CA 性能管理 Data Aggregator

管理员指南

2.4

ca technologies

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA 性能管理 Data Aggregator (Data Aggregator)
- CA 性能管理 Data Collector (Data Collector)
- CA Performance Center

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 产品管理

此部分包含以下主题：

如何设置 Data Repository 的自动备份（单一节点和群集安装）

在某些情况下，您必须备份 Data Repository。例如，在升级 Data Aggregator 之前或通过 cron 作业设置自动备份之前，您必须备份 Data Repository。在意外失败情况下，备份 Data Repository 为您提供一份要访问的 Data Repository 副本。

重要说明！ 初次备份 Data Repository 时，将执行完全备份。完成此完全备份可能需要花费很长时间，这取决于存在多少历史数据。初始备份执行完毕后，后续排定的备份将是增量备份。在每日都进行备份的情况下，增量备份仅仅会备份在过去 24 小时之内（如上次备份以来已经过去的时间段）发生的数据库活动。

要在执行完全备份之后执行增量备份，请为 Vertica 备份脚本提供与执行完全备份时相同的快照名称和备份目录。如果您更改这些名称，完全备份将会执行。

Vertica（数据库）创建用于存储数据的数据文件。这些文件在创建后就不会再修改；之后将创建新文件，并删除旧文件。此方法允许您使用标准 rsync 实用工具来备份 Data Repository，而此实用工具支持目标为其他计算机的快速文件复制功能。有关 rsync 的详细信息，请参阅 http://everythinglinux.org/rsync/。

要设置 Data Repository 的自动备份，请执行这些步骤：

1. 复查备份注意事项 (p. 10)。
2. 执行下列步骤之一：
   - 配置 Data Repository 备份到远程主机 (p. 11)。
   - 对同一主机配置 Data Repository 备份 (p. 13)。
3. 配置 Data Repository (p. 14)。

Data Repository 备份注意事项

在您备份 Data Repository 之前，请考虑以下信息：

- 备份 Data Repository 时，不需要停止 Data Repository 或 Data Aggregator。
- 备份将存储在用于备份数据库的配置文件中指定的位置内。在包含备份文件的目录中，会为备份到该位置的每个节点创建一个子目录。该子目录包含一个具有备份快照名称的目录。快照名称使用配置文件中的 snapshotName 选项进行设置。
- 每日执行增量备份。我们建议在非工作时间执行备份，因为备份处理会占用大量资源。
- 您可以将 Data Repository 备份到远程主机，也可以将其备份到同一主机。

  注意：如果备份到同一主机，请将备份保存到除编录和数据目录所使用的分区之外的其他分区。

- 每周执行完全备份。每日快照取决于完整备份。还原到任何快照都取决于完全备份的完整性。请注意以下有关完全备份的信息：
  - 为每周完全备份创建 .ini 文件。还原特定快照时需要 .ini 文件。为 .ini 文件分配唯一名称，且 .ini 文件第一次运行时，将执行完全备份。因此，注意您的磁盘空间非常重要。如果磁盘空间有限，建议您仅保留一或两个星期（当前周除外）的数据。此解决方案需要在新的一周开始时执行删除最早一周备份数据的额外维护步骤。
  - 通过运行 /opt/vertica/bin/vbr.py -setupconfig 命令生成新的 .ini 文件，或复制 .ini 文件的当前版本来执行完全备份。将现有 .ini 文件复制到新 .ini 文件，然后更改新 .ini 文件中的“snapshotName”值。

详细信息：

如何设置 Data Repository 的自动备份（单一节点和群集安装） (p. 9)

配置 Data Repository 备份到远程主机（单一节点和集群安装）

您可以将 Data Repository 备份到远程主机。

建议各个 Data Repository 节点都有自己的远程备份主机。例如，对于具有三个 Data Repository 节点的群集环境，各个 Data Repository 主机都需要专用的备份主机。

重要说明！对于群集环境，针对您计划用于备份*每个*群集节点的每个远程主机，执行下列步骤。必须备份群集中的每个节点。

请执行以下步骤：

1. 打开控制台，并登录到您计划以 root 用户身份作为远程备份主机的计算机。
2. 要在远程备份主机上创建 Vertica Linux 数据库管理员用户，请键入以下命令：

   ```
   useradd database_admin_user -s /bin/bash
   ```

   例如：

   ```
   useradd dradmin -s /bash/bin
   ```

   注意：在存在于 Data Repository 主机的远程备份主机上创建同样的 Vertica Linux 数据库管理员用户。确保 Data Repository 主机和远程备份主机不连接到 LDAP 或网络信息服务 (NIS)，并共享同一 Vertica Linux 数据库管理员用户。

3. 要设置 Vertica Linux 数据库管理员用户密码，请键入以下命令：

   ```
   passwd database_admin_user
   ```

   例如：

   ```
   passwd dradmin
   ```

4. 要在远程备份主机上创建 Vertica 目录，请键入以下命令：

   ```
   mkdir /opt/vertica/bin
   ```

   ```
   mkdir /opt/vertica/oss
   ```

5. 要更改 Vertica 目录的所有者，请键入以下命令：

   ```
   chown -R dradmin /opt/vertica
   ```

6. 注销远程备份主机。

7. 要为远程备份主机在 Data Repository 主机上设置无密码 ssh，请执行以下步骤：

   a. 打开控制台，并作为 Vertica Linux 数据库管理员用户登录到 Data Repository 主机。

   b. 键入以下命令：

      ```
      ssh-keygen -N "" -t rsa -f ~/.ssh/id_rsa
      cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys2
      chmod 644 ~/.ssh/authorized_keys2
      ```

   c. 要将 Vertica Linux 数据库管理员用户公钥复制到远程备份主机的授权密钥的列表，请键入以下命令：

      ```
      ssh-copy-id -i dradmin@backuphost
      ```

   d. 打开控制台，并作为 Vertica Linux 数据库管理员用户登录到远程备份主机。

   e. 要将 Vertica rsync 和 python 工具从 Data Repository 主机复制到远程备份主机，请键入以下命令：

      ```
      scp dradmin@<drhost>:/opt/vertica/bin/rsync /opt/vertica/bin
      scp -r dradmin@<drhost>:/opt/vertica/oss/python /opt/vertica/oss
      ```

8. 确认远程备份主机现在有新的 /opt/vertica/bin/rsync 文件目录和 /opt/vertica/oss/python 目录。

9. 要在远程备份主机上创建备份目录，请键入以下命令：

   ```
   mkdir backup_directory
   ```

backup_directory

表示要将 Data Repository 备份到的目录。选择一个具有大量可用空间的磁盘分区上的备份目录。如果数据库管理员用户无法对这些目录进行写入操作，请使用 chown 和 chmod 命令为该用户授予访问这些目录的权限。

注意：在群集安装中，请先创建备份目录，然后再备份数据库。您可以为每台主机选择不同的备份目录。

例如：

```
mkdir ~dradmin/backups
```

详细信息：

如何设置 Data Repository 的自动备份（单一节点和群集安装） (p. 9)

配置 Data Repository 备份到远程主机（单一节点和集群安装）

您可以将 Data Repository 备份到远程主机。在群集环境中，您必须在群集中备份每个节点。您可以为每台主机选择不同的备份目录。

请执行以下步骤：

1. 以数据库管理员用户的 Linux 用户帐户身份登录到 Data Repository。

   注意：在群集安装中，您可以从参与该群集的三台主机中的任意一台登录到 Data Repository。

2. 请确保数据库管理员用户的 Linux 用户帐户设置了无密码的 ssh 密钥。

   注意：在群集安装中，请确保为参与该群集的*每台*主机都设置了无密码的 ssh 密钥。

   请执行以下步骤：

   a. 要查看是否已设置无密码 ssh 密钥，请键入以下命令：

      ```
      ssh hostname ls
      ```

      hostname

      表示安装 Data Repository 的主机的名称。

      如果设置了无密码的 ssh 密钥，则系统*不会*提示您输入密码。您无需再执行任何操作。

b. 如果系统*提示*您输入密码，请忽略该提示并按 Ctrl+C。要为数据库管理员用户的 Linux 用户帐户设置无密码 ssh 密钥，请键入以下命令：

```
ssh-keygen -N "" -t rsa -f ~/.ssh/id_rsa
cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys2
chmod 644 ~/.ssh/authorized_keys2
```

要确认*不*向您提示输入密码，请重新输入以下命令：

```
ssh hostname ls
```

hostname

表示安装 Data Repository 的主机的名称。

重要说明！如果不设置无密码的 ssh 密钥，您将无法备份 Data Repository。即使将备份保存到同一计算机，也要设置无密码的 ssh 密钥。

3. 要创建备份目录，请键入以下命令：

```
mkdir backup_directory
```

backup_directory

表示要将 Data Repository 备份到的目录。选择一个具有大量可用空间的磁盘分区上的备份目录。如果数据库管理员用户无法对这些目录进行写入操作，请使用 chown 和 chmod 命令为该用户授予访问这些目录的权限。

注意：在群集安装中，请先创建备份目录，然后再备份数据库。您可以为每台主机选择不同的备份目录。

例如：

```
mkdir ~dradmin/backups
```

详细信息：

如何设置 Data Repository 的自动备份（单一节点和群集安装） (p. 9)

配置 Data Repository。

为自动备份配置 Data Repository。

请执行以下步骤：

1. 以数据库管理员用户的 Linux 用户帐户身份登录到 Data Repository。

注意：在群集安装中，您可以从参与该群集的三台主机中的任意一台登录到 Data Repository。但是，建议您登录将启动备份的 Data Repository 主机。

2. 要创建可重复使用的配置脚本，以用于备份和恢复 Data Repository，请以键入以下命令，作为数据库管理员用户的 Linux 用户帐户：

   ```
   /opt/vertica/bin/vbr.py --setupconfig
   ```

   注意：建议在配置文件的目标目录中启动此命令。数据库管理员用户的 Linux 用户帐户必须有权写入该目录。

   系统将提示您回答各种问题和陈述。问题和陈述列表及其典型回答的说明如下：

   - Snapshot name（快照名称）：*备份快照名称*
   - Back up vertica configurations?（备份 vertica 配置?） [y/n]: y
   - 还原点数目 (1): 7

     注意：还原点 7 可以将 Data Repository 还原到最近的备份或前 7 个增量备份中的任何一个。如果还原点设置为 1，则您只能将 Data Repository 还原到最近的备份或前一个增量备份。到达还原点限制后，将删除最旧的备份。要保持更多的还原点，请增大还原点或在配置文件中更改快照名称。但是，更改快照名称会启动一组新的完全备份，使备份所需的磁盘空间量增加一倍。
   - Specify objects (no default)（指定对象(无默认值)）: 不指定值，按回车键帮助确保所有对象都已备份。
   - Vertica user name (dradmin)（Vertica 用户名(dradmin)）: 按回车键接受默认值
   - Save password to avoid runtime prompt ?（保存密码以避免运行时提示?） (n) [y/n]: y
   - Password to save in vbr config file (no default)（要保存在 vbr 配置文件中的密码(无默认值)）: 提示时输入密码。

     注意: 此密码必须与 Vertica 中数据库管理员帐户的数据库密码对应。
   - Backup host name (no default)（备份主机名称(无默认值)）: *用于备份的主机名*

     注意：如果备份群集，系统将提示您输入对应于该群集中每个节点的主机名。您必须备份群集中的每个节点。
   - Backup directory (no default)（备份目录(无默认值)）: *要将 Data Repository 备份到的目录路径*

     注意: 如果备份群集，将提示您输入群集中每个节点的备份目录。您必须备份群集中的每个节点。

- Config file name (snapshot name.ini)（配置文件名称(快照名称.ini)）：按回车键接受默认值。

  确认您对创建 .ini 文件的目录具有写权限。如果您未输入 .ini 文件的完整路径，文件将保存到运行 /opt/vertica/bin/vbr.py --setupconfig 命令的路径。

  重要提示：生成的配置文件将包含明文密码。

- Change advanced settings?（更改高级设置?） (n) [y/n]:n

  将显示一条消息，表示 vbr 配置已保存到名为“快照名称.ini”的配置文件中。

3. 备份 Data Repository。键入以下命令：

   ```
   /opt/vertica/bin/vbr.py --task backup --config-file
   configuration_directory_path_filename
   ```

   configuration_directory_path_filename

   表示您先前创建的配置文件的目录路径和文件名。该文件位于您运行备份实用工具的位置 (/opt/vertica/bin/vbr.py)。

   例如：

   ```
   /opt/vertica/bin/vbr.py --task backup --config-file
   /home/vertica/vert-db-production.ini
   ```

   如果系统提示您确认主机的真实性，请回答“yes”。

   注意：在群集安装中，您只需在参与群集的其中一台主机上执行此步骤。

   备份 Data Repository。

4. （可选）如果您不想为未来的手动备份保留明文的 Data Repository 密码，请执行下列步骤：

   a. 确认下列行在 [数据库] 部分之下存在：

      ```
      dbPromptForPassword = True
      ```

   b. 从 [Database] 部分删除以下行：

      ```
      dbPassword = password
      ```

   注意：对于自动备份，必须在配置文件中加入 dbPassword 行，且提供相应的密码。将 dbPromptForPassword 设置为 False。

5. 要设置对 Data Repository 的自动每日备份（建议），请执行下列操作：

   a. 打开您首选的文本编辑器以创建新的包装程序 shell 脚本。

b. 包装程序 shell 脚本的内容应当包含以下单行：

```
/opt/vertica/bin/vbr.py --task backup --config-file
configuration_directory_path_filename
```

configuration_directory_path_filename

表示您先前创建的配置文件的目录路径和文件名。该文件位于您运行备份实用工具的位置 (/opt/vertica/bin/vbr.py)。

例如：

```
/opt/vertica/bin/vbr.py --task backup --config-file
/home/vertica/vert-db-production.ini
```

c. 将内容保存到您所选位置的名为“backup_script.sh”的新文件。

例如：

```
/home/vertica/backup_script.sh
```

d. 通过键入以下命令更改运行脚本的权限：

```
chmod 777 location_backup_script.sh/backup_script.sh
```

例如：

```
chmod 777 /home/vertica/backup_script.sh
```

e. 作为数据库管理员用户的 Linux 用户帐户，请键入以下命令：

```
crontab -e
```

f. 添加将运行您先前创建的备份脚本的 cron 作业。

注意：我们建议您创建 cron 作业，以便每日在非高峰期运行脚本。

例如：

```
00 02 * * *   /home/vertica/backup_script.sh >/tmp/backup.log  2>&1
```

此示例 cron 作业将在每天凌晨 2:00 运行备份脚本。

重要说明！初次备份 Data Repository 时，将执行完全备份。完成此完全备份可能需要花费很长时间，这取决于存在多少历史数据。初始备份执行完毕后，后续排定的备份将是增量备份。在每日都进行备份的情况下，增量备份仅仅会备份在过去 24 小时之内（如上次备份以来已经过去的时间段）发生的数据库活动。

还原 Data Repository

备份 Data Repository 之后，还可以进行还原。此过程假定数据库管理员用户是 sudoers 文件的一部分。

注意：通常将 Data Repository 还原到您从中备份的同一计算机。然而，您*可以*将 Data Repository 还原到不同的计算机。如同您备份 Data Repository 的计算机一样，必须以同样的方式配置还原的计算机。在群集环境中，如同您分别备份 Data Repository 节点的每台计算机一样，必须以同样的方式配置还原的每台计算机。

下列配置必须相同：

- IP 地址
- 主机名
- 目录和数据目录
- 目录和数据目录权限
- Vertica Linux 数据库管理员用户凭据
- 数据库管理员用户帐户凭据
- 数据库用户帐户凭据

请执行以下步骤：

1. 以 root 用户或有权访问有限命令集的 sudo 用户身份登录到安装有 Data Collector 的计算机，停止与 Data Aggregator 关联的所有 Data Collector 主机。打开命令提示符并键入以下命令：

   ```
   service dcmd stop
   ```

   Data Collector 主机停止。

2. 以 root 用户或有权访问有限命令集的 sudo 用户身份登录到安装有 Data Aggregator 的计算机，停止 Data Aggregator。打开命令提示符并键入以下命令：

   ```
   service dadaemon stop
   ```

   注意：有关创建可使用有限命令集的 sudo 用户的信息，请参阅《*Data Aggregator 安装指南*》。

   Data Aggregator 将停止。

3. 以数据库管理员用户（而*非* root 用户）身份登录到 Data Repository 所用的数据库服务器。

4. 键入以下命令：

   ```
   /opt/vertica/bin/adminTools
   ```

   此时将打开“Administration Tools”（管理工具）对话框。

5. 选择“(4) Stop Database”（(4) 停止数据库）。
6. 按数据库名称旁边的空白条，选择“确定”，然后按 Enter 键。

   系统将提示您输入数据库密码。

7. 输入数据库密码并按下 Enter 键。

   Data Repository 将停止。

   注意：如果 Data Repository 未停止，从“(7) Advanced Tools”（(7) 高级工具）菜单中选择“(2) Stop Vertica on Host”（(2) 停止主机上的 Vertica）。

8. 选择“退出”，然后按 Enter 键。
9. 要准备还原 Data Repository 备份，请以数据库管理员用户的 Linux 用户帐户身份登录到 Data Repository 所用的数据库服务器。

   在设置 Data Repository 的自动备份时，您已通过还原点 7 来配置配置文件。Data Repository 可以还原到最近的备份或任何前七个增量备份。

10. 执行下列步骤之一：

    a. 要将 Data Repository 还原到最近的备份，请键入以下命令：

       ```
       /opt/vertica/bin/vbr.py --task restore --config-file
       configuration_directory_path_filename
       ```

       configuration_directory_path_filename

       表示在运行备份配置过程时创建的配置文件的文件名和目录路径。该文件位于您运行备份实用工具的位置 (/opt/vertica/bin/vbr.py)。

例如：

```
/opt/vertica/bin/vbr.py --task restore --config-file
/home/vertica/vert-db-production.ini
```

注意：在群集安装中，您可以从参与群集的任意主机上运行还原任务。

b. 要将 Data Repository 还原到任何前七个增量备份，请键入以下命令：

```
/opt/vertica/bin/vbr.py --task restore --config-file
configuration__directory_path_filename  --archive_name
```

configuration_directory_path_filename

表示您希望还原特定存档的特定配置文件的文件名和目录路径。在运行备份配置程序时，已创建此配置文件。该文件位于您运行备份实用工具的位置 (/opt/vertica/bin/vbr.py)。

archive_name

表示希望还原到的特定还原点的名称。对还原点的配置文件表示的备份目录所做的更改。列出所有可用的还原点。确定希望还原到的还原点的存档名称。

例如：

```
/opt/vertica/bin/vbr.py --task restore --config-file myconfig.ini
--archive 20131020_170018
```

注意：在群集安装中，您可以从参与群集的任意主机上运行还原任务。

11. 通过以数据库管理员用户身份而*不是*以 root 用户身份登录到安装了 Data Repository 的计算机来重新启动 Data Repository。打开命令提示符并执行以下步骤：

a. 键入以下命令：

```
/opt/vertica/bin/adminTools
```

此时将打开“Administration Tools”（管理工具）对话框。

b. 选择 (3)“启动数据库”。

c. 按数据库名称旁边的空白条，选择“确定”，然后按 Enter 键。

系统将提示您输入数据库密码。

d. 输入数据库密码并按下 Enter 键。

Data Repository 将启动。

e. 选择“退出”，然后按 Enter 键。

12. 以 root 用户身份或有权访问有限命令集的 sudo 用户身份登录到安装了 Data Aggregator 的计算机来重新启动 Data Aggregator。键入以下命令：

```
/etc/init.d/dadaemon start
```

Data Aggregator 将启动。

13. 重新启动与 Data Aggregator 相关联的所有 Data Collector 主机：

a. 选择“管理”、“数据源设置”，然后单击一个 Data Aggregator 数据源。

b. 从“系统状态”菜单中单击“Data Collector”。

c. 选择所有与 Data Aggregator 关联的 Data Collector 主机，然后单击“启动”。

Data Collector 主机启动。

备份 Data Aggregator

在某些情况下，您必须备份 Data Aggregator。例如，升级之前，您必须备份 Data Aggregator 和 Data Repository。通过备份这些组件，您可以得到自己的设置及自定义认证的副本，以便在出现意外故障时访问。

备份 Data Aggregator 时，不需要停止 Data Repository、Data Collector 或 Data Aggregator 服务。

备份存储在您指定的位置，例如可以在 Data Aggregator 系统或不同的备份主机系统中。

注意：您必须具有 root 或 sudo 权限才能执行该任务。

请执行以下步骤：

1. 打开命令提示符。
2. 使用以下命令在同一或不同备份主机系统的安全位置创建备份目录：

```
mkdir DA_Backup
```

DA_Backup

指定备份目录的目录路径和名称。

3. 使用以下所有命令在 DA_Backup 中创建子目录：

```
mkdir DA_Backup/deploy_backup
mkdir DA_Backup/MIBDepot_backup
mkdir DA_Backup/CustomDeviceType_backup
```

4. 运行以下命令备份 DA 上的文件：

   - 该命令将备份自定义供应商认证。请不要备份该目录中的 local-jms-broker.xml 和自述文件。

     ```
     cp Data Aggregator installation
     directory/apache-karaf-2.3.0/deploy/im.ca.com.*.xml
     DA_Backup/deploy_backup
     ```

   - 该命令将备份 MIBDepot 目录中的所有自定义 MIB：

     ```
     cp Data Aggregator installation directory/apache-karaf-2.3.0/MIBDepot/*
     DA_Backup/MIBDepot_backup
     ```

   - 该命令将备份所有自定义设备子类型 xml 文件：

     ```
     cp Data Aggregator installation
     directory/apache-karaf-2.3.0/custom/devicetype/DeviceType.xml
     DA_Backup/CustomDeviceType_backup/
     ```

   Data Aggregator 安装目录

   指定 Data Aggregator 安装目录。

   默认：/opt/IMDataAggregator

还原 Data Aggregator

您可以还原备份的 Data Aggregator 信息。如果 Data Repository 保持不变，您可以只还原 Data Aggregator 组件。

您在还原之前不必停止 Data Aggregator。即使 Data Aggregator 正在运行，也可以将备份的文件放入正确的目录。

注意：您必须具有 root 或 sudo 权限才能执行该任务。

请执行以下步骤：

1. 打开命令提示符。
2. （可选）DA karaf 服务未运行的情况下，卸载现有的 Data Aggregator 并重新安装。

3. 运行以下所有命令：

   ```
   cp DA_Backup/deploy_backup/*.* Data Aggregator 安装目录
   /apache-karaf-2.3.0/deploy/
   cp DA_Backup/MIBDepot_backup/*.* Data Aggregator 安装目录
   /apache-karaf-2.3.0/MIBDepot/
   cp DA_Backup/CustomDeviceType_backup/*.* Data Aggregator 安装目录
   /apache-karaf-2.3.0/custom/devicetype/
   ```

   如果出现提示，请覆盖现有文件。

   DA_Backup

   指定备份目录的目录路径和名称。

   Data Aggregator 安装目录

   指定 Data Aggregator 安装目录。

   默认：/opt/IMDataAggregator

4. 等待几分钟，让 Data Aggregator 与 CA Performance Center 自动进行同步。Data Aggregator 与 Data Collector 主机建立连接后，Data Collector 主机将恢复轮询。

   Data Aggregator 将还原。

   注意：如果需要将 Data Collector 还原到先前的某个状态，可以卸载并重新安装 Data Collector。

查看 Data Aggregator 详细信息

您可以查看 Data Aggregator 所监视的可管理且可通过 ping 连接的设备的数量。

管理员可以查看 Data Aggregator 为所有承租方监视的可管理且可通过 ping 连接的设备的总数。每个承租方的设备总数也会显示在表中。

承租方管理员可以查看 Data Aggregator 为其承租方监视的可管理且可通过 ping 连接的设备的总数。

您还可以查看 Data Aggregator 的版本和内部版本号。

请执行以下步骤：

1. 以管理员身份打开 CA Performance Center。
2. 选择“管理”、“数据源设置”，然后单击一个 Data Aggregator 数据源。
3. 从“系统状态”菜单中单击“Data Aggregator”。

   此时会打开“Data Aggregator 列表”页面。其中将显示按承租方列出的可管理且可通过 ping 连接的设备的总数，以及所选 Data Aggregator 安装的版本和内部版本号。

查看 Data Collector 安装的列表

您可以查看可用 Data Collector 安装的列表，并可以更改其中某些设置。“Data Collector 列表”显示每个 Data Collector 安装所分配到的承租方和 IP 域，以及 Data Collector 状态和版本。还会显示每个 Data Collector 安装正在轮询的设备和组件数，以及分配给该 Data Collector 实例的总设备数，包括当前未轮询的设备。

管理员可以查看所有承租方的 Data Collector 安装列表。承租方管理员仅可以看到分配给其承租方的 Data Collector 安装。

请执行以下步骤：

1. 以管理员身份打开 CA Performance Center。
2. 选择“管理”、“数据源设置”，然后单击一个 Data Aggregator 数据源。
3. 从“系统状态”菜单中单击“Data Collector”。

   此时将打开“Data Collector 列表”页面，其中显示可用的 Data Collector 安装的列表。

详细信息：

管理 Data Collector 安装 (p. 25)

管理 Data Collector 安装

管理员必须为每个 Data Collector 安装选择一个 IP 域和一个承租方。每个 Data Collector 实例只能与一个 IP 域关联，与该 IP 域关联的相应 Data Collector 实例将执行发现请求。

*IP 域*是用于标识来自不同设备和网络的数据的逻辑分组。按域监视意味着，分别监视具有属于不同客户网络的关联接口或应用程序的 IP 地址。如果具有适当的权限，则可从单个控制台监视 IP 域，但用户只能查看他们所监视的域的数据。

*承租方*表示受管服务提供商管理的客户环境。每个承租方环境是独立的，并且有效地用作 CA Performance Center 的单独实例。每个实例可以包含不在承租方之间共享的多个用户和角色。

默认承租方代表受管基础架构内的受管服务提供商的承租方空间。如果未部署多承租方，请分配默认承租方。在单承租方环境中，默认承租方是用于监视整个基础架构的空间。

请执行以下步骤：

1. 以管理员身份打开 CA Performance Center。
2. 导航到“Data Collector”页面 (p. 24)。
3. 从列表中选择一个 Data Collector 实例。
4. 确认 Data Collector 可供分配。“已轮询项数目”列列出了分配给此 Data Collector 实例的轮询设备和组件的数目。

   重要说明！如果轮询的设备和组件的数目大于一个，则无法为 Data Collector 实例更改承租方或 IP 域分配。
5. 单击“分配”。

   此时会打开“分配 Data Collector”对话框。
6. 从下拉列表中选择想要分配给此 Data Collector 实例的承租方。

   此 Data Collector 实例发现的所有受管设备和组件会自动与此承租方相关联。

   如果您想要使用默认承租方，请选择“默认承租方”。
7. 选择要与此 Data Collector 实例关联的 IP 域。

   此 Data Collector 实例发现的所有受管设备和组件会自动与此 IP 域相关联。
8. 单击“保存”。

   此时会将承租方和 IP 域分配给 Data Collector 安装。

在 Data Collector 上重新平衡负荷

当 Data Collector 实例监视多个设备时，可能会超过 Data Collector 容量，Data Collector 可能会变为超负荷。您可以将工作负荷从一个超负荷的 Data Collector 实例传输到其他 Data Collector 实例。您可以通过以下两种方式在 Data Collector 上重新平衡负荷：

- 选择超负荷的 Data Collector 实例，然后选择“重新平衡”。产品使用其他可用的 Data Collector 实例自动重新平衡负荷。
- 将选定的设备从一个 Data Collector 实例移至另一个。

重要说明！建议您在高峰时间里不要在 Data Collector 上重新平衡负载，或将大量项从一个 Data Collector 实例移到另一个实例，因为这可能会影响最终用户性能。

请执行以下步骤：

1. 以管理员身份打开 CA Performance Center。
2. 选择“管理”、“数据源设置”，然后单击一个 Data Aggregator 数据源。
3. 从“系统状态”菜单中单击“Data Collector”。

   将显示每个 Data Collector 安装正在轮询的设备和组件数。还会显示分配给每个 Data Collector 实例的总设备数，包括当前未轮询的设备。

在 Data Collector 上自动重新平衡负荷

1. 选择要重新平衡的 Data Collector 实例，然后单击“重新平衡”。

   注意：确保选择同一 IP 域内的 Data Collector 实例。仅同一 IP 域内的 Data Collector 实例可以互相重新平衡设备。
2. 确认对话框将显示每一选定的 Data Collector 的当前设备数和已轮询项数，以及建议的产生的设备数和已轮询项数。

   注意：设备只能移至可以与其联系的 Data Collector 实例。
3. 单击“是”。

   注意：重新平衡轮询项会重新开始对所有已重新平衡轮询项的基准平均值计算。

将选定的设备移至特定 Data Collector 实例

1. 选择要从中移动选定设备的 Data Collector 实例。
2. 在“设备”表中，选择要移至其他 Data Collector 实例的设备，然后单击“移动设备”。
3. 此时将打开“将设备移至选定的 Data Collector”对话框。

4. 从下拉列表中选择要向其移动选定设备的 Data Collector 实例。

   注意：只能选择同一 IP 域内的 Data Collector 实例。

5. 单击“是”。

   注意：移动设备会重新开始对已移动设备的基准平均值计算。

对抽取非 SNMP (CAMM) 数据的数据收集器的负载平衡

通过将设备和组件从一个 Data Collector 实例移到另一个实例的 Data Collector 负载平衡仅适用于通过 SNMP 或 ICMP 监控的设备和组件。对于通过 CAMM 抽取非 SNMP 数据且需要重新平衡资源的 Data Collector 实例来说，您可以通过将设备包引擎分发给环境中的其他主机来执行该操作。此处是有关如何执行此重新平衡操作的说明。

1. 在安装期间将本地控制器 (LC) 安装到新服务器上，并指向适当的多控制器（MC）服务器
2. 将 LC 成功安装到新服务器之后，请检查 CAMMWEB 是否显示两个 LC。
   a. 打开 CAMMWEB -
   b. 单击“主机”，此时应该会显示“安装 LC”（新服务器）
3. 使用 CAMMWEB 选择新服务器，并部署要迁移的设备包引擎
4. 登录 MC 服务器并导航到：

