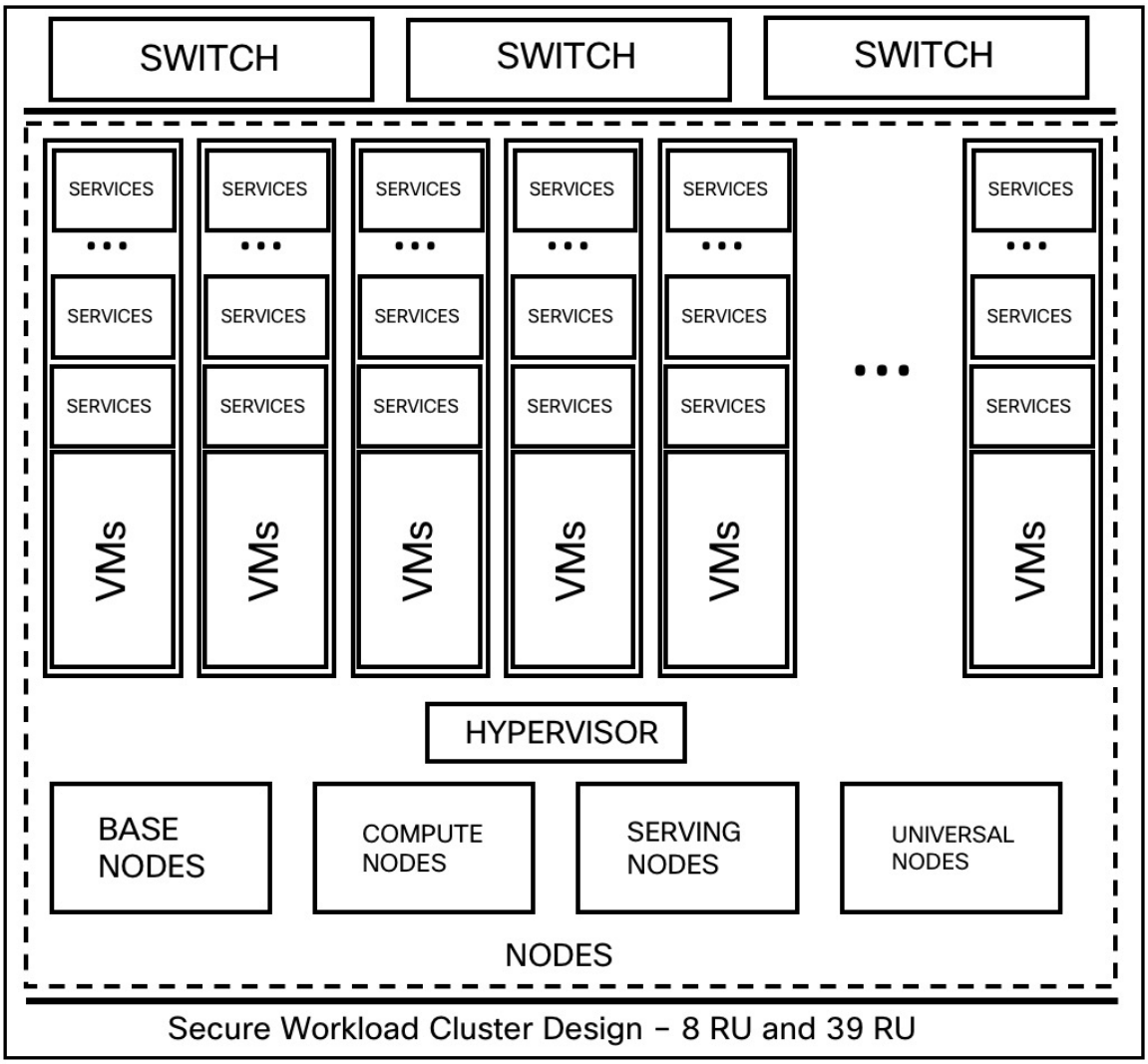


Table 10: Cisco Secure Workload 集集群件

属性/外形规格	**8 RU**	**39 RU**
节点数量	6	36
计算节点数量	-	16
基本节点数量	—	12
服务节点数量	—	8
通用节点数量	6	—
虚拟机数量	50	106

属性/外形规格	8 RU	39 RU
收集器的数量	6	16
网络交换机的数量	2	3

Cisco Secure Workload 中的高可用性限制

故障情形的影响和恢复详细信息

- 在任何时候都不会影响集群的运行。
- 无单点故障。如果集群中的任何节点或虚拟机发生故障，也不会导致整个集群发生故障。
- 服务、节点或虚拟机出现故障时，恢复停机时间最短。
- 软件代理与 Cisco Secure Workload 集群保持的连接不会受到影响。代理会与集群中所有可用的收集器进行通信。如果一个收集器或虚拟机发生故障，软件代理与其他收集器实例的连接可确保数据流不会中断，功能也不会丢失。
- 集群服务会与外部协调器通信。当服务的主实例发生故障时，辅助实例会接管，以确保与外部协调器的通信不会中断。

故障类型场景

高可用性支持以下故障场景：

- 服务故障
- VM 故障
- 节点故障
- 网络交换机故障

服务故障

当节点上的某个服务出现故障时，该特定服务的另一个实例会接替故障服务的功能并继续运行。

Figure 27: 正常运行

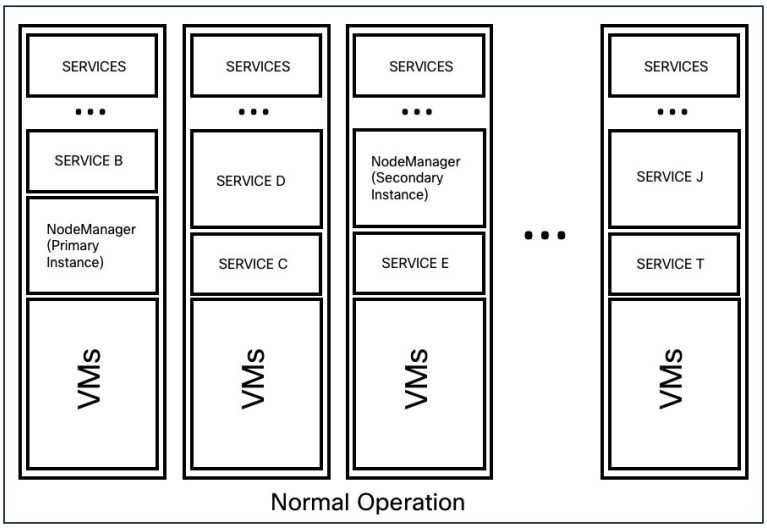


Figure 28: 服务的故障场景

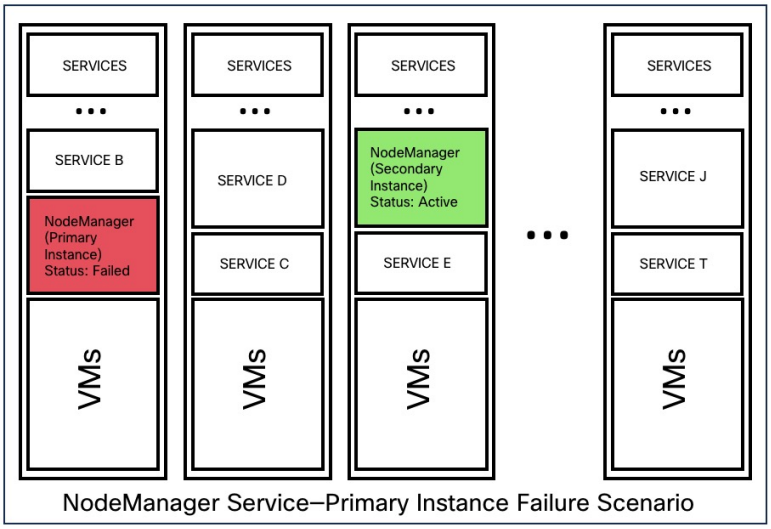


Table 11: 服务故障影响和恢复

影响	无明显影响。
恢复	• 将 UI 或相关服务从辅助实例继续运行的停机时间降至最短。 • 恢复会自动进行。

VM 故障

当其中一个虚拟机发生故障时，辅助虚拟机可用。辅助虚拟机上的服务会选择故障虚拟机正在运行的服务。同时，Cisco Secure Workload 会重启发生故障的虚拟机以将其恢复。例如， 如图：虚拟机的故障场景所示，当虚拟机（在此实例中为 VM1）发生故障时，其上运行的服务也会发生故障。辅助虚拟机继续运行，辅助实例选择故障虚拟机正在运行的服务。

Figure 29: 正常运行

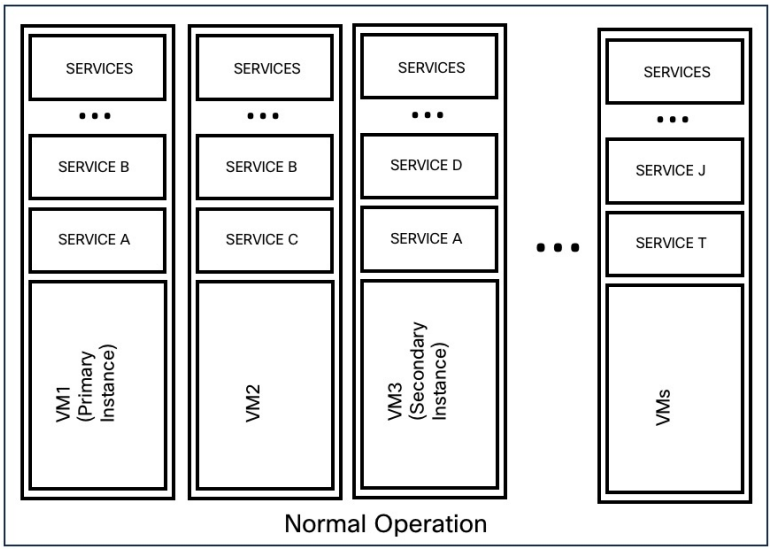
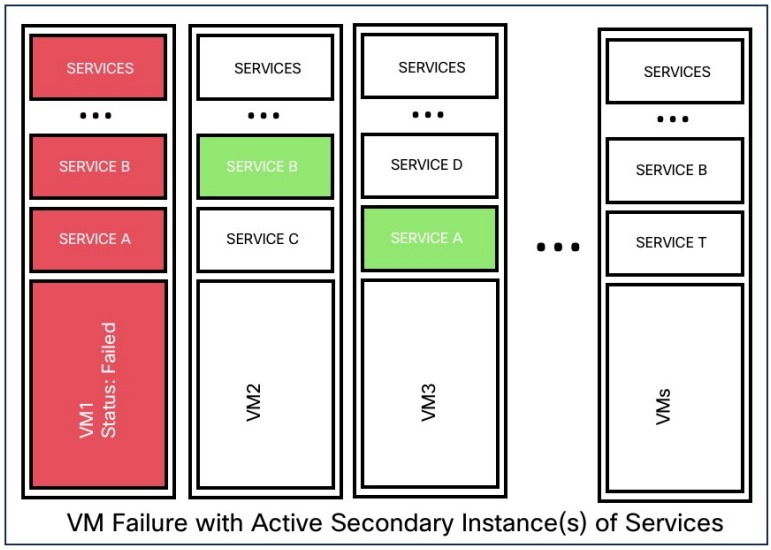


Figure 30: VM 的故障场景



对于对称虚拟机（如 collectordatamovers、datanode、nodemanager 和 druidHistoricalBroker 虚拟机）提供的服务，多个虚拟机可能会发生故障，但应用将降低容量继续运行。

Table 12: 对称 *VM* 类型

服务类型	虚拟机总数	支持的 VM 故障数
Datanode	6	4
DruidHistorical	4	2
CollectorDataMover	6	5
NodeManager	6	4
UI/ AppServer	2	1

Note 在相应的服务不可用之前，非对称 VM 类型仅允许一个 VM 故障。

Table 13: VM 故障影响和恢复

影响	无明显影响。
恢复	• 最大限度减少 UI 或相关服务从其他虚拟机上的辅助实例继续运行的停机时间。 • 恢复会自动进行。但是，如果 VM 仍然处于非活动状态，请联系思科技术支持中心以解决问题。在少数情况下，您可能需要更换裸机。

节点故障

Figure 31: 正常运行

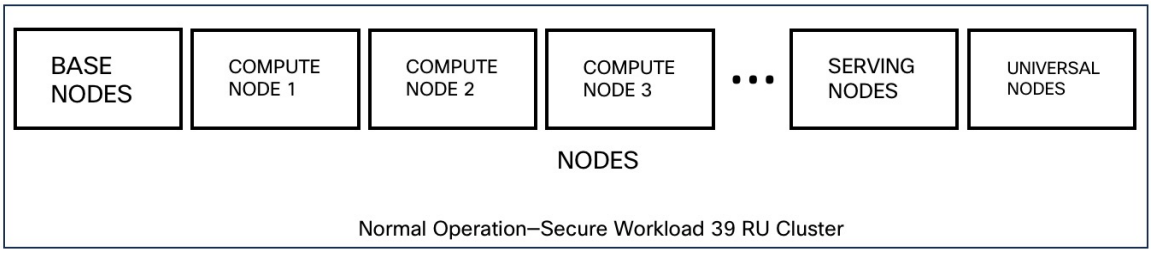


Figure 32: 节点的故障场景

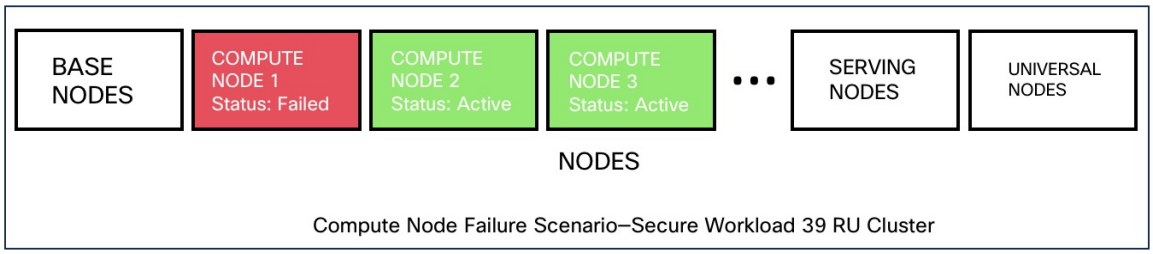


Table 14: 容许的节点故障数

节点故障数	8 RU	39 RU
高可用性允许的节点故障数	1	1*

* 在 39 RU 集群中，始终容许单节点故障。只要两个故障节点不托管 2 VM 或 3 VM 服务的虚拟机，例如协调器、Redis、MongoDB、Elasticsearch、enforcementpolicystore、AppServer、ZooKeeper、TSDB、Grafana 等，就可容许出现第二个节点故障。通常，第二个节点发生故障会导致关键服务因两个 VM 受到影响而变得不可用。

Caution 建议您立即恢复发生故障的节点，因为第二个节点发生故障很可能会导致中断。

Table 15: 节点故障影响和恢复

影响	不会影响集群的功能。但是，请联系思科技术支持中心以立即更换故障节点。第二个节点发生故障很可能会导致中断。
恢复	• 最大限度缩短停机时间。 • 如果某个节点发生故障，建议您联系思科技术支持中心寻求协助，以删除故障节点并将其替换为另一个节点。

网络交换机故障

Cisco Secure Workload 中的交换机始终保持活动状态。在 8RU 封装部署中，交换机发生故障不会造成任何影响。在 39RU 封装部署中，如果交换机发生故障，则集群的输入容量会减半。

Note Cisco Secure Workload 集群中的交换机没有建议的端口密度，无法支持公共网络的 VPC 配置。

Figure 33: 正常运行

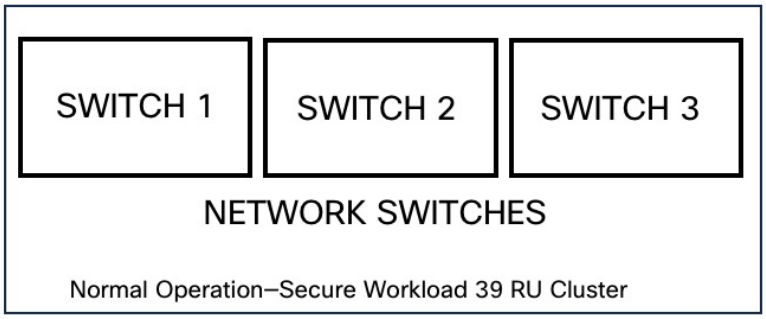


Figure 34: 交换机的故障场景

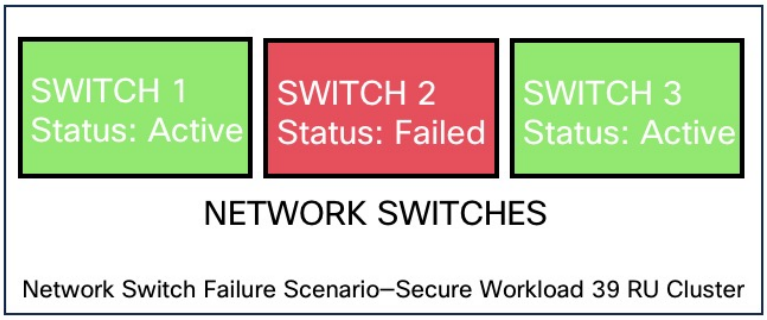


Table 16: 容许的交换机故障数

外形规格	**8 RU**	**39 RU**
高可用性允许的交换机故障数	1 **Note** 如果两台或更多交换机发生故障，可能会对集群的整个功能产生影响。	1 **Note** 单个交换机故障会导致输入容量减半。两个或更多故障可能会影响整个集群的功能。

Table 17: 网络交换机故障影响和恢复

影响	• 裸机上的故障交换机或网卡会导致集群内失去网络连接。 • 单个交换机故障不会影响集群的功能。但是，两个或更多故障可能会影响整个集群的功能。 • 与集群上的多个虚拟机的连接问题，或者间歇性和长期的连接问题会导致集群内出现不可预测的行为。

恢复	• 恢复会自动进行。 • 请联系思科技术支持中心，获取有关裸机上出现故障的交换机或网卡的帮助。

VM 信息

故障排除 (Troubleshoot) 菜单下的**虚拟机 (Virtual Machine)** 页面会显示属于思科 Cisco Secure Workload 集群的所有虚拟机。它会在集群启动或升级（如有）期间显示其部署状态，并且还会显示公共 IP。请注意，集群中的所有虚拟机都不属于公共网络，因此它们可能没有公共 IP。

升级 Cisco Secure Workload 集群

Cisco Secure Workload 支持两种类型的升级 - 完全升级和补丁升级。以下各部分介绍完整升级过程。在完全升级期间，集群中的所有虚拟机都会关闭，部署新 VM，并重新调配服务。在此升级期间，集群中的所有数据都将保留，但升级期间的停机时间除外。

集群升级选项

Cisco Secure Workload 集群支持的升级类型：

- **完全升级**：要启动完全升级，请从导航窗格中选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。在**升级 (Upgrade)** 选项卡中，选择**升级 (Upgrade)**。在全面升级过程中，虚拟机的电源被关闭，虚拟机被升级并重新部署。集群停机，在此期间无法访问 Cisco Secure Workload UI。
- **补丁升级**：补丁升级可尽可能减少集群停机时间。必须修补的服务会更新，并且不会导致 VM 重启。停机时间通常为几分钟。要启动补丁升级，请选择**补丁升级 (Patch Upgrade)**，然后点击**发送补丁升级链接 (Send Patch Upgrade Link)**。

系统会向注册的邮件地址发送一封包含链接的电子邮件，以启动升级。

Figure 35: 包含升级链接的邮件

Hello Site Admin!

We received a request that you intend to upgrade the cluster "50". You can do this through the link below.

Upgrade 50

The above link expires by Mar 26 09:29:50 pm (PDT).

If you didn't request this, please ignore this email.

Upgrade will not be triggered until you actually click the above link.

Cisco TetrationOS Software, Version 2.2.1.34.devel
TAC Support: http://www.cisco.com/tac
Copyright (c) 2015-2018 by Cisco Systems, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Cisco products are covered by one or more patents.

