CA Virtual Assurance for Infrastructure Managers

管理指南

版本 12.8

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA IT Asset Manager (CA ITAM)
- CA IT Client Manager (CA ITCM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Server Automation
- CA Service Desk Manager (CA SDM)
- CA Spectrum®
- CA SystemEDGE
- CA Systems Performance for Infrastructure Managers
- CA Virtual Assurance for Infrastructure Managers
- CA Software Delivery

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： 简介

此部分包含以下主题：

读者

本指南适用于安装、配置和使用 CA Virtual Assurance 来管理虚拟环境的管理员。本指南假定您熟悉环境中所使用的操作系统、虚拟化技术和 SNMP。

相关出版物

CA Virtual Assurance 文档包括以下交付成果：

管理指南

了解如何管理和使用 CA Virtual Assurance 以在您的环境中管理虚拟资源。

安装指南

包含简短的体系结构信息、各种安装方法、后继安装配置信息以及入门说明。

联机帮助

提供有关窗口详细信息和程序说明，以便使用 CA Virtual Assurance 用户界面。

参考指南

提供有关 AutoShell、CLI 命令、MIB 属性的详细信息。

性能度量标准参考

说明可用于监控支持的平台的系统性能的性能度量标准。

版本说明

提供有关操作系统支持、系统要求、已发布的修正、国际化支持、已知问题以及文档路线图。

服务响应监控用户指南

提供 SRM 的安装和配置详细信息。

SystemEDGE 用户指南

提供 SystemEDGE 的安装和配置详细信息。

SystemEDGE 版本说明

提供有关操作系统支持、系统要求和功能的信息。

约定

本指南使用以下约定：

区分大小写

在本指南中提到的所有类、命令、指令、环境参数、函数和属性的名称均区分大小写，您必须按显示的形式正确拼写它们。- 系统命令和环境变量名称 *可能*区分大小写，视操作系统的要求而定。-

交叉引用

对其他指南或本指南其他部分中信息的引用采用以下格式：

指南名称

指示其他指南的名称。

“章名称”

表示本指南或其他指南中的章节名称。

同义词

属性、对象和对象标识符 (OID) 等术语与本文档中的术语“变量”是同义的。

SystemEDGE 代理和 CA SystemEDGE 等术语与本文档中的 SystemEDGE 是同义的。

语法

语法和用户输入使用以下格式：

斜体

表示必须为其提供实际值的变量名或占位符。

{a|b}

表示选择强制性操作数（a 或 b）。

[ ] 或 [[ ]]

表示可选操作数。

语法示例

以下示例使用这些约定：

```
modify -t ZONE [-m zoneserver] -p psetname {-min mincpu|-max maxcpu} pset
-session ssh
```

操作数 -min 和 -max 是强制性的，但您可以只使用二者之一，具体视希望定义处理器集中 CPU 的最小数量还是最大数量而定。操作数 -m 不是该命令运行所必需的。该命令的所有其他部分必须按显示的形式进行输入。

默认目录

在路径语句中使用的 *CASYSEDGE* 表示在其中安装 SystemEDGE 的目录。**默认值：**C:\Program Files\CA\SystemEDGE。

安装路径

在路径语句中使用的 *Install_Path* 表示在其中安装 CA Virtual Assurance 或 CA Virtual Assurance 组件的目录。

默认值：

- Windows x86：C:\Program Files\CA
- Windows x64：C:\CA、C:\Program Files (x86)\CA 或 C:\Program Files\CA
- UNIX、Linux：/opt/CA

第 2 章： 概述

此部分包含以下主题：

体系结构

CA Virtual Assurance 是基于策略的产品，可自动监控物理和虚拟资源，以动态地满足复杂数据中心的负载需求。CA Virtual Assurance 使用面向服务的体系结构 (SOA) 并持续分析您的数据中心，以验证您的服务器是否经过最优开通来执行所需任务。使用基于 Web 的用户界面，可以管理数据中心并获得有关数据中心中每台受管计算机的详细信息。