   $CAMM_INSTALL/MC/repository/<旧服务器 IP>/COMPONENTS 目录
5. 执行以下命令：

   ‘cp –R ENGINE_<devicepack> $CAMM_INSTALL/MC/repository/<新服务器 IP>/COMPONENTS/’
6. 如果要迁移的设备包使用 sftp/ftp/copy 机制作为数据获取，那么
   a. 在新服务器的 $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/ 下创建以下目录
      - $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/tmp/input/inventory 下创建 tmp 目录
      - $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/tmp/input/performance 下创建 input 目录

b. 将以下文件从旧服务器复制到新服务器

- $CAMM_INSTALL/COMPONENTS/ENGINE_<devicepack>/tmp/input/inventory/.historyFile.Inventory 到 $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/tmp/input/inventory
- $CAMM_INSTALL/COMPONENTS/ENGINE_<devicepack>/tmp/input/performance/.historyFile.Performance 到 $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/tmp/input/performance

7. 从 CAMMWEB 启动设备包。

如何将 Data Collector 移至其他主机

Data Collector 是 Data Aggregator 的组件。您可以将 Data Collector 移至其他主机系统，无需重新发现网络设备和组件，也不会丢失历史数据。例如，如果您是工具管理员，您的服务器管理员可以指示您将 Data Collector 重新部署到其他主机。Data Collector 要轮询 500,000 个设备和组件，因此您不想丢失数据或执行重新发现。

即使您安装了设备包，也可以移动 Data Collector 组件。

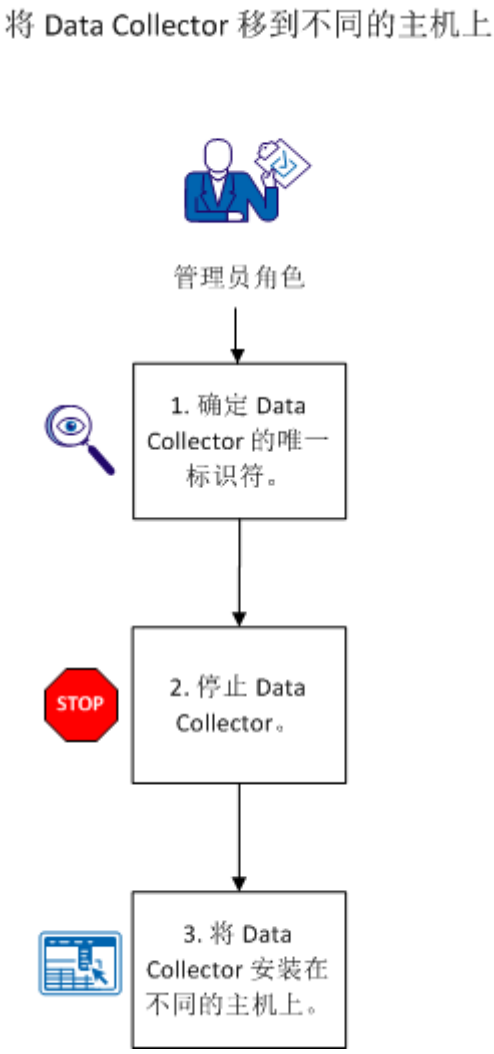
注意以下注意事项：

- 数据丢失量等于从关闭旧的 Data Collector 组件到部署完新的 Data Collector 组件所经过的时间。
- 如果旧 Data Collector 组件意外启动，则会导致 SNMP 数据的双倍轮询。您将在 Data Aggregator 的 karaf 日志中看到类似于以下内容的警告：

```
WARN  | Session Task-810 | 2013-01-02 13:52:09,062 | DCHeartBeatLog |
ore.collector.interfaces |
      | HeartBeat 消息未接收。预期：93，收到：255
```

若要修复此问题，停止或卸载旧的 Data Collector 组件。

下图显示如何将 Data Collector 移至其他主机：



要将 Data Collector 移至其他系统，请按照以下过程：

1. 确定 Data Collector 的唯一标识符 (p. 30)。
2. 停止 Data Collector (p. 30)。
3. （仅针对 CA Mediation Manager 集成）迁移设备包 (p. 32)。
4. 在其他主机上安装 Data Collector (p. 32)。

确定 Data Collector 的唯一标识符

将此组件移至其他主机之前为 Data Collector 确定唯一标识符。

使用以下方式之一检索 Data Collector ID：

- 以具有管理员角色的用户身份登录 CA Performance Center 并执行下列步骤：
  a. 选择“管理”，然后从菜单中选择 Data Aggregator 数据源。
  b. “Data Aggregator 管理 UI”打开。
  c. 从菜单中选择“系统状态”、“Data Collectors”。
  d. 查找要移动和标记其 ID 的 Data Collector 组件。
- 打开 Web 浏览器并发出下列 Web 服务调用：

  `http://DA_hostname:port/rest/dcms`

  DA_hostname:port

  指定 Data Aggregator 主机名和端口号。

  默认端口：8581

  查找其 HostName 和 IPAddress 与要移动的 Data Collector 匹配的 <DataCollectionMgrInfo> 部分。标记 <DcmID> 的值。

下一步，停止当前主机上的 Data Collector 服务。

停止 Data Collector

将 Data Collector 移至其他主机之前停止当前主机上的 Data Collector 服务。

请执行以下步骤：

1. 如果已为此 Data Collector 安装了设备包，请执行以下步骤。如果没有安装设备包，请继续进行步骤 2。
   a. 以具有管理员角色的用户身份登录到 CA Performance Center。
   b. 选择“管理”，然后从菜单中选择 Data Aggregator 数据源。

      “Data Aggregator 管理 UI”打开。
   c. 从“监视配置”菜单中选择“EMS 集成配置文件”。
   d. 右键单击与此 Data Collector 主机关联的配置文件，并且选择“停止”。执行与此 Data Collector 主机相关的每个 EMS 配置文件的步骤。
   e. 通过运行此命令存档 CA Mediation Manager 印证码：

      ```
      tar -zcvf filename
      /opt/IMDataCollector/apache-karaf-{n.n.n}/MediationCenter
      ```

      filename

      指定存档文件的名称。

      注意：此存档文件稍后将移动到新的 Data Collector 主机。
2. 登录到 Data Collector 主机并运行以下命令：

   ```
   /etc/init.d/dcmd stop
   ```
3. 确认 Data Collector 已经停止：
   a. 以具有管理员角色的用户身份登录到 CA Performance Center。
   b. 选择“管理”，然后从菜单中选择 Data Aggregator 数据源。
   c. 从菜单中选择“系统状态”、“Data Collectors”。
   d. 验证 Data Collector 状态显示“不连接”。

下一步，在新的主机上安装 Data Collector。

在其他主机上安装 Data Collector

停止旧主机上的 Data Collector 服务之后，在新的主机上安装 Data Collector。将来自旧主机的 Data Collector 数据在此程序期间导出到新主机。

请执行以下步骤：

1. （仅针对与 CA Mediation Manager 的集成）迁移设备包。在旧的 Data Collector 主机上，以 -t 标志运行 *$CAMM_HOME*/tools/migratePMtoCAMM 脚本。

   此步骤假定，您在安装了本地控制器的 Data Collector 服务器上运行脚本。您还必须在其他服务器上运行 CA Mediation Manager 控制台。

   注意：迁移的设备包将以 .zip 文件的形式复制到 *$CAMM_HOME*/MigratedIMDevicepacks。有关迁移设备包的详细信息，请参阅“如何迁移设备包”方案。

2. 登录到新的主机系统并打开命令 shell 会话。
3. 通过运行此命令，使用先前复制的 ID 设置环境变量：

   `export DCM_ID=`*`data collector id`*

4. 从同一会话，通过运行 **install.bin** 二进制文件安装 Data Collector。
5. 在同一服务器上安装 CA Mediation Manager LC。
6. 如果先前曾经为此 Data Collector 安装了设备包，则请执行这些其他步骤：

   a. 将您先前使用迁移脚本创建的 zip 文件复制到该主机上的本地目录。

   b. 使用 CA Mediation Manager Web 控制台部署这些设备包并启动它们。

      注意：您 *不*需要对 Data Aggregator 主机重新部署证书包。

注意：在几个轮询周期之后，请验证数据是由新的 Data Collector 主机收集。

作为最佳实践，验证正在新的主机上收集数据之后，请卸载旧的 Data Collector 并删除关联的任何 EMS 配置文件。此最佳实践为可选。

在与 Data Collector 主机断开网络连接期间 Data Aggregator 配置发生更改

有时，Data Aggregator 主机与 Data Collector 主机之间的连接会中断，例如，当网络断开时。如果 Data Aggregator 和 Data Collector 进程在连接断开期间正在运行，则可以更改 Data Aggregator 安装的配置。在这种情况下，将根据网络断开前的配置继续对 Data Collector 主机进行轮询。Data Aggregator 与 Data Collector 主机重新建立连接后，Data Collector 将下载新配置并相应地调整轮询。

例如，您要进行以下配置更改之一：

- 更改 SNMP 供应商认证用于计算度量标准系列中的值的表达式。
- 更改度量标准系列以轮询新的可操作度量标准。

当 Data Aggregator 与 Data Collector 主机之间的连接断开时，所做的更改无法生效。重新建立连接后，Data Collector 将开始轮询在新表达式中或计算新的操作度量标准时使用的新 SNMP MIB 对象。

在 Data Aggregator IP 地址变更时配置 Data Collector

要使 Data Collector 与 Data Aggregator 进行通信，请在更改 Data Aggregator IP 地址时配置 Data Collector。

注意：如果 Data Collector 使用主机名，仅需要重新启动 Data Collector 来保持 Data Collector 和 Data Aggregator 之间的通信。只有在其使用 IP 地址与 Data Aggregator 进行通信时才配置 Data Collector。

请执行以下步骤：

1. 如果 Data Collector 正在运行，请将其停止。打开命令提示符并键入以下命令：

   ```
   /etc/init.d/dcmd stop
   ```

2. 在下列文件中编辑主机名或地址：

   ```
   /opt/IMDataCollector/apache-karaf-2.3.0/etc/com.ca.im.dm.core.collector.cfg
   ```

   编辑以下行：

   ```
   collector-manager-da-hostname
   ```

   保存文件。

3. 在下列文件中更新 IP 地址：

   ```
   /opt/IMDataCollector/apache-karaf-2.3.0/jms/local-jms-broker.xml
   ```

4. 删除以下文件：

   ```
   /opt/IMDataCollector/apache-karaf-2.3.0/deploy/local-jms-broker.xml
   ```

5. 删除缓存。打开命令提示符并键入以下命令：

   ```
   rm -rf /opt/IMDataCollector/apache-karaf-2.3.0/data/cache/*
   ```

6. 启动 Data Collector 主机。打开命令提示符并键入以下命令：

   ```
   /etc/init.d/dcmd start
   ```

7. 确保“数据收集器列表”中显示的地址正确。
   a. 以管理员身份打开 CA Performance Center。
   b. 选择“管理”、“数据源设置”，然后单击一个 Data Aggregator 数据源。
   c. 从“系统状态”菜单中单击“Data Collector”。
   d. 各个数据收集器的 IP 地址显示在‘地址’列之下。
   e. 各个数据收集器的状态是“正在收集数据”。

当 Data Aggregator 主机不可用时，Data Collector 会缓存轮询的数据

Data Aggregator 和 Data Collector 主机之间偶尔会失去网络连接。这种情况下，Data Collector 会继续轮询并在内存中缓存轮询的数据，直至达到某个可配置的限制。当 Data Aggregator 主机可用时，缓存的轮询数据将发送至 Data Aggregator。

轮询的数据将按“先入先出”顺序来处理。也就是说，最早缓存的轮询数据会先发送至 Data Aggregator。如果达到了缓存内存限制，那么所有新轮询的数据都会丢失，直到 Data Aggregator 主机变得可用并且 Data Aggregator 主机已处理 9% 的已缓存数据。

重要说明！当 Data Aggregator 不可用时，Data Collector 系统上的内存使用量会显著增加。

您的内存存储要求取决于以下因素：

- 轮询的设备和组件的数目
- 轮询速度
- 当 Data Aggregator 主机不可用时，您希望保留多少数据

缓存内存限制的默认值是最大 Data Collector 进程内存的一半。最大内存使用量是在安装 Data Collector 时或在安装之后配置的。

Data Collector 需要专用的内存量才能正常运行。在 Data Collector 以五分钟的轮询速度轮询 50,000 个设备和组件的小规模环境中，需要 2 GB 的内存以进行基本操作。在 Data Collector 以五分钟的轮询速度轮询 500,000 个设备和组件的大规模环境中，需要 24 GB 的内存以进行基本操作。剩余的内存可以用于缓存轮询的数据。

计算轮询数据缓存所需的内存

缓存轮询数据时所需的内存量取决于以下信息：

- 环境的规模。
- 当 Data Aggregator 主机不可用时，您希望保留数据的时间为多长

要计算数据缓存所需的内存量，请使用以下公式：

所需的缓存 (GB)=（用于缓存数据的时间（秒）× 已轮询项的数量）/（262144 × 平均轮询速度（秒））

示例：计算一小时内缓存已轮询数据所需的内存

- 计算在 Data Collector 以五分钟的轮询速度轮询 50,000 个设备和组件的小规模环境中需要的内存。当 Data Aggregator 不可用时，您希望缓存一小时的轮询数据：

  所需的缓存 (GB)=(3600 ×50000)/(262144 ×300)

  所需的缓存 (GB)=2.3 GB

  注意：此计算是对基本操作内存要求的补充。小规模环境的基本操作内存要求为 2 GB。因此，需要的总内存为 4608 M (2 GB + 2.3 GB)。

- 计算在 Data Collector 以五分钟的轮询速度轮询 500,000 个设备和组件的大规模环境中需要的内存。当 Data Aggregator 不可用时，您希望缓存一小时的轮询数据：

  所需的缓存 (GB)=(3600 ×500000)/(262144 ×300)

  所需的缓存 (GB)=22.9 GB

  注意：此计算是对基本操作内存要求的补充。大规模环境的基本操作内存要求为 24 GB。因此，需要的总内存为 47 GB (24 GB + 22.9 GB)。

修改数据缓存内存限制

您可以修改当 Data Aggregator 不可用时 Data Collector 缓存的数据量。

请执行以下步骤：

1. 计算数据缓存所需的内存量 (p. 36)。
2. 记下数据缓存所需的内存量。
3. 登录到安装了 Data Collector 的计算机。以 root 用户身份或对有限命令具有访问权限的 sudo 用户身份登录。

   注意：有关 sudo 用户的详细信息，请参阅 *《Data Aggregator 安装指南》*。

4. 请使用以下命令停止 Data Collector：

   ```
   service dcmd stop
   ```

5. 修改 Data Collector 的 IM_MAX_MEM 内存设置：

   a. 访问 *Data Collector 安装目录* /apache-karaf-2.3.0/jms/local-jms-broker.xml 文件。

   b. 将 IM_MAX_MEM 限制更改为步骤中所述的值的两倍。2.确认此值不超过系统上的可用 RAM。

6. 在 Data Collector 上修改 JMS 代理的缓存内存限制：

   a. 访问 *Data Collector 安装目录* /apache-karaf-2.3.0/jms/local-jms-broker.xml 文件。

   b. 查找以下行：

      ```
      <memoryUsage limit=" value" />
      ```

      value

      是当前缓存限制设置。

   c. 使用您先前计算出的值修改当前缓存限制设置并保存文件。

7. 使 Data Collector 发现对 jms/local-jms-broker.xml 文件所做的更改。键入以下命令，以部署虚假 .lock 文件。虚假 .lock 文件使 Data Collector 认为存在非正常关闭：

   ```
   echo `date` > /opt/IMDataCollector/apache-karaf-2.3.0/.lock
   ```

8. 使用以下命令重新启动 Data Collector：

   ```
   service dcmd start
   ```

   已配置缓存内存限制。

Data Repository 审核流程

审核流程每天凌晨 3 点审核数据库，以计算 Data Aggregator 数据占用的总空间。该流程使用 Vertica 功能“审核”来估计数据库的大小。在估计数据库时，不包括存储在临时表中的数据、标记为待删除但未从数据库中清除的数据，以及 Vertica 监视表中的数据。

CA Technologies 与 Vertica 之间的许可协议规定存储在 Data Repository 中的总数据量不能超过 32 TB。

要查看审核的最新结果，请在浏览器中访问以下 URL：

http://*hostname:port*/rest/datarepositorymaintenance/audit

此 URL 返回 XML。“当前大小”标记显示 Data Repository 的当前大小（字节）。

重要说明！请定期检查审核结果。如果有值大于 32 TB，您便未遵守许可协议。请联系 CA 技术支持，以获得进一步指示。

Data Repository 检测信号监视进程

检测信号监视进程检查 Data Repository 是否会每隔 10 秒启动并运行一次。如果检测信号过程无法确认数据库在 5 分钟之内启动，Data Aggregator 将关闭。*Data Aggregator installation directory*/apache-karaf-2.3.0/shutdown.log 文件中将记录审核消息。

在群集环境中，每 10 秒会检查一次群集中所有节点的可用性。如果无法在 5 分钟之内联系到节点，会生成一个事件并将该事件记录在 CA Performance Center 中的 Data Aggregator 设备上。*Data Aggregator installation directory*/apache-karaf-2.3.0/shutdown.log 文件中将记录审核消息。

如果失败的 Data Repository 节点是主节点（所有 Data Aggregator 查询都是通过该节点进行的），Data Aggregator 会自动切换到下一个可用 Data Repository 节点。将生成一个事件并将该事件记录在 Data Aggregator 设备上。

重要说明！在高可用性故障转移期间发生的特定管理功能会中断，然后失败。一个轮询周期丢失。在 Data Repository 连接到群集环境中的其他节点之后，这些功能不会恢复。在 Data Repository 连接到群集环境中的其他节点之后，您执行的管理功能将按设计的方式工作。

如果所有 Data Repository 节点在群集环境中都失败了，Data Aggregator 将关闭。

与 Data Repository 的联系中断可能会导致 Data Aggregator 丢失数据。在重新启动 Data Aggregator 之前，请解决所有连接问题或 Data Repository 问题。如果在启动时无法连接到 Data Repository，Data Aggregator 会自动关闭。为了尽量减少数据损失，Data Collector 安装将在一段时间内继续在本地收集和存储数据，直至 Data Aggregator 重新启动。

要恢复故障节点，请在 admintools 实用工具的主菜单上选择“在主机上重新启动 Vertica”选项并按提示进行操作。在故障节点上重新启动 Vertica 过程并且具有成功的网络连接之前，Data Aggregator 不会在该节点上建立检测信号。

当所选主机出现故障时选择群集中的其他主机

如果在 Data Aggregator 安装期间指定的数据库主机在运行时出现故障，Data Aggregator 则会自动关闭。如果在群集中安装了 Data Repository，请将数据库连接指向群集中的其他主机，然后再重新启动 Data Aggregator。

请执行以下步骤：

1. 打开 Data Aggregator 主机上的 *Data Aggregator installation directory*/apache-karaf-2.3.0/etc/dbconnection.cfg 文件。
2. 在 dbconnection.cfg 文件中修改以下行。修改以下行，以引用已启动且正在运行的 Data Repository 群集主机之一的主机名或 IP 地址：

   ```
   dbUrl=jdbc:vertica://database server hostname:database server port/databasename?use35CopyFormat=true&BinaryDataTransfer=false
   ```

   database server hostname*:*database server port

   表示 Data Repository 的主机名或 IP 地址以及您在 Data Aggregator 安装期间输入的 Data Repository 端口号。

   默认端口号：5433

   示例：

   如果 host2 在群集中已启动且正在运行，并且您选择的数据库连接指向 host2，则更新的 dbUrl 条目可能类似于以下行：

   ```
   dbUrl=jdbc:vertica://host2:5433/mydatabasename?use35CopyFormat=true&BinaryDataTransfer=false
   ```

3. 保存 dbconnection.cfg 文件。
4. 要重新启动 Data Aggregator，请键入以下命令：

   ```
   /etc/init.d/dadaemon start
   ```

5. 要确信 Data Aggregator 仍然没有运行，请键入以下命令：

   ```
   Ps -ef | grep java | grep -v grep
   ```

   如果 Data Aggregator 未运行，Data Aggregator 进程不会返回。

   此时数据库连接将指向该群集中的指定主机。

如果 Data Repository 群集中的多个主机出现故障，Data Repository 和 Data Aggregator 将自动关闭。Data Repository 群集只能断开一个主机。

如果群集中的在 Data Aggregator 安装期间*未*指定的的单个主机与网络断开（例如，因为设置了防火墙，或以太网线被拔掉），Data Aggregator 便会关闭。如果您在 Data Aggregator 安装期间设置了 Data Aggregator 进程的自动恢复，Data Aggregator 便会自动重新启动。一旦脱机主机可用，请将该主机返回到该群集中。在 admintools 实用工具的主菜单上选择“在主机上重新启动 Vertica”选项并按提示进行操作。

注意：有关设置 Data Aggregator 进程的自动恢复的信息，请参阅《*Data Aggregator 安装指南*》。

如果通过 admintools 实用工具“高级”菜单上的“在主机上取消 Vertica 过程”选项停止了在 Data Aggregator 安装期间*未*指定的群集中的单个主机，Data Aggregator 会继续工作。一旦脱机主机可用，请将该主机返回到该群集中。在 admintools 实用工具的主菜单上选择“在主机上重新启动 Vertica”选项并按提示进行操作。

修改安装后的 Data Aggregator 和 Data Collector 组件的最大内存使用量（可选）

Data Aggregator 和 Data Collector 组件的默认最大内存使用量不足。要在大规模部署中有效运行，请修改 Data Aggregator 和 Data Collector 的最大内存使用量。可以在安装过程中或之后进行这种修改。默认情况下，Data Aggregator 和 Data Collector 的内存使用量为 2 GB。

重要说明！在此过程中对内存所做的修改假定 Data Aggregator 和 Data Collector 安装在不同的计算机上。此过程还假定这些计算机专门用于安装上述组件。

请执行以下步骤：

1. 打开控制台并键入以下命令：

   ```
   more /proc/meminfo
   ```

   此时将显示总内存使用量。

2. 请记下这一总内存值。

3. 执行以下步骤修改 Data Aggregator 的最大内存量：
   a. 访问 *Data Aggregator installation directory*/apache-karaf-2.3.0/bin/setenv 文件。
   b. 对于大规模部署环境，修改 IM_MAX_MEM=*number unit* 行。

      number unit

      表示最大内存量。*number* 为正整数，而 *unit* 为“G”或“M”。从您之前记下的总内存中减去 2 G，并在此处输入。2 GB 专供其他操作系统操作使用。

      例如：33544320 KB - 2G = 30 GB

      IM_MAX_MEM=30G

      例如：

      IM_MAX_MEM=4G

   c. 保存文件。
   d. 使用以下命令重新启动 Data Aggregator：

      ```
      service dadaemon start
      ```

      Data Aggregator 将启动并自动与 CA Performance Center 进行同步。

   e. 为了使内存设置更改在 Data Aggregator 升级期间保持不变，请修改 /etc/DA.cfg 文件，即替换属性 "da.memory" 的更新值。

      例如：

      ```
      da.memory=4G
      ```

4. 执行以下步骤修改所有 Data Collector 主机的最大内存量：
   a. 访问 *Data Collector installation directory*/apache-karaf-2.3.0/bin/setenv 文件。
   b. 对于大规模部署环境，修改 IM_MAX_MEM=*number unit* 行。

      number unit

      表示最大内存量。*number* 为正整数，而 *unit* 为“G”或“M”。从您之前记下的总内存中减去 2 G，并在此处输入。2 GB 专供其他操作系统操作使用。

      例如：33544320 KB - 2G = 30 GB

      IM_MAX_MEM=30G

      例如：

      IM_MAX_MEM=4G

c. 保存文件。

d. 使用以下命令重新启动 Data Collector 主机：

```
service dcmd start
```

e. 为了使内存设置更改在 Data Collector 升级期间保持不变，请修改 /opt/DCM.cfg，即替换属性“IM_MAX_MEM”的更新值。

例如：

```
IM_MAX_MEM=4G
```

此时已针对大规模部署环境配置了最大内存量。

示例：在安装 Data Aggregator 后为 Data Aggregator 配置最大内存使用量

以下示例将配置 Data Aggregator 的最大内存使用量，其中总内存为 3354432 KB：

1. 打开控制台并键入以下命令：

   ```
   more /proc/meminfo
   ```

   此时将显示以下结果：

   ```
   MemTotal: 33554432KB
   ```

2. 计算大规模部署环境所需要的最大内存量：

   公式：总内存 - 2 G = 适用于大规模部署环境的最大内存量

   解决方案：3354432 KB - 2G = 30G

3. 访问 *Data Aggregator installation directory*/apache-karaf-2.3.0/bin/setenv 文件。

4. 对于大规模部署环境，修改 IM_MAX_MEM=*number unit* 行：

   IM_MAX_MEM=30G

5. 保存文件。

6. 重新启动 Data Aggregator。

   此时已针对大规模部署环境修改了最大内存量。

安装后修改外部 ActiveMQ 存储限制 （可选）

Data Aggregator 安装程序计算系统容纳 ApacheMQ 进程所需的内存。但是，您可以手动修改内存限制设置，以便在您的 Data Aggregator 系统上微调 ActiveMQ。例如，您可以在下列情况下修改设置：

- 系统内存已经更改。
- Data Collector 系统的数目已经更改。
- 优化内存设置。
- 通过 ActiveMQ 度量标准监控 JConsole 或 CA 性能管理 自定义图表，已确定 ActiveMQs 性能降级。

请执行以下步骤：

1. 基于以下设置计算 ActiveMQ 的内存量：

   最大 Java 堆大小

   此值默认设为 20% 系统内存。最小值为 512M。

   初始的最小 Java 堆大小

   此值应是最大 Java 堆大小的 50%。

   所有消息的内存限制

   此值应是最大 Java 堆大小的 50%。

   每个队列的内存限制

   应根据您有的 Data Collector 安装数量计算此值。

   示例：每个队列的内存

   （所有消息的系统内存）/5/（Data Collector 计数）

2. 登录到安装了 Data Aggregator 的计算机。以 root 用户身份或对有限命令具有访问权限的 sudo 用户身份登录。

   注意：有关 sudo 用户的详细信息，请参阅 *《Data Aggregator 安装指南》*。

3. 键入以下命令以停止 ActiveMQ 代理：

   ```
   /etc/init.d/activemq stop
   ```

4. 修改 Java 堆大小以适合 ActiveMQ：

   a. 访问 broker/apache-activemq-*version*/bin 下的 **activemq** 文件。

   b. 找到定义 ACTIVEMQ_OPTS_MEMORY 的行。

   c. 将 -Xms 更改为初始最小 Jjava 堆大小。

d. 将 -Xmx 更改为最大 Java 堆大小。

e. 保存文件。

5. 为生产方数据流控制修改 ActiveMQ 内存限制：

a. 在 *Data Aggregator 安装目录的* /broker/apache-activemq-*version*/conf 文件中访问 activemq.xml 文件。

b. 找到下列行，并且将所有消息的值更改为“内存限制”：

```
<memoryUsage limit=" value" />
```

c. 找到下列行，将每个队列的值更改为“内存限制”：

```
<policyEntry queue=">" producerFlowControl="true"
memoryLimit="value"/>
```

注意：有关详细信息，请参阅 http://activemq.apache.org/producer-flow-control.html http://activemq.apache.org/producer-flow-control.html。

6. 键入以下命令以启动 ActiveMQ 代理：

```
./etc/init.d/activemq start
```

您的新设置已激活。

数据保留管理

Data Repository 的数据保留率是可管理的。设置 Data Repository 中的默认数据保留率，为大多数用户节省磁盘空间和改进报告功能。默认情况下，每 5 分钟就会为给定设备生成轮询数据，而且此数据表示产品内可用的最精细数据。将此类原始轮询数据设置为每小时间累加一次。累加数据是轮询值的聚合，可在报告中提供一个更高层次且更为简略的视图。每日累加和每周累加的保留时间大于轮询数据或每小时数据的保留时间，因为它们需要的存储磁盘空间更少。

不过，您可以更改 Data Repository 对于轮询数据、每小时累加数据、每日累加数据和每周累加数据的保留率。例如，您可以将轮询的数据保留值更改为 30 天以节省磁盘空间。寻找最适合需求和环境的平衡。

注意：有关如何更改数据保留率的信息，请参阅*《REST Web 服务指南》*。

默认情况下，数据在 Data Repository 中保留以下天数：

- 轮询的数据：45 天

  注意：如果您从 Data Aggregator 的以前版本升级到此版本，轮询数据保留期将仍为以前的默认值 10 天。

- 每小时累加数据：90 天
- 每日累加数据：365 天
- 每周累加数据：730 天

Data Repository 可以保留数据的最短天数如下所示：

- 轮询的数据：2 天
- 每小时累加数据：8 天
- 每日累加数据：31 天
- 每周累加数据：366 天

第 2 章： 重新启动组件服务

此部分包含以下主题：

停止并重新启动 Data Aggregator

在某些情况下，您必须停止并重新启动 Data Aggregator。例如，Data Aggregator 主机的操作系统需要升级时。停止 Data Aggregator，执行所需的操作，然后重新启动 Data Aggregator。Data Aggregator 随后将恢复处理。

Data Aggregator 计划停机期间，Data Aggregator 关闭之前收到的所有轮询数据将发送到 Data Repository。此轮询数据将得到保留，以便在报告时使用，或者用于其他用途。

当您计划停止 Data Aggregator 时，请考虑以下关于数据加载、累加和事件阈值处理的信息：

- 当前轮询周期内从 Data Collector 组件接收的所有数据已在 Data Aggregator 停止前处理完毕。数据未丢失。
- 如果在关闭时阈值事件处理已启动，则允许先处理完从 Data Collector 组件接收的数据处理，然后再停止 Data Aggregator。
- 阈值事件处理将在重新启动 Data Aggregator 后恢复。
- 如果在关闭时累加处理已启动，则允许先累加处理完所有从 Data Collector 主机收集的数据，然后再停止 Data Aggregator。
- 累加处理将在重新启动 Data Aggregator 后恢复。