在发送邮件之前，协调程序会进行多项验证检查，以确保集群可以升级。检查包括：

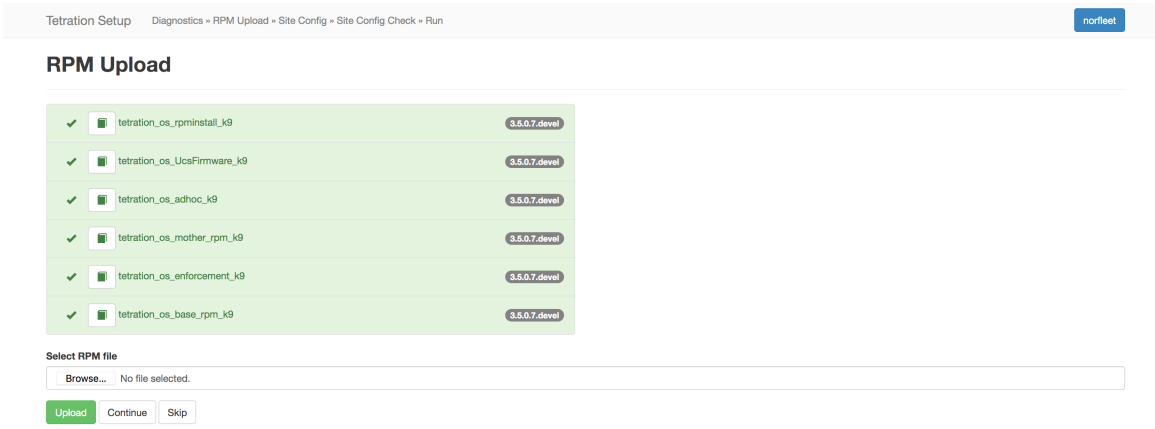
- 检查以查看没有已下线的节点。
- 检查每个裸机以确保没有硬件故障，包括以下内容：
  - 驱动器故障
  - 驱动器预测性故障。
  - 驱动器缺失
  - StorCLI 故障
  - MCE 日志失败
- 检查以确保裸机处于调试状态，39RU 服务器不少于 36 台，8RU 服务器不少于 6 台。

Note 如果出现任何故障，将不会向注册的邮件地址发送升级链接，并会显示 500 错误，其中包含硬件故障或主机丢失等信息，并检查协调程序日志以获取更多信息。在这种情况下，使用资源管理器对主机 orchestrator.service.consul 中的 /local/logs/tetration/orchestrator/orchestrator.log 执行 tail -100。日志提供了详细的信息，说明是哪三次检查导致了故障。这通常需要修复硬件并重新调试节点。重启升级进程。

上传 RPM

点击邮件中收到的升级链接后，系统将显示 **Cisco Secure Workload 设置 (Secure Workload Setup)** 页面。设置 UI 用于部署或升级集群。登录页面显示集群中当前部署的 RPM 列表。您可以上传 RPM 来升级集群。

***Figure 36: RPM* 上传**



按照设置 UI 上显示的顺序上传 RPM。未按正确的顺序上传 RPM 会导致上传失败，并且**继续 (Continue)** 按钮将保持禁用状态。顺序为：

1. tetration_os_rpminstall_k9
2. tetration_os_UcsFirmware_k9
3. tetration_os_adhoc_k9
4. tetration_os_mother_rpm_k9
5. tetration_os_enforcement_k9
6. tetration_os_base_rpm_k9

Note 对于在 vSphere 上部署的 Cisco Secure Workload 个虚拟集群，请确保同时升级 Tetration os_ova_k9 RPM，并且不上传 tetration_os_base_rpm_k9 RPM。

要查看每次上传的日志，请点击每个 RPM 左侧的日志符号。此外，失败的上传将以红色标记。

Figure 37: RPM 上传日志

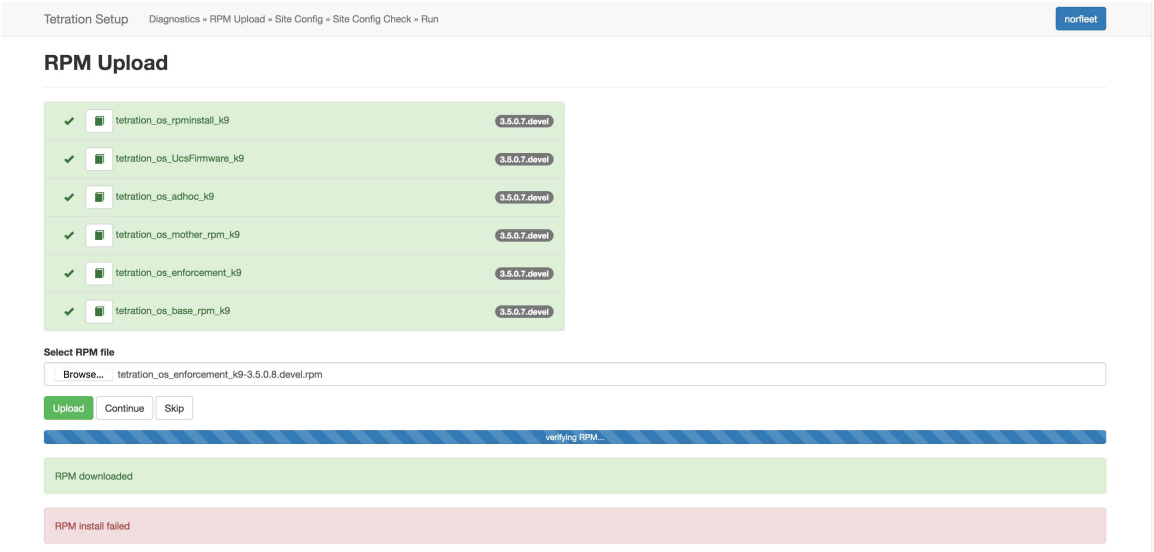
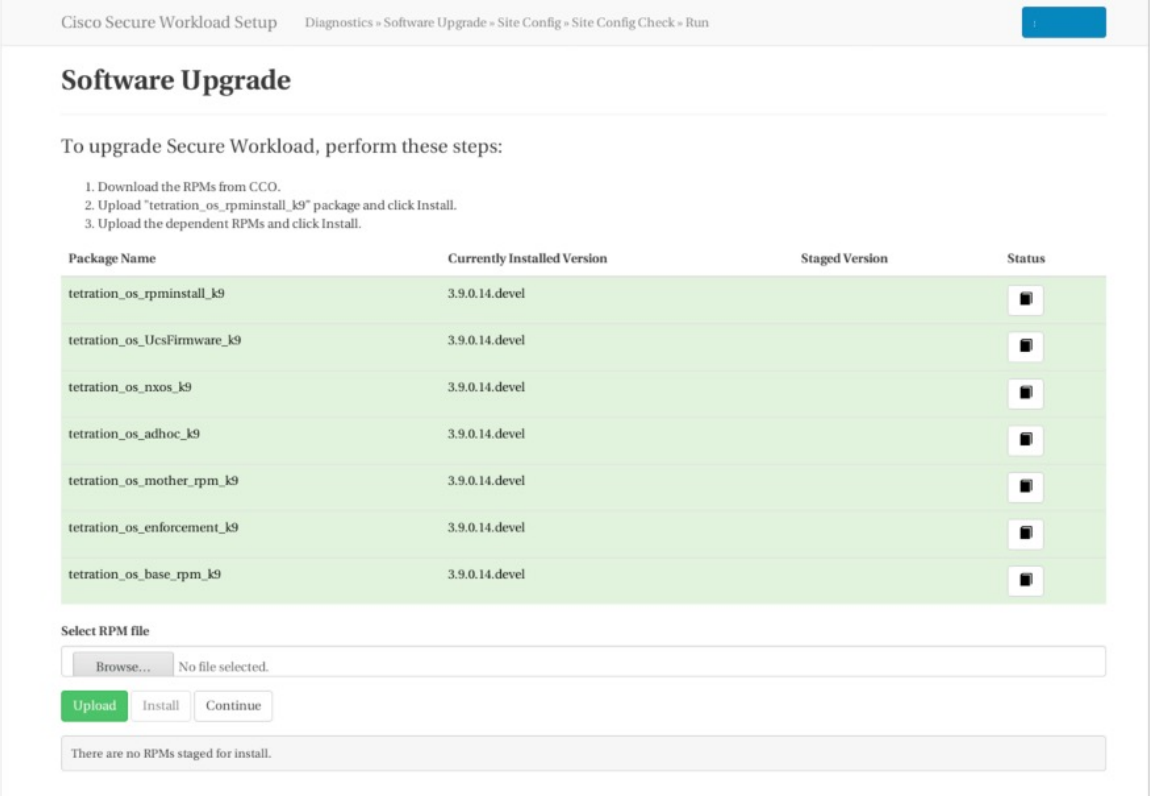


Figure 38: 上传 ***RPM***



有关详细说明，请参阅 Cisco Secure Workload 升级指南。

站点信息

升级集群的下一步是更新站点信息。并非所有站点信息字段都可更新。只能更新以下字段：

- SSH 公钥
- Sentinel 警报邮件（适用于 Bosun）
- CIMC 内部网络
- CIMC 内部网络网关
- 外部网络

Note 请勿更改现有外部网络，您可以通过附加到现有网络来添加其他网络。更改或删除现有网络将使集群无法使用。

- DNS 解析器
- DNS Domain

- NTP 服务器
- SMTP 服务器
- SMTP 端口
- SMTP 用户名（可选）
- SMTP 密码（可选）
- 系统日志服务器（可选）
- 系统日志端口（可选）
- 系统日志严重性（可选）

Note

- 系统日志服务器严重性范围为严重到信息性。对于 bosun 警报，需要将严重性设置为警告或更高（信息性）。
- 从 3.1 版本开始，**不支持通过设置 UI 的外部系统日志**。将 TAN 设备配置为将数据导出到系统日志。有关详细信息，请参阅将外部系统日志隧道移至 TAN。
- Cisco Secure Workload 支持使用 STARTTLS 命令与支持 SSL 或 TLS 通信的邮件服务器进行安全的 SMTP 通信。支持安全流量的服务器的标准端口通常是 587/TCP，但许多服务器也接受标准 25/TCP 端口上的安全通信。

  Cisco Secure Workload 不支持使用 *SMTPS* 协议与外部邮件服务器进行通信。

其余字段不可更新。如果没有更改，请点击**继续 (Continue)** 以触发升级前检查，否则更新字段，然后点击**继续 (Continue)**。

升级前检查

在升级集群之前，要对集群进行一些检查，以确保一切正常。系统将执行以下升级前检查：

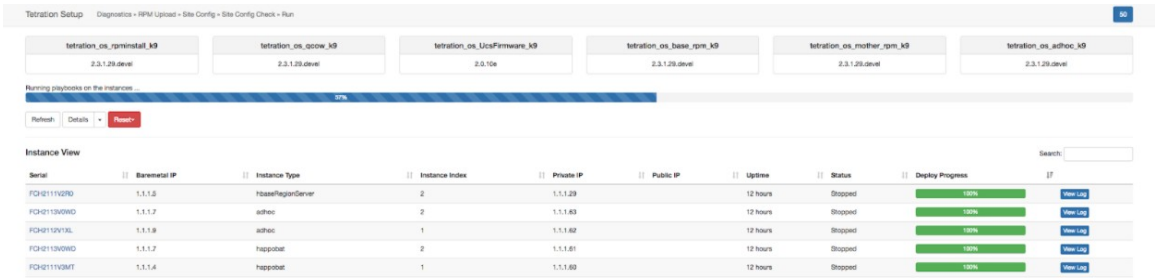
- RPM 版本检查：检查以确保所有 RPM 已上传且版本正确。它不会检查顺序是否正确，只会检查是否已上传。请注意，顺序检查会在上传过程中完成。
- 站点 Linter：执行站点信息 linting
- 交换机配置：配置枝叶或主干交换机
- 站点检查器：执行 DNS、NTP 和 SMTP 服务器检查。发送包含令牌的邮件，该邮件会被发送到主站点管理员帐户。如果未配置 DNS、NTP 或 SMTP 中的任何服务，则此步骤将失败。
- 令牌验证：输入在邮件中发送的令牌并继续升级过程。

升级 Cisco Secure Workload 集群

Caution

- 建议您不要选择**忽略停止故障 (Ignore Stop Failures)** 选项。这是某些服务未关闭时升级失败的恢复选项。使用此选项会关闭在服务变为活动状态时可能导致故障的虚拟机。
- 在监督下使用此选项。

Figure 39: 升级集群



Before you begin

完成升级前检查，然后输入在验证令牌邮件中收到的令牌。

Procedure

步骤 1 点击**继续 (Continue)** 开始升级。

步骤 2 （可选）点击集群名称以查看站点信息。

系统将显示 Cisco Secure Workload RPM 和版本。升级栏会显示升级进度。蓝色表示正在进行的活动，绿色表示已完成的活动，而红色表示失败的活动。

有四个按钮可用：

- 刷新 (Refresh)：刷新页面。
- 详细信息 (Details)：点击**详细信息 (Details)** 可查看在此升级期间已完成的步骤。点击日志旁边的箭头可显示日志。
- 重置 (Reset)：此选项包含重置协调器状态的选项。此选项会取消升级并回到起点。除非升级失败，并且在升级失败后几分钟已过，否则请勿使用此选项，以便在重启升级之前完成所有进程。
- 重启 (Restart)：当升级失败时，点击**重启 (Restart)** 可重启集群并启动新的升级。这可以帮助解决可能阻止升级过程的任何待处理清理操作或问题。

在实例视图中，系统会跟踪每个单独的 VM 部署状态。列包括：

- 串行 (Serial)：托管此虚拟机的裸机串行

- 裸机 IP (Baremetal IP)：分配给裸机的内部 IP
- 实例类型 (Instance Type)：VM 的类型
- 实例索引 (Instance Index)：VM 的索引 - 有多个同一类型的 VM 可实现高可用性。
- 专用 IP (Private IP)：分配给此虚拟机的内部 IP
- 公共 IP (Public IP)：分配给此虚拟机的可路由 IP - 并非所有虚拟机都有此 IP。
- 正常运行时间 (Uptime)：虚拟机的正常运行时间
- 状态 (Status)：可以是已停止、已部署、失败、未启动或正在进行。
- 部署进度 (Deploy Progress)：部署百分比。
- 查看日志 (View Log)：用于查看 VM 部署状态的按钮

集群升级日志

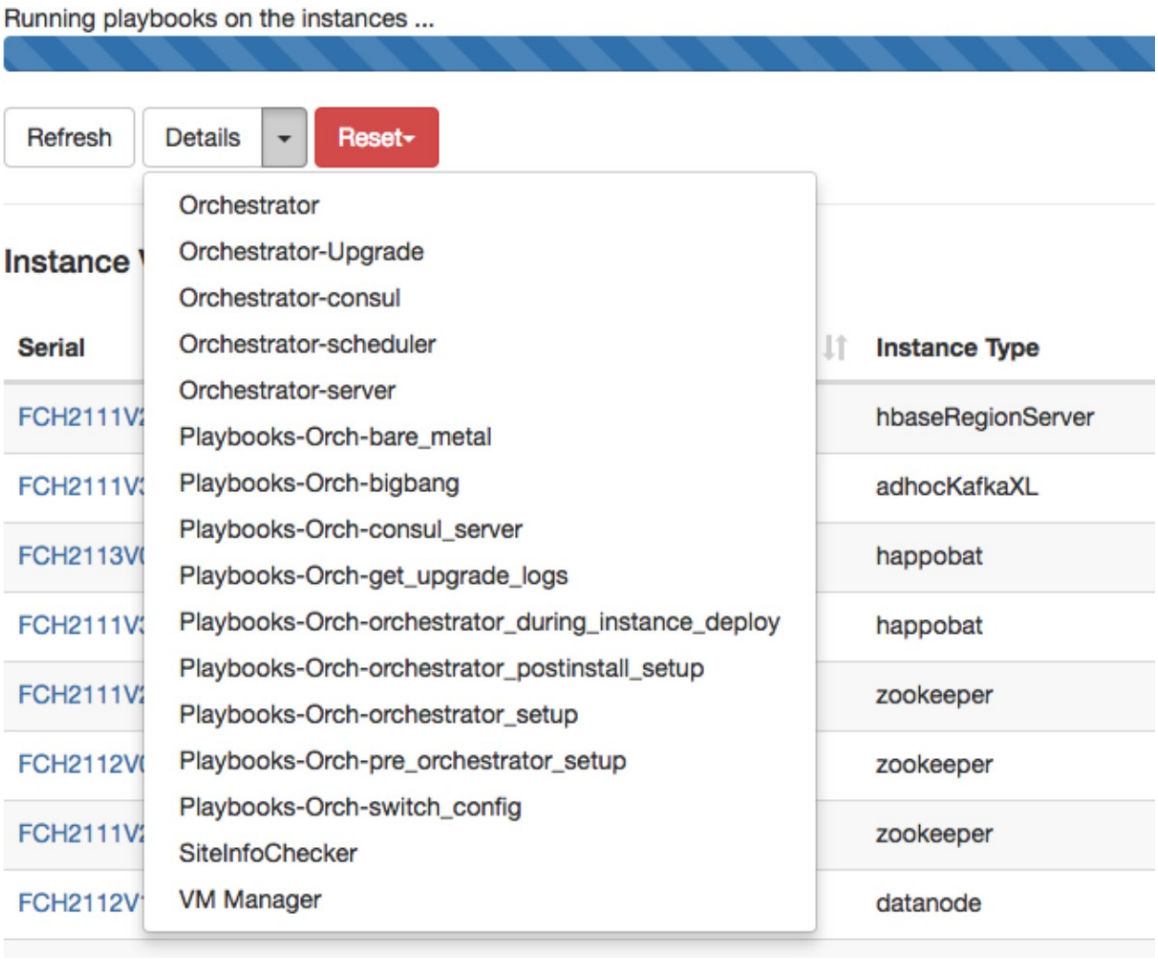
有两种类型的日志：

Procedure

步骤 1 **VM 部署日志**：点击**查看日志 (View Log)** 以查看 VM 部署日志。

步骤 2 **协调日志**：点击**详细信息 (Details)** 按钮旁边的箭头以查看协调日志。

Figure 40: 协调日志



每个链接都指向日志。

- 协调器 - 协调器日志 - 这是跟踪进度的第一个位置。任何故障都指向另一个要查看的日志。
- 协调器 - 升级 - 用于 2.3 的 NOP
- Orchestrator-consul - 在主协调器上运行的 Consul 日志。
- Orchestrator-Scheduler - 虚拟机计划程序日志 - 哪个虚拟机被放置在哪个裸机上以及计划日志。
- Orchestrator-server - 来自协调器的 HTTP 服务器日志。
- Playbooks-* - 在协调器上运行的所有 Playbook 日志。

运行升级前检查

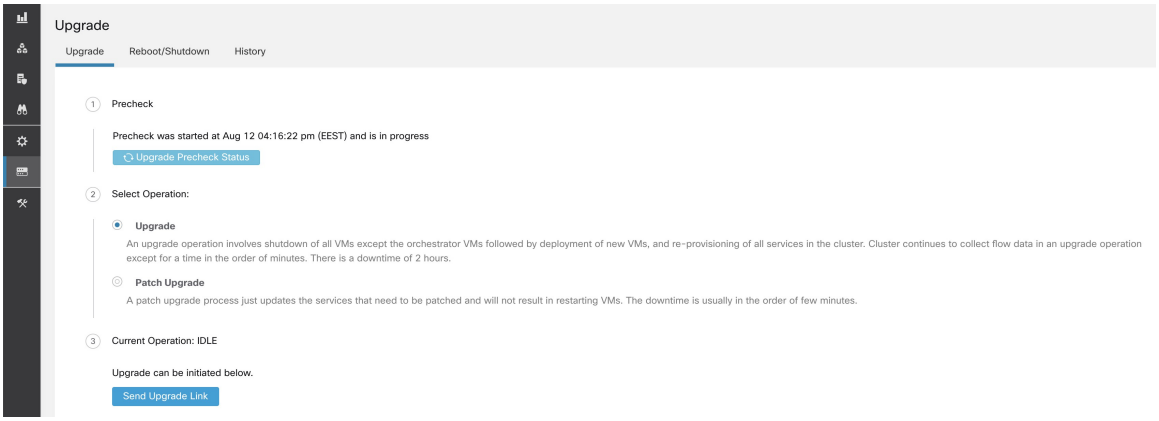
在计划升级和启动升级后，偶尔可能会出现硬件故障，或者集群还没有准备好进行升级。必须修复这些错误才能继续升级。您可以启动升级前检查，而不必等待升级窗口，这种检查可以随时运行且不限次数，但启动升级、补丁升级或重启时除外。

要运行升级前检查，请执行以下操作：

1. 在**升级 (Upgrade)** 选项卡中，点击**开始升级预检查 (Start Upgrade Precheck)**。

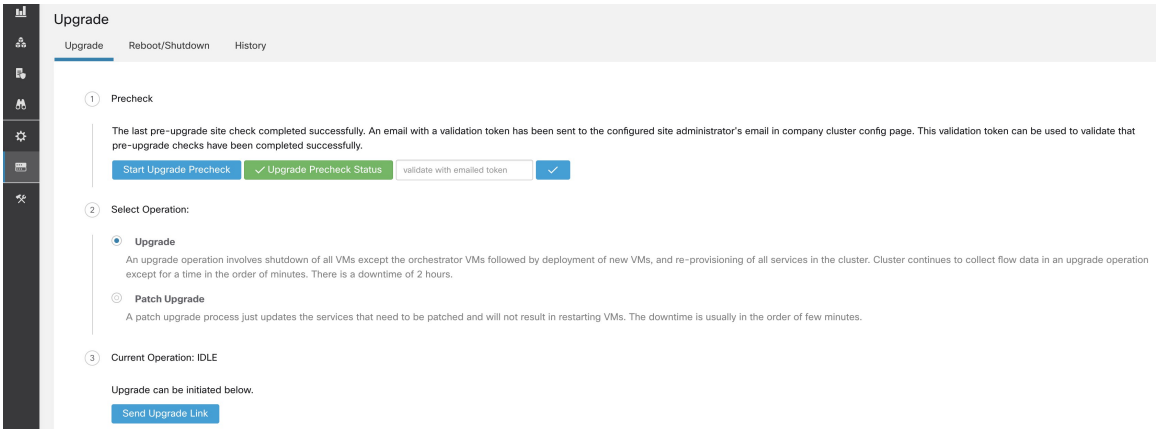
   这将启动升级前检查，并转换为运行状态。

   Figure 41: 运行升级前检查



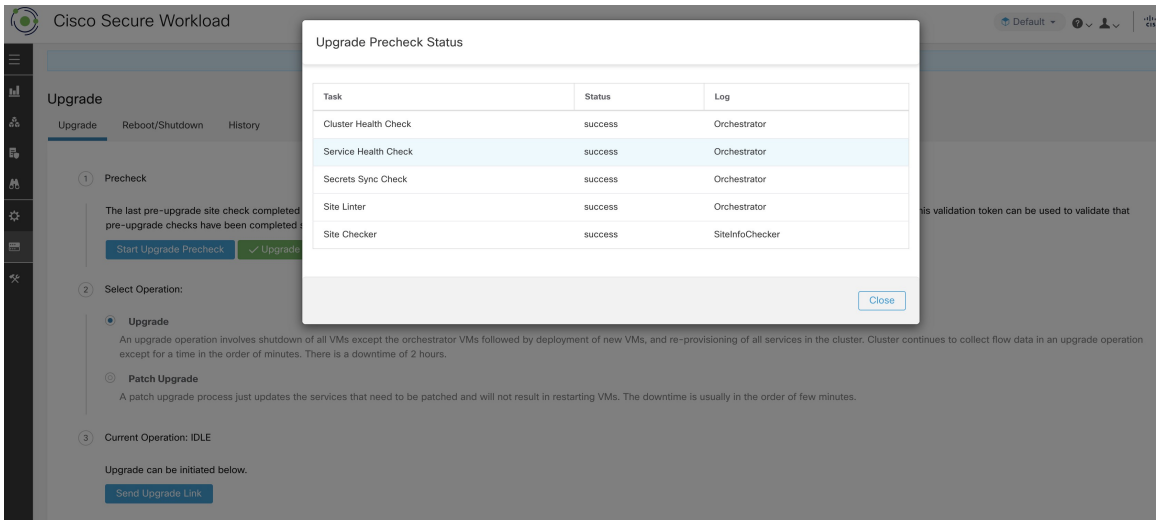
2. 在协调器运行的所有检查都通过后，一封带有令牌的邮件就会发送到注册的邮件 ID 上。输入令牌以完成升级前检查。

   Figure 42: 输入用于升级前检查的令牌



您可以验证检查的状态。如果在升级前检查过程中出现任何故障，您可以查看故障检查和相应的检查转换到故障状态。

Figure 43: 升级前检查的状态



数据备份和恢复 (DBR)