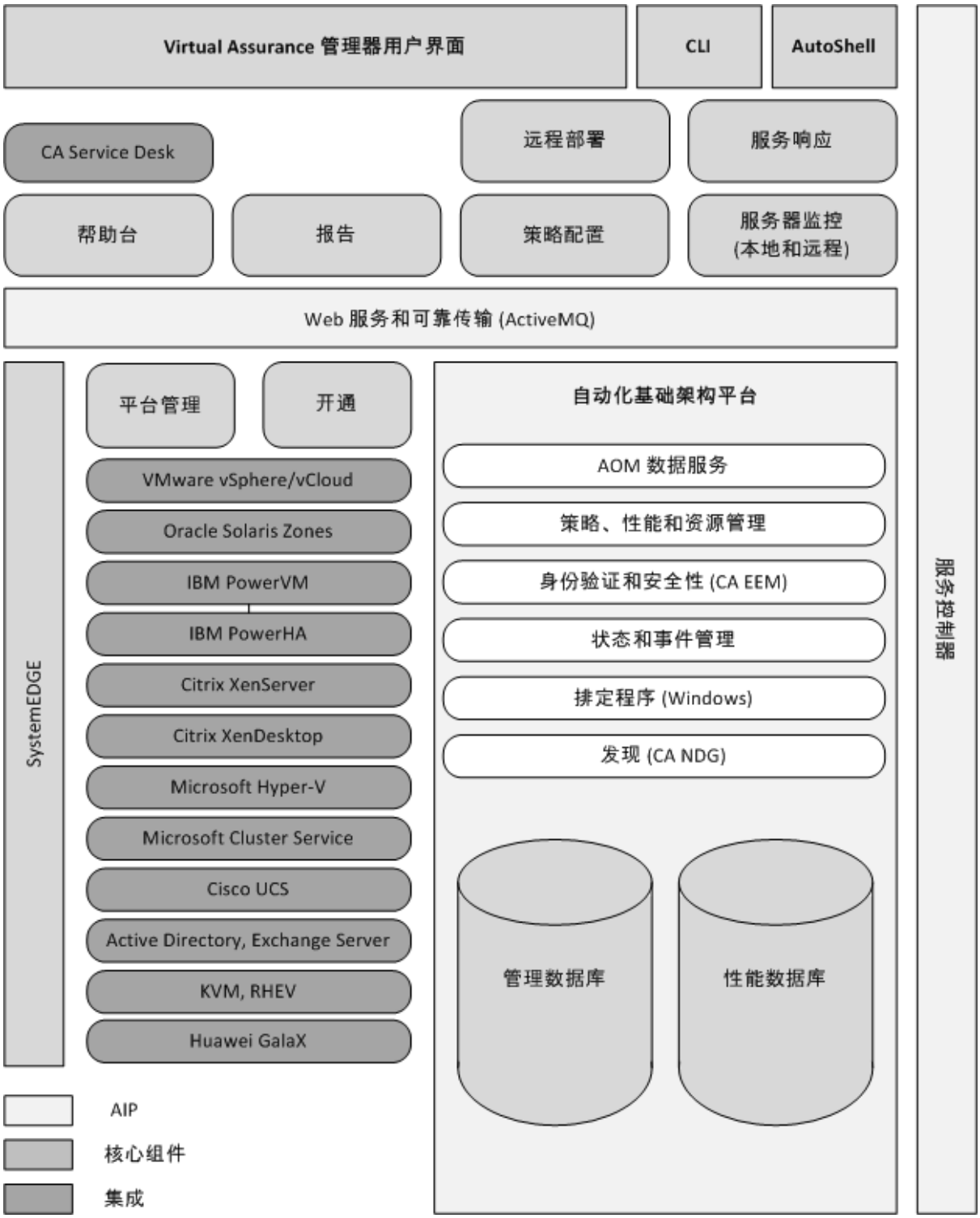
CA Virtual Assurance 与以下外部技术相集成：

- 思科统一计算系统
- Citrix XenDesktop
- Citrix XenServer
- Huawei GalaX
- IBM PowerHA
- 用于 AIX 虚拟化管理的 IBM PowerVM
- Microsoft 群集服务
- 用于虚拟机 (VM) 管理的 Microsoft Hyper-V Server 和用于开通的与 Microsoft System Center Virtual Machine Manager (SCVMM) 的可选集成
- Red Hat Enterprise Virtualization (RHEV)
- Solaris Zones 虚拟化管理
- 用于虚拟机 (VM) 管理的 VMware vCenter 服务器
- VMware vCloud