Data Aggregator 可能会出现计划外停机，如安装了 Data Aggregator 的计算机发生断电时。在这种情况下，Data Aggregator 将突然停止。在这种情况下，已轮询的数据和阈值事件信息可能会丢失。Data Aggregator 重新启动时，将恢复从 Data Collector 主机加载排队数据。排队数据的事件阈值处理和累加处理也将在 Data Aggregator 重新启动时恢复。

请执行以下步骤：

1. 登录到安装了 Data Aggregator 的计算机。以 root 用户身份或对有限命令具有访问权限的 sudo 用户身份登录。

   注意：有关 sudo 用户的详细信息，请参阅 *《Data Aggregator 安装指南》*。

2. 打开命令提示符并执行以下步骤：

   a. 如果您以根用户身份登录，请键入以下命令：

      ```
      service dadaemon stop
      ```

   b. 如果您以 sudo 用户身份登录，请键入以下命令：

      ```
      sudo service dadaemon stop
      ```

   如果在 Data Aggregator 停止时 Data Collector 正在运行并进行轮询，轮询将继续进行。Data Collector 将对轮询的数据进行排队，以便将来交付给 Data Aggregator。

3. 重新部署计算机，或执行任何其他管理任务。

4. 登录到安装了 Data Aggregator 的计算机。以 root 用户身份或对有限命令具有访问权限的 sudo 用户身份登录。

   注意：如果您以 sudo 用户身份安装了 Data Aggregator，则要为 /etc/init.d/dadaemon 命令设置 sudo 命令别名。使用 sudo 命令来运行 dadaemon 启动脚本。有关 sudo 用户的详细信息，请参阅 *《Data Aggregator 安装指南》*。

5. 打开命令提示符并键入以下命令：

   ```
   service dadaemon start
   ```

   Data Aggregator 将启动并自动与 CA Performance Center 进行同步。

当 Data Aggregator 启动时，会将 Data Collector 主机上所有排队的轮询数据发送给 Data Aggregator。如果排队的数据超过 Data Collector 系统上配置的磁盘空间限制，将丢弃最新的数据。因此，轮询的报告数据中有缺口。

停止并重新启动 Data Collector

在某些情况下，您必须停止并重新启动 Data Collector。例如，安装了 Data Collector 的计算机可能会断电或锁定。或者，想要重新部署计算机。在这种情况下，需要停止并重新启动 Data Collector。如果您要安装操作系统补丁程序，请停止并启动 Data Collector。

请执行以下步骤：

1. 登录到安装了 Data Collector 的计算机。以 root 用户身份或对有限命令具有访问权限的 sudo 用户身份登录。

   注意：有关 sudo 用户的详细信息，请参阅 *《Data Aggregator 安装指南》*。

2. 打开命令提示符并执行以下步骤：

   a. 如果您以根用户身份登录，请键入以下命令：

      ```
      service dcmd stop
      ```

   b. 如果您以 sudo 用户身份登录，请键入以下命令：

      ```
      sudo service dcmd stop
      ```

   Data Collector 停止后，所有正在进行的轮询都将停止。不得运行任何发现。

3. 重新部署计算机，或执行任何其他管理任务。

4. 通过登录到安装了 Data Collector 的计算机启动 Data Collector。以 root 用户身份或对有限命令具有访问权限的 sudo 用户身份登录。

   注意：如果您以 sudo 用户身份安装了 Data Collector，则要为 /etc/init.d/dcmd 命令设置 sudo 命令别名。使用 sudo 命令来运行 dcmd 启动脚本。有关 sudo 用户的详细信息，请参阅 *《Data Aggregator 安装指南》*。

5. 打开命令提示符并键入以下命令：

   ```
   service dcmd start
   ```

   Data Collector 重新启动后，将恢复排定的轮询。可以恢复运行发现。Data Collector 将自动与 CA Performance Center 重新同步。

详细信息：

启用承租方 (p. 95)

停止并重新启动 Data Repository

在某些情况下，您必须停止并重新启动 Data Repository。例如，安装了 Data Repository 的计算机可能会断电或锁定。或者，想要重新部署计算机。在这种情况下，需要停止并重新启动 Data Repository。如果要安装操作系统补丁程序或要升级到新版的 Data Repository，请停止并重新启动 Data Repository。

请执行以下步骤：

1. 登录到安装了 Data Aggregator 的计算机。以 root 用户身份或对有限命令具有访问权限的 sudo 用户身份登录。

   注意：有关 sudo 用户的详细信息，请参阅 *《Data Aggregator 安装指南》*。

2. 打开命令提示符并键入以下命令：

   ```
   service dadaemon stop
   ```

3. 以数据库管理员用户（而*非* root 用户）身份登录到 Data Repository 所用的数据库服务器。

4. 键入以下命令：

   ```
   /opt/vertica/bin/adminTools
   ```

   此时将打开“Administration Tools”（管理工具）对话框。

5. 选择“(4) Stop Database”（(4) 停止数据库）。

6. 按数据库名称旁边的空白条，选择“确定”，然后按 Enter 键。

   系统将提示您输入数据库密码。

7. 输入数据库密码并按下 Enter 键。

   Data Repository 将停止。

   注意：如果 Data Repository 未停止，从“(7) Advanced Tools”（(7) 高级工具）菜单中选择“(2) Stop Vertica on Host”（(2) 停止主机上的 Vertica）。

8. 选择“退出”，然后按 Enter 键。

9. 重新部署计算机，或执行任何其他管理任务。

10. 以数据库管理员用户（而*非* root 用户）身份登录到 Data Repository 所用的数据库服务器。

11. 键入以下命令：

    ```
    /opt/vertica/bin/adminTools
    ```

    此时将打开“Administration Tools”（管理工具）对话框。

12. 选择 (3)“启动数据库”。

13. 按数据库名称旁边的空白条，选择**“确定”**，然后按 Enter 键。

    系统将提示您输入数据库密码。

14. 输入数据库密码并按下 Enter 键。

    数据库启动。

15. 选择 (E)“退出”并按 Enter 键。

16. 通过登录到安装了 Data Aggregator 的计算机启动 Data Aggregator。以 root 用户身份或对有限命令具有访问权限的 sudo 用户身份登录。

    如果您以 sudo 用户身份安装了 Data Aggregator，则要为 service dadaemon 命令设置 sudo 命令别名。使用 sudo 命令来运行 dadaemon 启动脚本。

    注意：有关 sudo 用户的详细信息，请参阅 *《Data Aggregator 安装指南》*。

17. 打开命令提示符并且键入以下命令：

    ```
    service dadaemon start
    ```

    Data Repository 重新启动。

停止并重新启动 ActiveMQ 代理

如果 Data Aggregator 检测到 ActiveMQ 相关问题并且 Data Aggregator 无法成功重启代理，请重启 Apache ActiveMQ 代理。如有必要，您也可以手动停止并重新启动服务。

请执行以下步骤：

1. 从命令行打开以下目录：
   `cd da_install_dir/broker/apache-activemq-version/bin`

   da_install_dir

   指定 Data Aggregator 安装目录的位置。

   apache-activemq-*version*

   指定 Apache ActiveMQ 的版本。

   示例：apache-activemq-5.5.1b

2. 运行 stop 命令：

```
./activemq stop –jmxurl
service:jmx:rmi:///jndi/rmi://localhost:11099/jmxrmi
--jmxuser admin --jmxpassword activemq da_broker
```

–jmxurl service:jmx:rmi:///jndi/rmi://localhost:11099/jmxrmi

指定 ActiveMQ 代理的位置。此位置仅在用户修改端口或用户将代理外部化到其他系统时更改。

注意：支持修改端口号，但是不支持外部化该代理。

--jmxuser admin

指定关闭服务的用户名。

默认值： admin

--jmxpassword activemq

指定关闭服务的密码。

默认值： activemq

da_broker

指定将关闭的代理名称。

默认值： da_broker

3. 运行 start 命令：

```
./activemq start
```

第 3 章： 发现您的网络

此部分包含以下主题：

设备发现

*发现*是 Data Aggregator 发现和建模 IT 基础架构的过程。

发现过程进行以下操作：

- 确认设备回应的协议。Data Aggregator 始终确定设备是否能够回应 SNMP。如果选择 ICMP，Data Aggregator 将首先确定设备是否能够回应 ICMP。如果设备*确实*回应 ICMP，则 Data Aggregator 将确定设备是否能够回应 SNMP。如果设备*不*响应 ICMP，Data Aggregator 将确认设备不响应 SNMP。
- 检索所发现的每台设备的最少量信息，这些信息足以对此此设备进行分类，并将其添加到相应的设备集合中。

您可以使用两种方式来在 Data Aggregator 中发现设备：

- 您可以使用您在 Data Aggregator 中创建的发现配置文件发现您的基础架构环境中的特定设备。按照发现工作流，使用此方式管理设备。 (p. 54)
- 您可以发现来自 CA Performance Center 的设备 (p. 72)。

发现工作流

以下工作流提供一个最佳实践，该最佳实践可在执行清单发现时用作快速参考。

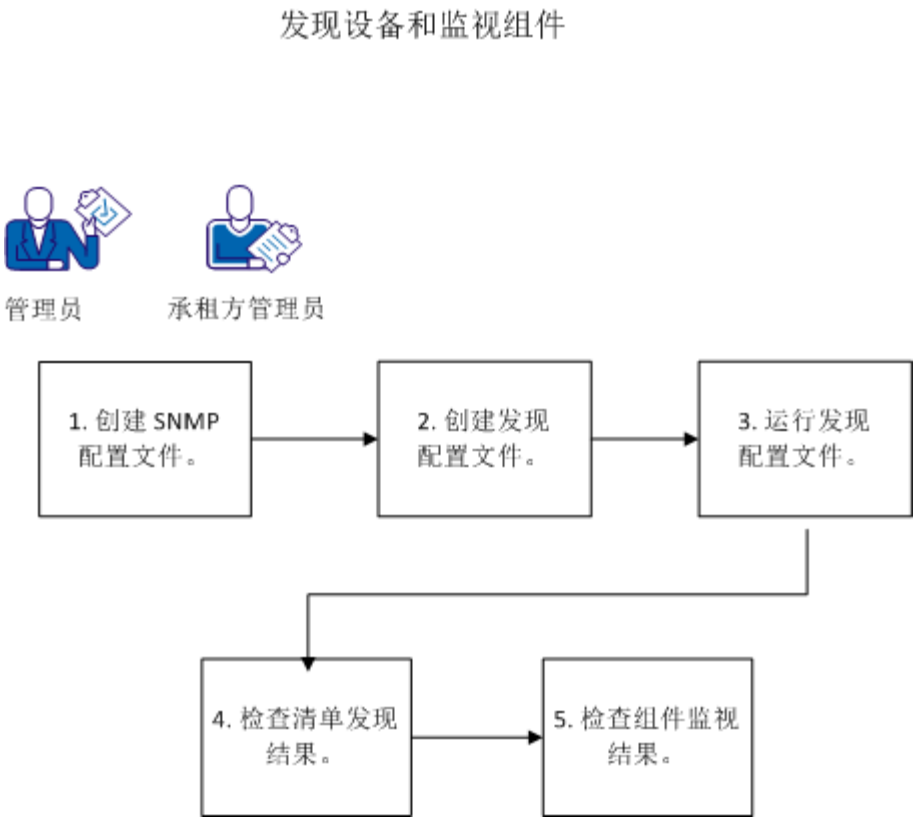
以具有管理员角色的用户身份或以承租方管理员身份执行此过程。

1. 如果您希望 Data Collector 对使用 SNMP 的设备 MIB 表执行查询，请在执行发现之前，在 CA Performance Center 中创建 SNMP 配置文件。

   注意：要将 SNMP 配置文件应用到承租方，必须由具有承租方管理员角色的用户在承租方空间*创建*该 SNMP 配置文件。有关创建 SNMP 配置文件的详细信息，请参阅 *《CA Performance Center 管理员指南》*。

2. 从 Data Aggregator 管理页面创建一个或多个发现配置文件 (p. 60)。
3. 运行一个或多个发现配置文件 (p. 67)。发现可按排定运行，也可手工运行。
4. 复查发现结果。
5. 审核组件监视结果 (p. 87)。使用这些结果来确定如何管理设备和组件。

此示意图展示了发现过程：



详细信息：

设备发现 (p. 53)

SNMP 配置文件

SNMP 配置文件是包含特定信息的定义，Data Collector 在对使用 SNMP 的设备 MIB 表进行查询时需要使用这些信息。Data Collector 可以与支持 SNMPv1、SNMPv2c 和 SNMPv3 的设备进行通信。团体字符串和凭据在 CA Performance Center 中存储时以及发送到 Data Aggregator 和 Data Collector 时，都会进行加密。

重要说明！使用 SNMPv3 团体名称时，CA 性能管理 要求任何身份验证密码或隐私密码的长度都要大于八个字符。如果为其配置的密码长度少于八个字符，SNMPV3 配置文件可能无法与设备成功地进行通信。

Data Collector 在清单发现期间使用 SNMPv1/SNMPv2c 和 SNMPv3 配置文件来确定在访问设备时要使用的凭据。CA Performance Center 会维护此配置文件列表。每个配置文件将进行分级，以便在访问设备时使用。在发现期间，针对设备的访问权限，将尝试每个配置文件。系统将使用可访问某一设备且分级最高的配置文件。

您可以在 CA Performance Center 中创建 SNMP 配置文件，并可以更改 SNMP 配置文件分级。在以下情况下，SNMP 配置文件的新分级列表将生效：

- 发现了新设备。
- 至少有两个轮询周期无法通过 SNMP 访问某个现有设备。
- 从 CA Performance Center 中删除了设备正在使用的 SNMP 配置文件。

否则，已经成功轮询的设备将继续使用现有 SNMP 配置文件，而不管您对 SNMP 配置文件的分级列表进行了何种更改。

注意：如果 SNMPv1/SNMPv2c 配置文件是可访问某一设备的排位最高的配置文件，并且该设备可使用 SNMPv1 和 SNMPv2c 进行访问，Data Collector 将使用 SNMPv2c 与该设备进行通信。

我们通过测试 Data Collector，确定了使用各种 SNMPv3 协议时增加的 CPU 负载。我们发现，与 SNMPv1 相比，SHA /AES 对 CPU 使用率的影响适中 (< 30%)。结果表明，MD5/DES、SHA/DES 和 SHA/3DES 对 CPU 使用率的影响较大 (> 30%)。

注意：执行该测试的服务器具有内置于 CPU 中的某些 AES 功能。

如果在环境中添加额外的 CPU 核心，Data Collector 可以平衡 CPU 负载。

您可以在 CA Performance Center 用户界面中或使用 CA Performance Center REST Web 服务创建 SNMP 配置文件。创建 SNMP 配置文件之后，它们将立即与 Data Aggregator 进行同步，并可供清单发现使用。

注意：有关创建 SNMP 配置文件的详细信息，请参阅 *《CA Performance Center 管理员指南》*和 *《CA Performance Center REST Web 服务指南》*。

运行发现之后，您可以访问“发现历史”视图来查看所使用的 SNMP 配置文件的列表以及设备所响应的排位最高的 SNMP 配置文件。

详细信息：

查看发现结果 (p. 70)

发现和轮询

*发现*是 Data Aggregator 发现和建模 IT 基础架构的过程。

发现过程进行以下操作：

- 根据您创建发现配置文件时选择的协议来确认设备响应的协议。例如，假定您选择了所有协议（SNMP 和 ICMP），则需要执行以下步骤。Data Aggregator 确定设备是否能够响应 ICMP。然后确定设备是否可以响应 SNMP。如果设备*不*响应 ICMP，Data Aggregator 将确认设备不响应 SNMP。
- 检索所发现的每台设备的最少量信息，这些信息足以对此此设备进行分类，并将其添加到相应的设备集合中。

清单发现是 Data Aggregator 标识网络上设备的过程。设备将使用您在发现配置文件中指定的 IP 域、IP 地址、IP 范围以及主机名来标识。具体来说，清单发现确定设备是否可管理（是否可通过 ping 命令连接上以及是否支持 SNMP），并且确定其分类（路由器、交换机等）。清单发现还确定供应商（Cisco、Juniper 等），并且确定类型（7700、8200 等）。

在此过程中发现的设备将自动添加到即用型设备集合中，具体取决于控制各设备集合成员身份的规则。您也可以在 CA Performance Center 中创建自定义设备集合，这些集合可在发生同步时在 Data Aggregator 中创建相应的自定义设备集合。在发现设备*后*与 CA Performance Center 的首次同步过程中，会根据为这些设备集合定义的规则将设备添加到自定义设备集合中。

注意：有关创建自定义设备集合并将其与 Data Aggregator 同步的更多信息，请参阅《*CA Performance Center 管理员指南*》。

组件监视是单独的过程。监视过程涉及特定设备组件（如 CPU、内存和接口）的各种操作数据的收集和分析。所有描述如何完成监控过程的信息都包含在您分配给设备集合的监视配置文件中。

监视配置文件与设备集合的关系主导组件监控。可以通过以下方式触发组件监视：

- 监视配置文件被分配给给定设备所属的设备集合。
- 设备被添加到已分配监视配置文件的设备集合。
- 对分配给设备集合的监视配置文件进行编辑，以包括要监视的新的度量标准。如果以前没有为该设备监视该组件，则会为该监视配置文件相连的集合中的每个设备自动监视与该度量标准系列关联的组件。
- 为监视配置文件中轮询的现有度量标准系列添加新的供应商认证。
- 监视配置文件指定变更检测率，并使“自动更新度量标准系列”选中。
- 您单击“受监视设备”视图的“轮询的度量标准系列”选项卡上的“更新度量标准系列”按钮。

*度量标准系列*定义要为给定技术收集和报告的值的集合。这些值已进行标准化处理，因此无论数据源为何，报告都是统一的。当包含在监视配置文件中时，度量标准系列决定要为与监视配置文件关联的设备收集哪些值。

轮询在清单发现和组件监视完成后自动开始。在已发现设备及其受监视组件上将轮询操作度量标准和配置数据。轮询的可操作度量标准和配置数据取决于您在监视配置文件中指定的度量标准系列。系统将定期收集和保留可操作度量标准，以便在报告中使用。可操作度量标准示例包括错误率、每日基准、每小时基准和端口性能。配置数据表示或标识一个组件或组件配置。

配置数据示例包括：

ifNumber

一个 MIB 变量，用于告知 Data Aggregator 某一设备拥有的端口数。

ifStackLastChange

一个 MIB 变量，用于表示接口堆栈表是否有更改。

已发现设备和受监视组件通常需要不超过 5 分钟的时间与 CA Performance Center 同步。同步进行的过程中发现和监视的设备和组件将在当前同步完成后进行同步。

详细信息：

查看受监视设备 (p. 87)
如何管理变更检测 (p. 97)

在 VMware 环境中发现和轮询

除了网络设备之外，您还可以发现并监视 VMware 虚拟机和 ESX 主机。虽然 VMware 设备和组件表现得就像物理组件一样，但发现和监控那些设备和组件的过程也不同于容纳 vCenter 的数据收集。虽然可以直接使用 SNMP 发现 VM 和 ESX 主机，但也可以通过 vCenter Server Application Insight Module (VCAIM) 收集 vCenter 数据。

您可以在 VMware 环境中发现 ESX 主机和虚拟机。

在清单发现期间，Data Aggregator 以下列方法识别 ESX 主机和虚拟机：

- 通过 ICMP
- 通过 SNMP（如果服务器部署 SNMP 代理）
- 通过服务器发现（运行带有 VCAIM 的 systemEdge）

虽然每个 ESX 主机和虚拟机可以通过 ICMP、SNMP 和 vCenter 被多次识别，但只创建一个设备。此设备表示 ESX 主机或虚拟机。

创建了 ESX 和 VM 设备以后，Data Aggregator 便开始轮询任何 vCenter 特定度量标准，并且可以发现和开始轮询通过 SNMP 代理识别的更多组件。

根据度量标准数据的源，VM 和 ESX 的一些轮询由设备上的直接轮询执行，同时轮询 VCAIM 以收集其他数据。

默认情况下，在 Data Aggregator 发现您的 VMware 环境之后，每隔 15 分钟，它将监视已添加或删除或者在 ESX 主机之间 VMotion 的虚拟机。默认情况下，每隔 24 小时，Data Aggregator 也会监视已添加或删除的 ESX 主机。

发现配置文件

发现配置文件指定清单发现的运行方式。作为管理员，您可以使用 CA Performance Center 用户界面或 Data Aggregator REST Web 服务管理发现配置文件。

在发现配置文件中，您可以指定要发现设备的 IP 地址、IP 地址范围和主机名。您也可以指定 IP 域。您只能为所创建的每个发现配置文件指定一个 IP 域。将在该 IP 域之内创建新发现的设备。

多个 Data Collector 主机部署于一个 IP 域时，每个 Data Collector 都会向该设备发出发现请求。

多个 Data Collector 可以联系相同设备时，将会选择特定 Data Collector 来监控设备。基于负载平衡的算法将决定此选择。

IP 域对于监视具有重叠 IP 地址的承租方环境也是必备的。一名承租方可拥有一个或多个 IP 域。如果承租方有重叠的 IP 地址，则网络中必定有多个 IP 域。重叠的 IP 地址可通过 IP 域来处理。

IP 域可在 CA Performance Center 中创建。在执行手工或自动同步时， 当进行手工或自动同步时，Data Aggregator 将发现新的 IP 域。

发现过程尝试跨可用的 Data Collector 实例分发设备，但此过程不考虑 Data Collector 实例当前正在监视的设备。

注意：有关创建和同步 IP 域的详细信息，请参阅*《CA Performance Center 管理员指南》*。

只有创建发现配置文件的承租方空间内的用户才能访问该发现配置文件。分配给“默认承租方”空间的用户可以使用“默认承租方”空间中存在的配置文件来运行发现，并且可以查看该发现的结果。

因此，在创建发现配置文件*之前*，以正确的承租方身份登录或进行管理非常重要。

注意：有关创建和管理承租方的详细信息，请参阅*《CA Performance Center 管理员指南》*。

详细信息：

创建发现配置文件 (p. 60)
删除发现配置文件 (p. 67)
编辑发现配置文件 (p. 64)
查看发现配置文件的列表 (p. 60)
删除 IP 域 (p. 93)

查看发现配置文件的列表

通过 SNMP 和 ICMP 的发现配置文件可以配置发现在环境中的运行方式。

您可以查看发现配置文件的列表以及每个配置文件的详细信息。您可以查看发现的状态以及上次运行发现的时间。这些详细信息可帮助您了解网络的发现方式。

注意：请以承租方管理员身份登录来执行该任务。

请执行以下步骤：

1. 选择“管理”、“数据源设置”，然后单击一个 Data Aggregator 数据源。
2. 从“受监视清单”菜单中单击“发现配置文件”。

   “发现配置文件列表”页面将打开，其中显示可用发现配置文件的列表。

详细信息：

发现配置文件 IP 范围 (p. 63)
创建发现配置文件 (p. 60)
删除发现配置文件 (p. 67)
编辑发现配置文件 (p. 64)
运行按需发现 (p. 67)
对发现进行排定 (p. 68)
发现配置文件 (p. 59)
查看发现结果 (p. 70)

创建发现配置文件

您可以创建发现配置文件，以指定清单发现在环境中的运行方式。

请以承租方管理员身份登录来执行该任务。只有创建发现配置文件的承租方空间内的用户才能访问该发现配置文件。

注意：有关承租方的详细信息，请参阅*《CA Performance Center 管理员指南》*。

请执行以下步骤：

1. 导航到可用发现配置文件的列表 (p. 60)。
2. 单击“新建”。
3. 请执行以下步骤：
   a. 在“名称”字段中键入发现配置文件的描述性名称。

      注意：不允许使用单引号、双引号、反斜杠、正斜杠和 & 符号。

   b. 从预配置域列表中选择 IP 域。
4. 选择“IPs/主机”选项卡，并且进行一个或多个以下操作：
   - （可选）导航并导入 IP 地址的 CSV 文件。CSV 文件可以包含 IPv4 地址、IPv6 地址、IPv4 地址范围以及主机名的逗号分隔列表。浏览以选择文件，然后单击“打开”。

     注意：对于要应用于别名的汉字，请采用 UTF-8 格式保存 CSV 文件。
   - 在“IP 地址范围”窗口项中键入要发现设备的相应 IP 地址范围。可接受逗号分隔的值。

     注意：如果 IP 范围包括来自设备（该设备具有主机名，并且映射到该主机名的 IP 也包含在 IP 范围内）的多个 IP 地址，清单发现将始终使用该设备主 IP 地址的主机 IP。
   - 在“IP 地址列表”窗口项中键入要发现设备的相应单个 IP 地址。可接受逗号分隔的值。
   - 在“主机列表”窗口项中键入要发现设备的相应主机名。可接受逗号分隔的值。
   - 将单个 IP 地址、IP 地址范围和主机名的列表复制到剪贴板，然后通过按 Ctrl+V 将该列表粘贴到列表视图。
   - 通过选择 IP 地址、范围或主机名，然后单击“删除”，从 IP 列表删除项。
   - 通过在“搜索”字段中输入 IP 地址、范围或主机名来搜索 IP 列表中的项。要返回 IP 列表中的完整项列表，请单击 X 按钮。或者，您可以按在键盘上的"Esc"按钮。

注意：通过双击 IP 列表中的 IP 地址、范围或主机名来对其进行编辑。按 "Enter" 键保存更改。按 "Esc" 键退出编辑模式并且不保存更改。

不要包括重复的 IP 地址或主机名。如果检测到重复项，将显示一条消息，指示发现了重复项并已将其忽略。

注意：不允许使用单引号、双引号、反斜杠、正斜杠和 & 符号。

5. （可选）选择“排定”选项卡。要创建运行此发现配置文件的排定，请执行以下步骤：
   - 要创建每日排定，请从“排定间隔”下拉框中选择“按日”。选择您希望发现每天开始的时间。
   - 要创建每周排定，请从“排定间隔”下拉框中选择“每周”。选择希望发现运行的每一天。选择您希望发现开始的时间。
6. 选择 SNMP 选项卡。如果希望使用所有 SNMP 配置文件，您不需要执行任何操作。默认选择所有 SNMP 文件。要使用特定 SNMP 配置文件，请选中“使用分配的 SNMP 配置文件的特定列表”复选框。从可用的配置文件的列表中选择一个或多个 SNMP 配置文件，并且把他们移至已分配列表。使用 SNMP 配置文件的子集有助于减少网络流量。
7. 选择“高级”选项卡并执行下列步骤：
   a. （可选）更改您希望命名已发现设备的优先级。在发现期间，发现配置文件创建的任何设备项均用可用的最高优先级命名约定来命名。如果设备的 MIB 中未设置命名约定，则该命名约定不可用，并将尝试下一个优先级最高的命名约定。
   b. （可选）如果希望保存*新发现配置文件*的命名顺序，请选择“另存为默认值”选项。下次创建发现配置文件时，命名顺序将自动按您保存的顺序显示。

      即用型默认命名顺序是“系统名称”、“主机名”、“IP 地址”。
   c. 如果您希望 Data Aggregator 确定设备在发现进程中是否响应 ICMP，请选择“使用 ICMP”。选择“创建可通过 Ping 连接的设备”以便在在发现期间创建可通过 Ping 连接的设备。取消选择“使用 ICMP”可以防止创建可通过 Ping 连接的设备。取消选定这些选项后，Data Aggregator 不确定设备是否能够响应 ICMP。

      如果要保存选定的 ICMP 发现选项，请选择“另存为默认值”。您下次创建发现配置文件时，ICMP 发现选项将自动选定。
8. 单击“保存”。

   发现配置文件被创建，并显示在“发现配置文件”列表中。

详细信息：

发现配置文件 IP 范围 (p. 63)
发现工作流 (p. 54)
发现配置文件 (p. 59)

发现配置文件 IP 范围

在您创建或编辑发现配置文件时，您可以输入要发现的 IPv4 的 IP 地址范围。IPv6 地址不支持范围发现。

在发现配置文件中指定 IP 范围时，以下规则适用：

- IPv4 范围可以包含通配符 (*)。通配符表示 IP 八进制数字的完整范围：0-255。
- IPv4 范围可以包含连字符 (-)。可以在 IP 地址段低端值与高端值之间使用连字符。也可以在低端 IP 地址段的 IP 八进制数字中使用连字符。
- 如果在低端 IP 地址段的项中使用了通配符或连字符，则这些符号将无法表示高端 IP 地址。

示例：有效的 IP 范围

- 以下两个示例都尝试发现从 10.25.1.0 到 10.25.1.190 的每个 IP 地址的设备：

  ```
  10.25.1.0-10.25.1.190
  ```

  OR

  ```
  10.25.1.0-190
  ```

- 以下两个示例尝试发现从 10.25.0.0 到 10.25.255.255 之间每个 IP 地址的设备：

  ```
  10.25.*.*
  ```

  OR

  ```
  10.25.0.0 - 10.25.255.255
  ```

- 以下两个示例尝试发现从 10.25.0.3 到 10.25.0.40 之间以及从 10.25.1.3 到 10.25.1.40 之间每个 IP 地址的设备：

  ```
  10.25.0-1.3-40
  ```

  OR

  ```
  10.25.0.3 - 10.25.0.40, 10.25.1.3 - 10.25.1.40
  ```

- 以下两个示例尝试发现从 10.25.0.0 到 10.25.0.5 之间、从 10.25.1.0 到 10.25.1.5 之间等等（一直到从 10.25.255.0 到 10.25.255.5 之间）每个 IP 地址的设备：

  ```
  10.25.*.0-5
  ```

  OR

  ```
  10.25.0.0 - 10.25.0.5, 10.25.1.0 - 10.25.1.5 ... 10.25.255.0 - 10.25.255.5
  ```

示例：无效的 IP 范围

- 由于高端 IP 地址不完整，因此以下示例是无效的：

  ```
  10.25.1.0 - 10.23
  ```

- 以下示例之所以无效，原因在于如果在低端 IP 地址段的八进制数字中使用了连字符 (-)，则该符号将无法表示高端 IP 地址：

  ```
  10.25.1.0-190 - 10.25.1.255
  ```

- 以下示例之所以无效，原因在于如果在低端 IP 地址段的八进制数字中使用了通配符 (*)，则该符号将无法表示高端 IP 地址：

  ```
  10.25.*.0 - 10.25.255.255
  ```

- 以下示例之所以无效，原因在于不清楚通配符八进制数字 (1*) 表示 10.25.10-19.0 还是 10.25.10-199.0：

  ```
  10.25.1*.0
  ```