如果在集群上启用了 **DBR**，另请参阅使用数据备份和恢复进行升级。

Cisco Secure Workload 集群快照

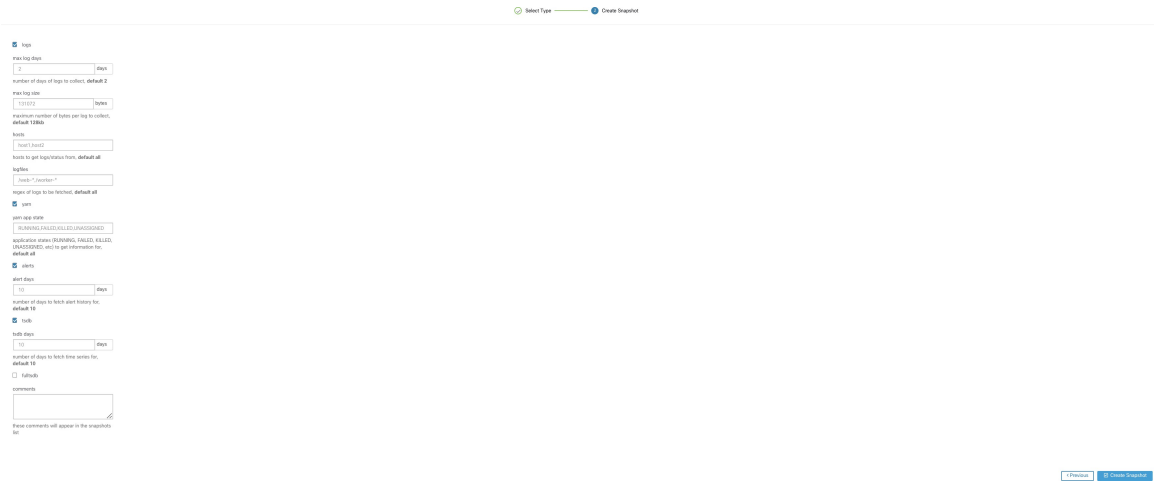
访问快照创建用户界面

具有**客户支持角色**的用户可以通过从窗口左侧的导航栏中选择**故障排除 (Troubleshoot)** > **快照 (Snapshots)** 来访问快照工具。

快照工具可用于创建经典快照或思科集成管理控制器 (CIMC) 技术支持捆绑包。点击“快照文件列表”(Create Snapshot) 页面上的创建快照按钮会加载一个页面，以选择经典快照或 CIMC 快照（技术支持捆绑包）。用于选择 CIMC 快照的选项在 Cisco Secure Workload 纯软件 (ESXi) 和 Cisco Secure Workload SaaS 上已被禁用。

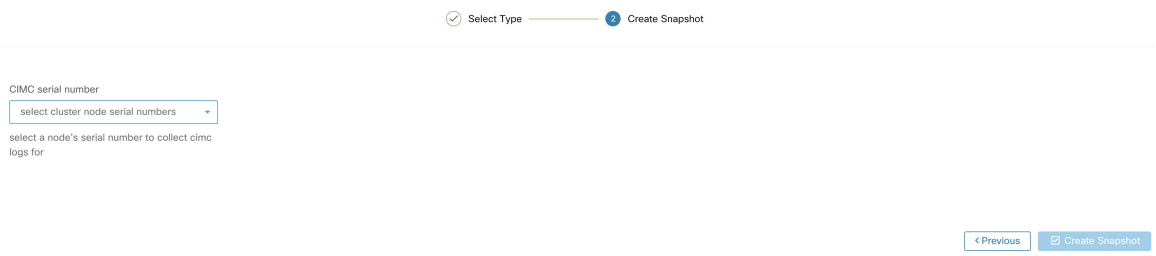
点击“经典快照”(Classic Snapshot) 按钮加载快照工具运行程序用户界面：

Figure 44: 快照工具运行程序



点击 CIMC 快照按钮会加载 CIMC 技术支持工具运行程序用户界面：

Figure 45: CIMC 技术支持运行程序



创建快照

使用默认选项选择**创建快照 (Create Snapshot)**，快照工具将收集：

- 日志
- Hadoop 或 yarn 应用和日志的状态
- 警报历史记录
- 大量 TSDB 统计信息

可以覆盖默认值并指定某些选项。

- logs 选项
  - max log days - 要收集的日志天数，默认为 2。
  - max log size - 要收集的每个日志的最大字节数，默认值为 128kb。
  - hosts - 要从中获取日志/状态的主机，默认为 all。
  - logfiles - 要获取的日志的正则表达式，默认为 all。

- yarn 选项
  - yarn app state - 要获取其信息的应用状态（RUNNING、FAILED、KILLED、UNASSIGNED 等），默认为 all。
- alerts 选项
  - alert days - 要收集的警报数据的天数。
- tsdb 选项
  - tsdb days - 要收集的 tsdb 数据的天数，增大此值可能会创建非常大的快照。
- fulltsdb 选项
  - fulltsdb - 一个 JSON 对象，可用于指定 startTime、endTime fullDumpPath、localDumpFile 和 nameFilterIncludeRegex，以限制收集哪些指标。
- comments - 可添加以说明收集快照的原因或人员。

选择创建快照后，“快照文件列表”(Snapshots file list) 页面的顶部会显示快照进度条。快照完成后，可以使用“快照文件列表”(Snapshots file list) 页面上的“下载”(Download) 按钮进行下载。一次只能收集一个快照。

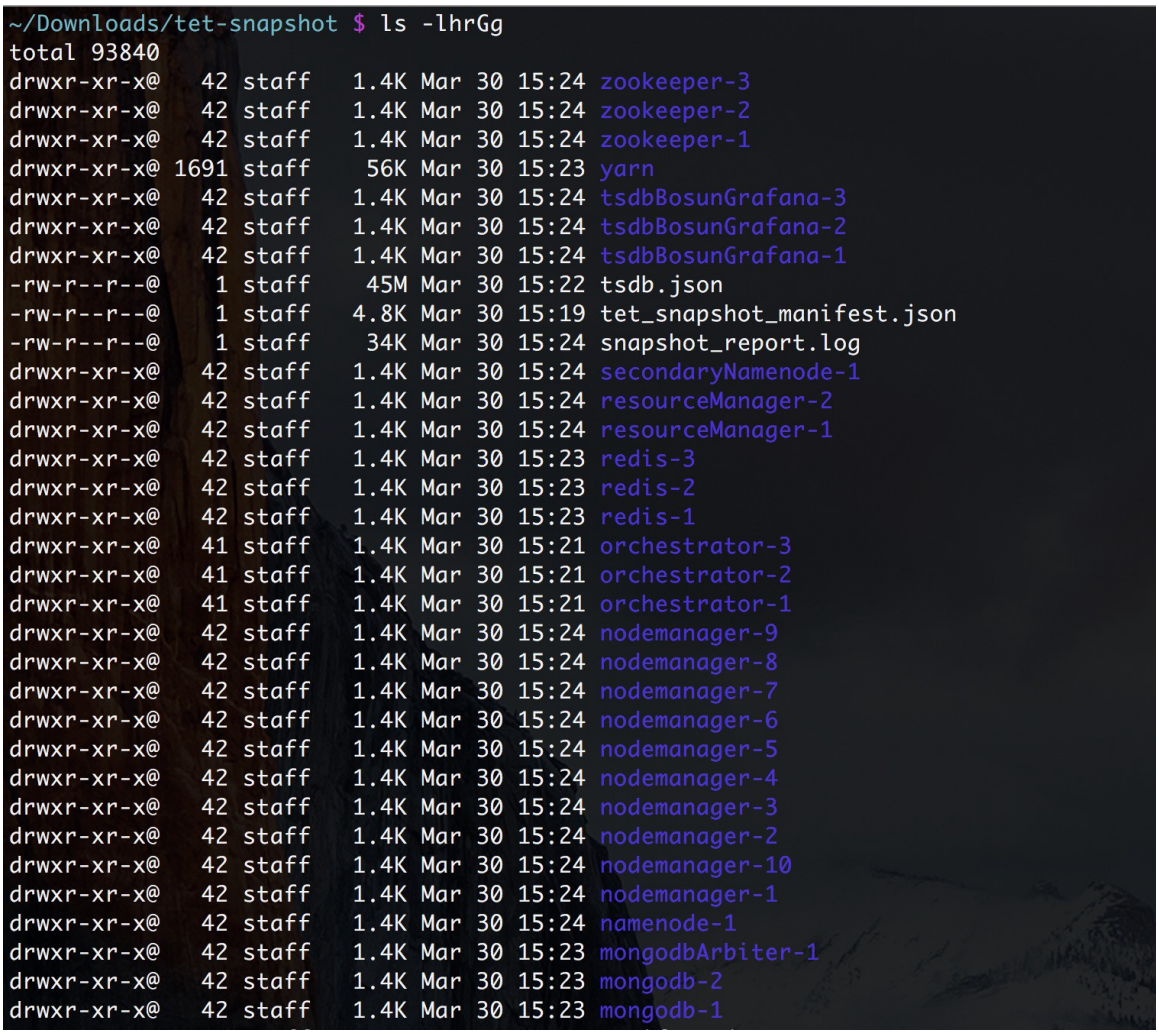
创建 CIMC 技术支持捆绑包

在CIMC快照（技术支持捆绑包）页面上，选择应为其创建CIMC技术支持捆绑包的节点的序列号，然后点击**创建快照 (Create Snapshot)** 按钮。快照文件列表页面中会显示 CIMC 技术支持软件包收集的进度条，而注释部分会显示 CIMC 技术支持软件包收集已被触发。CIMC 技术支持捆绑包收集完成后，可以从快照文件列表页面下载该文件。

使用快照

解压快照会创建一个 ./clustername_snapshot 目录，其中包含每台计算机的日志。日志会以文本文件的形式保存，其中包含来自多个计算机目录的数据。快照还会以 JSON 格式保存捕获的所有 Hadoop/TSDB 数据。

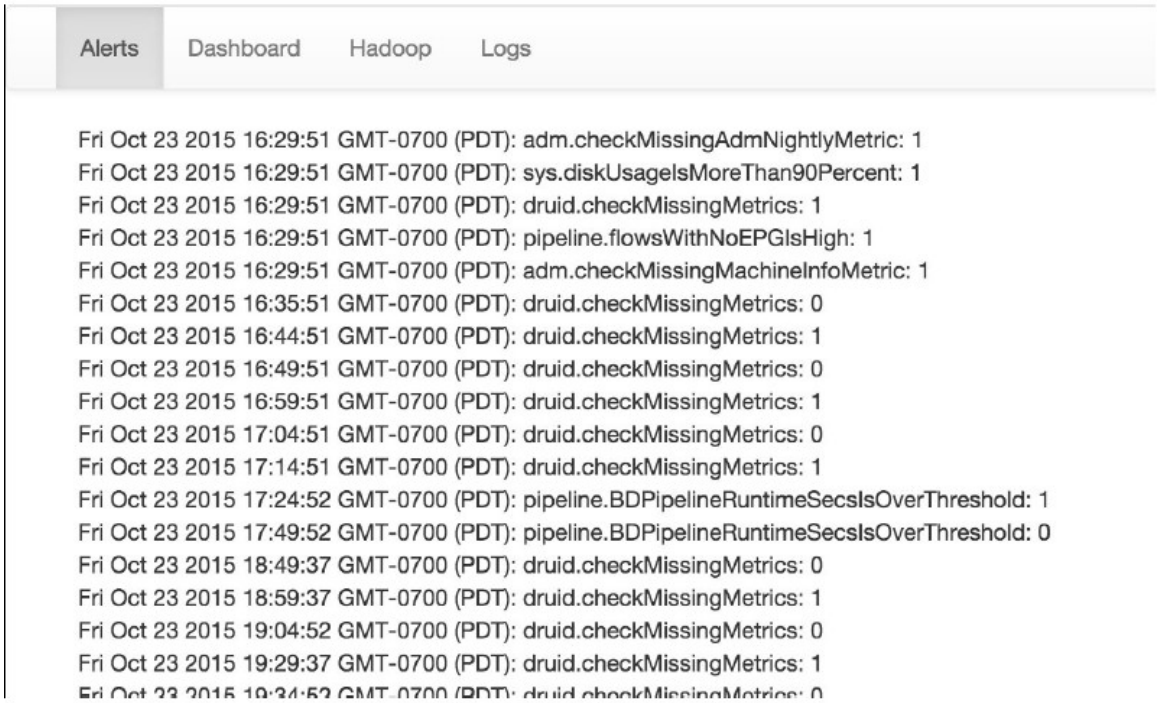
Figure 46: 使用快照



在浏览器中打开打包的 index.html 时，系统会显示以下选项卡：

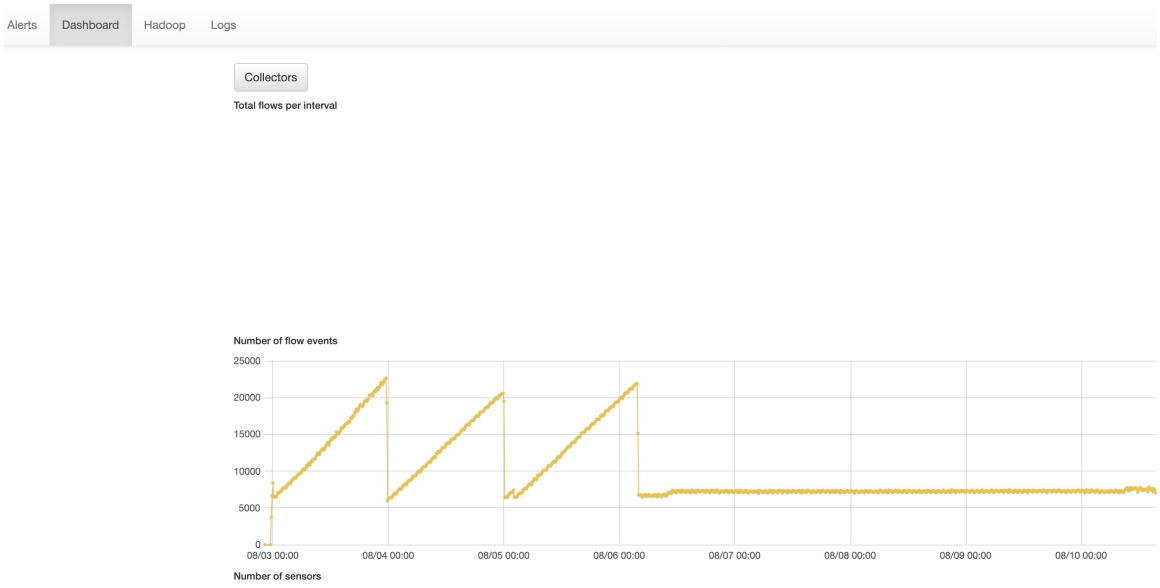
- 警报状态更改的简短列表。

Figure 47: 警报状态更改的简短列表



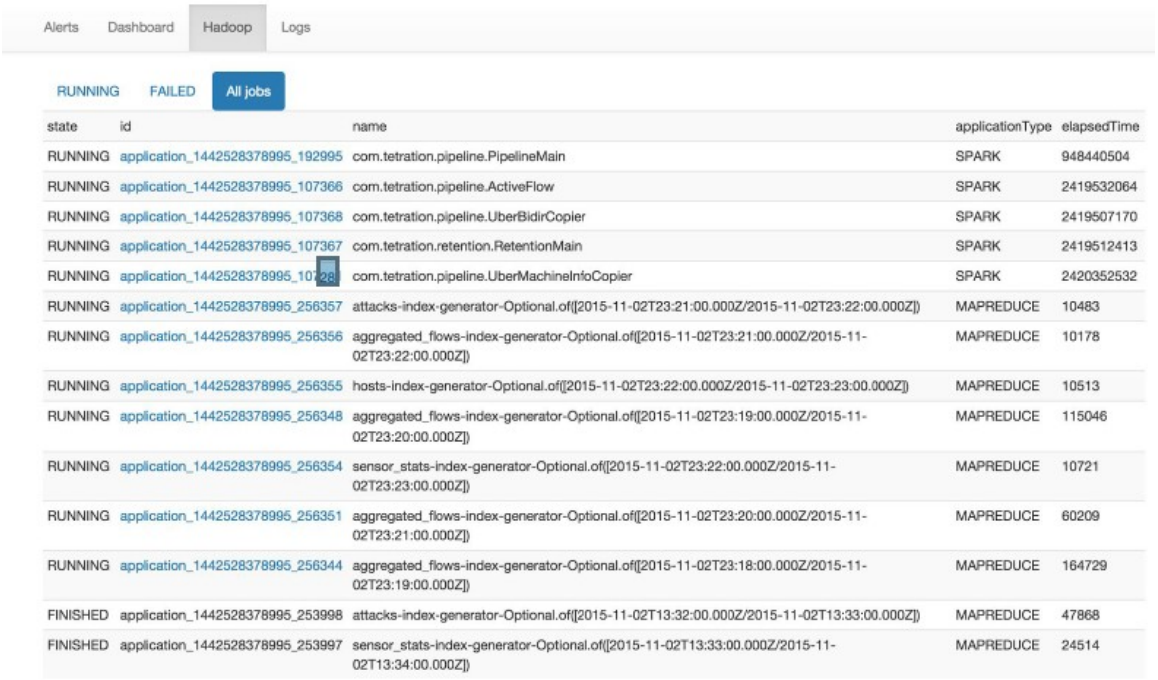
- 复制 Grafana 控制面板。

Figure 48: 复制 ***Grafana*** 控制面板



- 复制包含作业及其状态的 Hadoop 资源管理器前端。选择作业会显示该作业的日志。

Figure 49: 复制 ***Hadoop*** 资源管理器



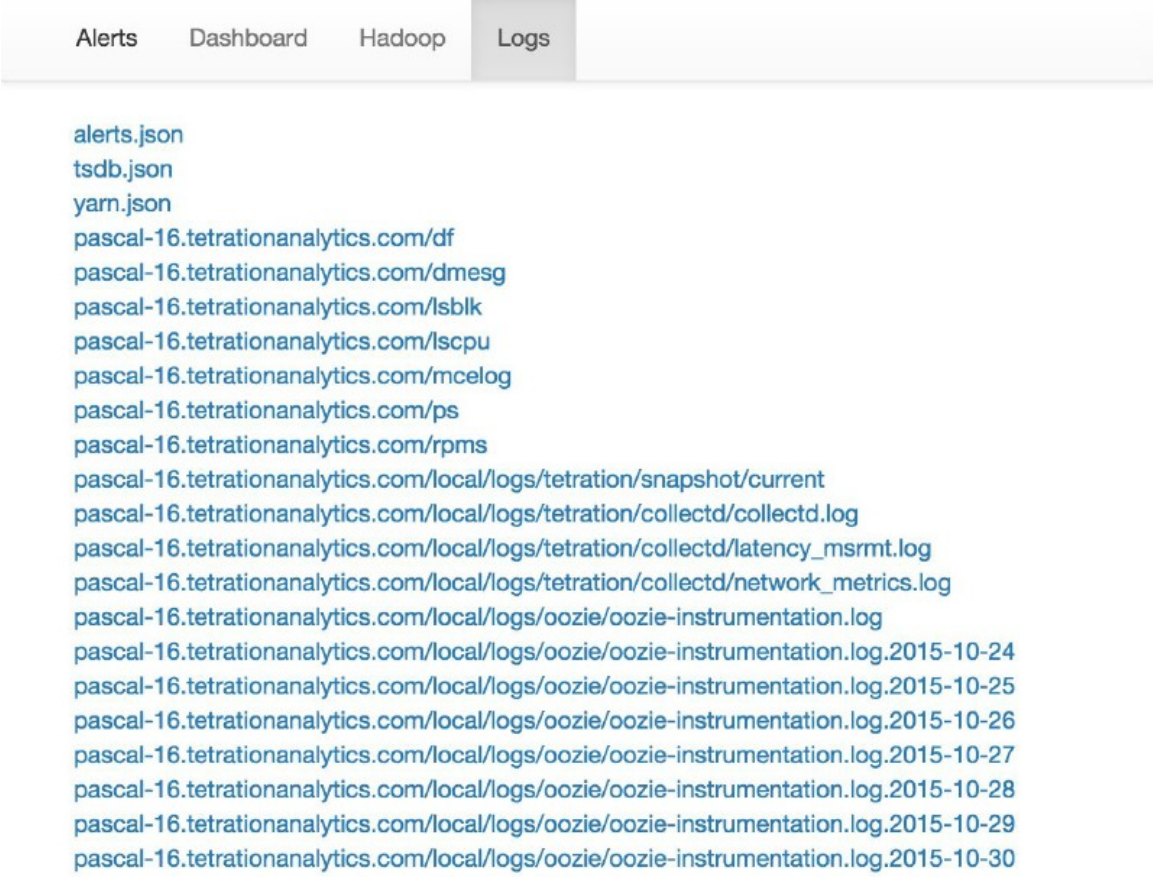
Alerts Dashboard Hadoop Logs

RUNNING FAILED All jobs

state	id	name	applicationType	elapsedTime
RUNNING	application_1442528378995_192995	com.tetration.pipeline.PipelineMain	SPARK	948440504
RUNNING	application_1442528378995_107366	com.tetration.pipeline.ActiveFlow	SPARK	2419532064
RUNNING	application_1442528378995_107368	com.tetration.pipeline.UberBidirCopier	SPARK	2419507170
RUNNING	application_1442528378995_107367	com.tetration.retention.RetentionMain	SPARK	2419512413
RUNNING	application_1442528378995_107[illegible]28	com.tetration.pipeline.UberMachineInfoCopier	SPARK	2420352532
RUNNING	application_1442528378995_256357	attacks-index-generator-Optional.of([2015-11-02T23:21:00.000Z/2015-11-02T23:22:00.000Z])	MAPREDUCE	10483
RUNNING	application_1442528378995_256356	aggregated_flows-index-generator-Optional.of([2015-11-02T23:21:00.000Z/2015-11-02T23:22:00.000Z])	MAPREDUCE	10178
RUNNING	application_1442528378995_256355	hosts-index-generator-Optional.of([2015-11-02T23:22:00.000Z/2015-11-02T23:23:00.000Z])	MAPREDUCE	10513
RUNNING	application_1442528378995_256348	aggregated_flows-index-generator-Optional.of([2015-11-02T23:19:00.000Z/2015-11-02T23:20:00.000Z])	MAPREDUCE	115046
RUNNING	application_1442528378995_256354	sensor_stats-index-generator-Optional.of([2015-11-02T23:22:00.000Z/2015-11-02T23:23:00.000Z])	MAPREDUCE	10721
RUNNING	application_1442528378995_256351	aggregated_flows-index-generator-Optional.of([2015-11-02T23:20:00.000Z/2015-11-02T23:21:00.000Z])	MAPREDUCE	60209
RUNNING	application_1442528378995_256344	aggregated_flows-index-generator-Optional.of([2015-11-02T23:18:00.000Z/2015-11-02T23:19:00.000Z])	MAPREDUCE	164729
FINISHED	application_1442528378995_253998	attacks-index-generator-Optional.of([2015-11-02T13:32:00.000Z/2015-11-02T13:33:00.000Z])	MAPREDUCE	47868
FINISHED	application_1442528378995_253997	sensor_stats-index-generator-Optional.of([2015-11-02T13:33:00.000Z/2015-11-02T13:34:00.000Z])	MAPREDUCE	24514

- 收集的所有日志的列表。

Figure 50: 收集的日志列表

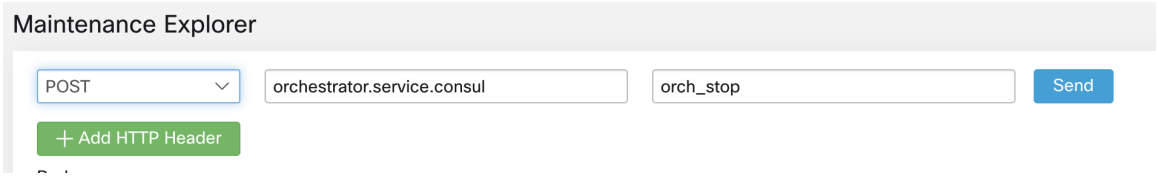


使用快照服务进行调试和维护

快照服务可用于运行服务命令，但需要具有客户支持权限。

使用探索工具（**故障排除 (Troubleshoot)** > **维护资源管理器 (Maintenance Explorer)**）您可以点击集群中的任意 URI：