详细信息：

创建发现配置文件 (p. 60)
查看发现配置文件的列表 (p. 60)

编辑发现配置文件

您可以编辑现有的发现配置文件。

注意：请以承租方管理员身份登录来执行该任务。

请执行以下步骤：

1. 导航到可用发现配置文件的列表 (p. 60)。

2. 选择要编辑的发现配置文件，然后单击“编辑”。根据需要在每个选项卡上修改不同的字段。
3. 执行下列步骤：
   a. 在“名称”字段中键入发现配置文件的描述性名称。

      注意：不允许使用单引号、双引号、反斜杠、正斜杠和 & 符号。

   b. 从预配置域列表中选择 IP 域。

      注意：如果已基于此发现配置文件运行发现，您不能更改 IP 域。
4. 选择“IPs/主机”选项卡，并且进行一个或多个以下操作：
   - （可选）导航并导入 IP 地址的 CSV 文件。CSV 文件可以包含 IPv4 地址、IPv6 地址、IPv4 地址范围以及主机名的逗号分隔列表。浏览以选择文件，然后单击“打开”。

     注意：对于要应用于别名的汉字，请采用 UTF-8 格式保存 CSV 文件。
   - 在“IP 地址范围”窗口项中键入要发现设备的相应 IP 地址范围。可接受逗号分隔的值。

     注意：如果 IP 范围包括来自设备（该设备具有主机名，并且映射到该主机名的 IP 也包含在 IP 范围内）的多个 IP 地址，清单发现将始终使用该设备主 IP 地址的主机 IP。
   - 在“IP 地址列表”窗口项中键入要发现设备的相应单个 IP 地址。可接受逗号分隔的值。
   - 在“主机列表”窗口项中键入要发现设备的相应主机名。可接受逗号分隔的值。
   - 将单个 IP 地址、IP 地址范围和主机名的列表复制到剪贴板，然后通过按 Ctrl+V 将该列表粘贴到列表视图。
   - 通过选择 IP 地址、范围或主机名，然后单击“删除”，从 IP 列表删除项。
   - 通过在“搜索”字段中输入 IP 地址、范围或主机名来搜索 IP 列表中的项。要返回 IP 列表中的完整项列表，请单击 X 按钮。或者，您可以按在键盘上的"Esc"按钮。

   注意：通过双击 IP 列表中的 IP 地址、范围或主机名来对其进行编辑。按 "Enter" 键保存更改。按 "Esc" 键退出编辑模式并且不保存更改。

   不要包括重复的 IP 地址或主机名。如果检测到重复项，将显示一条消息，指示发现了重复项并已将其忽略。

   注意：不允许使用单引号、双引号、反斜杠、正斜杠和 & 符号。

5. （可选）选择“排定”选项卡。要创建运行此发现配置文件的排定，请执行以下步骤：
   - 要创建每日排定，请从“排定间隔”下拉框中选择“按日”。选择您希望发现每天开始的时间。
   - 要创建每周排定，请从“排定间隔”下拉框中选择“每周”。选择希望发现运行的每一天。选择您希望发现开始的时间。
6. 选择 SNMP 选项卡。如果希望使用所有 SNMP 配置文件，您不需要执行任何操作。默认选择所有 SNMP 文件。要使用特定 SNMP 配置文件，请选中“使用分配的 SNMP 配置文件的特定列表”复选框。从可用的配置文件的列表中选择一个或多个 SNMP 配置文件，并且把他们移至已分配列表。使用 SNMP 配置文件的子集有助于减少网络流量。
7. 选择“高级”选项卡并执行下列步骤：
   a. （可选）更改您希望命名已发现设备的优先级。在发现期间，发现配置文件创建的任何设备项均用可用的最高优先级命名约定来命名。如果设备的 MIB 中未设置命名约定，则该命名约定不可用，并将尝试下一个优先级最高的命名约定。
   b. （可选）如果希望保存*新发现配置文件*的命名顺序，请选择“另存为默认值”选项。下次创建发现配置文件时，命名顺序将自动按您保存的顺序显示。

      即用型默认命名顺序是“系统名称”、“主机名”、“IP 地址”。
   c. 如果您希望 Data Aggregator 确定设备在发现进程中是否响应 ICMP，请选择“使用 ICMP”。选择“创建可通过 Ping 连接的设备”以便在在发现期间创建可通过 Ping 连接的设备。取消选择“使用 ICMP”可以防止创建可通过 Ping 连接的设备。取消选定这些选项后，Data Aggregator 不确定设备是否能够响应 ICMP。

      如果要保存选定的 ICMP 发现选项，请选择“另存为默认值”。您下次创建发现配置文件时，ICMP 发现选项将自动选定。
8. 单击“保存”。

   配置文件将得到更新，含有您的更改。下次运行此发现配置文件时，将应用您的更改。

详细信息：

故障排除：发现未启动 (p. 149)
发现配置文件 (p. 59)

删除发现配置文件

如果您不再需要某个发现配置文件，则可将其删除。例如，可以删除不再使用的发现配置文件、重复的发现配置文件等。您将无法重新发现已删除发现配置文件中指定的设备。

注意：请以承租方管理员身份登录来执行该任务。

请执行以下步骤：

1. 导航到发现配置文件的列表。
2. 选择要删除的发现配置文件，然后单击“删除”。

   此时将打开确认对话框。
3. 单击“是”。

   发现配置文件即被删除。

运行按需发现

清单发现是根据添加到发现配置文件中的信息在网络中发现设备的过程。您可以运行按需发现。

尝试发现设备的操作是通过 SNMP 和 ICMP 协议执行的。如果某个设备不使用您创建的 SNMPv1/SNMPv2c 或 SNMPv3 配置文件响应 SNMP，但*却*响应 ICMP，则会创建一个可通过 ping 连接的设备。（SNMP 配置文件可以使用 CA Performance Center 用户界面或 CA Performance Center REST Web 服务创建。）

可以承租方管理员或管理员身份来完成该任务。要以管理员身份运行发现，请在运行发现之前为“默认承租方”域配置 Data Collector。

注意：有关创建 SNMP 配置文件并将其与 Data Aggregator 进行同步的详细信息，请参阅*《CA Performance Center 管理员指南》*和*《CA Performance Center REST Web 服务指南》*。

请执行以下步骤：

1. 导航到 CA Performance Center 中的发现配置文件列表 (p. 60)。
2. 选择要运行发现的一个或多个发现配置文件，然后单击“运行”。

   注意：只能在状态为“就绪”的发现配置文件上运行发现。

   此时将打开确认对话框。
3. 单击“是”。

此时将启动发现，所选的发现配置文件的“状态”列指示“正在运行”，“最后运行时间”列将更新为启动发现的时间。

注意：要使“完成百分比”列在运行发现期间进行更新，请单击“刷新”。

此时将打开确认对话框。

4. 单击“确定”。

   发现的设备添加到设备集合中，这将会启动组件监控和轮询。此时将返回到“发现配置文件”页面。

   如果发现挂起 10 分钟以上，则其将被中止。如果在 10 分钟之内未发现任何新设备，*并且*所选的发现配置文件的状态在 10 分钟之内未更改，则发现将被视为挂起。将在 Data Aggregator 设备上生成一个审核事件。

   如果未成功发现任何设备，则所选的发现配置文件的“状态”列将指示“失败”，如果至少成功发现了一个设备，则“状态”列将指示“部分失败”。

   已发现的设备和受监视组件需要不超过 5 分钟的时间与 CA Performance Center 同步。同步完成后，已发现的设备和受监视组件将显示在 CA Performance Center 的“清单”选项卡中。

5. （可选）要立即将发现的设备和受监视组件与 CA Performance Center 进行同步，请执行下列步骤：

   a. 选择“管理”、“数据源设置”，然后单击一个 Data Aggregator 数据源。

   b. 从“系统状态”菜单中单击“Data Aggregator”。

   c. 选择“Data Aggregator”，然后单击“重新同步”按钮。

详细信息：

发现工作流 (p. 54)
如何设置和激活接口筛选 (p. 113)

对发现进行排定

清单发现是根据添加到发现配置文件中的信息在网络中发现设备的过程。您可以对发现进行排定，使其按日或按周运行。

注意：您可以通过选择发现配置文件并单击“运行”来随时运行排定的发现。但是，当为某一发现配置文件排定的发现正在进行时，您不能为该发现配置文件启动按需发现。

尝试发现设备的操作是通过 SNMP 和 ICMP 协议执行的。如果某个设备不使用您创建的 SNMPv1/SNMPv2c 或 SNMPv3 配置文件响应 SNMP，但*却*响应 ICMP，则会创建一个可通过 ping 连接的设备。（SNMP 配置文件可以使用 CA Performance Center 用户界面或 CA Performance Center REST Web 服务创建。）

要以管理员身份运行发现，请在排定发现之前为“默认承租方”域配置 Data Collector。

注意：有关创建 SNMP 配置文件并将其与 Data Aggregator 进行同步的详细信息，请参阅*《CA Performance Center 管理员指南》*和*《CA Performance Center REST Web 服务指南》*。

请执行以下步骤：

1. 导航到 CA Performance Center 中的发现配置文件列表 (p. 60)。
2. 执行下列步骤之一：
   - 选择一个要排定发现的现有发现配置文件，然后单击“编辑”。

     此时将打开“编辑发现配置文件”页面。
   - 单击“新建”，创建一个要排定发现的发现配置文件。

     此时将打开“发现配置文件”对话框。
3. 要创建运行此发现配置文件的排定，请执行以下步骤之一：
   - 要创建每日排定，请从“排定间隔”下拉框中选择“每日运行”，然后选择每天希望运行发现的时间。
   - 要创建每周排定，请从“排定间隔”下拉框中选择“每周运行”，并选择希望运行发现的每一天，然后选择希望运行发现的时间。

   注意：从“排定”下拉框中选择“无”可删除排定。
4. 单击“保存”。

   排定发现后，发现配置文件的“状态”列指示“已排定”，并显示下一排定的运行时间。

   排定的发现启动时，所选的发现配置文件的“状态”列指示“正在运行”，“最后运行时间”列将更新为启动发现的时间。

   注意：要使“完成百分比”列在运行发现期间进行更新，请单击“刷新”。

   发现的设备添加到设备集合中，这将会启动组件监控和轮询。此时将返回到“发现配置文件”页面。

如果发现挂起 10 分钟以上，则其将被中止。如果在 10 分钟之内未发现任何新设备，*并且*所选的发现配置文件的状态在 10 分钟之内未更改，则发现将被视为挂起。将在 Data Aggregator 设备上生成一个审核事件。

如果未成功发现任何设备，则所选的发现配置文件的“状态”列将指示“失败”，如果至少成功发现了一个设备，则“状态”列将指示“部分失败”。

已发现的设备和受监视组件需要不超过 5 分钟的时间开始与 CA Performance Center 同步。同步完成后，已发现的设备和组件将显示在 CA Performance Center 的“清单”选项卡中。

5. （可选）要立即将发现的设备和组件与 CA Performance Center 进行同步，请执行下列步骤：
   a. 选择“管理”、“数据源设置”，然后单击一个 Data Aggregator 数据源。
   b. 从“系统状态”菜单中单击“Data Aggregator”。
   c. 选择“Data Aggregator”，然后单击“重新同步”按钮。

查看发现结果

您可以查看在特定发现实例中发现的可通过 ping 连接 (ICMP) 且可管理 (SNMP) 的新设备数的摘要。您也可以查看有关这些已发现设备的具体详细信息，包括 IP 地址、型号、类型、供应商名称、位置以及所使用的协议。

发现结果也会指示找到了现有设备。同一或不同的发现配置文件之前已经发现了这些现有设备。要查看现有设备，请使用“未更改”筛选。显示不同 IP 地址的现有设备表示这些设备之前已被发现，并且正在使用不同的 IP 地址进行监视。

这种行为非常常见，而且也在意料之中，因为许多设备可以响应多个 IP 地址。Data Aggregator 为每台设备维护完整的 IP 地址集，并且将它们全部提供给 CA Performance Center。

请执行以下步骤：

1. 查看发现配置文件列表 (p. 60)。
2. 要查看一个发现配置文件的发现结果，选择该发现配置文件，然后单击“历史”按钮。

   注意：当还没有为所选择的发现配置文件运行发现时，“历史”按钮将被禁用。

3. 选择一个发现实例（如果适用）。
4. （可选）执行下列选项之一来筛选“发现的设备”表：
   - 通过从“设备类型筛选”列表中选择要显示的设备类型并单击“应用”，可以按设备类型进行筛选。
   - 通过从“状态”列表中选择要显示的状态并单击“应用”，可以按所发现设备的状态进行筛选。
   - 通过从“设备类型筛选”列表和“状态”列表中选择相应的项并单击“应用”，可以按设备类型和状态进行筛选。

   发现结果将显示在“发现的设备”表中。“SNMP 配置文件”列将显示设备所响应的排位最高的 SNMP 配置文件。

   具体而言，“状态”列将指示下列状态之一：

   新建

   表示运行此发现配置文件时首次发现的设备。

   已更改

   表示设备类型自先前发现以来已更改。例如，先前发现的可通过 ping 连接的设备现在被发现为可管理设备。或者，先前可管理的“交换机”类型的设备现在已更改为“路由器”设备类型，等等。仅属性更改（如主机名、系统说明等）的设备不会归类为“已更改”。

   未更改

   表示现有设备未更改。仅属性更改的现有设备也被归类为“未更改”。

   已删除

   表示运行发现之后从 Data Aggregator 中删除了该设备。

   注意：如果单个已发现设备无法被识别为可通过 ping 连接或可管理，其状态将显示为“不可连接”。然而，Data Aggregator *不*报告在 IP 范围中找到的不可连接的设备。

详细信息：

SNMP 配置文件 (p. 55)
发现工作流 (p. 54)

来自其他数据源的发现

您可以选择 Data Aggregator 是否通过其他数据源自动发现与 CA Performance Center 同步的设备。在您注册 Data Aggregator 时，或在编辑数据源选项时，该选项可用。默认情况下，此选项被禁用。

重要说明！启用时，Data Aggregator 尝试发现*所有*其他数据源发布的设备。您无法将此功能精确到特定的一组数据源。

启用时，Data Aggregator 尝试发现其从那时起所学习的任何新设备。如果您想让 Data Aggregator 尝试发现过去与 CA Performance Center 同步的设备，选择 Data Aggregator 数据源，单击“重新同步”，并且选择“执行完全重新同步”复选框。

如果可以通过 ICMP 或其他一些支持的协议连接一种可通过 ping 连接的或其他类型的设备，则发现尝试会在 Data Aggregator 中生成它。

注意：如果在启用该选项后随时禁用，Data Aggregator 将继续管理已经发现的任何设备。

要启用此选项，请在 CA Performance Center“管理数据源”页面的“编辑数据源”对话框上选择“从其他数据源发现设备”复选框。

详细信息：

设备发现 (p. 53)

设备类型修改

基于设备服务信息，Data Aggregator 可以自动将可管理设备分类为“路由器”、“交换机”和“服务器”类型。如果某个可管理设备无法标识为“路由器”、“交换机”或“服务器”，则会将其分类为“设备”设备类型。

如果某些 SNMP 可管理设备的类型未按照您的预期进行标识，您可以覆盖这些设备类型。在随 Data Aggregator 一起提供的 $KARAF_HOME/custom/devicetypes/DeviceTypes.xml 文件中，将设备的 sysObjectID MIB 值显式映射到正确的设备类型。

注意：您无法将新设备类型添加到 DeviceTypes.xml 文件中。

DeviceTypes.xml 文件包含一个模板，可以将 sysObjectID 映射到相应的设备类型。默认情况下，该文件不包含任何 sysObjectID-to-type 映射条目。如果您要使用特定的 sysObjectID 对设备类型进行分类，可以修改模板，将 sysObjectID-to-type 条目添加到文件中。在您添加 sysObjectID 前，取消对要添加的 sysObjectID 部分的注释。

注意：对 DeviceTypes.xml 文件的更新最多花一分钟得以应用。

一个设备可以归入多个设备类型。但是，“设备”这个类型与其他设备类型互斥。例如，如果您将一个 sysObjectID 添加到一个或多个“路由器”、“交换机”或“服务器”设备类型，同时又将该 sysObjectID 添加到“设备”设备类型，则“设备”设备类型将被丢弃并且无法识别。

注意：如果升级 Data Aggregator，DeviceTypes.xml 文件不会保留。然而，升级之前添加的配置会保留。

示例：将设备的 sysObjectID 映射到其他设备类型

请执行以下步骤：

1. 打开 $KARAF_HOME/custom/devicetypes/DeviceTypes.xml 文件。
2. 输入以下信息：

```
<DeviceType>
    <Routers>
     <sysObjectID>1.3.6.5.1.34</sysObjectID>
    </Routers>

    <Switches>
      <sysObjectID>1.3.6.5.5.3</sysObjectID>
      <sysObjectID>1.3.6.5.1.34</sysObjectID>
     </Switches>

    <Servers>
      <sysObjectID>1.3.6.5.567.1</sysObjectID>
    </Servers>

    <Device>
      <sysObjectID>1.3.6.5.49.1</sysObjectID>
    </Device>
<DeviceType>
```

3. 在包含这些设备的发现配置文件上运行发现。

   注意：在重新运行发现之前，您对 DeviceTypes.xml 文件所做的更改不会对现有设备生效。

运行发现时，将有以下结果：

- sysObjectID 为 1.3.6.5.1.34 的所有设备都分类为“路由器”和“交换机”设备类型。
- sysObjectID 为 1.3.6.5.5.3 的所有设备都分类为“交换机”设备类型。
- sysObjectID 为 1.3.6.5.567.1 的所有设备都分类为“服务器”设备类型。
- sysObjectID 为 1.3.6.5.49.1 的所有设备都分类为“设备”设备类型。

重新发现

当包含 IP 地址之一或主机名的发现配置文件运行时，相应的现有受监视设备可以被重新发现。在单击特定设备“详细信息”选项卡上的“重新发现”按钮时，可以重新发现一个受监视设备。

由于此发现，下面一组属性会被更新：

- 系统名称
- 主机名
- 设备类型（在 CA Performance Center 中显示）
- 位置
- 供应商
- 设备说明
- 设备型号

注意：对设备属性的更改可能会导致对设备所属的组和设备集合进行更改。对组和设备集合的更改可能会添加或删除监视配置文件。

设备属性的更改可能最多需要 5 分钟，才能在 CA Performance Center 清单或显示板视图中显示。

第 4 章： 管理基础架构

此部分包含以下主题：

自定义设备和组件管理工作流

您可以自定义您发现的设备和受监视组件的管理。选项包括修改配置文件、修改关联、创建新供应商认证以及导入度量标准系列。例如，您可以提高轮询关键接口的频率，或者将包含事件规则的自定义监视配置文件应用于自定义设备集合。

以下工作流提供一个最佳实践，可将该最佳实践用作自定义的快速参考。

以具有管理员角色的用户身份登录并执行下列步骤：

1. 创建新的监视配置文件（或创建工厂监视配置文件的副本），以便自定义监视设备时使用的轮询速度和度量标准。
2. （可选）将事件规则添加到自定义监视配置文件 (p. 125)。
3. （可选）如果工厂供应商认证及其关联的度量标准系列不能满足您的需求，请创建自定义供应商认证，并导入新的度量标准系列。此步骤可随时执行。

   注意：有关自定义度量标准系列和自定义供应商认证的详细信息，请参阅 *《Data Aggregator 自行认证指南》*。

4. 在 CA Performance Center 中创建自定义设备集合及相关规则，然后将其用作 Data Aggregator 设备集合。您可以立即将这些设备集合与 Data Aggregator 同步，也可以等待自动同步。发现完成后您可以手动将这些设备填充到设备集合中。

   注意：如果您是 MSP 或承租方，请以承租方管理员身份执行此步骤。有关创建受监视组和同步数据源的详细信息，请参阅*《CA Performance Center 管理员指南》*。

5. 自定义监视配置文件和设备集合关联，以确保使用所需的轮询速度 (p. 80)。创建自定义监视配置文件时，请将自定义监视配置文件与某个自定义设备集合相关联，以激活该监视配置文件及所有相关事件规则。

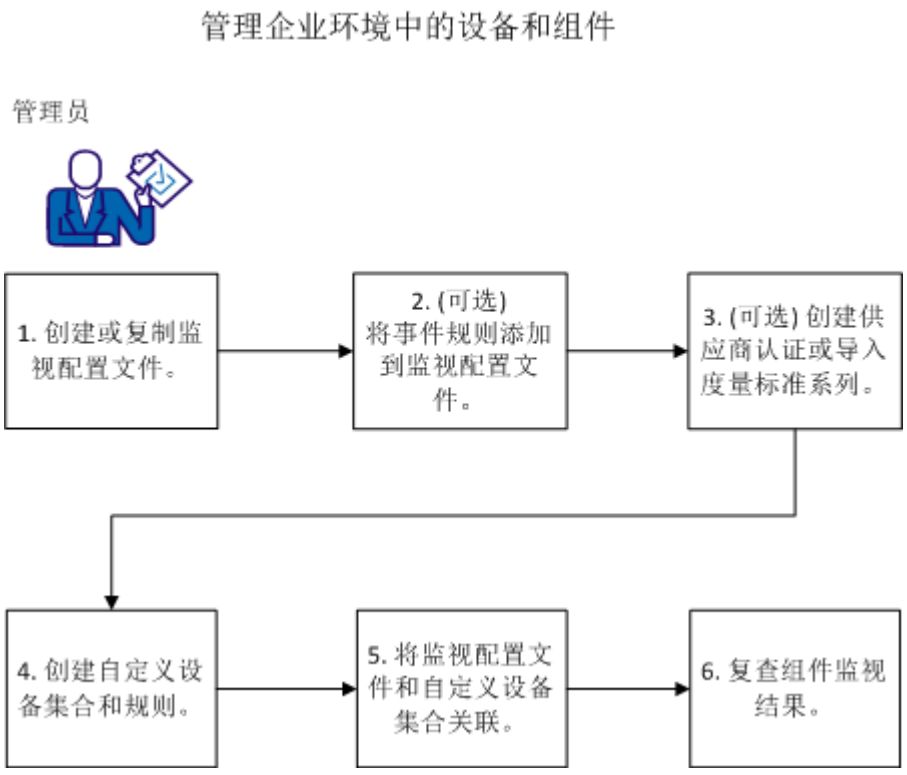
   注意：如果您是 MSP 或承租方，请以承租方管理员身份执行此步骤。

   自定义还可以包括删除工厂监视配置文件和设备集合之间的关联，以及将自定义监视配置文件与工厂或自定义设备集合相关联。

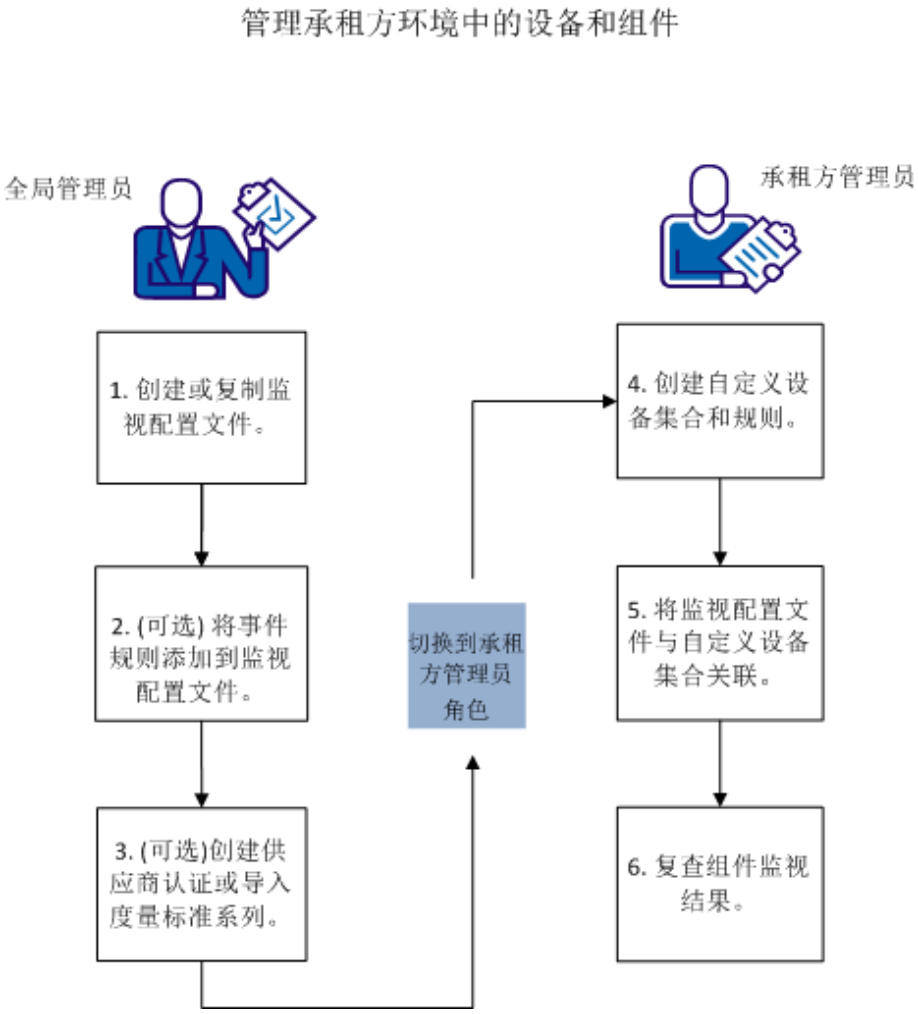
6. 在用于新配置的轮询开始验证您正在收集所需信息后，查看组件监控结果。 (p. 87)

   注意：如果您是 MSP 或承租方，请以承租方管理员身份执行此步骤。

此示意图展示了适用于企业的工作流：



此示意图展示了适用于承租方环境的工作流：



监视配置文件

监视配置文件用于确定轮询速度以及为某设备集合中的设备发现和轮询的统计信息。您可以选择工厂（即取即用）监视配置文件。工厂监视配置文件将自动应用于工厂设备集合，例如“所有路由器”设备集合。不能在系统中编辑或删除工厂监视配置文件，但可以从设备集合中复制或删除这些监视配置文件，以创建自定义配置文件。

您能够以管理员身份创建、编辑、复制或删除自定义的监视配置文件。自定义监视配置文件可在整个用户界面中使用，不局限于承租方范围，即使您是承租方工作区的 MSP 管理员也不例外。（但是，与监视配置文件相关联的设备集合仅限于承租方范围内）。例如，您可以创建“金牌服务路由器监视”监视配置文件，并将其用于所有金牌级别的承租方。您无需为*每个*金牌级别的承租方创建一个*单独*的“金牌服务路由器监视”监视配置文件。

在所有承租方之间，必须使用唯一的监视配置文件名。

使用 CA Performance Center 用户界面或 Data Aggregator REST Web 服务可以管理监视配置文件和查看这些配置文件与设备集合的关联。

工厂监视配置文件关联

监视配置文件指定要轮询的统计信息。工厂（即用型）监视配置文件会自动与设备集合关联，如下所述：

- 辅助功能监视配置文件与“所有设备”设备集合关联。
- 辅助功能监视配置文件与“所有设备”设备集合关联。
- 路由器监视配置文件与“所有路由器”设备集合关联。
- 物理服务器监视配置文件与“所有服务器”设备集合关联。
- 虚拟服务器监视配置文件与“所有服务器”设备集合关联。
- 交换机监视配置文件与“所有交换机”设备集合关联。
- Microsoft 群集服务监视配置文件与“所有服务器”设备集合关联。
- VMWare 监视配置文件与“所有 VMare vCenter”设备集合关联。
- 带有“所有 VMware vCenter”集合的 VMware ESX 主机监视配置文件。
- 带有“所有 VMware vCenter”集合的 VMware 虚拟机监视配置文件。

下列监视配置文件与设备集合之间不存在工厂关联。此设计可以防止大型发现影响性能。手动将这些监视配置文件分配给设备集合以收集其数据：

- 网络接口
- 响应路径
- MPLS
- CBQoS

详细信息：

工厂设备集合 (p. 82)
“所有设备”设备集合 (p. 83)
“所有路由器”设备集合 (p. 84)
在设备集合中分配或删除监视配置文件 (p. 80)

查看监视配置文件

管理员可以查看监视配置文件的列表及其与设备集合的关联：

- 管理员可以查看他们所管理的承租方的设备集合。
- 承租方管理员可以查看其自己的设备集合列表。

此信息可帮助您确定如何管理监视配置文件和轮询比率，并大致介绍可为设备集合生成的报表类型。

请执行以下步骤：

1. 从 Data Aggregator 数据源的“监视配置”菜单中单击“监视配置文件”。

   将填充监视配置文件的列表。

2. 如果您是管理员，您可以向系统中添加监视配置文件，也可以选择某个监视配置文件进行编辑、复制或删除。所有监视配置文件（包括自定义监视配置文件）都是全局性的。

   注意：工厂监视配置文件无法编辑或删除；只有自定义监视配置文件可以修改。

3. 选择一个监视配置文件。

4. 选定的监视配置文件的详细信息将填充选项卡，如下所述：

   - “度量标准系列”选项卡中填充与该特定监视配置文件关联的度量标准系列的列表。度量标准系列中包含轮询设备和接口所使用的度量标准。
   - 在“事件规则”选项卡中填充与该特定监视配置文件关联的事件规则的列表。作为管理员，您可以通过分配或删除规则来管理事件规则与选定的监视配置文件之间的关系。
   - “集合”选项卡由与该特定监视配置文件关联的设备集合列表填充。作为承租方管理员，您可以通过分配或删除配置文件来管理设备集合与选定监视配置文件之间的关联。

详细信息：

故障排除：对所发现的度量标准系列的轮询已停止 (p. 150)
自动更新设备重新配置 (p. 99)

在设备集合中分配或删除监视配置文件

管理员或承租方管理员可以添加或删除特定设备集合与系统中的监视配置文件之间的关联。通过这一功能，您可以启动或停止轮询与某设备集合中的设备和组件相关的监视配置文件关联的统计信息。

重要说明！将监视配置文件分配给设备集合时，可能发生重大 SNMP 请求。这些请求会影响设备性能。此外，不要将监视配置文件与“所有设备”设备集合关联。这样做会导致向仅可通过 ping 连接的设备发送额外的 SNMP 请求，并且会导致偶尔支持度量标准系列。

例如，您发现一个路由器有 1000 个物理和逻辑接口。另外，您创建接口监视配置文件，并将监视配置文件上的轮询速率设置为一分钟。如果将接口监视配置文件分配给您的路由器所在的设备集合，将为每个接口轮询 10 个 MIB 对象。该设置将推出 SNMP 代理每秒要回复 166 个 MIB 对象的比率。这个大的 SNMP 负荷会影响路由器的性能。

诸如 QoS、MPLS 和 IPSLA 等度量标准系列也可以是大的 SNMP 请求的重要因素。有关 SNMP 请求对您的网络设备的影响和限制的更多信息，请参阅供应商手册或联系供应商。

注意：将多个设备集合分配给同一监视配置文件时，Data Aggregator 将使用配置的最快轮询速率。当您希望使用自定义轮询速度时，请删除工厂监视配置文件与设备集合之间的关联。

请执行以下步骤：

1. 从 Data Aggregator 数据源的“监视配置”菜单中单击“集合”。

   此时显示收集列表。管理员可以查看他们所管理的承租方的设备集合。承租方管理员可以查看自己的（承租方）设备集合列表。

2. 选择一个集合，然后单击“监视配置文件”选项卡。

   此时显示一个列表，其中显示分配给选定设备收集的监控配置文件。

3. 单击“管理”。

   此时将打开“分配集合监视配置文件”对话框。

4. 执行以下任一操作：

   - 从“可用监视配置文件”列表中选择一个或多个监视配置文件，然后单击“添加”。

     所选的监视配置文件将移动到“分配的监视配置文件”列表中。

     将监视配置文件与设备集合相关联会激活包含在该监视配置文件中的事件规则。当设备集合中的设备满足事件规则条件时，会引发并清除事件。

   - 从“分配的监视配置文件”列表中选择一个或多个监视配置文件，然后单击“删除”。

     所选的监视配置文件将移动到“可用监视配置文件”列表中。

     注意：删除关系不会从系统中删除监视配置文件。

5. 单击“保存”。

   此时将保存您所做的更改，您可以重复步骤 2 验证这些更改。

详细信息：

工厂监视配置文件关联 (p. 78)
故障排除：对所发现的度量标准系列的轮询已停止 (p. 150)
自定义设备和组件管理工作流 (p. 75)
如何设置和激活接口筛选 (p. 113)

caim--配置监视配置文件轮询筛选

筛选指定要轮询的组件项，以及对其进行轮询的时间间隔。通过指定要轮询的组件项，可以仅监控您所关注的项。对于*自定义*监视配置文件，您可以为其指定其他筛选。

您可以在运行发现之前或之后添加或编辑筛选。Data Aggregator 将在发现之后应用筛选。仅轮询匹配筛选条件的组件项。如果您在运行发现之*后*添加或编辑筛选，针对这些组件项的轮询则会停止。

注意：您必须以管理员身份登录，才能执行此任务。

请执行以下步骤：

1. 选择您已在列表中创建的监控配置文件。

   选定监控配置文件的详细信息会显示在右侧窗格中。默认情况下会选择“度量标准系列”选项卡。

2. 单击列表中度量标准系列的名称。

   该窗格底部的“编辑筛选”和“清除筛选”按钮此时会变得可用。

3. 单击“编辑筛选”按钮。

   此时显示“筛选表达式”对话框。

4. 单击现有的 AND 条件，然后单击对话框右侧的逻辑按钮。

5. 选择属性和操作，然后为您的条件输入值。

6. 单击“添加条件”按钮。

   此时您所创建的条件已添加到筛选表达式。

7. 创建任何其他条件。

   通过单击“添加条件”按钮来添加每个条件。

8. 单击“保存”按钮。筛选表达式即被保存并且分配给选定的度量标准系列。

注意：查看组件项时，如果已为其分配筛选，那么在尚未分配筛选的每个组件项旁边会出现星号 (*)。

工厂设备集合

Data Aggregator 和 CA Performance Center 支持*设备集合*的概念，集合是指对受监视设备的逻辑分组。

系统提供若干工厂（即用型）设备集合，以便将数据快速送入 Data Aggregator 系统，并测试产品。在发现过程中检测到的设备将根据其类型添加到这些设备集合中。例如，路由器将添加到“所有路由器”工厂设备集合中。同步后，这些受监视设备将添加到 CA Performance Center 中的相应设备集合中。

然后，工厂监视配置文件将自动应用于工厂设备集合，以便立即开始收集数据，而无需您进行任何干预。收集数据之后，您可以运行数据报告，以便深入了解您的网络。

系统提供以下工厂设备集合：

- 所有设备 (p. 83)
- 所有路由器 (p. 84)
- 所有服务器 (p. 84)
- 所有交换机 (p. 84)
- 所有可管理设备 (p. 85)
- 所有 ESX 主机 (p. 85)
- 所有虚拟机 (p. 85)
- 所有 VMware vCenter (p. 86)

注意：工厂设备集合主要用于实验室或演示设置。在实际生产部署中，最佳实践是设计并配置自定义设备集合以拥有粒度控制和最佳数据集合。

可以访问“监视配置”菜单来查看设备集合列表，并查看应用于每个设备集合的的监视配置文件。管理员可以查看他们所管理的承租方的设备集合。承租方管理员可以查看其自己的设备集合列表。

详细信息：

工厂监视配置文件关联 (p. 78)
故障排除：对所发现的度量标准系列的轮询已停止 (p. 150)
自定义设备集合 (p. 86)

“所有设备”设备集合

“所有设备”设备集合是一个工厂设备集合。在发现过程中检测到的可管理且可通过 ping 连接的设备将自动放置到“所有设备”设备集合中。无法访问的设备不包括在“所有设备”设备集合中。

重要说明！此外，不要将监视配置文件与“所有设备”设备集合关联。这样做会导致向仅可通过 ping 连接的设备发送额外的 SNMP 请求，并且会导致偶尔支持度量标准系列。

详细信息：

工厂设备集合 (p. 82)
工厂监视配置文件关联 (p. 78)

“所有路由器”设备集合

“所有路由器”设备集合是一个工厂设备集合。在发现过程中检测到的路由器将自动放置到“所有路由器”设备集合中。

注意：路由器可能同时显示在“所有路由器”设备集合和“所有交换机”设备集合中。

详细信息：

工厂设备集合 (p. 82)
工厂监视配置文件关联 (p. 78)

“所有服务器”设备集合

“所有服务器”设备集合是一个工厂设备集合。在发现过程中检测到的物理和虚拟服务器（主机）将自动放置到“所有服务器”设备集合中。网络设备（如路由器和交换机）不包括在“所有服务器”设备集合中。

详细信息：

工厂设备集合 (p. 82)
工厂监视配置文件关联 (p. 78)

“所有服务器”设备集合

“所有交换机”设备集合是一个工厂设备集合。在发现过程中检测到的交换机将自动放置到“所有交换机”设备集合中。

注意：路由器可能同时显示在“所有路由器”设备集合和“所有交换机”设备集合中。

详细信息：

工厂设备集合 (p. 82)
工厂监视配置文件关联 (p. 78)

“所有可管理设备”设备集合

“所有可管理设备”设备集合是一个工厂集合。可管理设备收集高级性能统计信息，并使用协议（如 SNMP）进行监视。发现过程中检测到的可管理设备将自动放入“所有可管理设备”设备集合中。

对于可通过 Ping 连接的设备，只能监视其可用性，而不提供任何额外的性能度量标准。因此，可通过 Ping 连接的设备不包含在“所有可管理设备”设备集合中。

注意：可管理设备可同时出现在“所有设备”设备集合和“所有可管理设备”设备集合中。

详细信息：

工厂设备集合 (p. 82)

“所有 ESX 主机”设备集合

“所有 ESX 主机”设备集合是一个工厂设备集合。在发现期间检测到的 ESX 主机被自动放置到“所有 ESX 主机”设备集合内。

详细信息：

工厂设备集合 (p. 82)
工厂监视配置文件关联 (p. 78)

“所有虚拟机”设备集合

“所有虚拟机”设备集合是一个工厂设备集合。在发现期间检测到的 VMware 虚拟机被自动放置到“所有虚拟机”设备集合内。

详细信息：

工厂设备集合 (p. 82)
工厂监视配置文件关联 (p. 78)

“所有 VMware vCenter”设备集合

“所有 VMware vCenter”设备集合是一个工厂设备集合。在发现期间检测到的通过 VCAIM 运行 systemEdge 的所有服务器被自动放置到“所有 VMware vCenter”设备集合内。

详细信息：

工厂设备集合 (p. 82)
工厂监视配置文件关联 (p. 78)

自定义设备集合

工厂设备集合主要用于实验室或演示设置。在实际生产部署中，最佳实践是设计并配置自定义设备集合以对正在轮询的设备集合进行粒度控制。例如，通过取消设备与具有与其关联的监视配置文件的任何其他设备集合的关联，可禁用对该设备的轮询。如果您要将监视配置文件与工厂设备集合（如“所有路由器”）关联，则不能停止轮询单个设备。不能从工厂设备集合删除设备，因此您应取消关联监视配置文件，以便禁用轮询。然后，创建包含要应用同一轮询策略的设备的自定义设备集合。将监视配置文件（或自定义监视配置文件）与这些自定义设备集合关联，以便开始轮询。

在 CA Performance Center 中创建自定义设备集合，然后立即将它们与 Data Aggregator 同步，或等待自动同步。完成同步后，Data Aggregator 将创建对应的设备集合，用于监视设备。

注意：有关创建自定义设备集合并将其与 Data Aggregator 同步的更多信息，请参阅《*CA Performance Center 管理员指南*》。

可以访问“监视配置”菜单来查看设备集合列表，并查看应用于每个设备集合的的监视配置文件。管理员可以查看他们所管理的承租方的设备集合。承租方管理员可以查看其自己的设备集合列表。

详细信息：

工厂设备集合 (p. 82)

查看受监视设备

您可以查看受监视设备的详细信息，也可以查看其与设备集合、组件、监视配置文件和度量标准的关联。您还可以查看“筛选报告”。该信息有助于您了解上下文信息，例如，正在使用哪些监视配置文件轮询设备组件。

注意：某些功能需要管理员权限。

受监视的设备包括可管理的设备或是可通过 ping 连接的设备（即，可访问但不可管理的设备）。不可访问的设备是不受监视的设备。可以从“轮询的度量标准系列”选项卡查看受监视设备的组件。

请执行以下步骤：

1. 针对 Data Aggregator 数据源，在“受监视清单”菜单中单击“受监视设备”。

   此时将显示“树视图”选项卡。

2. 从下拉列表中选择“设备(按集合)”或“设备(按监视配置文件)”，并从相应的树视图中选择特定设备。

   注意：您也可以选择“搜索”选项卡，以便按主机名、设备名称或 IP 地址进行搜索。您可以输入部分名称或 IP 地址，以返回包含该部分匹配内容的设备的列表。不支持通配符和正则表达式。

   “详细信息”选项卡提供了选定的受监视设备的详细信息。详细信息包括设备 IP 地址、关联的 SNMP 配置文件、设备的状态等等。您可以编辑设备的 IP 地址、Data Collector 主机、SNMP 配置文件以及 SNMP 版本。

   您可以通过以下两种方式编辑设备 IP 地址：

   - 编辑“IP 地址”字段，然后单击“保存”。
   - 右键单击“IP 地址”表中的 IP 地址，选择“将此 IP 设置为设备的主 IP”，然后单击“保存”。

   注意：此视图中提供了可管理设备的详细信息。

（可选）单击“重新发现”以重新发现设备。由于此发现，下面一组属性会被更新：

- 系统名称
- 主机名
- 设备类型（在 CA Performance Center 中显示）
- 位置
- 供应商
- 设备说明
- 设备型号

注意：对设备属性的更改可能会导致对设备所属的组和设备集合进行更改。对组和设备集合的更改可能会添加或删除监视配置文件。

通过查找触发重新发现的事件确认已重新发现设备。要查看事件，请单击 CA Performance Center 中的“显示板”菜单，并在“操作显示”下选择“事件显示”。

3. （可选）选择一个度量标准系列，然后单击“更新度量标准系列”以便为任何配置更新重新 p 配置组件。例如，如果在服务器上添加磁盘驱动器，则可以使用“更新度量标准系列”按钮重新发现配置更新。配置更新会创建一个磁盘组件。

4. 选择其他选项卡：

   - “轮询的度量标准系列”选项卡将显示对设备进行轮询的度量标准系列的总集并显示其轮询比率。此总集数基于设备上所有监视配置文件的总数。选项卡还显示设备是否支持度量标准系列。

     某个给定度量标准系列的组件表可显示先前发现的度量标准系列组件的组件轮询状态。“状态”列显示下列状态之一：

     活动

     表示正在轮询组件。

     非活动

     表示对该组件的轮询已停止，因为不再为该设备监视该度量标准系列。

     已报废

     表示该组件不再位于该物理设备上。对该组件的轮询已停止。您可以查看历史数据，以便在报告中使用。默认情况下，报废的组件不与 CA Performance Center 同步。要启用此选项，请在 CA Performance Center“管理数据源”页面的“编辑数据源”对话框中选中“同步报废的项”复选框。

（可选）选择一个度量标准系列，然后单击“更新度量标准系列”以便为任何配置更新重新 p 配置组件。例如，如果在服务器上添加磁盘驱动器，则可以使用“更新度量标准系列”按钮重新发现配置更新。配置更新会创建一个磁盘组件。

- “阈值配置文件”选项卡将显示因所选设备所属的组而应用于该设备的阈值配置文件。
- 通过“监视配置文件”选项卡，您可以选择一个设备集合以查看关联的配置文件名称。将鼠标悬停在配置文件上可查看说明。
- “度量标准”选项卡，它是使用该设备支持的度量标准列表填充的。选择一个度量标准系列以查看其详细信息。查看实施供应商认证、供应商源（如果它是 SNMP 供应商认证，则显示 MIB 表源），以及用于计算每个度量标准的表达式。
- “筛选报告”选项卡显示在组件监视期间已使用哪些接口筛选条件。该选项卡还显示在设备上标识的所有接口以及这些接口是否匹配指定的筛选条件的报告。如果您更改关于自定义监视配置文件的规则，则“接口筛选条件”窗格不反映这些更改。如果您解除监视配置文件与组的关联，则“接口筛选条件”窗格不反映这些更改。重新发现设备可筛选基于您对筛选条件和监视配置文件所做更改的接口。

详细信息：

发现和轮询 (p. 56)
手工更新设备重新配置 (p. 100)
清除接口筛选 (p. 114)
故障排除：对所发现的度量标准系列的轮询已停止 (p. 150)
如何设置和激活接口筛选 (p. 113)

删除设备

您可以删除所发现的设备。例如，如果希望停止监视所发现的某一设备，您可以删除该设备。

删除设备时，将发生下列结果：

- 将删除所有关联的设备组件。
- 删除的设备和设备组件的历史数据无法再访问。

注意：如果重新运行任一现有的发现配置文件，可以再次发现已删除的设备。

请执行以下步骤：

1. 针对 Data Aggregator 数据源，在“受监视清单”菜单中单击“受监视设备”。

   此时将显示“树视图”选项卡。

2. 选择“搜索”选项卡。

   注意：请勿使用页面顶部的全局“搜索”框。

3. 要搜索您想要删除的监视设备，请在本地“搜索”框中输入文本。可以按主机名、设备名或 IP 地址进行搜索。您可以输入部分名称或 IP 地址，以返回包含该部分匹配内容的设备的列表。

   注意：不支持通配符和正则表达式。

   此时将返回匹配设备的列表。

4. 执行下列操作之一：

   - 选择要删除的单个或多个受监视设备，然后单击“删除”。
   - 选中“名称”列旁边的复选框并单击“删除”，删除结果列表中的*所有*设备。

   此时将打开确认对话框。

5. 单击“是”以确认删除。

   此时将删除该设备，并且该设备将不再显示在“受监视设备”清单中。如果另一数据源未管理这些设备，Data Aggregator 与 CA Performance Center 下次同步时，这些设备将不会再显示在“清单”视图中，也不会显示为组成员。

更改受监视设备的主 IP 地址

您可以更改受监视设备的主 IP 地址。

请执行以下步骤：

1. 针对 Data Aggregator 数据源，在“受监视清单”菜单中单击“受监视设备”。

   此时将显示“树视图”选项卡。

2. 从下拉列表中选择“设备(按集合)”或“设备(按监视配置文件)”，并从相应的树视图中选择特定设备。

   注意：您也可以选择“搜索”选项卡，以便按主机名、设备名称或 IP 地址进行搜索。您可以输入部分名称或 IP 地址，以返回包含该部分匹配内容的设备的列表。不支持通配符和正则表达式。

3. 通过执行下列步骤之一，更改主 IP 地址：
   - 编辑“IP 地址”字段，然后单击“保存”。
   - 右键单击“IP 地址”表中的 IP 地址，选择“将此 IP 设置为设备的主 IP”，然后单击“保存”。

   主 IP 地址已更改。

删除报废组件

Data Aggregator 包括删除报废组件的脚本。报废组件是不再存在于物理设备上的组件。过多的报废组件可能会影响用户界面性能。要删除报废组件，请了解如何使用此脚本。

注意：要自动删除报废组件，请参阅《*Data Aggregator 使用 REST Web 服务管理指南*》。

请执行以下步骤：

1. 打开命令提示符并访问 /opt/IMDataAggregator/scripts 目录。
2. 要调用删除报废组件的脚本，请键入以下命令：

   ```
   ./remove_retired_items.sh
   ```

   列出脚本参数并进行说明。

示例：返回报废组件的总数

1. 键入以下命令：

   ```
   ./remove_retired_items.sh -h host_name
   ```

   -h *host_name*

   指定要连接的 Data Aggregator 主机名。

   显示报废组件的总数。
2. （可选）输入数字 1，返回报废组件的*名称*列表。
3. （可选）输入数字 1，删除所有报废组件。

示例：按特定条件筛选报废组件列表

1. 要调用删除报废组件的脚本，请键入以下命令：

   ```
   ./remove_retired_items.sh
   ```

   列出脚本参数并进行说明。

2. 按特定条件删除报废组件：

   - 如果安装多个 Data Collector 实例，则可以有重复 IP 地址。要按 IP 地址筛选报废组件，请执行以下步骤：

     a. 键入以下命令：

     ```
     ./remove_retired_items.sh -h host_name -a device_IP_address
     ```

     b. **注意**：您无法输入一系列 IP 地址。

     c. （可选）输入数字 1，返回报废组件的*名称*列表。

     d. （可选）输入数字 1，删除所有报废组件。

   - 要按时限（按天数）删除报废组件，请键入以下命令：

     ```
     ./remove_retired_items.sh -h host_name -t
     filter_by_days_old_from_current_time
     ```

     例如，以下命令删除从当前时间起不到十天的报废组件：

     ```
     ./remove_retired_items.sh -h host_name -t 10
     ```

示例：删除大量报废组件

您可以轻松删除总数超过 10 万的所有报废组件：

- 要查看总数超过 10 万的所有报废组件，请键入以下命令：

  ```
  ./remove_retired_items.sh -h 主机名 -o 输出文件
  ```

  -o *输出文件*

  所有报废组件的输出。输出为 .csv 文件。

  例如，以下命令输出所有报废组件的列表。.csv 文件格式包括设备项 ID、设备显示名称、报废组件 ID 和报废组件显示名称：

  ```
  ./remove_retired_items.sh -h my_host_name -o myretired.csv
  ```

- 要删除总数超过 10 万的所有报废组件，并将信息记录到 .csv 文件，请键入以下命令：

  ```
  ./remove_retired_items.sh -h 主机名 -o 输出文件 -c Yes
  ```

  -o *输出文件*

  所有报废组件的输出。输出为 .csv 文件。

  –c Yes

  确认删除所有报废组件。

  例如，以下命令删除所有报废组件：

  ```
  ./remove_retired_items.sh -h my_host_name -o myretired.csv -c Yes
  ```

考虑有关删除报废组件的进一步详细信息：

- 如果按 IP 域名或 IP 域 ID 筛选报废组件，也请指定特定的 IP 地址以便返回正确结果。
- 如果筛选条件返回太多报废组件，则 REST 接口不会返回响应。使用其他筛选选项来缩小结果。更多筛选条件在 http://*主机名*:*端口* /rest/retired/xsd/filterselect.xsd 上可以找到。

删除 IP 域

您可以删除 IP 域。例如，当合并两个或两个以上域时，您可以删除一个 IP 域。您还可以删除用于测试的 IP 域。删除 IP 域将删除与其关联的所有设备和设备组件。删除 IP 域也会使与该 IP 域相关联的发现配置文件无效。

您可以在 CA Performance Center 中删除 IP 域。删除 IP 域后，请与 Data Aggregator 同步此删除操作，或等待自动同步。

注意：有关删除和同步 IP 域的详细信息，请参阅*《CA Performance Center 管理员指南》*。

当 Data Aggregator 注意到某个 IP 域已删除时，将发生下列结果：

- 与删除的 IP 域相关联的所有设备和设备组件都将被删除。
- 与删除的 IP 域关联的 Data Collector 将停止。其状态将显示为“未在收集数据”。

  注意：您可以在 Data Collector 关闭时删除 IP 域。当 Data Collector 恢复运行后，*Data Collector installation directory*/apache-karaf-2.3.0/shutdown.log 文件中将显示一条错误消息，Data Collector 将立即关闭。
- 指定已删除 IP 域的所有发现配置文件都将无效，并且无法运行。其状态显示“无 IP 域”。已删除的 IP 域中所有正在运行的发现都将中止。

  注意：通过指定一个要发现设备的有效 IP 域，可以将无效的发现配置文件状态更改回到“就绪”。
- 对于每个已删除的设备，在所关联的承租方项上都会生成一个审核事件。

详细信息：

发现配置文件 (p. 59)

删除承租方

您可以删除承租方。例如，如果您是托管服务提供商 (MSP)，并且某一承租方不再是您的客户，则可以删除该承租方。删除承租方将删除与该承租方相关联的所有设备、设备组件、IP 域、SNMP 配置文件以及发现配置文件。

注意：不能删除默认承租方。

您可以在 CA Performance Center 中删除承租方。删除承租方后，请手动与 Data Aggregator 同步此删除操作，或等待自动同步。

注意：有关删除和同步承租方的详细信息，请参阅*《CA Performance Center 管理员指南》*。

当 Data Aggregator 注意到承租方已被删除后，将发生下列事件：

- 与已删除承租方相关联的所有设备、设备组件、IP 域、SNMP 配置文件以及发现配置文件都将被删除。
- 对删除的设备和设备组件的轮询将停止。
- 删除的设备和设备组件的历史数据无法再访问。
- 对于每个已删除的承租方，在 Data Aggregator 设备上都会生成一个审核事件。
- 删除的设备及其删除的组件上的所有阈值事件都将被删除。

注意：您可以在 Data Collector 关闭时删除承租方。当 Data Collector 恢复运行后，*Data Collector installation directory*/apache-karaf-2.3.0/shutdown.log 文件中将显示一条错误消息，然后 Data Collector 将立即关闭。

禁用承租方

您可以禁用承租方。例如，如果您是管理服务提供商 (MSP)，并且希望停止某一承租方基础架构的主动监视，则可以禁用该承租方。

注意：您必须以管理员身份登录，才能执行此任务。

您需要在 CA Performance Center 中禁用承租方。禁用承租方后，请与 Data Aggregator 同步此禁用操作，或等待自动同步。

注意：有关禁用承租方的详细信息，请参阅*《CA Performance Center 管理员指南》*。

当 Data Aggregator 注意到承租方已被禁用后，将发生下列结果：

- Data Aggregator 系统停止所有与禁用的承租方关联的 Data Collector 主机。然后，Data Collector 主机状态显示为“未在收集数据”。（重新启用承租方时，必须手动重新启动 Data Collector 主机。）

  注意：对于禁用的承租方的任何新的 Data Collector 安装，均会显示“未在收集数据”状态。只有再次启用了承租方，才允许运行发现。
- 与已禁用承租方相关联的所有设备、设备组件、IP 域、SNMP 配置文件以及发现配置文件都将继续存在。
- 对当前代表禁用的承租方监视的任何设备和组件的轮询将停止。
- 有关承租方的设备和组件的历史数据仍可访问。
- 与禁用的承租方关联的发现配置文件将无效，并且无法运行。发现配置文件的状态将显示为“已禁用承租方”。
- 如果在发现配置文件上正在运行发现时使该配置文件失效，则发现将中止。
- 对于禁用的承租方，在 Data Aggregator 设备上会生成一个审核事件。

详细信息：

启用承租方 (p. 95)

启用承租方

您可以启用之前禁用的承租方。例如，如果您是托管服务提供商 (MSP)，并且希望重新启动某一承租方基础架构的主动监视，则可以启用该承租方。

注意：您必须以管理员身份登录，才能执行此任务。

您可以在 CA Performance Center 中启用承租方。启用承租方后，请执行以下操作：

1. 与 Data Aggregator 同步此启用操作，或等待自动同步。

   注意：有关启用承租方的详细信息，请参阅*《CA Performance Center 管理员指南》*。

   将发生下列结果：

   - Data Aggregator 将注意到承租方已启用。
   - 与启用的承租方关联的发现配置文件将生效。发现配置文件将显示其当前状态。
   - 对于该承租方，在 Data Aggregator 设备上会生成一个审核事件。

2. 手动重新启动所有与该承租方关联的 Data Collector 主机 (p. 48)。

   将发生下列结果：

   - 对当前代表启用的承租方监视的任何设备和组件的轮询将重新启动。
   - 与启用的承租方关联的发现配置文件将可以运行。

详细信息：

禁用承租方 (p. 94)
故障排除：发现未启动 (p. 149)

设备重新配置

在 Data Aggregator 中，可以自动或手工监视和更新设备的重新配置更改，以使设备组件保持最新。设备重新配置包括对物理设备组件所做的更改和软件配置更改，如监视协议的响应路径测试。Data Aggregator 使用相同的方法来监视这两种类型的重新配置。

重新配置更改的其他示例包括：

- 向设备中添加主板，这将向设备中添加更多端口。
- 向发现的设备中添加内存、CPU、物理接口或任何度量标准系列。
- 重新配置虚拟交换机。
- 更改设备的配置，使发现的设备参与路由协议。

当检测到更改时，Data Aggregator 将生成重新配置事件，并且可以更新其度量标准系列表述，以反映对设备组件所做的更改。通过选择“显示板”、“操作”、“事件显示”，查看重新配置事件。

了解变更检测在 Data Aggregator 中的工作方式，可以帮助您选择最适合在您的环境中监视设备重新配置的方案。例如，您可以设置变更检测监视的频率。

详细信息：

如何管理变更检测 (p. 97)

如何管理变更检测

变更检测管理计划有助于确保 Data Aggregator 根据您的需求在您的环境中检测和监视设备重新配置。首次设置 Data Aggregator 以发现新设备时，可以提前计划任何设备的重新配置。您也可以在设备发现之后的任何时候编辑这些选项。

您做出的选择基于以下因素：

- 更改的可能性。
- 预期的更改频率。
- 对数据过时程度的容忍度。

对于某些度量标准系列（如 CPU），您不希望监控重新配置的频率过高。对于其他更具动态性的度量标准系列（如虚拟系统），可以选择更频繁的比率。

设置变更检测的基本过程是：

1. 创建或编辑*自定义*监视配置文件 （您也可以复制工厂监视配置文件并编辑副本）。
2. 选择“启用变更检测”，并在监视配置文件中设置“更改检测设置，比率”。

   “更改检测设置，比率”选项用于设置 Data Aggregator 检查变更的频率。可以分钟或小时为单位设置检测率。默认情况下，比率设置成 24 小时。

   注意：考虑度量标准系列可能更改的频率，以及监控配置文件应用的设备数量。避免过高的设置更改检测率。

3. 更新度量标准系列的 Data Aggregator 表述。

   在设置变更检测率之后，您可以选择两种方式来更正 Data Aggregator 配置：度量标准系列的自动更新或手工更新。此选项不更新度量标准系列，而是通过确保监视正确的组件集，来更新度量标准系列的表述。

   - 选择“自动更新度量标准系列”选项（默认情况下会选中）意味着在检测到重新配置时无需您介入。Data Aggregator 会在发生重新配置事件时自动开始监视任何新组件，并报废不会再检测到的所有组件。

     查看“事件显示”显示板以查看重新配置事件：

     - 如果组件对于某一设备发生了变更，关于关联设备的事件将生成。此事件说明检测到组件更改并稍后应用。
     - 在应用组件调整之后，生成其他事件。此事件说明多少组件被添加、被淘汰和保持不变。

   - 取消选中“自动更新度量标准系列”选项意味着 Data Aggregator 不会自动开始监视新组件或报废旧组件。

     查看“事件显示”显示板以查看重新配置事件：

     - 如果组件对于某一设备发生了变更，关于关联设备的事件将生成。此事件说明组件更改发生，但是协调未发生。

     要应用重新配置更改，请手动单击设备“轮询的度量标准系列”页面上的“更新度量标准系列”按钮。

4. 要激活监视配置文件，请为设备集合分配自定义监视配置文件。

示例：

- 如果您知道您的环境将进行重大维护，可以关闭自动更新，直到该重大维护完成为止。对于较小的定期更改，启用自动更新功能有助于确保您的 Data Aggregator 保持最新。
- 监视配置文件被分配给包含设备的设备集合。如果有希望以不同方式监视的特殊设备，请为这些特殊设备创建自定义设备集合，并分配一个包含您所需的变更检测设置的自定义监视配置文件。例如，您可以通过创建关键核心路由器设备集合并分配每小时执行变更检测的自定义监视配置文件，来比其他路由器更频繁地监视关键核心路由器。通过使用工厂监视配置文件（不包含任何变更检测）或自定义监视配置文件（将变更检测设置得不那么频繁），其他路由器可以保留在“所有路由器”设备集合中。

详细信息：

发现和轮询 (p. 56)
手工更新设备重新配置 (p. 100)
自动更新设备重新配置 (p. 99)

自动更新设备重新配置

对发现的设备进行的重新配置更改可能会影响与该设备关联的度量标准系列。可以将设备重新配置设置为在分配了度量标准系列的监视配置文件中自动更新，这适用于监视配置文件包含的所有度量标准系列。在您创建自定义监视配置文件时，默认已设置了此选项，但您也可以随时对其进行编辑。此过程说明了在之前已取消选择“自动更新度量标准系列”选项的情况下，如何在现有的自定义监视配置文件中设置该选项。