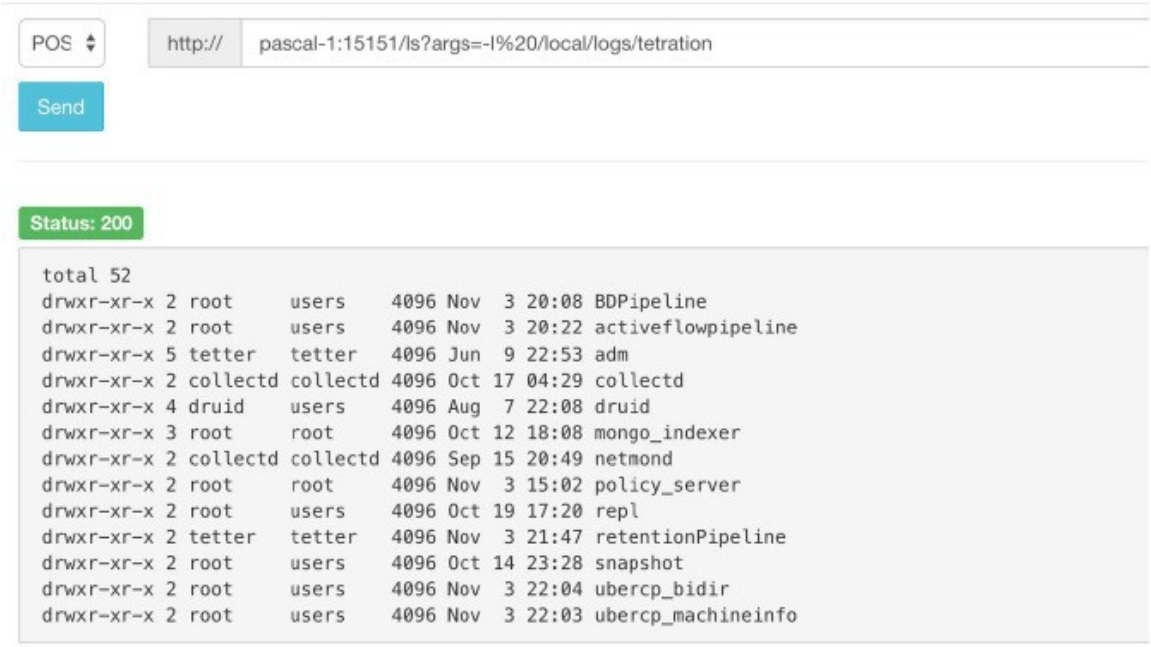
Figure 51: 用于调试和维护的快照服务



只有拥有客户支持权限的用户才能使用探索工具。

快照服务在每个节点的 15151 端口上运行。它只侦听内部网络（不暴露在外部），并为各种命令提供 POST 终端。

Figure 52: 使用快照服务进行调试和维护



必须点击的 URI 是 **POST** http://<hostname>:15151/<cmd>?args=<args>，其中 args 为空格分隔和 URI 编码。它不使用 shell 来运行命令。这样可以避免允许运行任何操作。

快照的终端针对以下对象定义：

- **快照 0.2.5**

  Is

  svstatus, svrestart - 运行 sv status、**sv restart** 示例：1.1.11.15:15151/svrestart?args=snapshot

  hadoopls 运行 hadoop fs -ls <args>

  hadoopdu - 运行 hadoop fs -du <args>

  ps 示例：1.1.11.31:15151/ps?args=eafux

  du

  ambari - 运行 ambari_service.py

  monit

  MegaCli64 (/usr/bin/MegaCli64)

  service

  hadoopfsck - 运行 hadoop -fsck

- **快照 0.2.6**

  makecurrent - 运行 make -C /local/deploy-ansible current

  netstat

- 快照 **0.2.7**（以 **uid** “**nobody**” 身份运行）

  cat

  head

  tail

  grep

  ip -6 neighbor

  ip address

  ip neighbor

还有另一个终端 POST /runsigned，它将运行由 Cisco Secure Workload签名的 shell 脚本。它对已 POST 的数据运行 gpg -d。如果可以根据签名进行验证，它就会在 shell 下运行加密文本。这意味着作为 Ansible 设置的一部分，需要在每台服务器上导入公钥，并且需要确保私钥的安全。

运行手册

具有客户支持权限的用户可以通过从窗口左侧的导航栏中选择**故障排除 (Troubleshoot)** > **维护资源管理器 (Maintenance Explorer)** 来使用运行手册。从下拉菜单中选择 **POST**。（否则，您将在运行命令时收到“找不到页面”(Page Not Found) 错误。）

使用快照 **REST** 终端重启服务：

- **druid: 1.1.11.17:15151/service?args=supervisord%20restart**

  - druid 主机的 IP 均为 0.17 至 0.24； .17、.18 是协调器，.19 是索引器，0.20-.24 是代理

- **hadoop** 管道启动器：

  1.1.11.25:15151/svrestart?args=activeflowpipeline

  1.1.11.25:15151/svrestart?args=adm

  1.1.11.25:15151/svrestart?args=batchmover_bidir

  1.1.11.25:15151/svrestart?args=batchmover_machineinfo

  1.1.11.25:15151/svrestart?args=BDPipeline

  1.1.11.25:15151/svrestart?args=mongo_indexer

  1.1.11.25:15151/svrestart?args=retentionPipeline

- 策略引擎

  1.1.11.25:15151/svrestart?args=policy_server

- **wss**

  1.1.11.47:15151/svrestart?args=wss

探索或快照终端概述

要运行任何终端，您需要从窗口左侧的导航栏中转至**故障排除 (Troubleshoot)** > **维护资源管理器 (Maintenance Explorer)** 页面。

您还可以通过在任何主机上运行 **POST** 命令（如 **<end- point>?usage=true**）来查看探索页面中的每个终端概述。

例如：**makecurrent?usage=true**

get 命令

终端	说明
bm_details	显示裸机信息
endpoints	列出主机上的所有终端
members	显示当前的 Consul 成员列表，以及他们的状态
port2cimc	• 列出端口连接到的 IP • 应**仅在协调器主机**上运行
status	显示主机上快照服务的状态
vm_info	• 显示位置的 VM 信息 • 应**仅在裸机主机**上运行 • 以 **vm_info?args=<vmname>** 格式运行终端

post 命令

***Table 18: post* 命令**

终端	说明
bm_shutdown_or_reboot	• 通过首先关闭该主机上的所有虚拟机，然后向裸机发出关闭或重启命令，正常关闭或重启该主机。您还可以使用此终端获取关闭或重启状态。 • 要获取节点的关闭或重启状态，请使用：`bm_shutdown_or_reboot? query=serial=FCH2308V0FH` • 要启动正常的裸机关机，请使用：`bm_shutdown_or_reboot? method=POST`，并将正文设置为描述主机序列号的 JSON 对象。例如：`{"serial": "FCH2308V0FH"}` • 要启动正常的裸机重启，请使用：`bm_shutdown_or_reboot? method=POST`，并将正文设置为描述主机序列号的 JSON 对象，同时包含设置为“true”的重启密钥。例如：`{"serial": "FCH2308V0FH", "reboot": true}`
cat	*cat* Unix 命令的封装程序命令
cimc_password_random	• 随机化 CIMC 密码。 • 应**仅在协调器主机**上运行
cleancmdlogs	清除 `/local/logs/tetration/snapshot/cmdlogs/snapshot_cleancmdlogs_log` 中的日志
clear_sel	• 清除系统事件日志 • 应**仅在裸机主机**上运行

终端	说明
cluster_fw_upgrade	• 这是一项**测试版**功能。 • 在整个集群中运行 UCS 固件升级。 • 成功完成此操作后，需要重启每个裸机以激活 BIOS 和其他组件固件。 • 运行方式：**cluster_fw_upgrade** • 此终端会启动并监控固件升级，并在升级阶段开始或完成时更新日志文件。 • 要获取升级状态，请使用 **cluster_fw_upgrade_status** 终端。
cluster_fw_upgrade_status	• 这是一项**测试版**功能。 • 获取完整集群 UCS 固件升级的状态。 • 以 **cluster_fw_upgrade_status** 运行
cluster_powerdown	• 关闭集群。 • 请谨慎使用，因为集群已关闭。 • 作为 `cluster_powerdown?args=-start` 运行终端。
collector_status	• 显示收集器的状态。 • 应仅在收集器主机上运行。
consul_kv_export	• 以 JSON 格式显示来自 consul 的 k-v 对 • 应仅在协调器主机上运行。
consul_kv_recurse	• 以表格格式显示来自 Consul 的 k-v 对 • 应仅在协调器主机上运行。
df	*df* Unix 命令的封装程序命令
dig	*dig* Unix 命令的封装程序命令
dmesg	*dmesg* Unix 命令的封装程序命令
dmidecode	*dmidecode* Unix 命令的封装程序命令
druid_coordinator_v1	显示 druid 统计信息。

终端	说明
du	*du* Unix 命令的封装程序命令
dusorted	*dusorted* Unix 命令的封装程序命令
externalize_change_tunnel	• 更改将被用于通过隧道传送 CIMC UI 的收集器 IP • 运行方式：**externalize_change_tunnel?method=POST** • 在正文中传递 **{“collector_ip”：“<IP>”}** • 应**仅在协调器主机**上运行
externalize_mgmt	• 显示每个服务器的外部化 CIMC UI 的状态 • 显示用于外部化的剩余地址和时间 • 应**仅在协调器主机**上运行
externalize_mgmt_read_only_password	• 更改交换机和 CIMC UI 的只读密码 (ta_guest) • 仅当更改被外部化时。 • 运行方式：**externalize_mgmt_read_only_password?method=POST** • 传递正文中的 **{“password”：“<password>”}** • 应**仅在协调器主机**上运行
fsck	• *fsck* Unix 命令的封装程序命令 • 应**仅在裸机主机**上运行
get_cimc_techsupport	• 输入裸机的内部 IP 地址。 • 检索 CIMC 技术支持捆绑包。 • 完成后，即可从 UI 中的快照页面进行下载。 • 这可以从集群上的任何主机运行，并且需要裸机内部 IP 地址作为参数。 • 示例：**get_cimc_techsupport?args=1.1.0.9**

终端	说明
syslog_endpoints	• 控制一个或多个 UCS 服务器的系统日志配置。 • 运行带有 *-h* 的命令可获取参数的完整列表。
grep	*grep* Unix 命令的封装程序命令
hadoopbalancer	• 在所有节点之间均匀分布 HDFS 数据 • 必须在**具有 HDFS 的主机**上运行。例如，启动程序主机
hadoopdu	• 打印 hdfs 的目录利用率 • 应在**具有 HDFS 的主机**上运行。例如，启动程序主机
hadoopfsck	• 运行 hadoop fsck 并报告所提供的 HDFS 文件系统的状态 • 它还将“-delete”作为参数以清除损坏或缺失的块 • 在删除之前，请确保所有 DataNodes 都已启动，否则我们可能会丢失数据 • 应仅在启动器主机上运行。 • 报告运行状态为：`hadoopfsck?args=/raw` • 要删除损坏的文件，请运行以下命令：`hadoopfsck?args=/raw -delete`
hadoopls	• 列出 Hadoop 文件系统 • 应在**具有 hdfs 的主机**（例如启动器主机）上运行。

终端	说明
hbasehbck	• 检查一致性和表完整性问题并修复损坏的 HBase • 应**仅在 HBase 主机**上运行 • 要识别不一致，请运行以下命令：`hbasehbck?args=-details` • 要修复损坏的 HBase，请运行以下命令：`hbasehbck?args=-repair` • 写入 /local/logs/tetration/snapshot/crdlogs/snapshot_hbasehbck_log.txt 中的输出 • 谨慎维修
hdfs_safe_state_recover	• 从安全状态删除 HDFS • 如果 HDFS 因容量已满而处于 READ_ONLY_STATE 且空间已被清空，则为必填 • 应**仅在启动器主机**上运行 • 运行方式：**hadoopfs-rm‘{{ hdfs_safe_state_marker_location }}/HDFS_READ_ONLY’**
initctl	*initctl* Unix 命令的封装程序命令
head	*head* Unix 命令的封装程序命令
internal_haproxy_status	• 打印内部 haproxy 状态和统计信息 • 应**仅在协调器主机**上运行
ip	*ip* Unix 命令的封装程序命令
ipmifru	• 打印现场可更换单元 (FRU) 信息 • 应**仅在裸机主机**上运行
ipmilan	• 打印 LAN 配置 • 应**仅在裸机主机**上运行

终端	说明
ipmisel	• 打印系统事件日志 (SEL) 条目 • 应**仅在裸机主机**上运行
ipmisensorlist	• 打印 IPMI 传感器信息 • 应**仅在裸机主机**上运行
jstack	打印给定 Java 进程或核心文件的 Java 线程的 Java 堆栈跟踪
ls	*ls* Unix 命令的封装程序命令
lshw	*lshw* Unix 命令的封装程序命令
lsof	*lsof* Unix 命令的封装程序命令
lvdisplay	*lvdisplay* Unix 命令的封装程序命令
lvs	*lvs* Unix 命令的封装程序命令
lvscan	*lvscan* Unix 命令的封装程序命令
makecurrent	• 将处理标记的管道重置或快进至当前时间戳 • 应**仅在协调器节点**上运行 • 作为 **makecurrent?args=－start** 运行终端
mongo_rs_status	• 显示 mongo 复制状态 • 应在 **mongodb 或 enforcementpolicystore 主机**上运行
mongo_stats	• 显示 mongo 统计信息 • 应在 **mongodb 或 enforcementpolicystore 主机**上运行
mongodump	• 从数据库转储集合 • 应在 **mongodb 或 enforcementpolicystore 主机**上运行 • 作为 mongodump?args=<collection>[－db DB] 运行
monit	*monit* Unix 命令的封装程序命令

终端	说明
namenode_jmx	显示主名称节点 jmx 指标
ndisc6	*ndisc6* Unix 命令的封装程序命令
netstat	*netstat* Unix 命令的封装程序命令
ntpq	*ntpq* Unix 命令的封装程序命令
orch_reset	• 将协调器状态重置为 IDLE • 在调试或下线失败后运行 • 应仅在 **orchestrator.service.consul** 主机上运行 • **请勿在未咨询客户支持的情况下使用此命令**
orch_stop	• 停止主协调器并触发切换 • 应仅在 **orchestrator.service.consul** 主机上运行 • **请谨慎使用**
ping	*ping* Unix 命令的封装程序命令
ping6	*ping6* Unix 命令的封装程序命令
ps	*ps* Unix 命令的封装程序命令
pv	*pv* Unix 命令的封装程序命令
pvs	*pvs* Unix 命令的封装程序命令
pvdisplay	*pvdisplay* Unix 命令的封装程序命令
rdisc6	*rdisc6* Unix 命令的封装程序命令
rebootnode	• 重启节点 • 应仅在裸机主机上运行
recover_rpmdb	• 恢复节点上损坏的 RPMDB • 可以在裸机或 VM 上运行

终端	说明
recoverhbase	• 恢复 HBase 和 TSDB 服务 • 应**仅在协调器主机**上运行 • 应在 HDFS 运行状况正常时运行
recovervm	• 尝试通过 stop/fsck/start 恢复 VM • 应**仅在协调器主机**上运行 • 作为 **recovervm?args=<vmname>** 运行终端
restartservices	• 停止和启动所有非 UI 服务 • 应**仅在 orchestrator.service.consul 主机**上运行 • **请谨慎使用** • 作为 **restartservices?args= – start** 运行终端
runsigned	• 运行思科提供的签名脚本 • 遵循脚本准则中提供的步骤
service	*service* Unix 命令的封装程序命令
smartctl	• 运行 smartctl 可执行文件 • 应仅在裸机节点上运行
storcli	*storcli* Unix 命令的封装程序命令
sudocat	仅适用于 /var/log 或 /local/logs 的 *cat* 命令的封装程序
sudogrep	仅在 /var/log 或 /local/logs 下工作的 *grep* 命令的封装程序
sudohead	仅在 /var/log 或 /local/logs 下工作的“head”命令的封装程序
sudols	仅在 /var/log 或 /local/logs 下工作的“ls”命令的封装程序
sudotail	仅在 /var/log 或 /local/logs 下工作的“tail”命令的封装程序

终端	说明
sudozgrep	仅在 /var/log 或 /local/logs 下工作的“zgrep”命令的封装程序
sudozcat	仅在 /var/log 或 /local/logs 下工作的“zcat”命令的封装程序
svrestart	重新启动输入的服务。以 `svrestart?args=<servicename>` 格式来运行命令
svstatus	打印输入服务的状态，以 `svstatus?args=<servicename>` 运行
switchinfo	获取有关集群交换机的信息。
switch_namenode	• 从主节点或辅助节点手动确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移名称节点 • 应仅在 **orchestrator.service.consul** 主机上运行 • 在重新启用或下线名称节点主机时运行 • 作为 **switch_namenode?args=--start** 运行终端
switch_secondarynamenode	• 将 secondarynamenode 从辅助节点手动故障转移到主节点 • 应仅在 **orchestrator.service.consul** 主机上运行 • 在重新启用或下线名称节点主机时运行 • 作为 **switch_secondarynamenode?args=--start** 运行终端
switch_yarn	• 从主资源管理器或辅助资源管理器手动进行故障转移，反之亦然 • 应仅在 **orchestrator.service.consul** 主机上运行 • 在资源管理器主机下线或下线时运行 • 作为 **switch_yarn?args=－start** 运行终端
tail	*tail* Unix 命令的封装程序命令

终端	说明
toggle_chassis_locator	• 在节点序列号指定的物理裸机上切换机箱定位器。 • 从任何节点运行：**toggle_chassis_locator?method=POST** • 将正文设置为描述主机序列号的 JSON 对象（一次仅支持一个序列号），例如：**{“serials”: [“FCH2308V0FH”]}**
tnp_agent_logs	• 创建包含注册为外部协调器的负载均衡器代理提供的所有日志文件的快照 • 应在启动器主机 hosts 上运行
tnp_datastream	• 使用注册为外部协调器的负载均衡器策略执行代理使用的策略流数据创建快照 • 应在协调器主机上运行 • 要下载策略状态流数据，请作为 **tnp_datastream?args=－ds_type datasink** 运行终端
ui_haproxy_status	打印外部 haproxy 的 haproxy 统计信息和状态
uptime	*uptime* Unix 命令的封装程序命令
userapps_kill	• 终止所有正在运行的用户应用 • 应**仅在启动器主机**上运行
vgdisplay	*vgdisplay* Unix 命令的封装程序命令
vgs	*vgs* Unix 命令的封装程序命令
vmfs	• 列出 VM 上的文件系统 • 应**仅在裸机主机**上运行 • 以 **vmfs?args=<vmname>** 格式运行终端
vminfo	• 打印 VM 信息 • 应**仅在裸机主机**上运行 • 以 **vminfo?args=<vmname>** 格式运行终端

终端	说明
vmlist	• 裸机上所有 VM 的列表 • 应**仅在裸机主机**上运行 • 以 **vmlist?args=<vmname>** 格式运行终端
vmreboot	• 重启 VM • 应**仅在裸机主机**上运行 • 以 **vmreboot?args=<vmname>** 格式运行终端
vmshutdown	• 正常关闭 VM • 应**仅在裸机主机**上运行 • 以 **vmshutdown?args=<vmname>** 格式运行终端
vmstart	• 启动 VM • 应**仅在裸机主机**上运行 • 以 **vmstart?args=<vmname>** 格式运行终端
vmstop	• 强制关闭 VM • 应**仅在裸机主机**上运行 • 以 **vmstop?args=<vmname>** 格式运行终端
yarnkill	• 终止正在运行的 Yarn 应用 • 应**仅在启动器主机**上运行 • 以 **yarnkill?args=<application id>** 格式运行终端 • 要终止所有应用，请以 **yarnkill?args=ALL** 运行
yarnlogs	• 转储最后 500 MB 的 yarn 应用日志 • 应**仅在启动器主机**上运行 • 以 **yarnlogs?args=<application id> <job user>** 格式运行终端
zcat	*zcat* Unix 命令的封装程序命令

终端	说明
zgrep	*zgrep* Unix 命令的封装程序命令

服务器维护

服务器维护包括更换任何有故障的服务器组件，如硬盘、内存或更换服务器。

Note 如果集群上有多个服务器需要维护，则一次只对它们中的一个服务器进行维护。同时下线多个服务器可能会导致数据丢失。

要执行服务器维护中涉及的所有步骤，请从导航窗格中选择**故障排除 (Troubleshoot)** > **集群状态 (Cluster Status)**。所有用户都可以访问它，但操作只能由**客户支持**用户来执行。它显示思科 Cisco Secure Workload 机架中所有物理服务器的状态。

Figure 53: 服务器维护

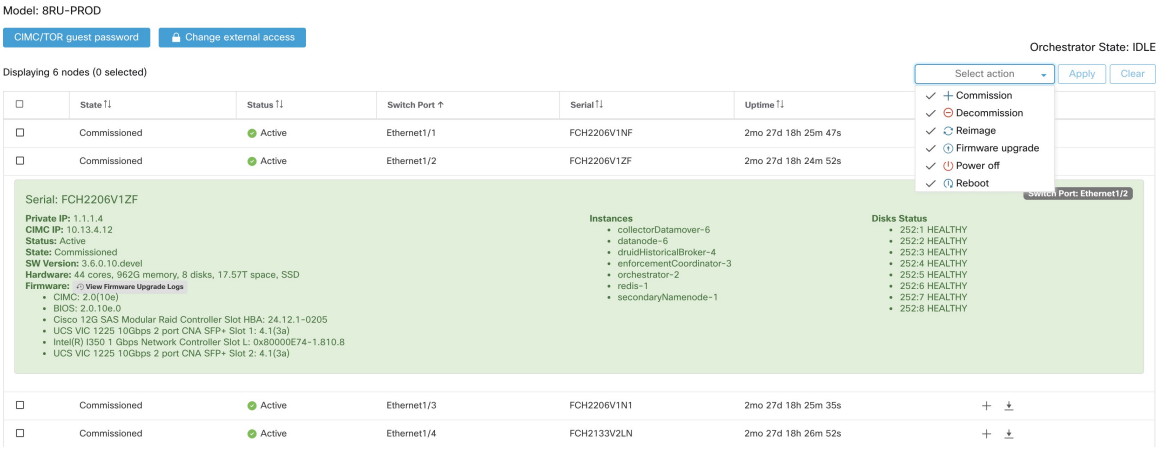
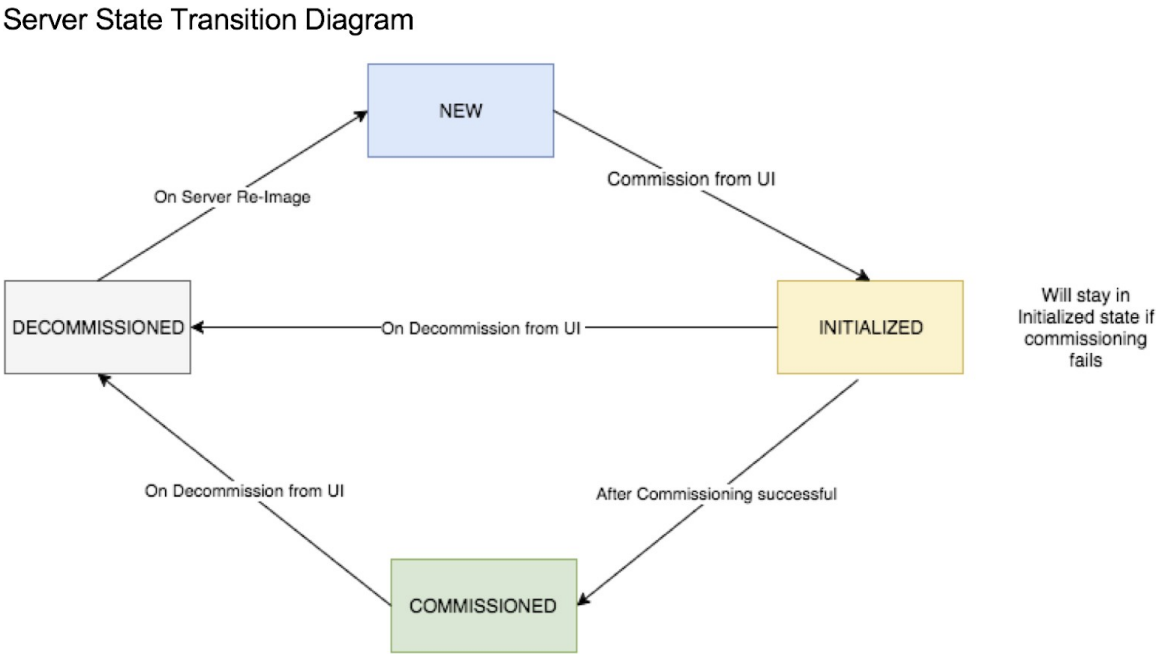


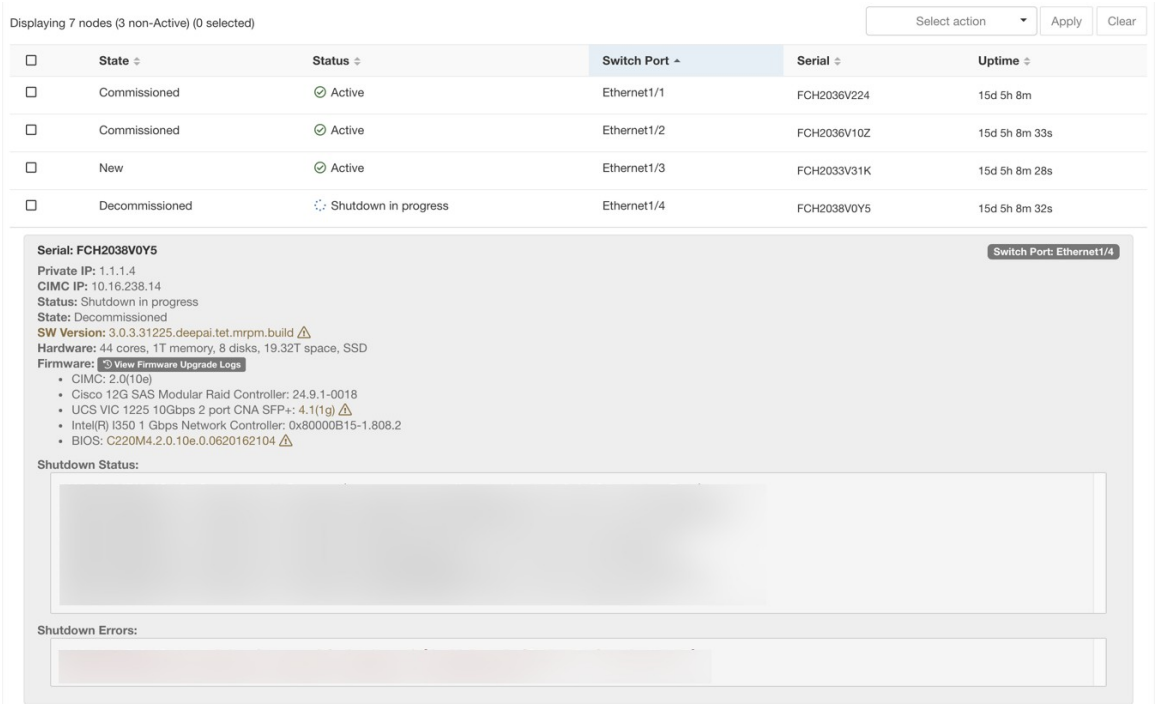
Figure 54: 服务器状态转换图



服务器或组件更换涉及的步骤

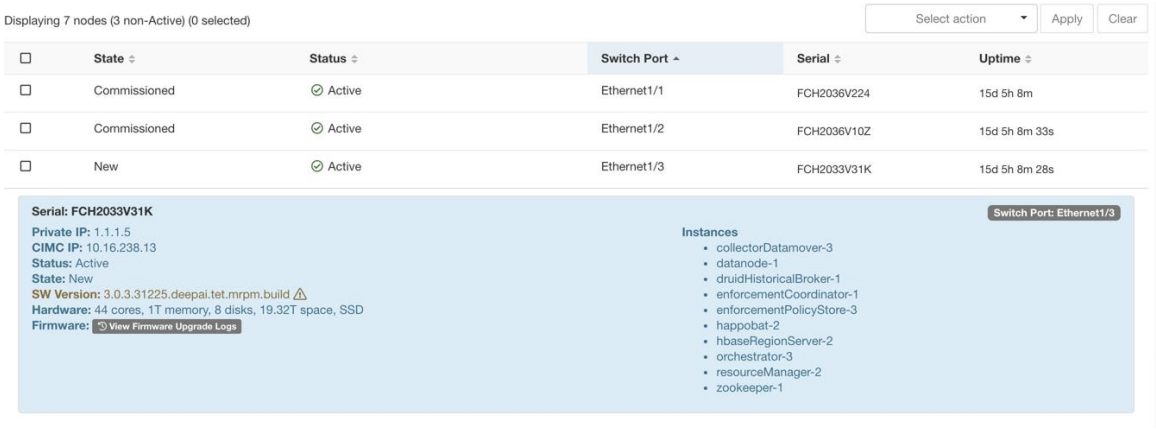
- **确定需要维护的服务器**：这可以使用集群状态 *(Cluster Status)* 页面中的服务器序列号或服务器连接到的交换机端口来完成。记下要替换的服务器的 CIMC IP。它将显示在集群状态 *(Cluster Status)* 页面上的服务器框中
- **检查特殊 VM 的操作**：从服务器框中找出服务器上存在的 VM 或实例，然后检查是否必须对这些 VM 执行任何特殊操作。下一部分列出了在服务器维护期间适用于 VM 的操作。
- **下线服务器**：执行任何下线前操作时，请使用**集群状态 (Cluster Status)** 页面来下线服务器。即使服务器发生故障并在页面上显示为非活动，您仍然可以执行所有服务器维护步骤。即使服务器已关闭，也可以执行下线步骤。

Figure 55: 下线服务器



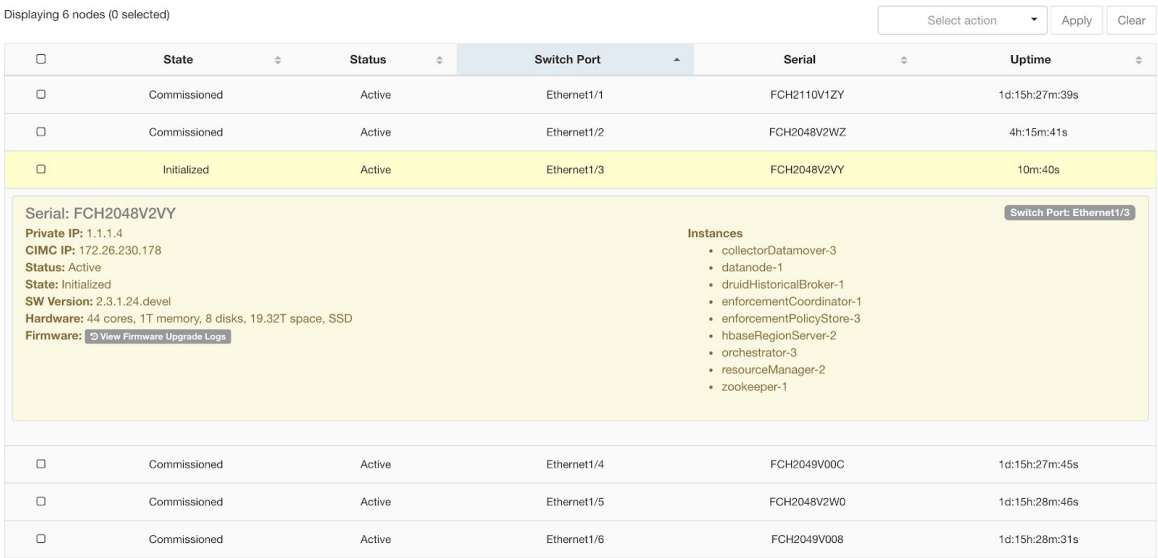
1. **执行服务器维护**：在节点在**集群状态 (Cluster Status)**页面上标记为已下线 *(Decommissioned)* 后，对虚拟机执行任何下线后特殊操作。现在就可以更换任何组件或服务器。如果更换了整个服务器，则应将新服务器的 CIMC IP 更改为与被更换服务器的 CIMC IP 相同。**集群状态 (Cluster Status)** 页面上提供了每台服务器的 CIMC IP
2. **更换组件后重新映像**：在更换组件后使用**集群状态 (Cluster Status)** 页面重新映像服务器。重新映像大约需要 30 分钟，并且需要对服务器进行 CIMC 访问。重新映像完成后，服务器将标记为新 *(NEW)*。
3. **更换整个服务器**：如果更换整个服务器，则服务器将在**集群状态 (Cluster Status)** 页面上显示为新 *(NEW)* 状态。服务器的 s/w 版本可在同一页面上查看。如果软件版本与集群版本不同，则要重新映像服务器。

Figure 56: 更换服务器



4. **调试服务器：**将服务器标记为新 *(NEW)* 后，我们可以从**集群状态 (Cluster Status)** 页面启动节点调试。此步骤会在服务器上调配虚拟机。调试服务器大约需要 45 分钟。在完成后，服务器将标记为已调试 *(Commissioned)*。

Figure 57: 调试服务器

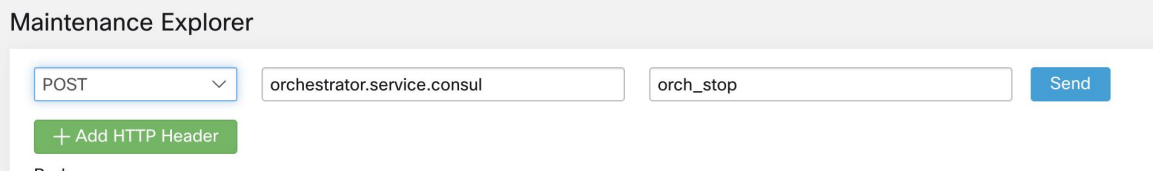


服务器维护期间虚拟机的操作

某些 VM 需要在服务器维护过程中执行一些特殊操作。这些操作可以是下线前、下线后或启用后。

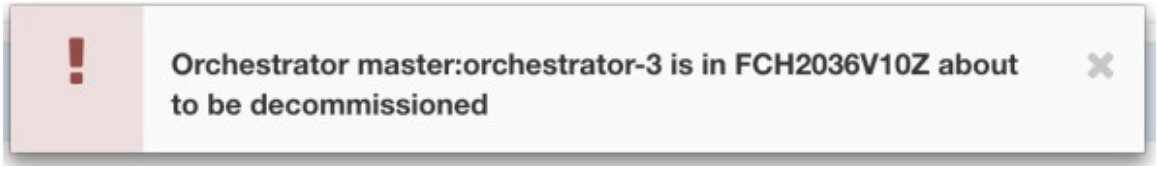
- **主协调器：**这是一项下线前操作。如果正在进行维护的服务器上有主协调器，则在执行下线之前，请从探索页面向 orchestrator.service.consul 发送 *orch_stop* 命令。这会切换主协调器。

Figure 58: 维护资源管理器



如果您尝试下线具有主协调器的服务器，则会显示以下错误。

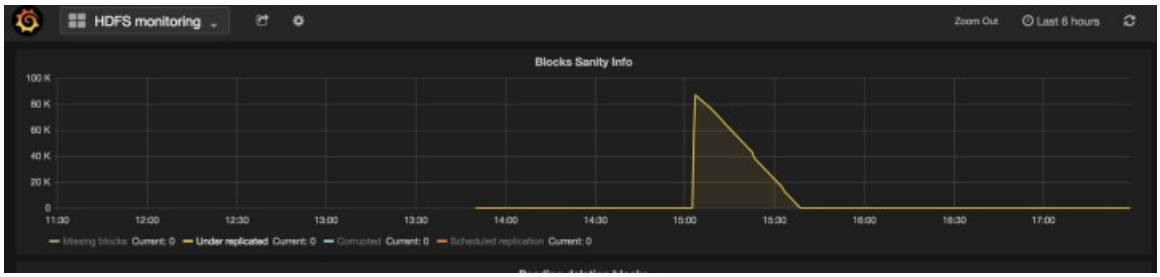
Figure 59: 下线服务器并显示主协调器错误



要确定主协调器，请在任何主机上运行探索命令 `primaryorchestrator`。

- **名称节点**：如果正在进行维护的服务器上有 namenode 虚拟机，则在下线后，从探索页面 POST orchestrator.service.consul 上的 *switch_namenode*，然后在调试后在 orchestrator.service.consul 上 POST *switch_namenode*。这是下线和启用后的操作。
- **辅助名称节点**：如果正在进行维护的服务器上有 secondarynamenode 虚拟机，则在下线后从探索页面 POST *switch_secondarynamenode* 上的 switch_secondarynamenode，然后在调试后在 orchestrator.service.consul 上 POST *switch_secondarynamenode* 。这是下线和启用后的操作。
- **主资源管理器**：如果正在进行维护的服务器上具有主资源管理器，则从探索页面在 orchestrator.service.consul 上发布 *switch_yarn*。这是下线和启用后的操作。
- **数据节点**：集群一次仅允许一个数据节点故障。如果具有数据节点虚拟机的多台服务器需要维修，则一次只对它们执行服务器维护。每次服务器维护后，等待 Monitoring | hawkeye | hdfs-monitoring | Block Sanity Info、Missing blocks 和 Under replicated counts 下的图表为 0。

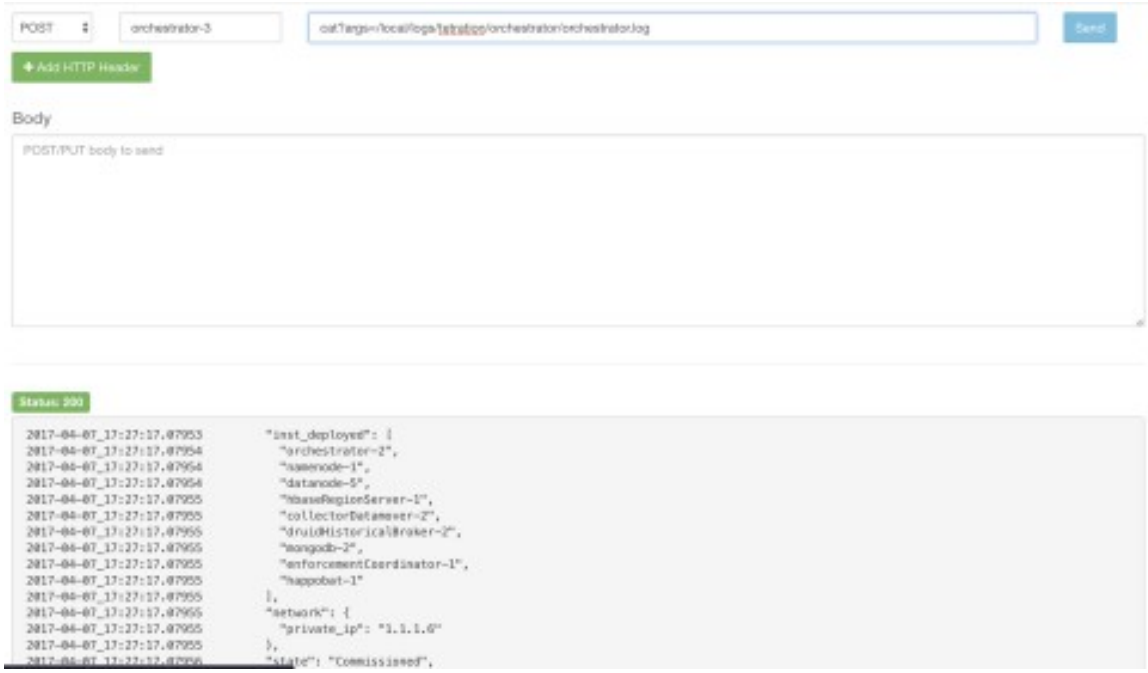
Figure 60: 服务器维护：数据节点



对服务器维护进行故障排除

- **日志**：所有服务器维护日志都是协调器日志的一部分。位置为 orchestrator.service.consul 上的 `/local/logs/tetration/orchestrator/orchestrator.log`。

Figure 61: 服务器维护日志



- 下线
  - 此步骤会删除服务器上的虚拟机或实例。
  - 然后，它会删除后端 Consul 表中这些实例的条目。
  - 此步骤大约需要 5 分钟。
  - 完成此步骤后，服务器将标记为已下线 *(Decommissioned)*。

Note 下线并不意味着服务器已关闭。下线只会删除服务器上的 Cisco Secure Workload 内容。

  - 如果服务器已关闭，它将被标记为**非活动**状态。我们仍然可以从集群状态页面在此服务器上运行下线。但由于服务器已关闭，因此虚拟机的删除步骤不会运行。确保此服务器不会重新加入处于下线状态的集群。必须重新映像并重新添加到集群。

- 重新映像
  - 此步骤将在服务器上安装 Cisco Secure Workload 基本操作系统或虚拟机监控程序操作系统。
  - 它还会格式化硬盘驱动器，并在服务器上安装几个 Cisco Secure Workload 库。
  - 重新映像会运行名为 **mjoltir** 的脚本来启动服务器映像。mjolnir 运行大约需要 5 分钟，然后实际映像开始。映像大约需要 30 分钟。映像过程中的日志只能在正在重新成像的服务器控

制台上看到。用户可以使用 ta_dev 密钥来检查有关重新映像的其他信息，例如 pxe 启动期间的 /var/log/Nginx 日志，/var/log/messages 可检查 DHCP IP 和 pxe 启动配置。

- 重新映像需要使用源自协调器的 CIMC 连接。检查 CIMC 连接性的最简单方法是使用探索页面并从 orchestrator.service.consul 发送 ping?args=<cimc ip>。**请记住**在更换服务器时更改 CIMC IP，并将 CIMC 密码设置为默认密码
- 此外，在部署集群时，应在站点信息中设置 cimc 网络，以便交换机配置正确的路由。如果集群 CIMC 连接设置不正确，您将在协调器日志中看到以下结果。

- **调试**
  - 在服务器上调试虚拟机的计划，并在虚拟机中运行 Playbook 以安装 Cisco Secure Workload 软件。
  - 调试大约需要 45 分钟才能完成。
  - 工作流程与部署或升级类似。
  - 日志会指明调试期间的任何故障。
  - 集群状态页面上的服务器将在调试期间初始化，只有在完成步骤后才会标记为已调试。

裸机排除：bmexclude

如果在关机后重启集群时检测到硬件故障，当前集群会陷入一种状态，我们既无法运行重启工作流来稳定服务，也无法运行调试工作流，因为停机服务会导致调试失败。在这种情况下，该功能可允许用户在硬件损坏的情况下重启（升级），然后对故障裸机执行常规的 RMA 流程。

用户应使用 POST 来探索终端，并将裸机的序列排除在外：

1. 操作：POST
2. 主机：orchestrator.service.consul
3. 终端：exclude_bms?method=POST
4. 正文：{“baremetal”: [“BMSERIAL”]}

协调器会执行一些检查，以确定排除是否可行。在这种情况下，它会设置几个控制键，并返回一条成功信息，指明下一次重启/升级工作流程中将排除哪些裸机和虚拟机。如果裸机包括某些虚拟机，但无法按下文“限制”部分所述将其排除，探索终端将会回复一条消息，说明无法排除的原因。在探索终端上成功执行 POST 后，用户可以通过主 GUI 启动重启/升级，并照常继续重启。在升级结束时，我们会删除排除 bm 列表。如果需要在排除 BM 的情况下再次运行升级或重启，用户应再次发布到 bmexclude 探索终端。

限制

无法排除以下 VM：

- namenode

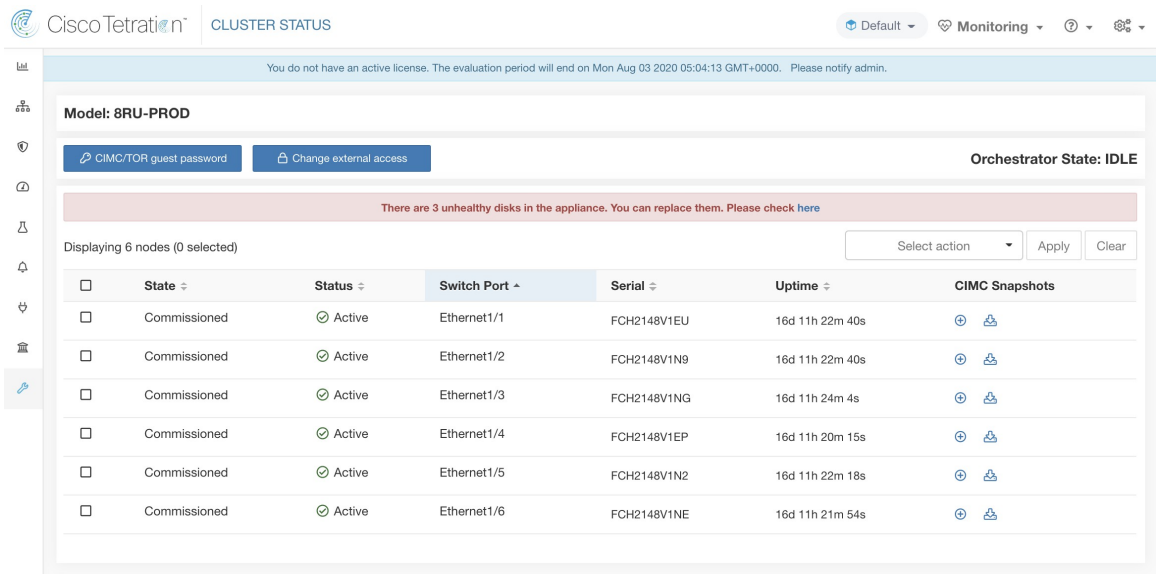
- secondaryNamenode
- mongodb
- mongodbArbiter