度量标准系列更新后，Data Aggregator 将具有精确的设备配置表述。您生成的报告将反映准确信息。

请执行以下步骤：

1. 导航到所有监视配置文件的列表。
2. 选择您想自动更新的监视配置文件，然后单击“编辑”。
3. 选择“启用变更检测”，然后执行下列步骤：
   - 设置“更改检测设置，比率”的值，该值必须大于零。

     注意：考虑度量标准系列可能更改的频率，以及监控配置文件应用的设备数量。避免过高的设置更改检测率。
   - 选择“自动更新度量标准系列”。
   - 单击“保存”。

   更改与此监视配置文件关联的设备的配置时，将自动更新该设备配置。

   设备配置更新后，Data Aggregator 将执行以下操作：
   - 在受监视的设备上生成一个事件。
   - 标识并创建新组件。

- 标识并报废不再存在的组件。

  注意：默认情况下，报废的组件不与 CA Performance Center 同步。要启用此选项，请在 CA Performance Center“管理数据源”页面的“编辑数据源”对话框中选中“同步报废的项”复选框。

- 标识自先前发现以来已更改的现有组件。如果适用，“名称”列将更改。

  注意：可以访问并报告历史数据。

详细信息：

如何管理变更检测 (p. 97)

手工更新设备重新配置

对发现的设备进行的重新配置更改可能会影响与该设备关联的度量标准系列。如果未在关联的监视配置文件中选择“自动更新度量标准系列”选项，可以手工更新设备重新配置。在这种情况下，您需要查看事件日志，以确定要为其更新度量标准系列的重新配置事件。

度量标准系列更新后，Data Aggregator 将具有精确的设备配置表述。您生成的报告将反映准确信息。

请执行以下步骤：

1. 查看事件日志，以确定要为其更新度量标准系列的重新配置事件 (p. 129)。
2. 针对 Data Aggregator 数据源，在“受监视清单”菜单中单击“受监视设备”。

   此时将打开“树视图”选项卡。

3. 从下拉列表中选择“设备(按收集)”，然后从对应的树形视图中选择已更新的受监视设备。

   “已轮询度量标准系列”选项卡显示与设备相关联的整合监视配置文件。设备只有一个整合的监视配置文件。每个整合的监视配置文件将列出可以在设备上轮询的每个度量标准系列，以及设备是否支持度量标准系列。

4. 选择您想更新其配置的度量标准系列，然后单击“更新度量标准系列”。

   设备配置更新完毕后，Data Aggregator 将执行以下操作：

   - 在受监视的设备上生成一个事件。
   - 标识并创建新组件。
   - 标识并报废不再存在的组件。

     注意：默认情况下，报废的组件不与 CA Performance Center 同步。要启用此选项，请在 CA Performance Center“管理数据源”页面的“编辑数据源”对话框中选中“同步报废的项”复选框。
   - 标识自先前发现以来已更改的现有组件。如果适用，“名称”列将更改。

     注意：可以访问并报告历史数据。

详细信息：

查看受监视设备 (p. 87)
如何管理变更检测 (p. 97)

第 5 章： 管理接口

此部分包含以下主题：

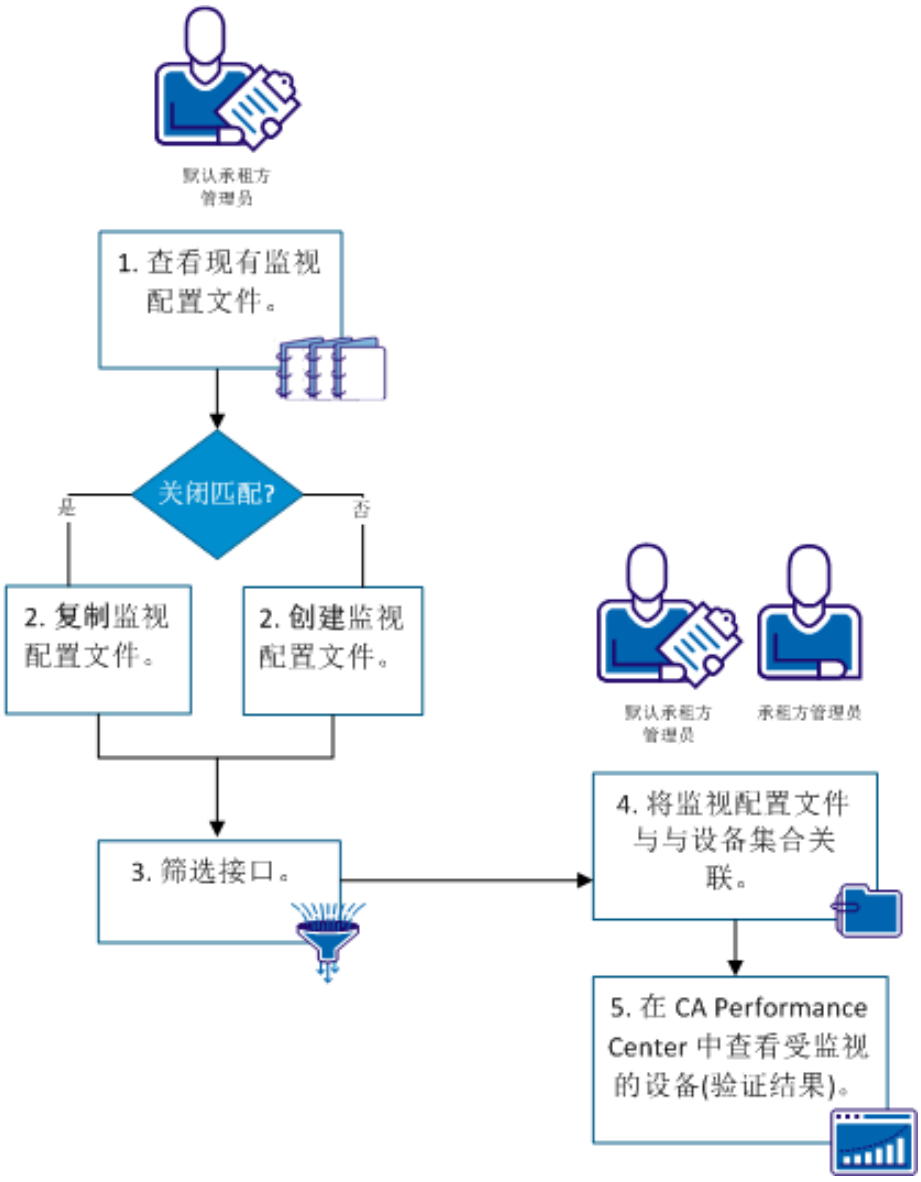
如何以比非关键接口更快的速度轮询关键接口

作为管理员，在最大化性能管理系统总体性能的同时，您还需要最关键系统的频繁数据。达到上述目标的一种方式是仅以较高速度轮询关键接口，而以正常或较慢速度轮询非关键接口。您可以针对与监视配置文件相关联的接口度量标准系列使用筛选，从而以不同速度进行轮询。通过谨慎地快速轮询接口，可以减少不必要的网络通信量和性能管理系统负荷，同时仍然足以监视网络系统的运行状况。

例如，您的数据中心入口交换机将许多应用程序服务器仅连接到了二个聚合交换机。您决定以较高速度轮询支持这些聚合交换机的接口。这些链路非常关键，因为它们支持到所有其他连接交换机的网络通信量。然而，以较高速度轮询*所有*接口将导致不必要的网络通信，浪费系统资源并可能导致网络性能问题。在与网络操作团队和工程团队商量之后，您认为普通轮询速度足以满足连接每个相连服务器的接口。要应用不同的轮询速度，您为接口实施了两个监视配置文件。

注意：当应用于监视配置文件的事件规则触发事件时，则会忽略您在度量标准系列上所设置的筛选。

下图显示了如何对监视配置文件进行配置以便以不同的速度轮询接口：



过程
查看现有的监视配置文件 (p. 105)。
复制工厂网络接口监视配置文件 (p. 106)。
在针对接口度量标准系列设置筛选 (p. 108)。
将监视配置文件与设备集合关联 (p. 110)。
查看受监视设备以检验您的结果 (p. 111)。

注意：有关监视配置文件如何与设备集合以及度量标准系列协同运行的更多信息，请参阅《*Data Aggregator 概述指南*》。

查看监视配置文件

作为 CA Performance Center 管理员，您决定尽量多地轮询关键接口。然而，您想最小化以如此之快的速度轮询*所有*接口可能产生的不必要的网络通信量。您决定为接口创建两个监视配置文件 — 一个为普通轮询速度，一个为较快轮询速度。

创建监视配置文件之前，您复查现有的监视配置文件以便找出最符合您需求的配置文件。

请执行以下步骤：

1. 在 Data Aggregator 数据源的“监视配置”菜单中单击“监视配置文件”。

   将填充监视配置文件的列表。

2. 选择一个监视配置文件。

   选定监视配置文件的详细信息将填充选项卡：

   - “度量标准系列”选项卡 — 显示与该特定监视配置文件关联的度量标准系列的列表。度量标准系列中包含轮询设备和组件所使用的度量标准。
   - “集合”选项卡 — 显示与该特定监视配置文件关联的设备集合列表。

详细信息：

故障排除：对所发现的度量标准系列的轮询已停止 (p. 150)

复制工厂监视配置文件

作为 CA Performance Center 管理员，您发现工厂网络监视配置文件最符合您的需求且仅需要一些很小的改动。因此，您创建一个副本，并使用该副本以更快的轮询速度仅轮询关键接口。

注意：您必须以管理员身份登录，才能执行此任务。

请执行以下步骤：

1. 导航到 CA Performance Center 中的所有监视配置文件的列表 (p. 105)。
2. 选择网络接口监视配置文件，然后单击“复制”。

   注意：工厂监视配置文件无法编辑或删除。所有监视配置文件（包括自定义监视配置文件）都是全局性的。

   此时将打开“创建/编辑监视配置文件”对话框。
3. 输入监视配置文件的以下信息：
   - **名称：**Uplink Interfaces
   - **说明**（可选）：监视所有关键上行链路设备的接口性能。
   - **SNMP 轮询比率：** 1 分钟

   注意：我们建议您重命名该配置文件。跨所有承租方实施唯一命名。

   请考虑有关轮询速度的以下信息：
   - 更改轮询速度时，最多需要两个周期，可使新轮询速度生效。当使用 60 分钟速度轮询现有设备时，会在具有默认时间范围“过去 1 小时”的显示板视图中显示“无数据可显示”消息。如果将显示板设置更改为前一个小时，可能会显示早期数据。但是，在新轮询周期完成之前，此视图不会显示最新数据。
   - 针对分配给多个具有不同轮询速度的监视配置文件的接口，使用所分配的最快速度进行轮询。

4. 将变更检测设置、比率值保留为 24 小时。

   请考虑有关变更检测率的以下信息：

   - *变更检测率*是 Data Aggregator 检查设备上的任何组件是否已被重新配置的频率。变更可能包括已创建的新组件，或者已淘汰的现有组件。

     注意：度量标准系列中指定的调整算法定义要查看的配置更改。有关变更检测和设备重新配置如何运作的详细信息，请参阅*《Data Aggregator 管理员指南》*。

   - “更改检测设置，比率”选项用于设置 Data Aggregator 检查变更的频率。可以分钟或小时为单位设置检测率。默认情况下，比率设置成 24 小时。

   - 将以您为与设备集合关联的所有监视配置文件指定的最快速率来检测更改。

5. 保持“自动更新度量标准系列”复选框为选中状态。

   此选项控制检测到更改或重新配置后 Data Aggregator 将如何响应。选择此选项将使得 Data Aggregator 能够自动开始监视新组件或停止监视已停用的组件。如果不选中此选项，则可以手动控制组件的监视，如下所示：

   a. 手动检查“事件显示”显示板，查看配置事件。

   b. 导航到 Data Aggregator 管理菜单，“受监视设备”，“轮询的度量标准系列”视图。

   c. 选择适当的度量标准系列，然后单击“更新度量标准系列”，以确保 Data Aggregator 获取此项设备最新的重新配置。

   注意：如果应用接口筛选，Data Aggregator 将只监视重新配置之后通过筛选条件的接口。

6. 在“已选择度量标准系列”列表中将接口度量标准系列作为唯一的度量标准系列。

7. 单击“保存”。

   您复制的监视配置文件将添加到“监视配置文件”列表中。然而，此监视配置文件直到您将其分配给某个设备集合才变为活动状态。

详细信息：

发现和轮询 (p. 56)
查看事件 (p. 129)
如何管理变更检测 (p. 97)
故障排除：对所发现的度量标准系列的轮询已停止 (p. 150)
发现工作流 (p. 54)
如何设置和激活接口筛选 (p. 113)

设置接口筛选

默认情况下，工厂网络接口监视配置文件包括一个筛选，以防止建模管理员关闭的接口。筛选减少了监视的接口数，从而减少不需要的数据收集和网络流量。

除了仅轮询管理员打开的接口之外，您还希望更频繁地轮询最关键的接口。要仅隔离和更快地轮询这些接口，您将第二个筛选条件添加到与您的自定义监视配置文件关联的接口筛选中。第二个筛选条件通过仅查找在其说明中包含“uplink”的接口，来隔离出那些关键的接口。

注意：您必须以管理员身份登录，才能执行此任务。

请执行以下步骤：

1. 在“监视配置文件”页面中选择您的接口监视配置文件（称为“Uplink Interfaces”） (p. 106)。
2. 在“度量标准系列”选项卡中单击“接口度量标准系列”行，然后单击“编辑筛选”。

   注意：不要直接单击度量标准系列名称，因为这样会链接到度量标准系列定义。请改为单击度量标准系列名称所在的行，以激活“编辑筛选”选项。
3. 单击“添加条件”按钮。

   注意：可以通过“and”运算连接多个条件。也就是说，必须符合所有条件才能被筛选。
4. 添加包含下列选项的筛选条件，然后单击“保存”：
   - 属性：说明
   - 操作：包含
   - 筛选值：uplink

   注意：“筛选值”字段区分大小写。

假设您使用其他属性的以下详细信息进行筛选：

- 对于“传入速度”和“传出速度”，可以在文本字段中使用小数（如 1.544），并可指定 bps、Kbps、Mbps 或 Gbps。
- 有关配置类型（即 ifType）的详细信息，请转至 iana 网站：http://www.iana.org/assignments/ianaiftype-mib http://www.iana.org/assignments/ianaiftype-mib。
- 对于“说明”和“别名”，仅在您选择“匹配正则表达式”或“不匹配正则表达式”运算时，才可使用正则表达式进行筛选。

保存您的更改时，过滤条件将显示在“度量标准系列”选项卡上。您现在可以将此监视配置文件应用于适当的集合，以开始轮询选定的接口。

注意：Data Aggregator 会在发现之后应用筛选。此时不会轮询与筛选条件不匹配的接口项。如果您在运行发现*之后*添加或编辑接口筛选，则这些项上的轮询将停止。这些接口项*不*显示在 CA Performance Center 显示板和数据视图中。

有关接口筛选和多个监视配置文件的注意事项

将多个监视配置文件分配给设备集合后，匹配条件的筛选将遵循 "or" 规则。因此，Data Aggregator 会监视满足此组中任意监视配置文件之条件的所有接口。

一些监视配置文件可能有筛选，另一些可能没有。另外，这些配置文件还可以指定不同的轮询速率。在这种情况下，Data Aggregator 会监视匹配任何监视配置文件的接口，但轮询速率可以不同。如果有多个监视配置文件应用于接口，Data Aggregator 会以最快的轮询速率轮询接口。

- 监视配置文件 1—筛选：“说明”中包含“X”，轮询速率：1 分钟
- 监视配置文件 2—筛选：无，轮询速率：5 分钟
- 监视配置文件 3—筛选：“说明”中包含“Y”，轮询速率：10 分钟

在本示例中，系统会每分钟轮询一次匹配监视配置文件 1 的接口。所有其他接口将每 5 分钟轮询一次。匹配监视配置文件 3 的接口也将匹配监视配置文件 2（不包含筛选）。将应用最快的轮询速率，因此没有接口会按 10 分钟的间隔时间轮询。

在这种情况下，如果一个监视配置文件不含筛选，可能会导致许多接口被过于频繁地轮询。因此，在您设置筛选之后，应从其他监视配置文件中删除关联，以确保仅监视与指定筛选相匹配的组件。

将监视配置文件分配给设备集合

作为管理员或承租方管理员，您可以将新的“上行链路接口”监视配置文件与设备集合相关联以开始轮询。在这种情况下，您要将该配置文件与“交换机”设备集合进行关联，该集合即与工厂“网络接口”监视配置文件相关联的同一设备集合。轮询速度将应用于此设备集合中的接口，如下所示：

- 快速轮询：满足 Uplink Interfaces 监视配置文件的筛选条件的接口。
- 普通轮询：网络接口监视配置文件发现的所有其他网络接口。

重要说明！所有自定义监视配置文件都是全局性的且对承租方管理员可见。但是，监视配置文件与特定设备集合的关联范围可以限定为承租方。

请执行以下步骤：

1. 在 Data Aggregator 数据源的“监视配置”菜单中单击“集合”。

   此时将显示设备集合列表。管理员可以查看他们所管理的承租方的设备集合。承租方管理员可以查看自己的（承租方）设备集合列表。

2. 选择“所有交换机”设备集合，然后单击“监视配置文件”选项卡。

   此时将有一个列表显示分配给选定设备集合的监视配置文件。该列表中已存在“网络接口”设备集合。

3. 单击“管理”。

   此时将打开“分配集合监视配置文件”对话框。

4. 选择 Uplink Interfaces 监视配置文件，然后单击“添加”。

   选定监视配置文件移到“分配的监视配置文件”列表。

5. 单击“保存”。

   将保存您所做的更改。

详细信息：

工厂监视配置文件关联 (p. 78)
故障排除：对所发现的度量标准系列的轮询已停止 (p. 150)
发现工作流 (p. 54)
如何设置和激活接口筛选 (p. 113)

查看受监视设备以验证结果

设置了您的监视配置文件之后，复查受监视设备和筛选报告，确认仅关键设备以较高速度轮询。该信息有助于您了解上下文信息，例如，正在使用哪些监视配置文件轮询设备组件。验证结果可以帮助您识别任何必要的调整，以便帮助您获得想要的轮询成果。

注意：受监视设备包括可管理设备以及可通过 ping 连接的设备（即，可访问但不可管理的设备）。不可访问的设备不是受监视设备。可以从“轮询的度量标准系列”选项卡查看受监视设备的组件。

请执行以下步骤：

1. 运行按需发现。

   注意：如果您的发现配置文件自动运行，则可以等待下一个排定发现。有关发现的详细信息，请参阅*《Data Aggregator 管理员指南》*。

2. 针对 Data Aggregator 数据源，在“受监视清单”菜单中单击“受监视设备”。

3. 从下拉列表中选择其中一个选项来定位相应树视图中的某个聚合交换机设备：

   - 设备(按集合)－您的设备显示在“所有交换机”设备集合下面。
   - 设备(按监视配置文件)－您的主要接口显示在“上行链路接口”监视配置文件下方的“设备”下面。

   注意：您也可以选择“搜索”选项卡，以便按主机名、设备名称或 IP 地址进行搜索。您可以输入部分名称或 IP 地址，以返回包含该部分匹配内容的设备的列表。不支持通配符和正则表达式。

   “已轮询度量标准系列”选项卡显示与交换机设备相关联的整合监视配置文件。设备只有一个整合的监视配置文件。每个整合的监视配置文件都会列出要在设备上轮询的各个度量标准系列，以及该设备是否支持该度量标准系列。

4. 选择接口度量标准系列。

   接口度量标准系列的“组件”表显示发现的接口组件的下列轮询状态之一：

   活动

   表示正在轮询组件。

   非活动

   表示对该组件的轮询已停止，因为不再为该设备监视该度量标准系列。

已报废

表示该组件不再位于该物理设备上。对该组件的轮询已停止。您可以查看历史数据，以便在报告中使用。默认情况下，报废的组件不与 CA Performance Center 同步。要启用此选项，请在 CA Performance Center“管理数据源”页面的“编辑数据源”对话框中选中“同步报废的项”复选框。

已筛选（仅限于接口组件）

表示该组件不传递筛选条件，并且对组件的轮询已停止。

注意：筛选的接口不显示在 CA Performance Center 显示板和数据视图中。

5. （可选）选择度量标准系列，然后单击“更新度量标准系列”。

   Data Aggregator 针对任何配置更新重新配置组件。例如，如果在服务器上添加磁盘驱动器，则可以使用“更新度量标准系列”按钮重新发现配置更新。配置更新会创建一个磁盘组件。

6. 单击“筛选报告”选项卡并执行这些步骤：

   a. 查看其他每个接口监视配置文件中的筛选，以确定它们是否在监视您要筛选的同一设备集合。

   b. 删除其他接口监视配置文件与将阻止筛选条件的设备集合之间的任何关联关系 (p. 80)。例如，如果新的接口监视配置文件与“所有路由器”设备集合关联，则删除*其他*接口监视配置文件与“所有路由器”集合之间的关系。

   c. 再运行一次发现，并复查更新的筛选报告，以确认新的筛选条件处于活动状态。如果筛选报告显示包含了不需要的监视配置文件，请重复上一步，直到您仅监视要监视的接口为止。

   “筛选报告”选项卡显示在组件监视期间已使用哪些接口筛选条件。该选项卡还显示在设备上标识的所有接口以及这些接口是否匹配指定的筛选条件的报告。

   注意：如果您更改自定义监视配置文件的规则，“接口筛选条件”窗格不反映这些更改。如果您解除监视配置文件与组的关联，则“接口筛选条件”窗格不反映这些更改。重新发现设备可筛选基于您对筛选条件和监视配置文件所做更改的接口。

详细信息：

发现和轮询 (p. 56)
手工更新设备重新配置 (p. 100)
清除接口筛选 (p. 114)
故障排除：对所发现的度量标准系列的轮询已停止 (p. 150)
如何设置和激活接口筛选 (p. 113)

如何设置和激活接口筛选

默认情况下，监视配置文件包括一个筛选，以防止对出于管理目的而关闭的接口进行建模。

筛选可减少受监视的度量标准系列数量，从而减少不需要的数据收集。对于您的*自定义*监视配置文件，您可以为度量标准系列指定其他筛选。

注意：当应用于监视配置文件的事件规则触发事件时，则会忽略您在度量标准系列上所设置的筛选。

当多个接口监视配置文件分配给一个设备集合时，筛选匹配条件遵循 "or" 规则。在这种情况下，匹配任何一个筛选条件的接口将被监视。

您可以在运行发现之前或之后添加或编辑度量标准系列。Data Aggregator 将在发现之后应用筛选。仅轮询符合筛选条件的组件项。如果您在运行发现*之后*添加或编辑度量标准系列筛选，则针对这些度量标准系列的轮询将会停止。这些度量标准系列*不*显示在 CA Performance Center 显示板和数据视图中。

注意：您必须以管理员身份登录，才能执行此任务。

要设置和激活度量标准系列筛选，请执行以下过程：

1. 如果自定义监视配置文件不存在，请创建一个配置文件，或复制一个配置文件以创建自定义配置文件。您不能为工厂监视配置文件编辑或设置筛选。
2. 从“监视配置文件”页面中选择一个自定义监视配置文件。从“度量标准系列”选项卡中单击某个度量标准系列对应的行，再单击“编辑筛选”，然后编辑筛选条件。

   注意：不要直接单击度量标准系列名称，因为这样会链接到度量标准系列定义。请改为单击度量标准系列名称所在的行，以激活“编辑筛选”选项。

   - “筛选值”字段区分大小写。
   - 对于传入速度和传出速度，可在文本窗口项中使用小数（如 1.544）指定 Mbps 值。
   - 有关配置类型的详细信息，请转至 iana 网站：http://www.iana.org/assignments/ianaiftype-mib http://www.iana.org/assignments/ianaiftype-mib。

   保存您的更改时，过滤条件将显示在“度量标准系列”选项卡上。
3. 将监视配置文件与设备集合关联 (p. 80)。

4. 运行发现 (p. 67)，然后在“受监视设备”页面上复查筛选报告 (p. 87)。查看每个接口监视配置文件中的筛选，以确定它们是否在监视您要筛选的同一设备集合。
5. 删除其他监视配置文件与能够阻止筛选条件的设备集合之间的任何关联关系 (p. 80)。例如，您的接口监视配置文件可能与“所有路由器”设备集合关联。在此情况下，删除*其他*监视配置文件和“所有路由器”设备集合之间的关联关系。
6. 复查更新的筛选报告，以确认新的筛选条件处于活动状态。如果筛选报告显示包括了不需要的监视配置文件，请重复以前的步骤。最后，不包括不需要的监视配置文件，您仅监视想要监视的度量标准系列。

清除接口筛选

接口筛选可与自定义监视配置文件结合使用，以减少监视的接口数。当您要为与自定义监视配置文件关联的所有设备集合收集数据时，可以清除接口筛选。

注意：您必须以管理员身份登录，才能执行此任务。

请执行以下步骤：

1. 导航到监视配置文件的列表。
2. 从列表中选择监视网络接口的自定义监视配置文件。

   将填充“度量标准系列”选项卡。
3. 选择一个接口度量标准系列，然后单击“清除筛选”。

   注意：只有选择设置了筛选的接口度量标准系列时，才会启用此选项。

   此时将打开确认对话框。
4. 单击“是”。

   您的更改即被保存，在“度量标准系列”选项卡上筛选状态显示星号 (*)，表示未设置筛选。筛选将应用于下一排定的发现（也可以手动运行发现）。

详细信息：

查看受监视设备 (p. 87)

接口组件命名约定

由接口供应商认证或高速接口供应商认证支持的接口组件命名约定基于以下逻辑：

- 如果 ifName 属性存在并具有值，接口则使用此值作为其名称。
- 如果 ifName 属性*不*存在或*不*具有值，接口则将使用 ifDescr 的值作为其名称。

注意：接口度量标准系列的新认证可以为接口名称提供不同的表达式。

接口使用率计算

Data Aggregator 为所有接口提供一种覆盖“传入速度”和“传出速度”值的方式，以帮助确保使用率计算使用适当的值。例如，您可能使用带宽命令来在您的路由器接口上配置 ifSpeedIn 和 ifSpeedOut，以影响路由判断。在这种情况下，通过 Data Aggregator 提供覆盖速度，以帮助确保正确计算使用率。

您在设备上所进行的设置可能会将该值更改为某个高于或低于实际可用数据速率的值。因此，由于对带宽的此操纵，为接口所进行的的使用率计算可能无法准确显示。为了帮助确保接口使用率得到正确计算，您要在 Data Aggregator 内针对接口提供覆盖速度。

覆盖接口上的传入速度和传出速度值

默认情况下，使用率是使用接口所属设备报告的“传入速度”和“传出速度”值计算得出的。但是，您可以覆盖这些速度值。这样，关于接口使用率的报告可能会更准确。

请执行以下步骤：

1. 针对 Data Aggregator 数据源，在“受监视清单”菜单中单击“受监视设备”。

   此时将显示“树视图”选项卡。

2. 从下拉列表中选择“设备(按集合)”和“设备(按监视配置文件)”。选择要覆盖其中接口传入速度和传出速度的设备，并在“轮询的度量标准系列”选项卡中选择适当的接口度量标准系列。

   此时设备上受监视的接口组件将显示在“接口组件”表中。

3. 选择要覆盖其传入速度和传出速度的接口组件并单击“编辑”。

此时显示“编辑接口”对话框。对话框显示默认的已发现“传入速度”和“传出速度”值。

4. 以每秒比特数为单位输入传入速度和传出速度并单击“保存”。

   注意：您可以通过单击“清除”并单击“保存”来删除覆盖。然后继续操作，CA Performance Center 中该接口的带宽使用率表将使用设备报告的速度值显示使用率。将在接口上生成一个事件，指示已删除速度覆盖。可以在 CA Performance Center 中的“事件显示”显示板中看到该事件。

   此时对话框关闭。被覆盖的接口传入速度和传出速度将带星号显示在“接口组件”表中。

   将在接口上生成一个事件，指示在接口上已覆盖“传入速度”和“传出速度”值。可以在 CA Performance Center 中的“事件显示”显示板中看到该事件。

   继续操作，CA Performance Center 中该接口的带宽使用率表将使用您指定的速度值显示使用率。

第 6 章： 事件

此部分包含以下主题：

事件性能方针

下列配置用于验证和衡量事件性能：

- 系统完全符合推荐的规范，适用于 500K 轮询项的“中等”生产系统（请参考系统大小规范）。
- 10 个事件规则，遍布要在轮询项中使用的超过 7 个监控配置文件中。
  - 有 1 个要对度量标准系列按 1 分钟比率评估的事件规则，其中包含大约 33% 的轮询项。
  - 有 1 个要对度量标准系列按 15 分钟比率评估的事件规则，其中包含大约 33% 的轮询项。
  - 剩余的规则应用于一部分要按 5 分钟比率被轮询的剩余项。
  - 事件规则平均分布在超过 4 个度量标准系列。
  - 每个规则各有 1 个固定条件和 1 个标准偏差条件。
  - 6 个事件规则有 5 分钟的持续时间以及 15 分钟的窗口。
  - 4 个事件规则有 15 分钟的持续时间以及 60 分钟的窗口。

  注意：为了获得最佳性能，请将同一度量标准系列的事件规则的监控配置文件数目限制到最小。例如，将监控配置文件应用于同一设备集时，在“接口”度量标准系列中，一个包含 10 个规则的监控配置文件的性能优于包含 1 个规则的 10 个监控配置文件。
- 与 100K 轮询项关联的事件规则的数目不确定。
- 有 5 个 Data Collector 系统，每个轮询大约 1/5 的项。

如何监控事件处理

要确定您是否执行过多的事件，需要监控 Data Aggregator 中的一些关键性能指标。Data Aggregator 中的事件按批次处理（如，一次性为大量项组评估和生成事件）。为此，我们使用通过 Data Aggregator 系统的自我监控机制跟踪的各种度量标准来评估 Data Aggregator 系统的运行状况。要查看这些重要度量标准，请将自定义 IM 设备 MultiTrend 视图添加到显示板中。使用下列来自度量标准系列 **Data Aggregator 事件计算时间**的度量标准编辑显示板：