磁盘维护

磁盘维护涉及更换一台或多台服务器的任何故障硬盘。协调器会监控集群中每台服务器上 bmmgr 报告的磁盘运行状况。如果有任何故障磁盘，系统会在**集群状态 (Cluster Status)** 页面上显示一条横幅错误消息。从导航窗格中，选择**故障排除 (Troubleshoot)** > **集群状态 (Cluster Status)**。

横幅显示处于**不正常 (UNHEALTHY)** 状态的磁盘的数量。点击横幅上的此处，您将进入磁盘更换向导。您只能访问磁盘更换页面，但在向导的帮助下，**客户支持**可以执行磁盘维护所需的所有步骤。

Figure 62: 故障磁盘横幅

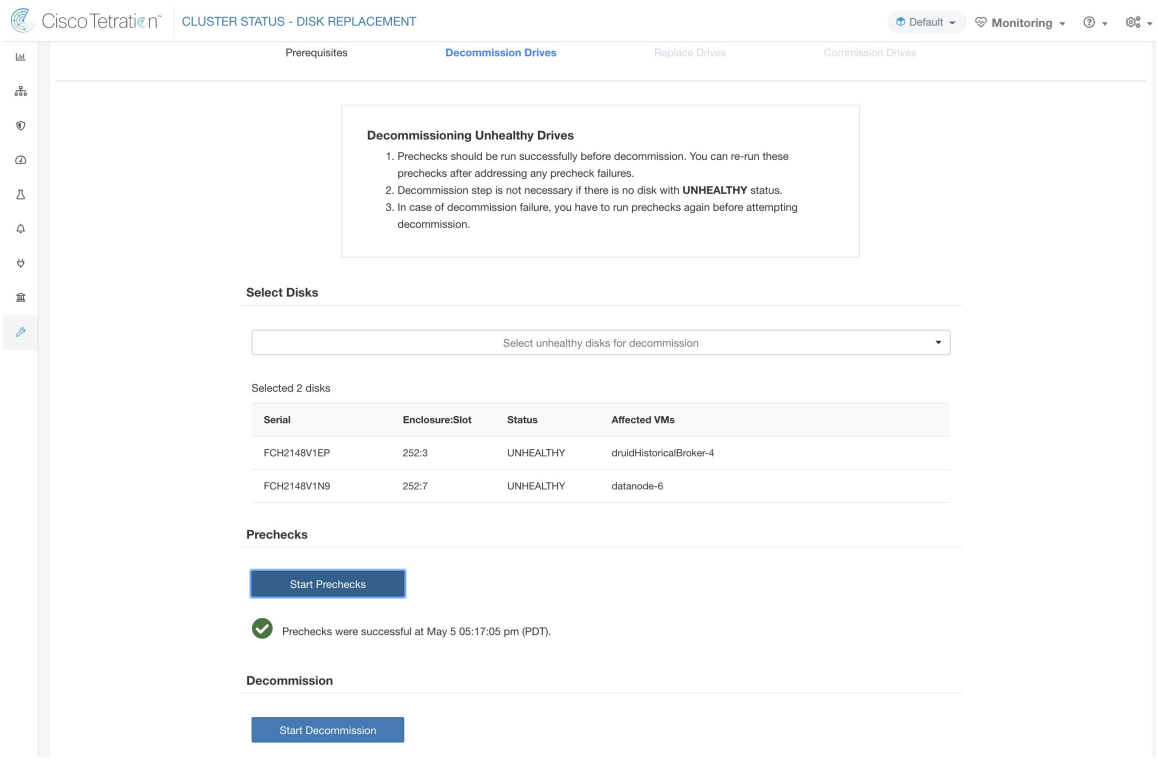


要求预先检查

在执行磁盘下线或调试之前，系统会在后端执行各种检查。所有检查必须均已通过，然后才能继续下线或调试磁盘。

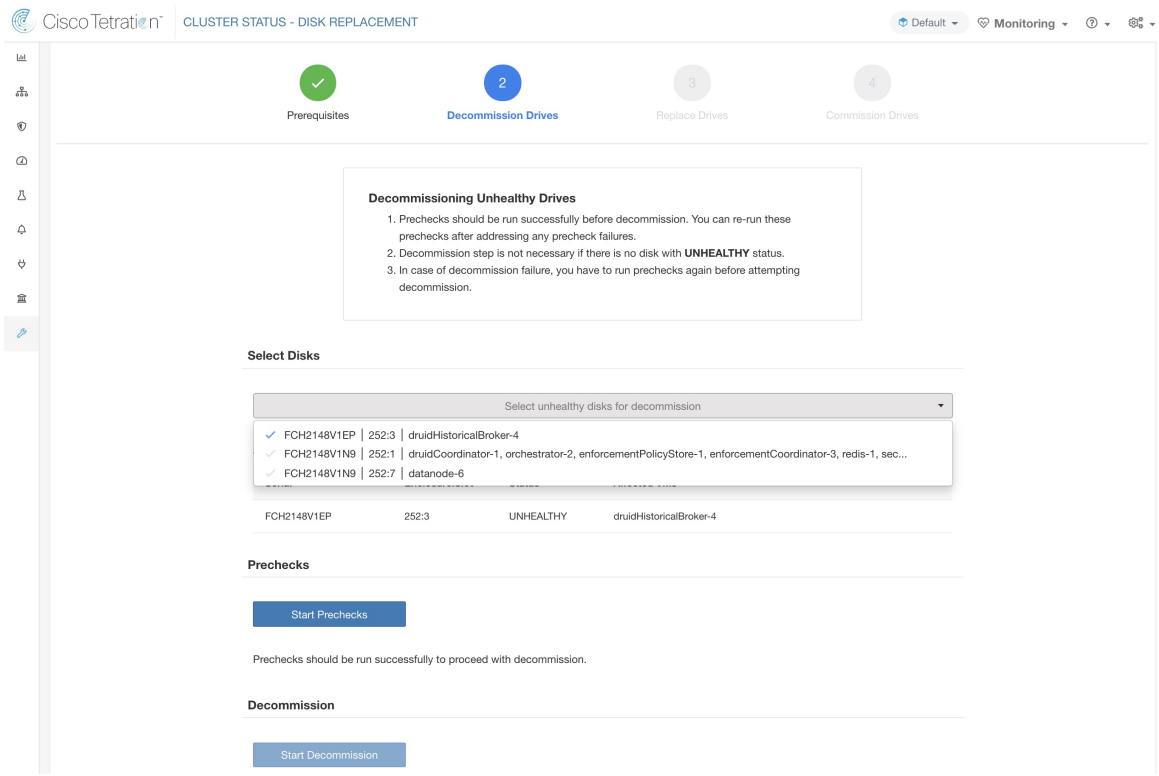
磁盘更换向导上会报告失败的检查，并提供失败详细信息和纠正措施，在继续下一步之前必须注意这一点，例如，一次只能下线一个数据节点。不能同时下线 Namenode 和 secondaryNamenode；此外，请在调试磁盘之前检查 Namenode 是否正常。

Figure 63: 磁盘更换预先检查



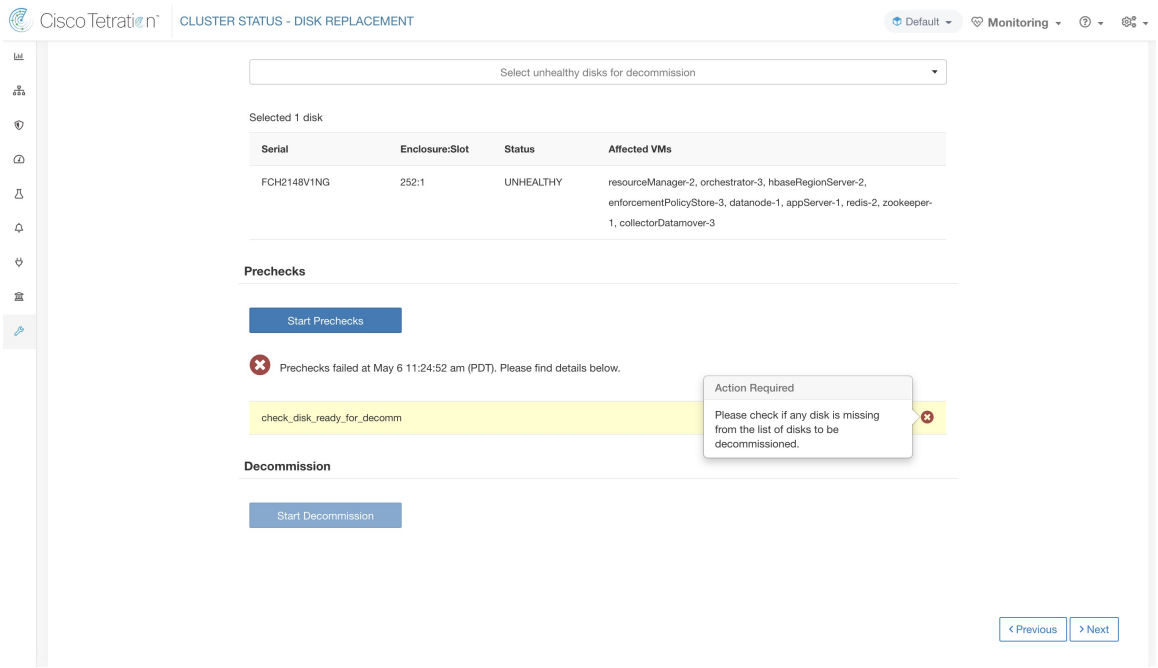
您可以选择要一起下线的任意一组故障磁盘，并启动下线预先检查。更改故障磁盘组需要重新运行预先检查。在开始下线或调试磁盘之前，请再次检查预先检查。确保在上次运行预先检查与开始下线任务期间没有新的预先检查失败。

Figure 64: 待下线的磁盘运行不正常



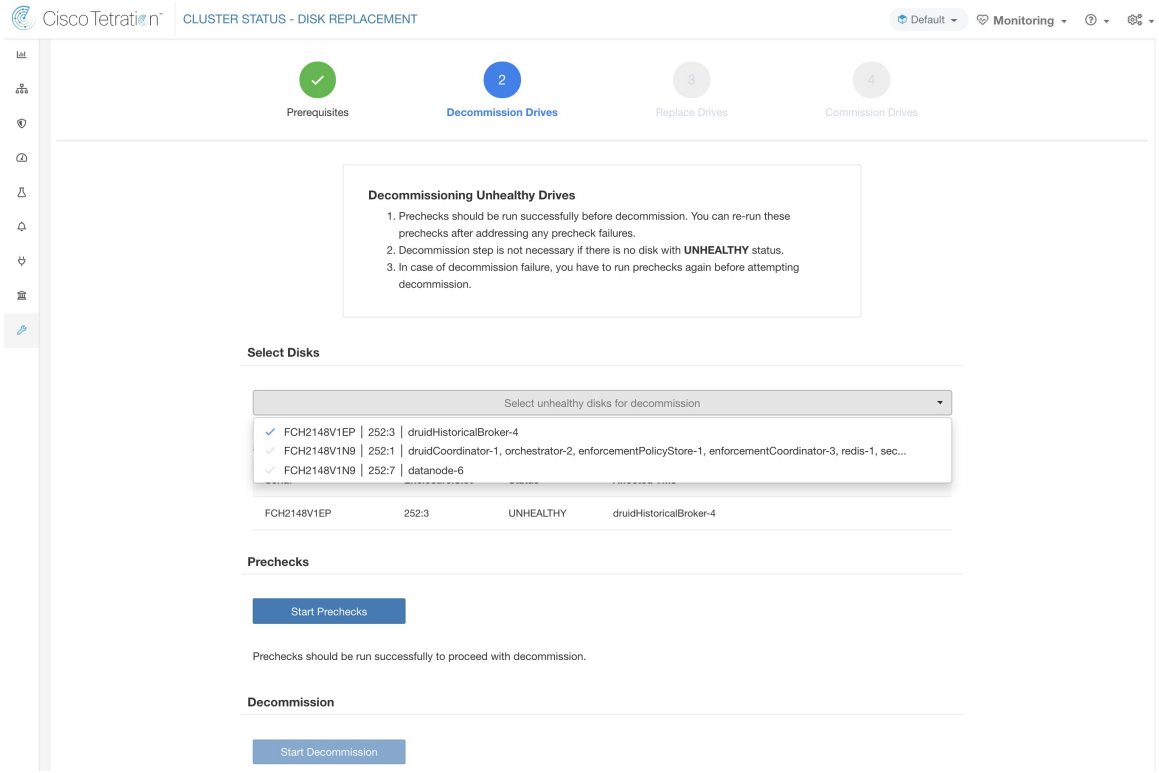
如果预先检查失败，则系统会显示详细消息。点击故障消息，当指针停留在十字按钮上时，弹出窗口中将显示建议的操作。

Figure 65: 预先检查失败的建议操作



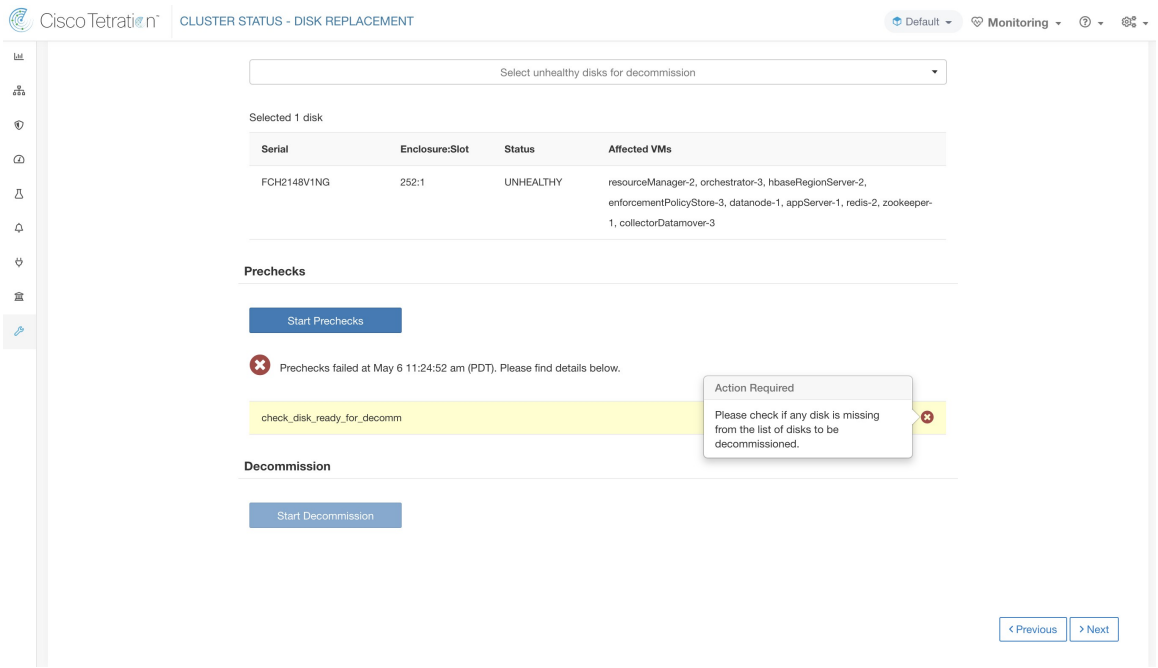
您可以选择要一起下线的任何故障磁盘集，并启动下线预先检查。更改故障磁盘组需要重新运行预先检查。在任务（下线或调试）开始之前，会再次检查相同的预先检查，以确保在上次运行预先检查和开始下线任务之间没有新的预先检查失败

Figure 66: 选择要下线的“不正常”***(UNHEALTHY)***磁盘



在任何预先检查失败的情况下，点击失败消息可看到详细的信息，当指针停留在红色十字按钮上时，弹出窗口会显示建议的操作。

Figure 67: 预先检查失败的弹出窗口中的建议操作



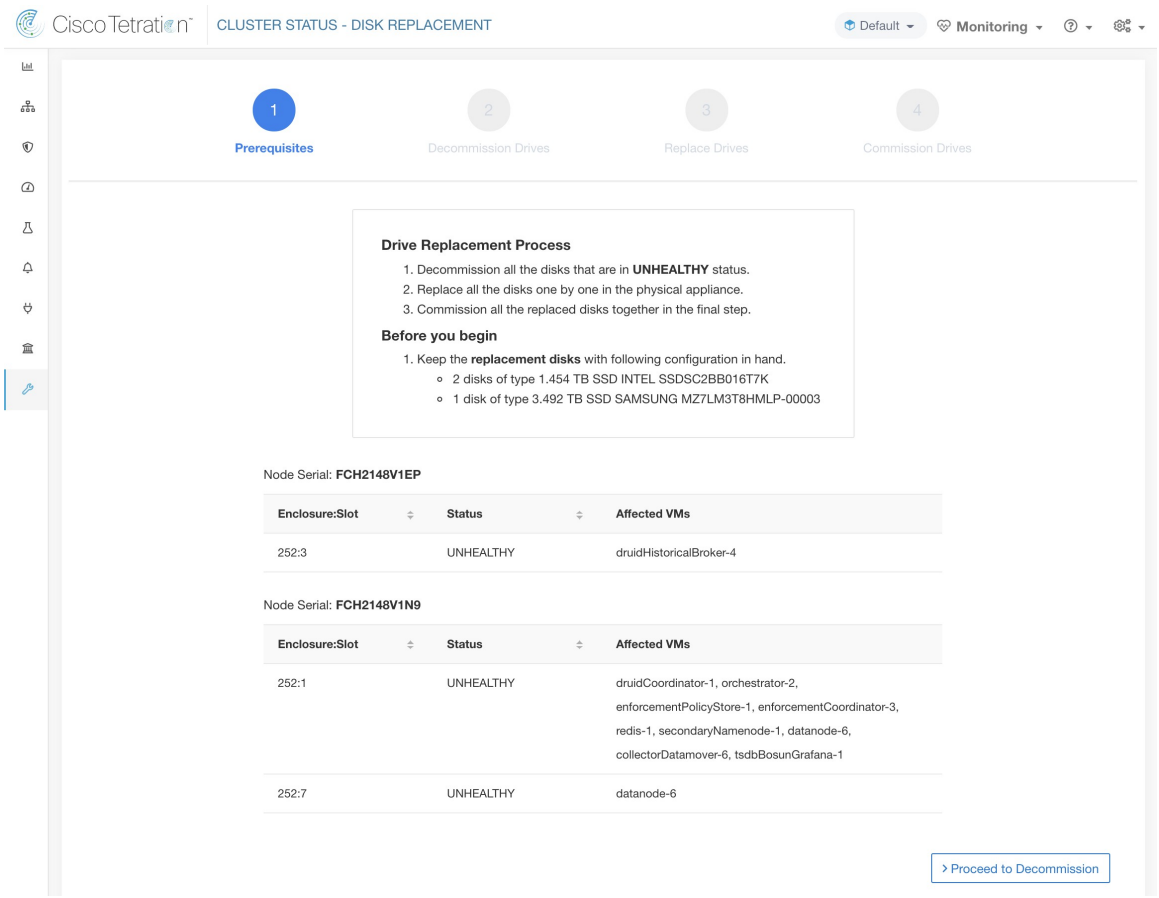
磁盘更换向导 - 非热插拔

准备工作

在开始更换运行状况不佳的磁盘之前，请确保准备好新的磁盘。

磁盘更换向导 (Disk Replacement Wizard) 会显示故障磁盘的详细信息，包括需要更换的每个磁盘的大小、类型、品牌和型号。此外，您还可以查看使用每个磁盘的所有 VM 的插槽 ID 和列表。

Figure 68: 磁盘更换向导



Note 从物理上讲，驱动器和硬件都支持热插拔。

磁盘状态转换

在任何集群中，非 RAID 的硬盘都有六种状态 - **正常 (HEALTHY)**、**不正常 (UNHEALTHY)**、**未使用 (UNUSED)**、**已更换 (REPLACED)**、**新 (NEW)** 和**已初始化 (INITIALIZED)**。部署或升级集群后，集群中每个磁盘的状态均为**正常 (HEALTHY)**。一个或多个磁盘的状态可能会根据各种错误检测更改为**不正常 (UNHEALTHY)**。

Note 非热插拔驱动器仅适用于 M4 和 M5 集群。

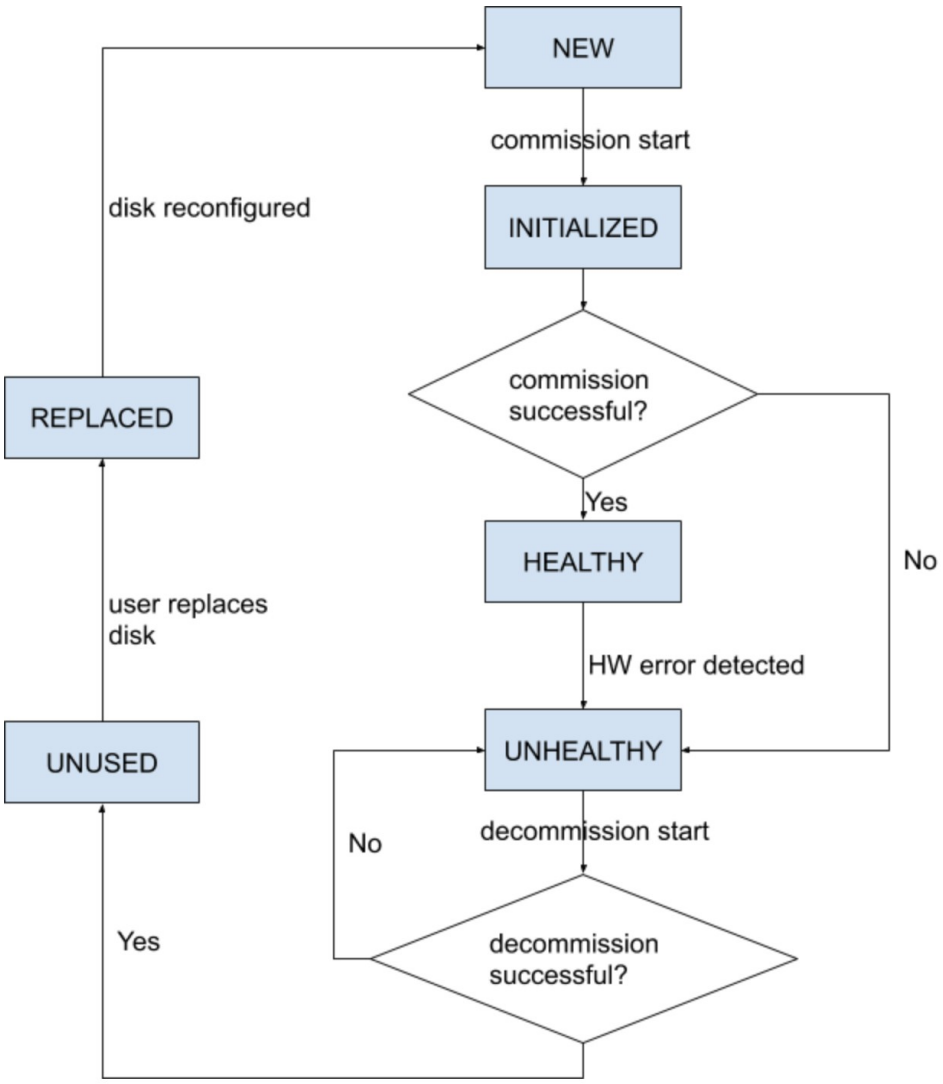
除非磁盘的状态更改为**不正常 (UNHEALTHY)**，否则不会执行任何操作。在开始调试磁盘之前，部署作为下线过程一部分而移除的所有虚拟机。

在成功调试磁盘且没有任何错误后，磁盘的状态会更改为**正常 (HEALTHY)**。如果磁盘调试不成功，状态将显示为**不正常 (UNHEALTHY)**。对于状态为**不正常 (UNHEALTHY)** 的磁盘，启动磁盘下线过程。如果下线过程成功，则磁盘的状态会变为**未使用 (UNUSED)**，如果磁盘在下线期间发生故障，请重复此过程，直到磁盘的状态变为**未使用 (UNUSED)**。

从集群中删除**不正常 (UNHEALTHY)** 的磁盘并替换为新磁盘，状态会变为**已更换 (REPLACED)**。重新配置替换磁盘并扫描硬件，查找任何异常。如果未检测到异常，磁盘的状态会更改为**新 (NEW)**，否则，您可能需要对问题进行故障排除；状态转换最多可能需要三分钟。

要了解如何处理磁盘状态转换，请参阅下面的流程图：

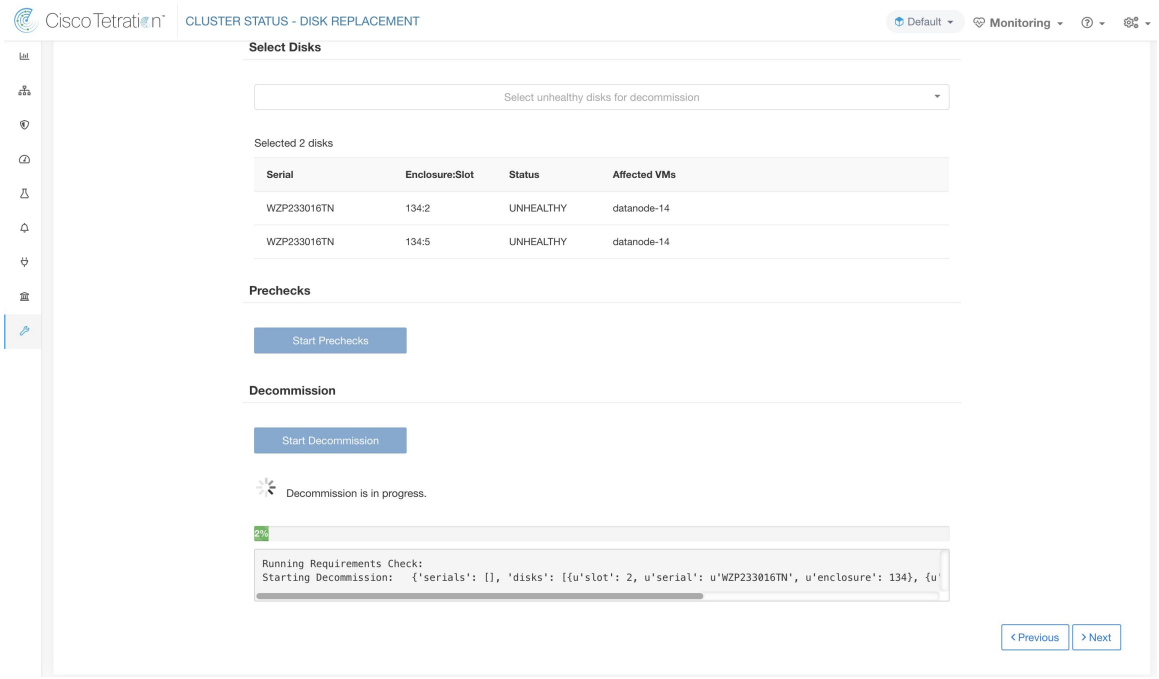
Figure 69: 磁盘状态转换



下线磁盘

通过预先检查后，您可以继续下线磁盘。磁盘更换向导中将显示下线进度。当下线进度达到 100% 时，所有已下线磁盘的状态都会更改为“未使用”(UNUSED)。

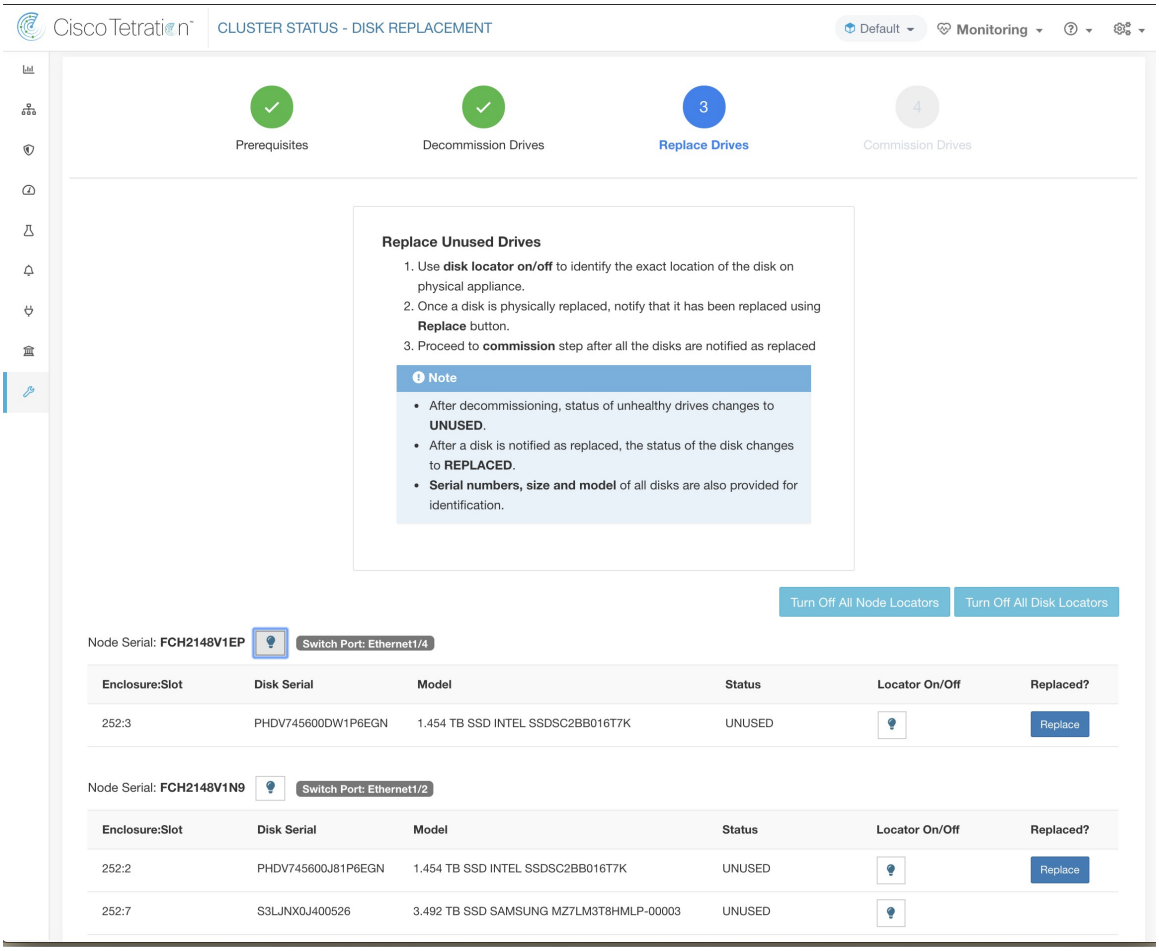
Figure 70: 监控磁盘下线进度



更换磁盘

下线磁盘后，移除磁盘并更换为新磁盘。为了帮助完成此过程，我们在替换页面上添加了磁盘和服务器定位器 LED 访问权限。确保关闭服务器和磁盘定位器 LED。

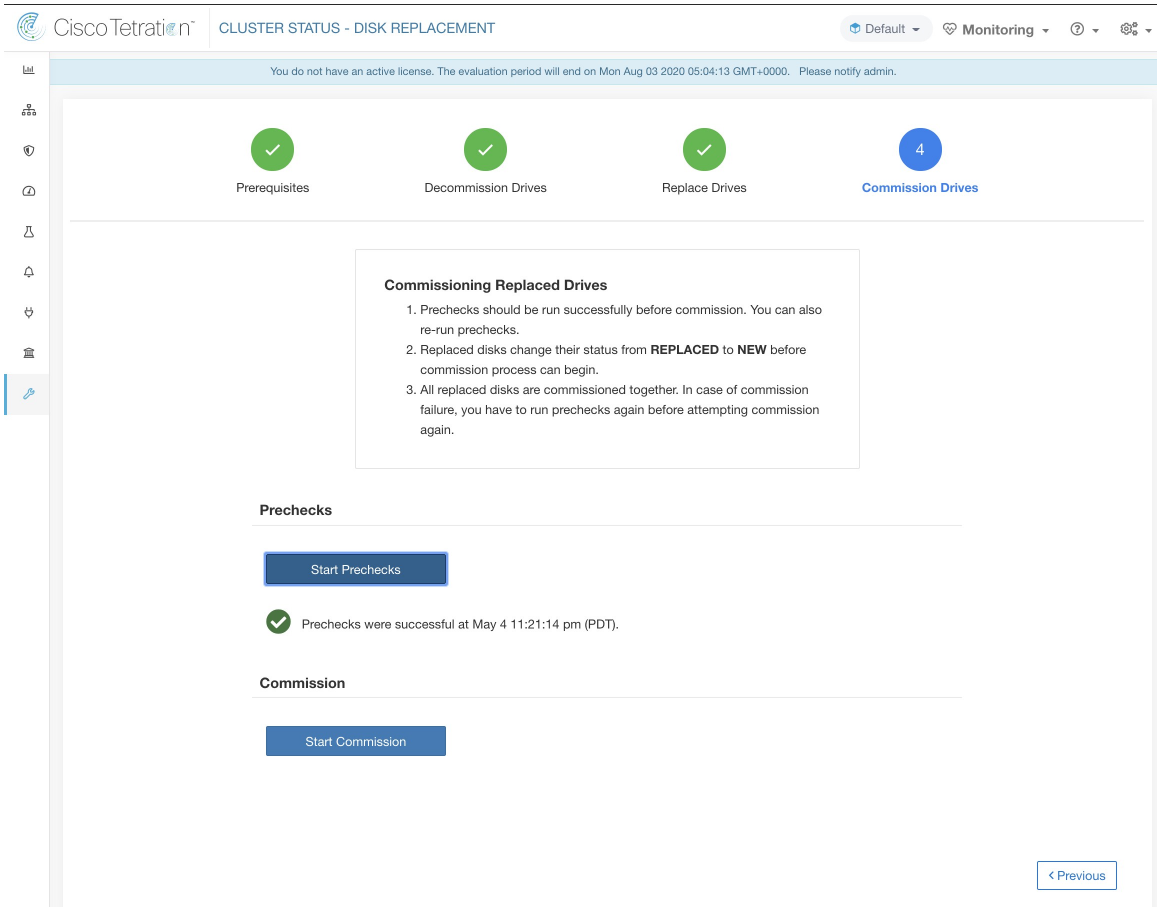
Figure 71: 重新配置新添加的磁盘（不可热插拔）



磁盘可以按任何顺序进行物理更换，但必须按照给定服务器的从最小到最大的插槽编号进行重新配置。此顺序通过在 UI 和后端上执行。在 UI 上，对于插槽号最小且状态为“未使用”(UNUSED) 的磁盘，您将看到一个活动的替换按钮。

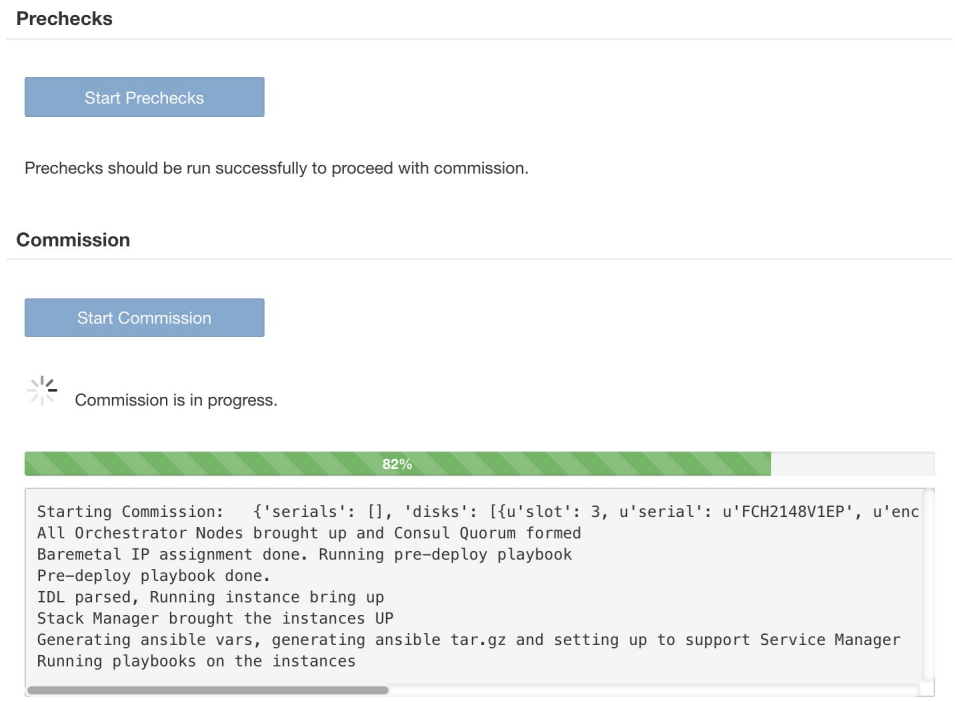
调试磁盘

更换所有磁盘后，继续进行调试。与下线类似，我们需要先运行一系列预先检查，然后才能继续调试。



在磁盘调试页面上监控调试进度。调试成功结束后，所有磁盘的状态都会变为“正常”(HEALTHY)。

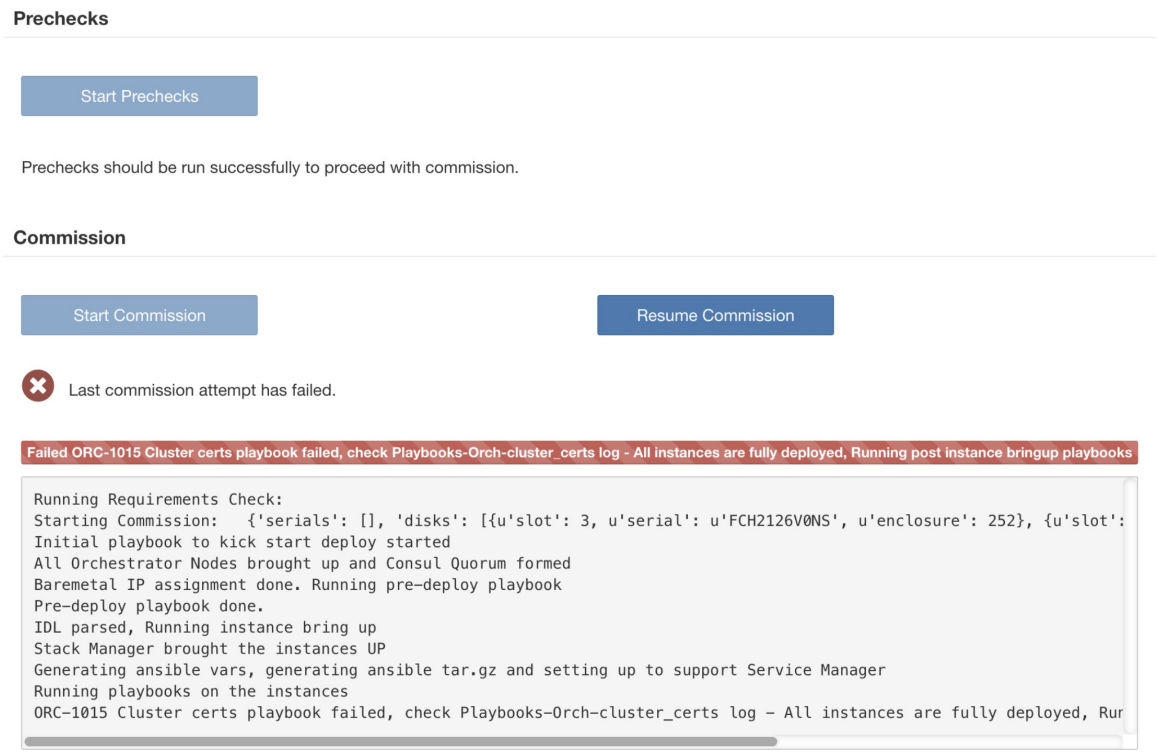
Figure 72: 调试进度



磁盘调试期间的故障恢复

在部署虚拟机且出现故障后，您可以使用**恢复调试 (Resume Commission)** 按钮进行恢复。要继续调试磁盘，请点击**恢复调试 (Resume Commission)** 按钮以重启部署后 Playbook。

Figure 73: 恢复调试



如果在部署虚拟机之前出现任何故障，则之前调试的磁盘的状态将更改为“不正常”(UNHEALTHY)。这将要求我们从下线“不正常”(UNHEALTHY) 磁盘以重启替换过程。

调试期间的磁盘故障

如果在磁盘调试过程中，正在更换的磁盘以外的任何其他磁盘发生故障，则在调试过程结束后，无论是成功还是失败，磁盘更换向导上都将显示该故障的通知。

在可恢复故障的情况下，用户将有两个选择来决定下一步采取什么措施。

1. 他们可以尝试恢复并完成当前调试，稍后再对新故障执行磁盘更换程序。
2. 或者，它们可以开始下线新出现的故障磁盘，并对所有磁盘一起执行调试。

在出现不可恢复故障时，第二种路径是唯一可用的路径。如果部署后故障是由于新出现故障的磁盘造成的，虽然我们有恢复按钮，但第二条路径仍将是唯一的前进方向。

已知问题和故障排除

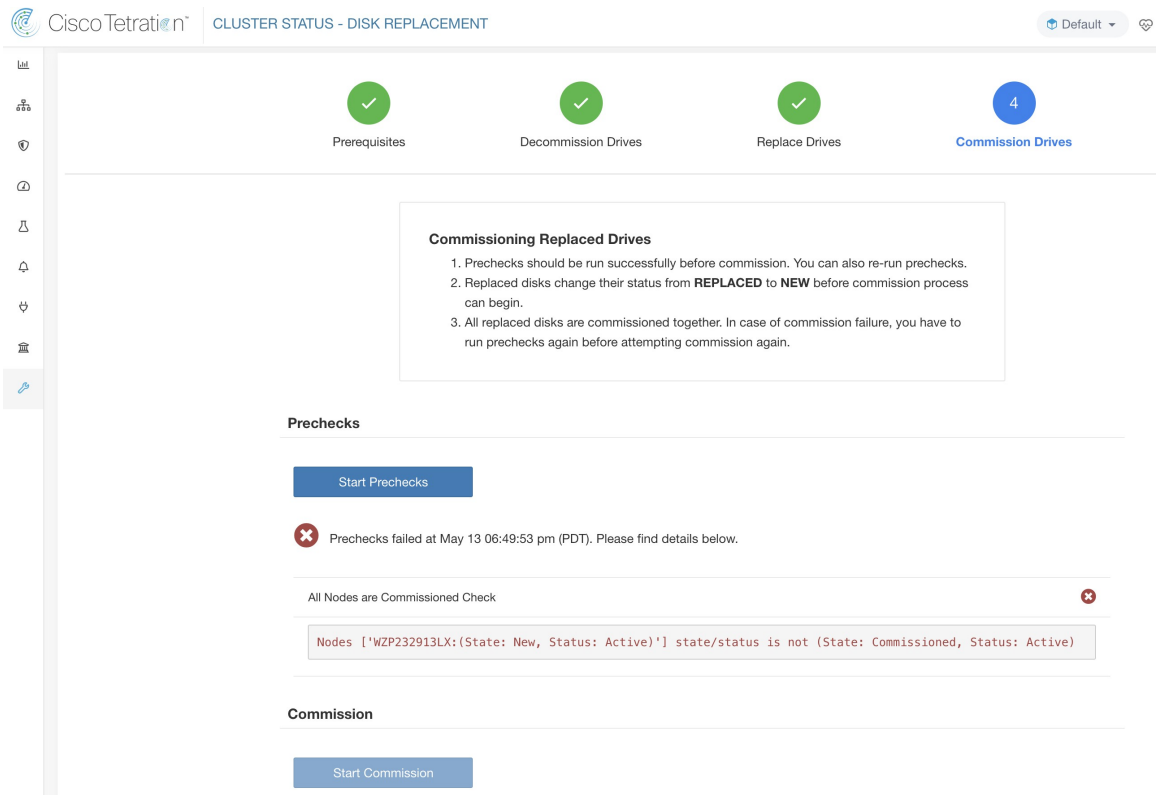
- 无法使用此程序来更换包含服务器根卷的磁盘。此类磁盘故障必须使用服务器维护流程来进行纠正。
- 只有当所有服务器均处于活动状态且处于调试状态时，才能进行磁盘调试。请参阅特殊处理部分，该部分介绍在需要同时更换磁盘和服务器的情况下如何继续操作。

- SSD 磁盘过于昂贵，而且故障率极低，因此我们不想失去宝贵的冗余数据存储容量。
- 在最初使用 3.8 软件部署的 M6 集群上，当服务器使用 3.9 软件调试时，将在硬盘驱动器上应用 RAID 配置。这将导致集群包含一些使用 RAID 的节点和一些使用 3.8 中的非 RAID 磁盘配置的节点。您的 Cisco Secure Workload 39RU 硬件最初随附的可能已安装 3.9，但某些早期的 M6 部署了 3.8。
- 如果在升级到 3.9 软件后，在所有服务器上逐步执行服务器下线和调试，则可以将集群转换为 RAID。
- M6 8RU 集群是全固态盘节点，固态盘驱动器上没有配置 RAID，因此 8RU 没有 RAID。
- 较早版本 (M4/M5) 上的驱动器配置使我们无法在这些版本的 Cisco Secure Workload 硬件上支持 RAID。

磁盘和服务器更换

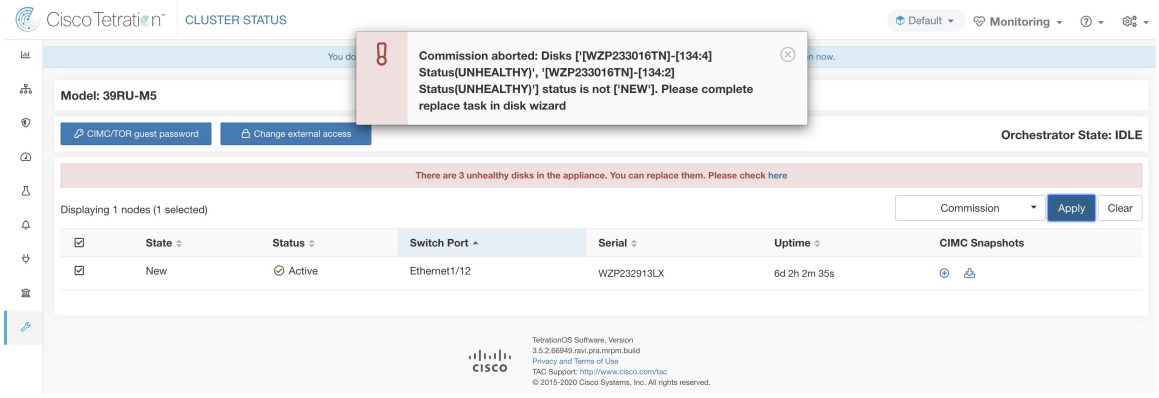
在需要同时调试磁盘和服务器的故障场景中，用户需要下线并更换可以下线的所有磁盘。通过预先检查，可以防止这些磁盘运行，以确保

1. 所有运行不正常的磁盘的状态均为“新”(NEW)
2. 所有服务器均处于已调试 *(Commissioned)* 状态，且状态为活动 *(Active)*



一旦所有“不正常”(UNHEALTHY) 的磁盘都处于“新”(NEW) 状态，预计将使用服务器维护程序下线/重新映像/重新启用故障服务器。

现在，如果有任何磁盘的状态不是“正常”(HEALTHY) 或“新”(NEW)，则会阻止服务器调试。服务器调试成功也会使所有磁盘的状态变为“正常”(HEALTHY)。



集群维护操作

本部分介绍影响整个集群的维护操作。

关闭 Cisco Secure Workload 集群

关闭集群会停止所有正在运行的 Cisco Secure Workload 进程，同时关闭所有单个节点。执行以下步骤以关闭集群。

启动集群关闭

Procedure

步骤 1 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 2 点击**重启/关闭 (Reboot/Shutdown)** 选项卡。

步骤 3 选择**关闭 (Shutdown)**，然后点击**发送关闭链接 (Send Shutdown Link)**。关闭链接将被发送到邮件地址。

Figure 74: 关闭邮件

Hello Site Admin!