- **事件过程队列大小** - 显示事件处理队列的大小。0，1 或 2 的常数值表示此系统运行正常并且能够维护当前事件。大于 2 的常数值表示系统能够维护当前事件负载，尽管系统可能落后（处理较早的轮询，而不是当前轮询周期）。没有后续恢复的队列大小增加（呈现下降趋势）表示事件已备份并且您的系统可能处于风险中。
- 以下两个度量标准互为补充。
  - **已清除事件计数** - 报告解决方案窗口中的已清除事件数目。
  - **已创建事件计数** - 报告解决方案窗口中的已提出事件数目。

  已提出或清除的连续大量事件可能会影响事件管理器数据库。

  如果这两个度量标准的组合总数在 5 分钟的轮询周期内检查 900 个事件，则超出了为中等系统推荐的 2-3 个事件/秒的生成速率。事件生成/清除在 5 分钟的轮询周期内集中检查 900 个事件是可以接受的。
- **已处理事件规则评估计数** -- 事件规则评估是单个事件规则针对单个项的评估 此度量标准跟踪事件规则的总数，乘以这些规则适用的项数。评估的数目越高，您的系统正在处理的任务越多。然而，并非所有评估都相等。例如，与包含较少固定条件且使用较小持续周期和窗口的评估相比，包含更多条件、更多的标准偏离条件或较大持续周期和窗口的评估更加昂贵。因此，您可以根据事件规则执行较多或较少的评估。

  如之前所述，在测试环境中，我们看到 5 分钟轮询周期内超出 150K 的评估会使系统面临风险。
- **计算事件的总时间–** 处理此度量标准系列的事件所需的总时间。如果此数目超出报告解决方案窗口的秒数，则表示事件当时已延迟或积压。

随着时间推移观察所有度量标准，您可以判断系统中事件性能的状况。另外，如果 Data Aggregator 系统中的 Karaf 日志包含数据库和/或其他错误，这可能表示系统处于压力之下。总之，这些自我监控的度量标准应该保持稳定。然而，在事件小时（默认为 2 到 4 AM UTC 之间）期间会运行一些数据库密集型作业，这可能导致自我监控度量标准的波动。如果度量标准恢复到稳定状态，系统仍可以被视为正常状态（尽管事件可能在系统繁忙时延迟）。

建议您缓慢开启事件，并在转向其他规则前判断系统的运行状况。我们也建议您在每个后续更改之后监控系统 24 小时的运行状况，因为夜间处理可能会有影响，尽管事件在白天运行时看似平稳。

超出阈值时如何修正

要在超出阈值时进行修正，请执行以下过程：

1. 每次关闭一个事件规则。在您在关闭其他规则之前、关闭每个规则之后，检查性能。
2. 减少正在被轮询的项数。
3. 减少带有正在轮询项的事件规则的监控配置文件数。
4. 如果这些步骤无法改善性能，请与 CA 支持部门联系。

性能管理事件

您可以使用事件规则定义两种类型的性能管理事件。将事件规则添加到监视配置文件。

超时阈值事件

在监测度量标准与时间窗口内指定持续时间的一组固定值不同时，被常量（固定值）规则触发。

示例：

可以定义一个事件，以在进行 5 分钟间隔轮询时，在给定 10 分钟时间窗口内，带宽使用率持续 5 分钟超过 80% 时生成事件。

偏离正常事件

在监测度量标准与时间窗口内指定持续时间的“正常”标准不同时，被标准偏差规则触发。“正常”基于计算的基准平均值。最初，收集有限信息后，将计算每天相同小时的基准平均值。有更多数据后，Data Aggregator 会将计算其平均值切换到一周内同一天同一小时的每小时平均值。

示例：

可以定义一个事件规则，在进行 5 分钟间隔轮询时，在给定 10 分钟时间窗口内，如果带宽使用率持续 5 分钟超出所计算的一周内同一天同一小时的平均值 1 个标准偏差，便生成事件。

基准平均值

根据收集的轮询数据量，计算*基准平均值*的方式有两种：

- 最初，作为同小时的每小时平均值的平均值（无论哪天）。
- 收集足够数据后，将其用作一周内同一天同一小时的每小时平均值的平均值。

基准平均值有助于说明选定监视度量标准的过去性能，并帮助评估当前性能。系统每隔一小时就会持续计算基准平均值和相关的标准偏差。标准偏差提供了有关在考虑计算基准平均值的情况下总数据中存在多大可变性的统计指示器。

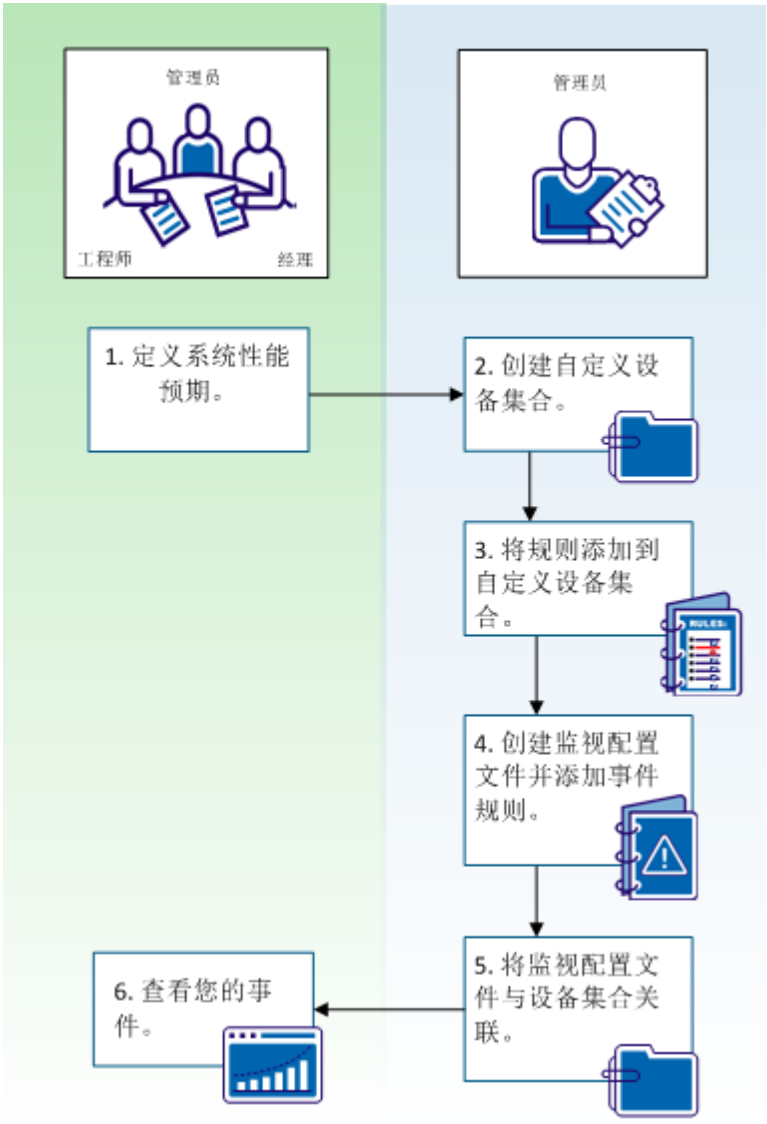
在 Data Aggregator 中，在一个时间窗口内在指定持续时间里被视为“正常”的基于计算的基准平均值。

如何使用事件监视设备性能

经理（如操作中心经理）和工程师（如 IT 操作员或 IT 架构师）需要其系统运行状况方面的连续信息。他们与工具管理员相互配合来配置 Data Aggregator，以针对偏离正常性能预期的设备生成事件。这些事件可帮助他们主动监视网络运行状况，并在需要时采取补救措施来修正性能问题。

例如，您的组织最近虚拟化若干对业务至关重要的应用程序，籍此提高效率。IT 架构师和运营中心经理希望监视这些虚拟服务器，以便确保他们可以应付来自这些应用程序的负载。工具管理员可以创建监视配置文件并添加事件规则，以发现虚拟设备集合中过度使用 CPU 和虚拟内存的问题。Data Aggregator 在为每一设备的每次轮询后，自动评估集合中的所有设备。需要时，如果设备满足事件规则条件，Data Aggregator 会生成或清除事件。

下列图示说明如何自动生成事件，以帮助您监视设备性能问题：



如图所示，工具管理员与工程师和经理们合作为一组设备定义性能预期。在此次讨论后，管理员决定创建一个自定义设备集合，创建一个监视配置文件，并将事件规则分配给监视配置文件。为了开始监视设备，管理员将监视配置文件及为其分配的事件规则与自定义设备集合关联起来。因为 CA Performance Center 生成事件，所以管理员、工程师和经理可以在 CA Performance Center 中查看事件。

过程
创建自定义设备集合 (p. 123)。
向自定义设备集合中添加规则 (p. 124)。

过程
创建监视配置文件并添加事件规则 (p. 125)。
将监视配置文件分配给自定义设备集合 (p. 128)。
查看您的事件 (p. 129)。

使用事件规则监视度量标准

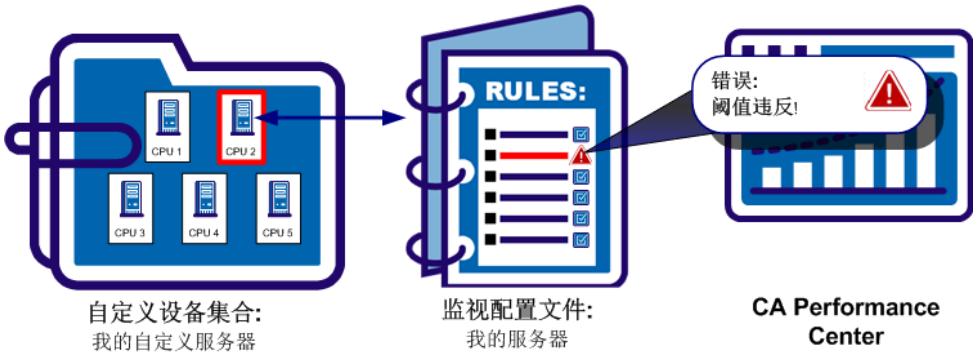
当监视网络环境的运行状况和状态时，事件提供有用的信息。此外，通过与 CA Spectrum 集成，您还可以使用事件来自动化基于事件消息中的数据的过程。

Data Aggregator 使用监视配置文件来处理事件。事件配置文件可以包含一组事件规则。这些规则使用度量标准（来自度量标准系列）定义您要监视的条件。

要实施事件规则，请将监视配置文件与设备集合关联。

重要说明！ *启动和停止监视过程的关键是设备集合。* Data Aggregator 无法使用监视配置文件，除非您将其与至少一个设备集合关联。

Data Aggregator 会立即将该监视配置文件中的规则应用于该设备集合中的设备。规则根据需要使用为这些设备轮询的度量标准值触发和清除事件。



事件显示在 CA Performance Center 显示板中。

注意：您可以基于已处理并在 Data Aggregator 中记录的事件，在 CA Spectrum 中生成用户可见的警报。有关详细信息，请参阅 CA Spectrum 文档。

创建自定义设备集合

作为 Data Aggregator 的工具管理员，您收到监视新的一组虚拟服务器的性能的请求。IT 架构师和操作中心经理想跟踪 CPU 使用率和内存使用率。这些虚拟服务器承载关键的应用程序，因此他们希望获得持续的状态更新。

注意：我们假定您已经在网络上运行了初始发现，并且已经发现了一些虚拟服务器。

由于没有用于虚拟服务器的工厂（即用型）设备集合，因此您决定先创建一个自定义设备集合来对所发现的虚拟服务器进行分组。要创建自定义设备集合，您需要先在 CA Performance Center 中创建一个自定义设备集合。自动同步在 Data Aggregator 中创建相应的设备集合。

请执行以下步骤：

1. 以具有管理员角色的用户身份登录到 CA Performance Center。
2. 选择“管理”、“自定义设置”、“组”。

   此时将打开“管理组”对话框。

3. 右键单击“受监视集合”，然后选择“添加新组”。

   此时将打开“添加组”对话框。默认选择“新建”选项卡。

4. 为下列参数提供值：

   组名称

   指定组的名称。在本示例中，将该组命名为“虚拟服务器”。

   注意：不要在组名称中使用以下特殊字符：/&\,%。

   说明

   （可选）帮助您标识组。

5. 单击“保存”。

   “虚拟服务器”组即显示在“受监视组”树中。等候与 Data Aggregator 的自动同步。完成同步后，Data Aggregator 将创建相应的设备集合，以用于设备监视。同步可能需要等待长达 5 分钟的时间才会。

向自定义设备集合中添加规则

网络和系统一直在变化。发现设备集合后，该集合会自动更新以包括这些设备。然而，要使自定义设备集合保持最新状态可能非常困难。因此，您可以使用规则来填充自定义设备集合。新发现的满足规则规范的设备将添加到集合中。同样，如果设备不满足规则要求或不再受监视，就会将其删除。

可将组规则添加到各组中，以基于各种条件自动填充和更新组内容。在这种情况下，您希望将组规则添加到“虚拟服务器”自定义设备集合中，以保持它使用最新发现的虚拟服务器。对于此方案，我们假定虚拟机的 IP 地址在指定范围之内。

请执行以下步骤：

1. 从 CA Performance Center 主菜单中选择“管理”、“自定义设置”，然后单击“组”。

   此时将打开“管理组”对话框。

2. 在“组树”中选择您想填充的组。

   注意：通过手工方式直接添加到组中的设备会在“组属性”窗格中显示为“直接项”。由于添加到组中的组件是受管设备的子项，因此它们是“组属性”中的“继承项”。

3. 单击“规则”选项卡，然后单击“添加规则”。

   此时将打开“添加规则”对话框。

4. 在“规则名称”字段中为规则提供一个名称。
5. 从“添加”列表中选择“设备”。
6. 单击“添加条件”。

   此时将出现一行下拉列表和字段。
7. 请执行以下操作：
   - 从第一个列表中选择“设备地址”。
   - 从第二个列表中选择“介于”作为匹配方式。
   - 在第三个列表中输入“从 *开始 IP 地址* 到 *结束 IP 地址*”，以指示可以找到虚拟机 IP 地址的范围。
8. 单击“预览结果”，确认新规则包含您想要的设备。

   结果将显示在“组规则预览”窗口中。您可以展开每个设备类型，以查看添加的特定设备。
9. 单击“保存”或单击“保存并运行规则”：
   - 保存－保存但不运行规则。该组在下一次全局同步时填充，全局同步每 5 分钟左右运行一次。
   - 保存并运行规则－保存规则并立即填充该组。

创建监视配置文件并添加事件规则

要设置监视“虚拟服务器”自定义设备集合中的虚拟服务器性能的进程，您需要先创建一个监视配置文件，并将事件规则添加到该监视配置文件。

事件规则不包括在工厂（即取即用型）监视配置文件中，您无法修改工厂监视配置文件以添加事件规则。您可以复制现有的监视配置文件，以作为创建类似但有一些更改的配置文件的基础。您将对自定义监视配置文件进行的更改就是添加事件规则。

通过与 IT 架构师和运行中心经理合作，您决定创建一个监视配置文件，并添加下列事件规则：

- 添加 VMware 内存使用率规则，如下所示：
  - 在一个 900 秒（15 分钟）窗口内，当内存使用率持续 300 秒（5 分钟）超过 80% 时，即出现违规。
  - 在一个 900 秒（15 分钟）窗口内，内存使用率持续 300 秒（5 分钟）等于或低于 75% 时，清除违规。

- 添加 VMware CPU 使用率规则，如下所示：
  - 以下两个条件*都*满足时，即会出现违规：
    - 条件 1：CPU 使用率高于 70%。
    - 条件 2：CPU 使用率高于一个标准偏离。
  - 这些条件在 900 秒窗口内持续 300 秒。

请执行以下步骤：

1. 选择“管理”、“数据源设置”，然后单击一个 Data Aggregator 数据源。
2. 从 Data Aggregator 管理页面上的“监视配置”菜单中单击“监视配置文件”。

   将填充监视配置文件的列表。
3. 选择“虚拟服务器”监视配置文件，然后单击“复制”。

   此时将打开“创建/编辑监视配置文件”对话框。
4. 将该监视配置文件的名称更改为“自定义虚拟服务器”。
5. 单击“保存”。

   复制的监视配置文件将被添加到“监视配置文件”列表中。
6. 选择“自定义虚拟服务器”监视配置文件。
7. 单击“事件规则”选项卡。
8. 创建 VMware 内存使用率事件规则，如下所示：
   a. 单击“新建”。
   b. 为您的新事件规则输入以下值：
      - **名称**：VirtualMemUsageTooHigh
      - **说明（可选）**：VMware 内存使用率
      - **度量标准系列**：VMware 虚拟机
      - **持续时间**：300

        注意：在此示例中，我们假定以 300 秒的默认速率轮询设备。“持续时间”值将用作违反阈值和清除阈值。
      - **时间窗口**：900

        注意：“时间窗口”值将用作违反阈值和清除阈值。
      - **重要级别**：重大
   c. 在“符合所有条件时发生违反”部分，选择以下值：
      - **度量标准**：VM 内存使用率

- **操作数：** 以上
- **值：**80
- **条件类型：**固定值

d. 在“以下条件下清除违反”部分，选择以下值：

- **操作数：**等于或低于
- **值：**75

e. 单击“保存”。

9. 单击“事件规则”选项卡。
10. 使用多个条件创建 VMware CPU 使用率事件规则，如下所示：

a. 在“事件规则”组框中单击“新建”。

b. 为您的新事件规则输入以下值：

- **名称：**VMwareCpuUtil
- **说明（可选）：**VMware CPU 使用率
- **度量标准系列：**VMware 虚拟机
- **持续时间：**300
- **时间窗口：**900
- **重要级别：**重大

c. 在“符合所有条件时发生违反”部分，选择以下值：

- **度量标准：**CPU 使用率
- **操作数：** 以上
- **值：**70
- **条件类型：**固定值

d. 单击“添加条件”。

e. 在“符合所有条件时发生违反”部分，选择以下值：

- **度量标准**：CPU 使用率
- **操作数**： 以上
- **值**：1
- **条件类型**：标准偏差

注意：多条件事件规则仅限于一个度量标准系列内的度量标准。在此示例中，我们假定度量标准系列已可用于 Data Aggregator。有关创建自定义度量标准系列的更多信息，请参阅《*Data Aggregator 自我认证指南*》。

如果定义了多个条件，当任何条件不再为真时，则会发出清除事件。

重要说明！从开始监视 Data Aggregator 的某个度量标准系列，到针对每个小时计算基准可能耗时长达 48 个小时。标准偏差规则需要基准数据。

11. 单击“保存”。

您的事件规则已保存。系统会筛选事件规则以获得“自定义虚拟服务器”监视配置文件中的度量标准系列，来帮助确保评估您定义的所有规则。

将监视配置文件分配给自定义设备集合

您已创建“自定义虚拟服务器”监视配置文件并添加事件规则来监视运行关键业务应用程序的虚拟机。要开始监视您的虚拟设备并激活事件规则，您需要将“我的虚拟服务器”监视配置文件分配给“虚拟服务器”自定义设备集合。

重要说明！*启动和停止监视过程的关键是设备集合*。Data Aggregator 无法使用监视配置文件，除非您将其与至少一个设备集合关联。

请执行以下步骤：

1. 从 Data Aggregator 管理页面上的“监视配置”菜单中单击“集合”。

   此时将显示设备集合列表。

2. 选择“虚拟服务器”设备集合，然后单击“监视配置文件”选项卡。

   列表将显示分配给选定设备集合的监视配置文件。此列表将为空。

3. 单击“管理”。

   此时将打开“分配集合监视配置文件”对话框。

4. 从“可用监视配置文件”列表中选择“我的虚拟服务器”监视配置文件，然后单击“添加”。

   该监视配置文件将移到“分配的监视配置文件”列表中。

5. 单击“保存”。

   Data Aggregator 即开始使用您的监视配置文件和事件规则监视此设备集合。生成的事件会显示在“事件显示”显示板中。

查看事件

CA Performance Center 将事件显示在称作“事件”视图的报告中。首先显示的是最近的事件。您可以控制事件报告的内容，显示与您最为相关的事件数据。报告内容的控制功能包括时间控制以及排序和筛选功能。

示例：

- **跟踪配置更改**--当您*没有*在自定义监视配置文件中选择“自动更新度量标准系列”选项时，您必须查看事件日志文件来了解是否有任何配置更改，然后在“受监视设备”的“轮询的度量标准系列”视图中手动单击“更新度量标准系列”，确保 Data Aggregator 选取设备重新配置。
- **排查性能问题**--要排查特定服务器的性能问题，您可以按服务器的 IP 地址筛选事件。“事件”视图可以筛选事件的完整列表，仅显示选定服务器的事件。

要查看事件，请单击 CA Performance Center 中的“显示板”菜单，并在“操作显示”下选择“事件显示”。

此时将打开“事件”视图。此表将显示选定时间范围内发生的事件，并最先列出最近发生的事件。

注意：有关事件的详细信息，请参阅*《CA Performance Center 操作员指南》*和 CA Performance Center 联机帮助。

如何从事件管理器配置通知

可以为从 Data Aggregator 发送至事件管理器的事件配置通知。系统将根据您为通知条件配置的条件评估传入事件。只有当满足这些条件时，事件管理器才会采取通知操作。如果事件未触发通知，事件仍然可以显示在事件列表中。

在“创建/编辑通知”向导中提供了以下通知类型：

陷阱

将陷阱通知发送到您环境中的故障或网络管理系统 (NMS)，例如 CA Spectrum。支持多个目标。第一个目标是必填的。

在“通知”向导中提供了两种 MIB 选择，以便为客户系统提供兼容性。

支持的角色：具有管理员角色的用户可以配置陷阱通知。

电子邮件

在引发或清除事件时，向一个或多个收件人发送电子邮件通知。电子邮件提供一个链接，用于查看触发警报的设备或组件的上下文页面。

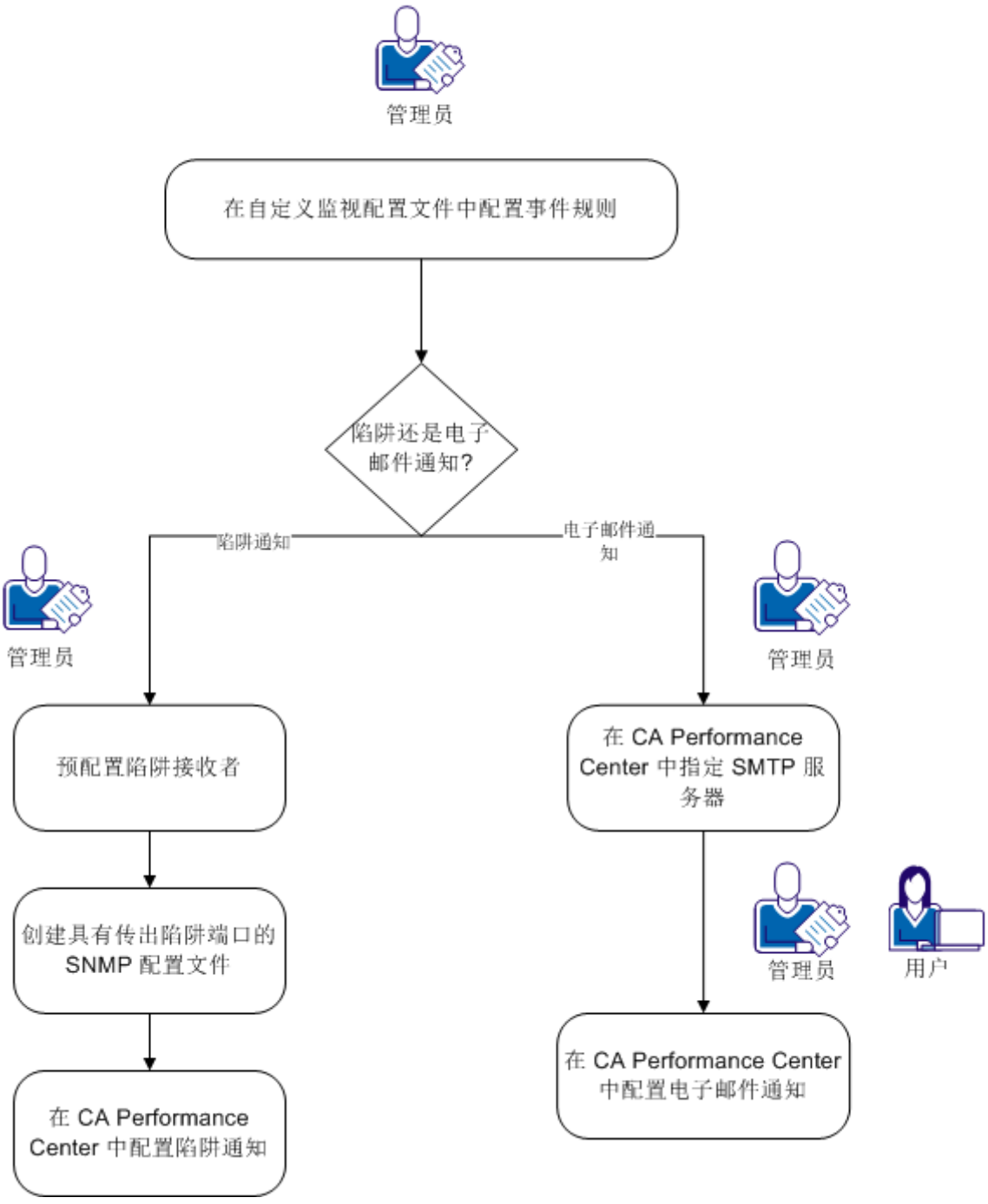
支持的角色：具有“创建通知”角色权限的用户可以配置电子邮件通知。

用户仅可以配置和接收自己有访问权限的组中的设备的事件通知。

考虑以下信息：

- 通知特定于用户；用户无法看到其他用户创建的通知。
- 只有当事件管理器被启用且处于已同步的“可用”状态时，才会显示“通知”选项。
- 删除事件通知的操作不影响实际或将来事件。

下图显示事件通知选项的可能工作流：



可以使用以下过程配置陷阱或电子邮件通知：

1. 在 Data Aggregator 数据源管理页面的监视配置文件的“事件规则”选项卡中配置事件规则。
2. （仅适用于陷阱）必须预先配置陷阱接收器，才能接收陷阱。每个目标可以具有其自身的 SNMP 社区和 IPV4 目标配置。有关陷阱格式的详细信息，请参阅适用于您的陷阱接收器的相应 NMS 文档。
3. （仅适用于陷阱）在创建通知之前使用传出陷阱端口（通常 162）创建 SNMP 配置文件。
4. （仅电子邮件）通过从 CA Performance Center 中选择“管理”、“系统设置”菜单选择“电子邮件服务器”，来配置 SMTP 服务器设置。
5. 执行以下操作之一：
   - （管理员）通过在 CA Performance Center 中选择“管理”、“通知”，来创建通知。对于陷阱通知，选择您在第 2 步中创建的 SNMP 配置文件。

     注意：作为默认承租方管理员，您可以在实际用户上下文中为承租方管理员或承租方用户创建通知。以承租方管理员或承租方用户身份登录。或者，默认承租方管理员可以管理承租人，然后代理用户创建针对承租方的通知。
   - （用户）通过在 CA Performance Center 中选择“我的设置”、“通知”来创建电子邮件通知。

   注意：管理员也可以使用事件管理器 API 来管理通知。使用此 URL http://*hostname*:8281/EventManager/webservice/notifications/documentation，访问事件管理器主机上的自我描述接口。

事件类型

在 CA 性能管理 中创建的每个事件都包括事件类型和可能的事件子类型信息。此信息可以帮助 CA 性能管理 正确处理事件，让您随时了解基础架构的状态和运行状况。

CA 性能管理 中提供的标准事件类型包括以下信息：

- 轮询事件－适用于轮询或轮询数据分析引起的事件
- 陷阱事件－适用于陷阱输入引起的事件
- 阈值事件－适用于由设备上的阈值违反触发的事件
- 重新配置更改－适用于已创建、损坏或修改的设备

- 未知事件－表示未知类型的事件
- 任何－表示一个特殊的通配符事件类型，使用它可以将提交到事件引擎的每个事件通知给订阅者。

事件类型在事件创建后自动分配。但是，CA 性能管理 使您可以定义自定义事件类型，以便于对事件进行一致的管理。使用自定义事件类型，您可以定义适用于您独特网络环境的事件系列。创建事件类型时，您需要确定该类型的必要属性。这样，单个事件类型的所有事件会始终提供相同的信息。

创建自定义事件类型之后，您可以设置事件标准化规则，将这些原始事件映射到您的自定义事件类型。有了规范化的事件，在定义事件处理方式时，您便可以忽略供应商和版本之间的差异。因此，CA 性能管理 可以处理规范化事件，以更具体地满足您的管理需求。

注意：有关事件的详细信息，请参阅*《CA Performance Center 操作员指南》*。

第 7 章： 报告

此部分包含以下主题：

如何使用视图

视图和报告可用于逻辑工作流，从而借助逻辑工作流查看整个企业以识别问题，进而深入到具体设备和组件以便隔离问题。在已知要对哪个系统或应用程序执行排除故障时，还可以直接导航到该设备和组件。视图中的信息还可用于主动发现潜在问题、制定容量规划以及编写有关网络运行状况的每月报告。

注意：轮询数据和您在视图和报表中看到这些数据之间可能会有延迟。如果数据加载错误，消息将记录在 Data Aggregator 设备上。

提供以下类型的视图和报告：

显示板

包含一系列视图，该视图可将轮询的数据视作有意义的信息并为整个企业的上层设备生成报告。选择“显示板”，然后从列表中选择特定的显示板以打开该显示板。您可以在需要时深入查看某个设备，然后深入查看设备组件。

设备视图

将轮询的数据显示为指定设备的一系列默认视图。从显示板深入查看，或者选择“清单”、“设备”，然后选择特定设备以查看来自该设备的数据视图。选择选项卡以按照性能类别查看设备上下文视图。