We received a request that you intend to shutdown the cluster "98". You can do this through the link below.

Shutdown 98 (For best results, please use Google Chrome)

The above link expires by Jul 22 08:34:30 pm (PDT).

If you didn't request this, please ignore this email.

Shutdown will not be triggered until you actually click the above link.

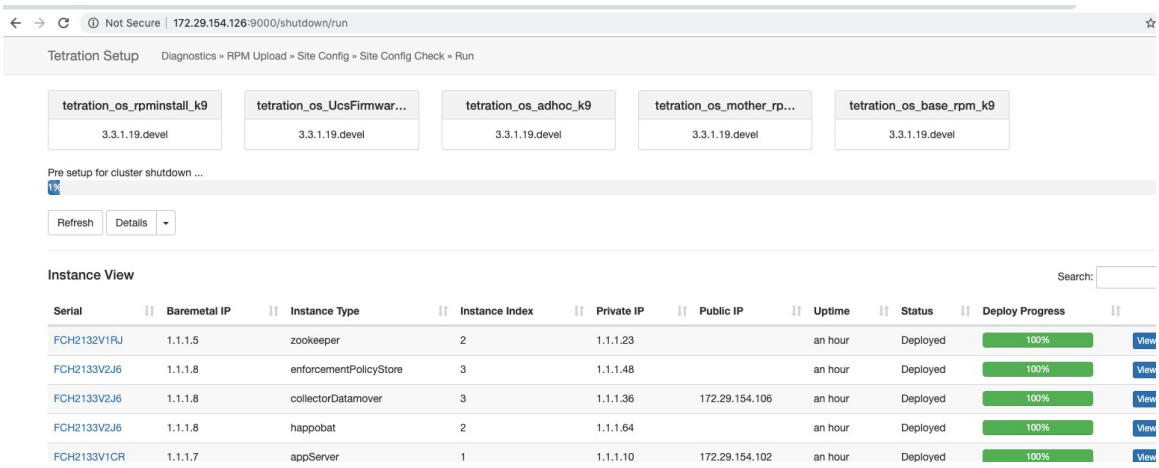
步骤 4 在**集群关闭 (Cluster Shutdown)** 页面上，点击**关闭 (Shutdown)**。

Important 无法在点击**关闭 (Shutdown)** 按钮后取消关闭。

集群关闭进度

启动集群关闭后，系统会显示关闭进度和状态。

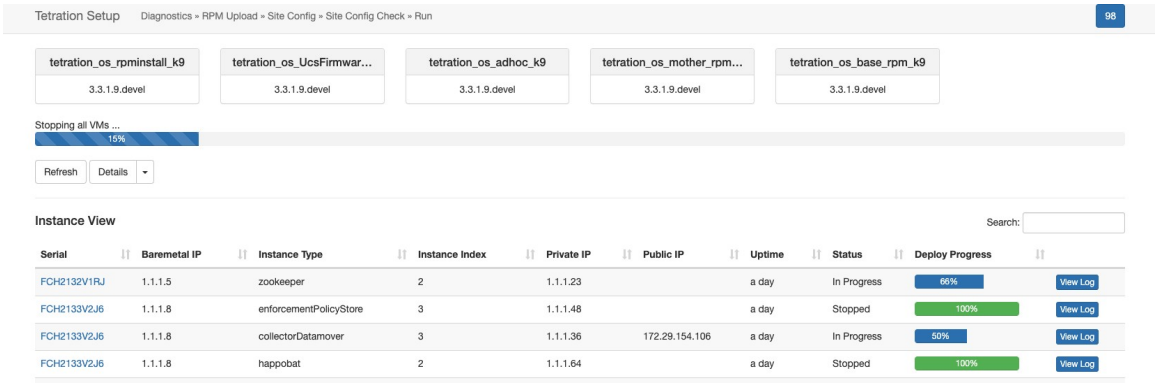
Figure 75: 集群关闭进度



如果在初始关机预先检查中发生错误，进度条将变为红色，在修复错误后，点击恢复按钮可重启关机。

完成预先检查后，虚拟机将停止。随着虚拟机逐渐停止，系统将显示进度。该页面类似于升级下的 VM 停止。有关详细信息，请参阅每个字段的升级部分。停止所有虚拟机最多可能需要 30 分钟。

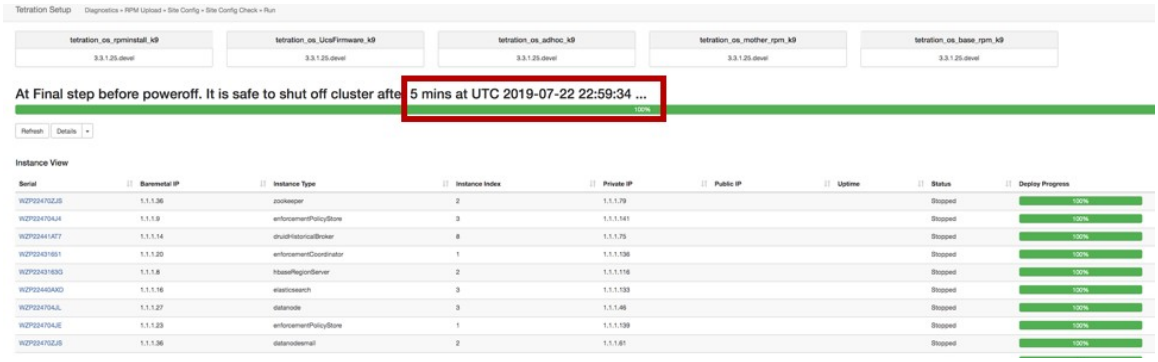
Figure 76: 停止虚拟机



当集群准备好关闭时，进度条将变为100%，并指明可以安全关闭集群电源的时间。请参阅以下屏幕截图中突出显示的内容。

Note 在等待进度条上显示的时间之前，请勿关闭集群。

Figure 77: 100% 关闭



重启 Cisco Secure Workload 集群

要在关闭后恢复集群，请打开裸机电源。当所有单独的裸机都正常运行时，即可访问UI。登录集群后，重启集群以使集群正常运行。

Note 您必须在关闭后重启集群才能使其正常运行。

启动集群重启

Procedure

步骤 1 从导航窗格中，依次选择**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**。

步骤 2 点击**重启/关闭 (Reboot/Shutdown)** 选项卡。

步骤 3 选择**重启 (Reboot)**，然后点击**发送重启链接 (Send Reboot Link)**。

点击您的邮件 ID 上收到的链接，以便重启集群。在设置 UI 页面上，启动集群重启。在重启期间，将执行受限升级操作。

查看集群维护作业的历史记录

要查看之前运行的集群维护作业，请执行以下操作：

1. 导航至**平台 (Platform)** > **升级/重启/关闭 (Upgrade/Reboot/Shutdown)**，然后点击**历史记录 (History)** 选项卡。

   集群操作列列出了集群任务，例如部署、升级、重启或关闭。

2. 要下载集群作业的日志，请点击**下载日志 (Download Logs)**。

数据分流管理员：数据分流

数据分流

Note Cisco Secure Workload 支持写入数据分流的 Kafka 代理 0.9.x、0.10.x、1.0.x 和 1.1.x。

要从 Cisco Secure Workload 集群发送警报，则必须使用已配置的数据分流。数据分流管理员用户可以配置和激活新的或现有的数据分流。您可以查看**租户**的数据分流。

Figure 78: 可用数据分流

要管理数据分流，请在导航窗格中选择**管理 (Manage)** > **数据分流管理员 (Data Tap Admin)**。

建议的 Kafka 配置

在配置 Kafka 集群时，建议使用 9092、9093 或 9094 中的端口，因为 Cisco Secure Workload 会为 Kafka 的传出流量打开这些端口。

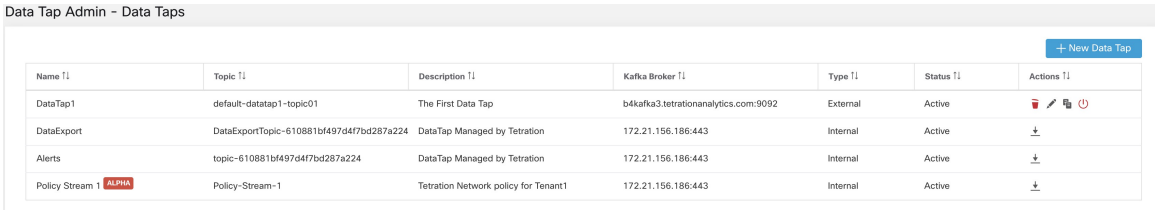
以下是 Kafka 代理的建议设置：

```
  broker.id=<incremental number based on the size of the cluster>
  auto.create.topics.enable=true
  delete.topic.enable=true
  listeners=PLAINTEXT://:9092
  port=9092
  default.replication.factor=2
  host.name=<your_host_name>
  advertised.host.name=<your_adversited_hostname>
  num.network.threads=12
  num.io.threads=12
  socket.send.buffer.bytes=102400
  socket.receive.buffer.bytes=102400
  socket.request.max.bytes=104857600
  log.dirs=<directory where logs can be written, ensure that there is sufficient space to
hold the kafka journal logs>
  num.partitions=72
  num.recovery.threads.per.data.dir=1
  log.retention.hours=24
  log.segment.bytes=1073741824
  log.retention.check.interval.ms=300000
  log.cleaner.enable=false
  zookeeper.connect=<address of zookeeper ensemble>
  zookeeper.connection.timeout.ms=18000
```

数据分流管理员部分

数据分流管理员可以查看可用的数据分流，并通过导航至**管理 (Manage)** > **数据分流管理员 (Data Tap Admin)** > **数据分流 (Data Taps)**进行配置。数据分流按**租户**进行配置。

Figure 79: 所有可用数据分流

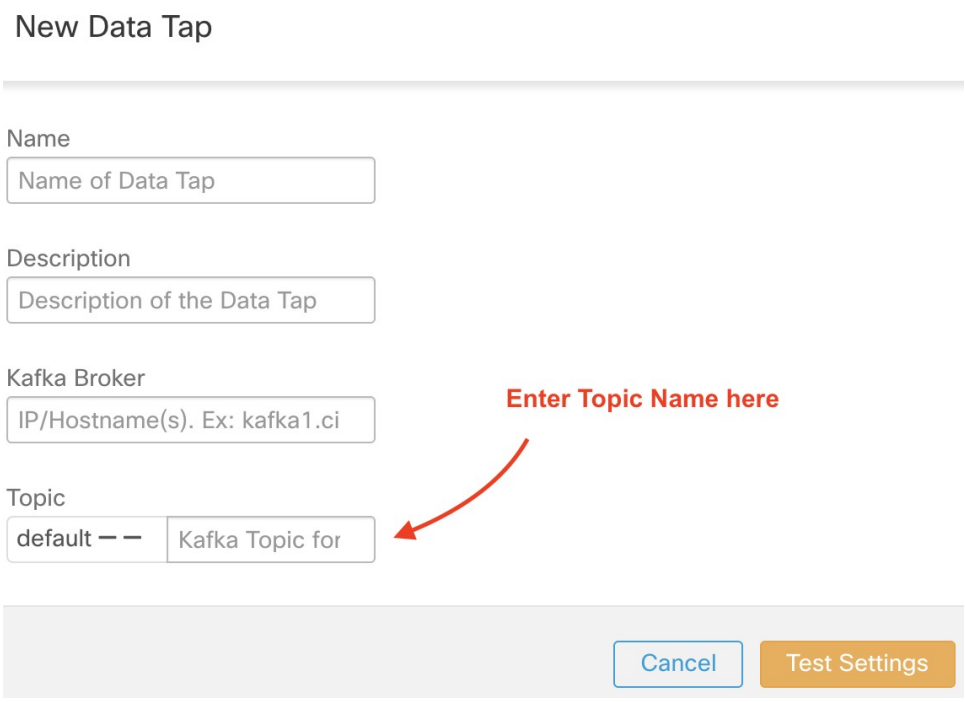


添加新的数据分流

数据分流管理员可以点击 

以添加新的数据分流。

Figure 80: 添加新的数据分流

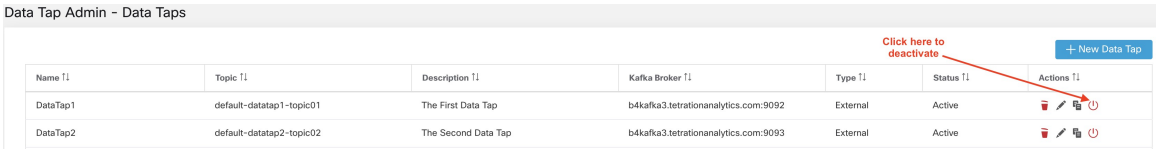


Note 更改数据分流值需要验证设置。

停用数据分流

要暂时阻止从 Cisco Secure Workload传出消息，数据分流管理员可以停用数据分流。不会向该数据分流发送任何消息。数据分流可随时重新激活。

Figure 81: 停用数据分流



删除数据分流

删除数据分流会删除任何依赖于该应用的 Cisco Secure Workload 应用实例。例如，如果用户已指定应将合规性警报发送到 DataTap A（在警报 Cisco Secure Workload 应用中），并且管理员删除了 DataTap A，则警报应用不会再将 DataTap A 列为警报输出。

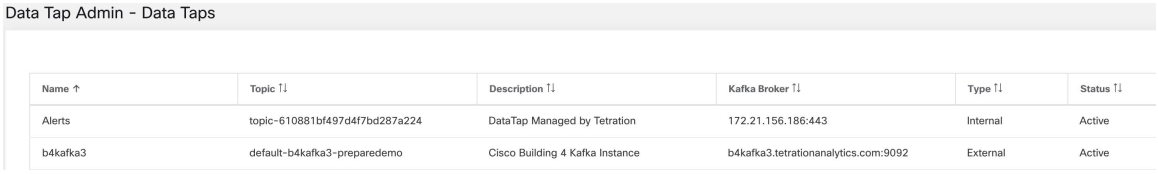
托管数据分流

托管数据分流 (MDT) 是在 Cisco Secure Workload 集群中托管的数据分流。它在身份验证、加密和授权方面都很安全。要从 MDT 收发消息，必须对客户端进行身份验证，并对通过网络发送的数据进行加密，并且只有授权用户才能从 Cisco Secure Workload MDT 读取消息或向 MDT 写入消息。Cisco

Secure Workload 提供要从 GUI 下载的客户端证书。Cisco Secure Workload 使用 Apache Kafka 1.1.0 作为消息代理，建议客户端使用与同一版本兼容的安全客户端。

在创建根范围后会自动创建 MDT。每个根范围都会创建一个警报 MDT。要从 Cisco Secure Workload 集群检索警报，则必须使用警报 MDT。只有数据分流管理员用户可以下载证书。您可以查看**根范围**的 MDT。

Figure 82: 已配置数据分流列表



默认情况下，所有 Cisco Secure Workload 警报都会被发送到 MDT，但可以更改为其他数据分流。

下载证书有两种选择：

- Java 密钥库：JKS 格式适用于 Java 客户端。
- 证书：常规证书更易于与 Go 客户端配合使用。

Figure 83: 下载证书

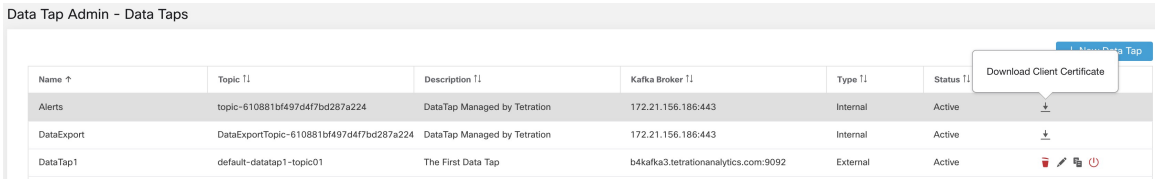
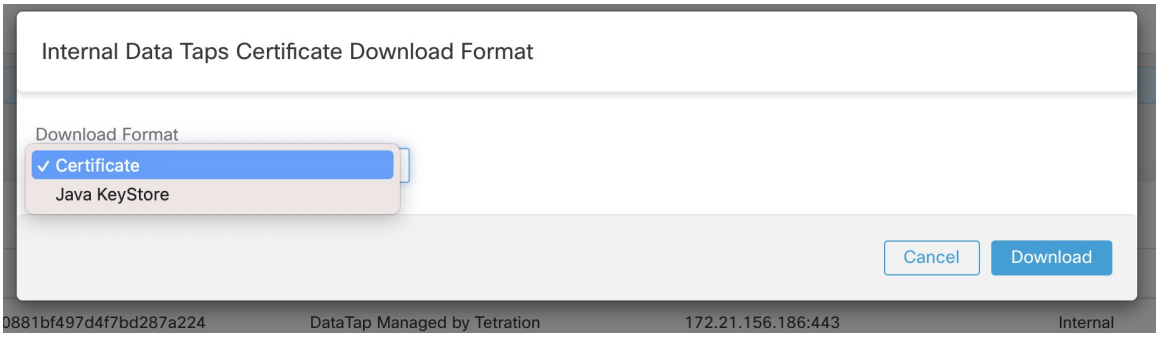


Figure 84: 证书类型



Java 密钥库

下载 *alerts.jks.tar.gz* 后，您应看到以下文件，其中包含连接到 Cisco Secure Workload MDT 以接收消息的信息：

- kafkaBrokerIps.txt：此文件包含 Kafka 客户端用于连接到 Cisco Secure Workload MDT 的 IP 地址字符串。

- topic.txt：此文件包含此客户端可从中读取消息的主题。主题的格式为 topic<root_scope_id>。在 Java 客户端中设置其他属性时，请使用此 root_scope_id。
- keystore.jks：Kafka 客户端应在连接设置中使用的密钥库，如下所示。
- truststore.jks：Kafka 客户端应在连接设置中使用的信任存储区，如下所示。
- passphrase.txt：此文件包含要用于 #3 和 #4 的密码。

在设置使用密钥库和信任库的使用者属性（Java 客户端）时，应使用以下 Kafka 设置：

```
security.protocol=SSL
ssl.truststore.location=<location_of_truststore_downloaded>
ssl.truststore.password=<passphrase_mentioned_in_passphrase.txt>
ssl.keystore.location=<location_of_truststore_downloaded>
ssl.keystore.password=<passphrase_mentioned_in_passphrase.txt>
ssl.key.password=<passphrase_mentioned_in_passphrase.txt>
```

在 Java 代码中设置 Kafka 使用者时，请使用以下属性：

```
    Properties props = new Properties();
    props.put("bootstrap.servers", brokerList);
    props.put("group.id", ConsumerGroup-<root_scope_id>);  // root_scope_id is same as
mentioned above
    props.put("key.deserializer",
"org.apache.kafka.common.serialization.StringDeserializer");
    props.put("value.deserializer",
"org.apache.kafka.common.serialization.StringDeserializer");
    props.put("enable.auto.commit", "true");
    props.put("auto.commit.interval.ms", "1000");
    props.put("session.timeout.ms", "30000");
    props.put("security.protocol", "SSL");
    props.put("ssl.truststore.location", "<filepath_to_truststore.jks>");
    props.put("ssl.truststore.password", passphrase);
    props.put("ssl.keystore.location", <filepath_to_keystore.jks>);
    props.put("ssl.keystore.password", passphrase);
    props.put("ssl.key.password", passphrase);
    props.put("zookeeper.session.timeout.ms", "500");
    props.put("zookeeper.sync.time.ms", "250");
    props.put("auto.offset.reset", "earliest");
```

证书

如果要使用证书，请使用 Go 客户端通过 Serama Kafka 库连接到 Cisco Secure Workload MDT。下载 *alerts.cert.tar.gz* 后，您应看到以下文件：

- kafkaBrokerIps.txt：此文件包含 Kafka 客户端用于连接到 Cisco Secure Workload MDT 的 IP 地址字符串
- topic：此文件包含此客户端可从中读取消息的主题。主题的格式为 topic<root_scope_id>。在 Java 客户端中设置其他属性时，请使用 root_scope_id。
- KafkaConsumerCA.cert：此文件包含 Kafka 使用者证书。
- KafkaConsumerPrivateKey.key：此文件包含 Kafka 使用者的私钥。
- KafkaCA.cert：此文件应在 Go 客户端的根 CA 证书列表中使用。

要查看 Go 客户端连接到 Cisco Secure Workload MDT 的示例，请参阅使用 MDT 发出的警报的 Go 客户端示例。

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。