设备组件视图

在一个报告中同时显示设备组件的多个视图。从设备视图深入查看，或者选择“清单”、“设备组件”，然后选择组件以查看设备组件页面。

注意：有关自定义显示板和视图的信息，请参阅 CA Performance Center 联机帮助。

如果某个视图中不显示数据，请直接从该视图深入查看“受监视设备”页面以解决该问题。选择**“设置”**按钮，然后单击**“设备管理”**。此选项需要名为**“从视图进入 DA 管理页面”**的角色权限，该权限可以被分配给任何用户。默认情况下，全局管理员拥有此角色权限。

基准平均值

根据收集的轮询数据量，计算*基准平均值*的方式有两种：

- 最初，作为同小时的每小时平均值的平均值（无论哪天）。
- 收集足够数据后，将其用作一周内同一天同一小时的每小时平均值的平均值。

基准平均值有助于说明选定监视度量标准的过去性能，并帮助评估当前性能。系统每隔一小时就会持续计算基准平均值和相关的标准偏差。标准偏差提供了有关在考虑计算基准平均值的情况下总数据中存在多大可变性的统计指示器。

在 Data Aggregator 中，在一个时间窗口内在指定持续时间里被视为“正常”的基于计算的基准平均值。

第 95 百分位

百分位是特定百分比的观测数据都在其范围内的变量的值。例如，第 95 百分位是发现 95% 的观测数据都在其范围之内的值（或分值）。

*第 95 百分位监视*与带宽有关。该统计信息在度量数据吞吐量方面非常有用，因为它可以更准确地反映易受带宽影响的应用程序的受监视链路所需的容量。根据第 95 百分位所示，在 95% 的时间内，带宽使用量均在该数量之下。在剩余的 5% 的时间内，带宽使用量高于该数量。在使用第 95 百分位来执行容量规划时，我们建议为所监视的设备将轮询时间间隔设置为至少 1 分钟间隔。

计算第 95 百分位是出于累加和报告目的。

*累加*是指汇总度量标准值的过程。在按小时累加中，1 分钟、5 分钟、15 分钟、30 分钟和 60 分钟轮询的度量标准值每小时汇总一次。在按日累加中，每小时的度量标准值每天汇总一次。在按周累加中，每天的度量标准值每周汇总一次。

标准偏差

*标准偏差*显示与平均值（平均数或预期值）相差的变化量。标准偏差低表示数据点非常接近平均值。标准偏离高表示数据点值的分布范围很大。

计算标准偏差是出于累加、事件和报告目的。

*累加*是指汇总度量标准值的过程。在按小时累加中，1 分钟、5 分钟、15 分钟、30 分钟和 60 分钟轮询的度量标准值每小时汇总一次。在按日累加中，每小时的度量标准值每天汇总一次。在按周累加中，每天的度量标准值每周汇总一次。

最小值及最大值

所计算的最小值和最大值用于累加和报告。可通过这些值观察给定时间范围内的性能上限和下限。

*累加*是指汇总度量标准值的过程。在按小时累加中，1 分钟、5 分钟、15 分钟、30 分钟和 60 分钟轮询的度量标准值每小时汇总一次。在按日累加中，每小时的度量标准值每天汇总一次。在按周累加中，每天的度量标准值每周汇总一次。

按小时累加：

- 最小值：轮询值的最小值。
- 最大值：轮询值的最大值。

按日累加：

- 最小值：每小时最小值中的最小值。
- 最大值：每小时最大值中的最大值。

按周累加和更大时间单位的累加：

- 最小值：每日最小值中的最小值。
- 最大值：每日最大值中的最大值。

五分钟分辨率报告：

- 最小值：轮询值的最小值。
- 最大值：轮询值的最大值。

一小时分辨率报告：

- 最小值：每小时最小值中的最小值。
- 最大值：每小时最大值中的最大值。

一天分辨率报告：

- 最小值：每日最小值中的最小值。
- 最大值：每日最大值中的最大值。

附录 A： 计算

此部分包含以下主题：

基准平均值计算

最初，会在收集到有限数量的数据后，于每一周前一天的同一小时计算基准平均值。例如，在记录两天之后，通过计算连续两天同一时段的每小时累加，计算上午 9:00 到上午 10:00 的基准平均值。

最终，有更多数据后，会自动改变计算方法。Data Aggregator 通过计算一周内同一天前可用天数的每小时样本的平均值，来确定“正常”性能。然后，这种方法会考虑使用率中的星期日期模型。此方式生成更趋于“正常”的近似值，其可以减少未命中违规和误报事件的生成数目。在上述同一个示例中，记录三周后，通过计算这三个星期内三个星期一的上午 9:00 到上午 10:00 的每小时累加数据的平均值，来确定基准平均值。

注意：默认情况下，在至少一周内三天中同一小时的数据样本适用于过去 12 个周时，会出现这种自动改变。当所需的数据点数量不再可用时，Data Aggregator 自动切换回到每天同小时计算方式。这些默认设置是可配置的。有关更改这些默认设置的信息，请参阅 *《Data Aggregator REST Web 服务指南》*。

计算基准平均值是出于事件和报告生成目的。

示例：计算 CPU 使用率的同小时平均值和总体标准偏差

下例显示，在星期一、星期二和星期三有 3 个上午 2:00 数据点时，将针对特定设备的 CPU 使用率计算“同小时”平均值（中间数）和总体标准偏差。

请执行以下步骤：

1. 收集 3 个数据点。

天：	星期一	星期二	星期三
平均数（平均值）CPU 利用率：	76	65	10

2. 计算总体平均数。

   计算总体平均数的公式如下所示：

   总体平均值 = 数据点值之和除以数据点总数/数量。

   此示例的公式如下所示：

   (76+65+10)/3

   总体平均数= 50.33

3. 计算每个数据点与平均值之差。

   此示例的差值是：

   25.67 14.67 -40.33

4. 计算每个数据点的差值的平方。

   此示例的平方值是：

   658.78 215.11 1,626.778

5. 计算平方值的总和：

   此示例的平方的总和是 2,500.67。

6. 计算平方值的总和除以数据点的总数。

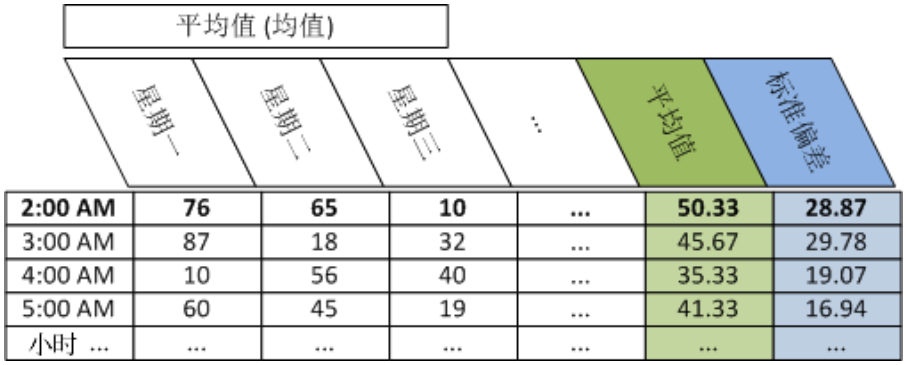
   此示例的结果是 833.56。

7. 根据总体平均值计算数据点值的平方之和的平方根。

   该示例的平方根为 28.87。

   该示例的标准偏差为 28.87。

下表说明每天比率数据的每小时平均值（平均数）、每小时平均值的平均值（平均数）和同小时的每小时平均值的总体标准偏差：



2:00 AM	**76**	**65**	**10**	**...**	**50.33**	**28.87**
3:00 AM	87	18	32	...	45.67	29.78
4:00 AM	10	56	40	...	35.33	19.07
5:00 AM	60	45	19	...	41.33	16.94
小时 ...	...	...	...	...	...	...

示例：计算 CPU 使用率的星期中同天同小时平均值和总体标准偏差

下例显示，在三个星期一上午 2:00 有 3 个 数据点时，将针对特定设备的 CPU 使用率计算平均值（中间数）和总体标准偏差。

请执行以下步骤：

1. 收集 3 个数据点。

   星期一： 1 2 3

   平均数（平均值）CPU 利用率： 76 4 6

2. 计算总体平均数。

   计算总体平均数的公式如下所示：

   总体平均值 = 数据点值之和除以数据点总数/数量。

   此示例的公式如下所示：

   (76+4+6)/3

   总体平均数 = 28.67

3. 计算每个数据点与平均值之差。

   此示例的差值是：

   47.33 -24.67 -22.67

4. 计算每个数据点的差值的平方。

   此示例的平方值是：

   2,240.44 608.44 513.78

5. 计算平方值的总和：

   此示例的平方的总和是 3,362.67。

6. 计算平方值的总和除以数据点的总数。

   此示例的结果是 1,120.89。

7. 根据总体平均数计算数据点值的平方之和的平方根。

   该示例的平方根为 33.48。

   该示例的标准偏差为 33.48。

下表说明每天比率数据的每小时平均值（平均数）、每小时平均值的平均值（平均数）和星期中同天同小时的每小时平均值的总体标准偏差：

	平均值 (均值)							
	第 1 周		第 2 周		第 3 周		星期一	
	星期一	...	星期一	...	星期一	...	平均值	标准偏差
2:00 AM	**76**	**...**	**4**	**...**	**6**	**...**	**28.67**	**33.48**
3:00 AM	87	...	71	...	56	...	71.33	12.66
4:00 AM	10	...	27	...	58	...	31.67	19.87
5:00 AM	60	...	3	...	32	...	31.67	23.27
小时 ...	...	...	...	...	...	...	...	...

示例：与正常值偏差，使用 CPU 使用率的星期中同天同小时平均值和总体标准偏差

假设 Data Aggregator 每 5 分钟轮询 CPU 使用率数据一次。您可以定义事件规则，在 CPU 使用率大于单个 5 分钟轮询间隔的均值之上的某个标准偏差时生成事件。

在此示例中，将事件规则持续时间以及窗口设置为 5 分钟。

计算何时生成事件的公式如下所示：

```
CPU 使用率 = 平均值 + 1（标准偏差值）
```

因此，之前一周内同一天同一小时（星期一早晨 2:00）的替换均值和标准偏差值如下所示：

```
CPU 使用率 = 28.67 + 1 (33.48)

CPU 使用率 = 62.15
```

因此，如果 CPU 使用率在星期一上午 1:05 和上午 2:00 之间超过 62.15 的持续时间为单个 5 分钟轮询时间间隔，便会生成事件。此事件表示 CPU 使用率偏离正常值的持续时间为该时间段。

示例：在趋势图视图中检查 CPU 使用率事件

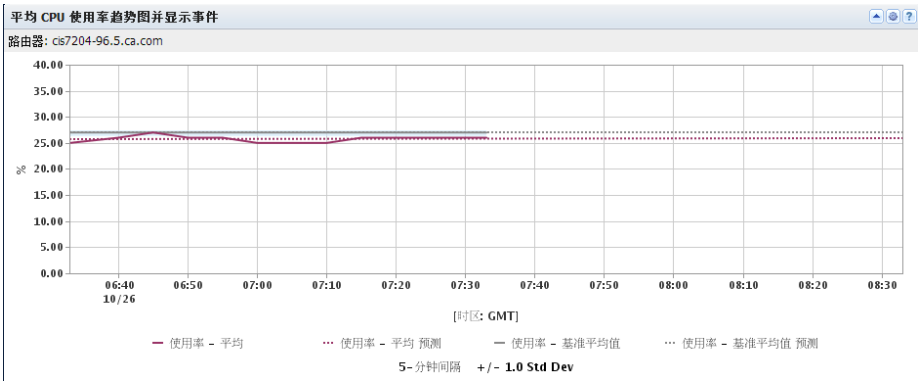
假设 Data Aggregator 每 5 分钟轮询 CPU 使用率数据一次。在此示例中，您想让系统在其中一个业务关键服务器上的 CPU 使用率低于预期水平时发出报警。您可以定义事件规则，在 CPU 使用率大于单个 5 分钟轮询间隔的均值之上的某个标准偏差时生成事件。

仅供说明，假定从星期一上午 12:00 到星期日上午 12:00，CPU 使用率是 50%。从星期日上午 12:00 到星期一上午 12:00，CPU 使用率下降到 10%。您预计到此次使用率会下降。但是，在 Data Aggregator 开始计算基准平均值时，系统会在 CPU 利用率下降到 10% 时生成事件。当 CPU 利用率返回到 50% 时清除事件。由于起初在系统收集限量的数据时会计算每天同一小时的基准平均值，而不考虑星期日期使用率的差异，因此会生成错误事件。Data Aggregator 预期 CPU 使用率*总是*保持 50%。

在三周之后，便可提供一周内三个同一天同一小时数据样本，基准平均值的计算方法也会随之改变。Data Aggregator 通过计算一周内相同天数的每小时样本的平均值，来确定“正常”性能。Data Aggregator 现在预期 CPU 使用率在每个星期日的上午 12:00 到星期一上午 12:00 达到 10%。将不再生成于之前每个星期日上午 12:00 生成的错误事件。

下列视图演示了最初如何计算每天同一小时的基准平均值。有更多数据后，会自动改变计算方法。Data Aggregator 会计算一周内同一天的每小时样本的平均值。

此视图还演示了在计算发生改变时不再生成错误事件。



第 95 百分位计算

计算第 95 百分位是出于累加、事件和生成报告目的。

累加：

- 对于按小时累加，第 95 百分位计算为一个连续的轮询值百分位。
- 对于按日累加，第 95 百分位计算为一个连续的每小时第 95 百分位。
- 对于按周累加和更大时间单位的累加，第 95 百分位计算为一个连续的每日第 95 百分位。

报告：

- 当时间分辨率少于一天时，第 95 百分位计算为一个连续的轮询值百分位。
- 当时间分辨率为一天或更大时，第 95 百分位计算为第 95 百分位的第 95 百分位。

示例：计算第 95 百分位

以下示例假定计算时段为 1 小时，轮询周期为 5 分钟，说明如何计算第 95 百分位。

请执行以下步骤：

1. 以 5 分钟轮询周期收集相当于 1 小时的数据。

   1 2 3 4 5 6 7 8 9 10 11 12

   30 10 20 70 60 30 80 10 90 20 70 50

   重新排序

   10 10 20 20 30 30 50 60 70 70 80 90

2. 计算行号 (RN)、最小行号 (FRN) 和最大行号 (CRN) 值。

   计算 RN、FRN 和 CRN 的公式如下所示：

   - RN = 1+((N-1)*P)

     N

     表示收集的轮询值的数目。

     P

     表示百分位值。

   - FRN = floor(RN)

     FRN

     表示不大于 RN 的最大整数。

   - CRN = ceiling(RN)

     CRN

     表示不小于 RN 的最小整数。

   此示例的公式如下所示：

   ```
   RN = 1+((12-1)*0.95) = 11.45
   FRN = floor(RN) = 11
   CRN = ceiling(RN) = 12
   ```

3. 计算第 95 百分位。

   计算第 95 百分位的公式如下所示：

   ```
   if (CRN = FRN = RN) then
   (value of expression from row at RN)
   else
   (value of expression for row at FRN) + (RN - FRN) * (CRN row - FRN row value)
   ```

   此示例的公式如下所示：

   ```
   (80) + (11.45 - 11)*(90-80) = 84.5000
   ```

   此示例的第 95 百分位是 84.5000。

标准偏差计算

计算标准偏差是出于累加、事件和生成报告目的。

累加：

- 对于按小时累加，标准偏差根据轮询值进行计算。
- 对于按日累加，标准偏差根据每小时平均值进行计算。
- 对于按周累加和更大时间单位的累加，标准偏差根据日平均值进行计算。

事件：

- 标准偏差提供了有关在考虑计算基准平均值的情况下总数据中存在多大可变性的统计指示器。

报告：

- 对于按小时报告，标准偏差根据轮询值进行计算。
- 对于按日报告，标准偏差根据每小时平均值进行计算。
- 对于按周报告和更大时间单位的报告，标准偏差根据日平均值进行计算。

示例：计算人口的标准偏差

以下示例给定 12 个数据点，说明如何计算人口的标准偏差。

*人口*指的是一组潜在值，同时包括观测到的用例和潜在的可观测到的用例。

计算该标准偏差的公式是：

```
population deviation = Square root of (Sum ( X - population mean)/number of data points)
```

X

是人口的数据点值。

请执行以下步骤：

1. 收集 12 个数据点。

   1 2 3 4 5 6 7 8 9 10 11 12

   30 10 20 70 60 30 80 10 90 20 70 50

2. 计算总体平均数。

   总体平均值 = 数据点值之和除以数据点总数/数量。

   此示例的人口平均值是 45。

3. 计算每个数据点与平均值之差。

   此示例的差值是：

   -15 -35 -25 25 15 -15 35 -35 45 -25 25 5

4. 计算每个数据点的差值的平方。

   此示例的平方值是：

   225 1225 625 625 225 225 1225 1225 2025 625 625 25

5. 计算平方值的总和：

   此示例的平方值的总和是 8900。

6. 计算平方值的总和除以数据点的总数。

   此示例的商是 741.6666667。

7. 根据总体平均值计算数据点值的平方之和的平方根。

   该示例的平方根为 27.23355773。

   该示例的标准偏差为 27.23355773。

总数计算

计算计数器度量标准是出于累加、事件和生成报告目的。计数器度量标准将对所设时段内所有示例的总和进行计算。当您在综合趋势视图类型的动态趋势视图中对所有项的总和进行计算时，将对视图中全部所选项的值的总和进行计算。另一方面，标尺度量类型将用于计算所设时段内所有示例的平均值。

示例：计算总和

以下示例假定计算时段为 1 小时，轮询周期为 5 分钟，并说明如何计算总和。

请执行以下步骤：

1. 以 5 分钟轮询周期收集 1 小时的数据。

   1 2 3 4 5 6 7 8 9 10 11 12

   40 10 30 60 70 20 50 20 80 30 40 60

2. 计算 12 个示例的总和。

   此示例的总和为：510。

考虑标尺和计数器度量类型时，聚合是指对某一视图中的所有项或所有组的值进行求和或计算平均值。在您计算大量聚集项中的标尺时，将分别添加这些项的平均值。随后，项目的数量将除以平均值的总和从而得出标尺。同样，通过获取所聚合每个项目的值的总和并对所有总和进行求和，即可计算出计数器。

示例：计数器和标尺度量指标

如果计算某一路由器下所有接口的计数器度量标准，则可查看吞吐量比特数。如果要查看所有接口的利用率，则须计算标尺度量标准。

最小值及最大值

所计算的最小值和最大值用于累加和报告。可通过这些值观察给定时间范围内的性能上限和下限。

*累加*是指汇总度量标准值的过程。在按小时累加中，1 分钟、5 分钟、15 分钟、30 分钟和 60 分钟轮询的度量标准值每小时汇总一次。在按日累加中，每小时的度量标准值每天汇总一次。在按周累加中，每天的度量标准值每周汇总一次。

按小时累加：

- 最小值：轮询值的最小值。
- 最大值：轮询值的最大值。

按日累加：

- 最小值：每小时最小值中的最小值。
- 最大值：每小时最大值中的最大值。

按周累加和更大时间单位的累加：

- 最小值：每日最小值中的最小值。
- 最大值：每日最大值中的最大值。

五分钟分辨率报告：

- 最小值：轮询值的最小值。
- 最大值：轮询值的最大值。

一小时分辨率报告：

- 最小值：每小时最小值中的最小值。
- 最大值：每小时最大值中的最大值。

一天分辨率报告：

- 最小值：每日最小值中的最小值。
- 最大值：每日最大值中的最大值。

附录 B： 故障排除

此部分包含以下主题：

故障排除：发现未启动

症状：

我选择了发现配置文件，然后单击“运行”运行发现，但发现未启动，或者“运行”按钮被禁用。

解决方案：

发现失败或“运行”按钮被禁用的可能原因如下：

- 先前在发现配置文件中指定的 IP 域已被删除。向 IP 域分配该发现配置文件。
- 还没有为选定发现配置文件中指定的 IP 域安装 Data Collector。

  注意：有关安装 Data Collector 主机的详细信息，请参阅 *《Data Aggregator 安装指南》*。
- 为选定发现配置文件中指定的 IP 域安装了一台或多台 Data Collector 主机。但是，为该 IP 域安装的所有的 Data Collector 主机都已停止。启动 Data Collector 主机。
- 承租方已被停用。激活承租方。

详细信息：

编辑发现配置文件 (p. 64)
启用承租方 (p. 95)

故障排除：对所发现的度量标准系列的轮询已停止

症状：

当我从“受监视设备”页面选择了设备之后发现该设备所支持的度量标准系列已停止轮询。但我并未打算停止对该度量标准系列进行轮询。

解决方案：

遵循以下过程以确定轮询停止的原因，并执行适当的步骤来解决这一问题：

1. 验证是否已定义监视配置文件，并将其设置为轮询所需的度量标准系列 (p. 79)。

   如果未满足该要求，请创建或编辑一个监视配置文件，并在其中定义所需的度量标准系列。

2. 确认该设备与设备集合关联 (p. 82)。

   如果该设备未与设备集合关联，请将设备添加到设备集合中。

   注意：有关向设备集合中添加设备的详细信息，请参阅《*CA Performance Center 管理员指南*》。

3. 确认该监视配置文件已与该设备集合和设备关联 (p. 79)。

   如果未关联监视配置文件，请创建监视配置文件和设备集合之间的关联关系 (p. 80)。

完成上述操作之一以重新启动轮询之后，请在“受监视设备”页面上选择设备以验证：

- “轮询的度量标准系列”选项卡中的度量标准系列的状态已更改。
- “接口组件”表中的状态已更改为“活动”。

轮询将自动在现有设备上恢复。

可通过以下方法之一发现新设备：

- 在“受监视设备”页面上选择所轮询的度量标准系列，然后单击“更新度量标准系列” (p. 87)。
- 在该度量标准系列的监视配置文件中设置变更检测率，并将自动发现设置为 True。

故障排除：轮询阻止事件消息

症状：

“轮询已停止”事件显示在我的事件列表中。为什么？

解决方案：

默认情况下，Data Aggregator 控制 SNMP 轮询，有助于确保过多的轮询请求不破坏设备。控制轮询流量的一种方式是 SNMP 超时阈值。默认阈值为 15。因此，当 15 个或更多 SNMP 请求超时时，轮询由于当前剩余轮询周期被暂停。事件生成，向您通知情况。

注意：轮询在每个轮询周期开始时恢复。如果完整的 5 分钟轮询周期内未发生超时，将生成“清除”事件。

故障排除：我的敏感设备未完成轮询

症状：

我必须监控一台关键设备，但是轮询无法在单个轮询周期内完成。有时，过多的网络流量会导致我的设备完全停止运行。此设备被认定为敏感，但是我如何才能可靠地轮询此设备来确保良好的性能？

解决方案：

轮询对于监控设备尤为重要。然而，过多的轮询可能导致大量网络流量，并降低成功监控设备的能力。如果大量网络流量正在破坏您的敏感设备，您可以尝试以下调整以减少到设备的总流量：

- 调整您的监控的置文件，以便从轮询删除不必要的度量标准系列。
- 在监控配置文件中应用筛选，以减少轮询接口的数目。
- 调整您的监控配置文件以降低轮询频率（例如，将 SNMP 轮询率更改到 15 分钟，而不是默认的 5 分钟）。
- 调整 SNMP 流量阈值，以降低同时发送给设备的 SNMP 请求的数目。
- 调整 SNMP 超时阈值以控制导致当前轮询周期暂停轮询的轮询超时数目。

故障排除：非预期 Data Aggregator 关闭

症状：

Data Aggregator 意外关闭。

解决方案：

如果 Data Aggregator 与 Data Repository 失去联系，那么它将关闭。如果与 Data Repository 失去联系，将在 *Data Aggregator 安装目录* /apache-karaf-2.3.0/shutdown.log 文件中记录一条审核消息。

注意： *Data Aggregator installation directory*/apache-karaf-2.3.0/shutdown_details.log 记录 Data Aggregator 和 Data Repository 之间的检测信号消息，以及出于调试目的的任何 Data Aggregator 关闭。

要解决任何连接问题或其他 Data Repository 问题，请执行以下步骤：

1. 确认 Data Repository 进程正在运行。请执行以下操作：
   a. 以数据库管理员用户（而非 root 用户）身份登录到 Data Repository 所用的数据库服务器。
   b. 键入以下命令：

      ```
      /opt/vertica/bin/adminTools
      ```

      此时将打开“Administration Tools”（管理工具）对话框。
   c. 选择“(1) 查看数据库群集状态”。

      返回的窗口应该说明：“主机”为“全部”，而“状态”为“启动”。
2. 如果 Data Repository 未运行，请尝试通过执行以下步骤来启动它：
   a. 登录到用于 Data Repository 的数据库服务器。
   b. 键入以下命令：

      ```
      /opt/vertica/bin/adminTools
      ```

      此时将打开“Administration Tools”（管理工具）对话框。
   c. 选择 (3)“启动数据库”。
   d. 按数据库名称旁边的空白条，选择**“确定”**，然后按 Enter 键。

      系统将提示您输入数据库密码。
   e. 输入数据库密码并按下 Enter 键。

      Data Repository 数据库启动。

      注意：如果您看到一条错误消息，指出由于用户名或密码错误而导致无法连接，则很可能是因为更改了数据库密码，导致 Data Aggregator 从 Data Repository 断开。
   f. 选择 (E)“退出”并按 Enter 键。

      如果 Data Repository 未启动，请与 CA 技术支持人员联系。

3. 如果 Data Repository 正在运行，则您的网络连接有问题，如发生了网络延迟问题。解决您的网络连接问题。
4. 一旦 Data Aggregator 重新运行，请立即设置 Data Aggregator 过程的自动恢复。

   注意：有关设置 Data Aggregator 过程的自动恢复的信息，请参阅*《Data Aggregator 安装指南》*。

故障排除：我无法备份 Data Repository

症状：

在我运行 vbr.py 脚本以备份 Data Repository 时，出现消息“另一个 vbr 实例已在运行”。

解决方案：

此消息表示之前的一个备份尝试失败，原因有多种，例如，未正确设置无密码的 ssh。

要重新尝试备份 Data Repository，请执行以下步骤：

1. 从安装有您要备份的 Data Repository 的计算机中删除 /tmp/.initiator.mutex 文件。

   下一排定的备份将正常进行。

故障排除：多个 SNMP 设备触发器入侵报警

症状：

我在更受限制的防火墙配置背后有许多 SNMP 设备（如 DMZ 网络）。出于安全原因，SNMP 设备有不同团体字符串。我为每个不同的团体字符串定义了 SNMP 配置文件，但是现在，我收到入侵警报并已从 CA Performance Center 被注销。

解决方案：

为了为设备找到正确的 SNMP 配置文件，CA Performance Center 尝试所有 SNMP 配置文件。此行为可触发器入侵警报并且使您从 CA Performance Center 注销。

要解决此问题，请执行以下过程：

1. 为关键的 SNMP 设备创建单独的发现配置文件。
2. 使用正确的团体字符串为发现配置文件分配 SNMP 配置文件。
3. 针对所有关键 SNMP 设备重复执行第一步和第二步。

在发现运行时，仅使用分配的 SNMP 配置文件。

词汇表

Data Collector

Data Collector 协调数据收集并密集轮询，以获取用于报告和事件分析的数据。在已发现设备及其受监视组件上将轮询操作度量标准和配置数据。收集的数据将通过 Data Aggregator 传递，并存储在 Data Repository 中。

工厂

Data Aggregator 中的术语“*工厂*”描述 CA Technologies 提供的并且通常随产品一起安装的项。例如，Data Aggregator 提供工厂供应商认证、监视配置文件等。有了这些即用型项，您可以在安装后立即运行 Data Aggregator。它们举例说明了如何创建或导入同一项的自定义版本。大多数情况下，Data Aggregator 用户无法编辑这些工厂项。

发现配置文件

*发现配置文件*指定清单发现的运行方式，包括用于定位您的设备的 IP 地址、IP 地址范围和主机名。

设备集合

*设备集合*是受监视设备的逻辑分组，如服务器或路由器。

度量标准系列

*度量标准系列*定义要为给定技术收集和报告的值的集合。这些值已进行标准化处理，因此无论数据源为何，报告都是统一的。当包含在监视配置文件中时，度量标准系列决定要为与监视配置文件关联的设备收集哪些值。

标准偏差

*标准偏差*显示与平均值（平均数或预期值）相差的变化量。标准偏差低表示数据点非常接近平均值。标准偏离高表示数据点值的分布范围很大。

项

*项*可以是 Data Aggregator 监视的设备、组件或接口。

监视配置文件

*监视配置文件*与一组设备相关联，以指定要轮询的信息以及轮询比例。这些参数将应用于该设备集合中的每台设备。您可以根据设备类型（如路由器、交换机和服务器）选择默认监视配置文件。
监视配置文件还包含事件规则，这些规则应用于关联设备集合中的每个设备项。对设备集合中的每个设备项和事件规则中指定的每个度量标准应用规则评估。这些规则评估将生成引发事件或清除事件。然后将这些活动发送给 CA Performance Center 的事件管理器、CA Spectrum 以及 CA Performance Center 通知程序以期进一步操作。

基准平均值

根据收集的轮询数据量，计算*基准平均值*的方式有两种：

- 最初，作为同小时的每小时平均值的平均值（无论哪天）。
- 收集足够数据后，将其用作一周内同一天同一小时的每小时平均值的平均值。

基准平均值有助于说明选定监视度量标准的过去性能，并帮助评估当前性能。系统每隔一小时就会持续计算基准平均值和相关的标准偏差。标准偏差提供了有关在考虑计算基准平均值的情况下总数据中存在多大可变性的统计指示器。

在 Data Aggregator 中，在一个时间窗口内在指定持续时间里被视为“正常”的基于计算的基准平均值。

第 95 百分位监视

*第 95 百分位监视*与带宽有关。该统计信息在度量数据吞吐量方面非常有用，因为它可以更准确地反映易受带宽影响的应用程序的受监视链路所需的容量。根据第 95 百分位所示，在 95% 的时间内，带宽使用量均在该数量之下。在剩余的 5% 的时间内，带宽使用量高于该数量。

累加

*累加*是指汇总度量标准值的过程。在按小时累加中，1 分钟、5 分钟、15 分钟、30 分钟和 60 分钟轮询的度量标准值每小时汇总一次。在按日累加中，每小时的度量标准值每天汇总一次。在按周累加中，每天的度量标准值每周汇总一次。