CA Virtual Assurance 利用以下现有技术：

- 用于请求升级和解决的 CA SDM 集成
- CA EEM，用于安全
- 用于轻型独立发现功能的通用发现

下图显示产品体系结构：


Virtual Assurance 管理器用户界面
CLI
AutoShell
CA Service Desk
远程部署
服务响应
帮助台
报告
策略配置
服务器监控
(本地和远程)
Web 服务和可靠传输 (ActiveMQ)
SystemEDGE
平台管理
开通
VMware vSphere/vCloud
Oracle Solaris Zones
IBM PowerVM
IBM PowerHA
Citrix XenServer
Citrix XenDesktop
Microsoft Hyper-V
Microsoft Cluster Service
Cisco UCS
Active Directory, Exchange Server
KVM, RHEV
Huawei GalaX
自动化基础架构平台
AOM 数据服务
策略、性能和资源管理
身份验证和安全性 (CA EEM)
状态和事件管理
排定程序 (Windows)
发现 (CA NDG)
管理数据库
性能数据库
服务控制器
AIP
核心组件
集成

每个组件在启动时向服务控制器注册。服务控制器是用于标识所有组件的位置和状态的中心组件。在注册组件后，服务控制器将提供其 Web 服务描述语言 (WSDL) 位置并发布其事件，以供其他组件订阅和接收数据中心更改的实时通知。

开通组件可为 vCenter 服务器、Hyper-V 和 Solaris Zones 提供开通功能。此外，还可以将 CA Virtual Assurance 提供的 SystemEDGE 和 AIM 部署到远程服务器。

资源管理器组件负责更新产品中的所有资源，如创建和更新用户定义的服务。

初始组件支持与 Microsoft 调度程序集成以进行作业排定。例如，可将长期运行的维护任务和操作排定为作业。

CA EEM 用于所有基于安全和基于角色的管理。

CA Virtual Assurance Event Manager 可捕获 CA Virtual Assurance 组件生成的所有事件并提供 SNMP 转发。SNMP 转发可用于将事件转发给任何 CA 产品或能够接收 SNMP 陷阱的第三方产品。

策略组件用于分析所收集的数据。

性能监视器组件与 SystemEDGE 集成以收集系统性能数据。除非使用远程监控 AIM 从远程监控未安装其他任何软件（零印记）的 Windows 服务器，否则必须在要从中收集基本系统度量标准的服务器安装 SystemEDGE。所有性能度量标准都存储在性能数据库中。

在使用受管服务器填充管理数据库后，性能监视器开始收集信息以确定服务器是否可以收集性能度量标准。

策略组件将分析所收集的数据以确定违反了哪些用户定义的业务规则，并对目标服务器或服务运行操作。您需要提前定义用于解决特定问题的规则和操作。策略组件使用参数做出明智的决策。在确定服务器或服务后，可以执行各种操作来解决问题。例如，运行自定义脚本、开通新系统等。

最后，可以直接从图形用户界面中通过图形和图表或者通过 CA Virtual Assurance 生成的报告监控数据中心性能。CA Virtual Assurance 还允许您查看其当前组件状态、配置组件、验证设置或创建用户访问列表。

映像服务

CA Virtual Assurance 可以开通新虚拟机、逻辑分区或 Solaris Zones，并且在适当的时候重新制作现有资源的映像。开通功能使您可以克隆、迁移、配置和更改虚拟机的属性，还可以创建和管理 LPAR 和 Solaris Zones。

映像服务组件使用以下技术并与其集成以执行开通操作：

- 用于虚拟机开通的 VMware vCenter 服务器集成。
- 用于 VM 开通的 Hyper-V 集成，该集成基于 Hyper-V 服务器的开箱即用本地模板。
  - 与 Microsoft System Center Virtual Machine Manger (SCVMM) 集成以重复使用现有 SCVMM 映像库。
- 用于区域开通的 Solaris Zones 集成。
- 用于 VM 开通的 Citrix XenServer 集成。
- 用于 VM 开通的 VMware vCloud Director 集成。
- 用于 KVM 开通的 Red Hat Enterprise Virtualization 集成

映像服务可为以下行为生成事件：

- 映像作业已提交给映像服务器。
- 映像作业状态发生更改。
- 在映像作业成功后，发现目标计算机。

数据库

产品既使用管理数据库，又使用性能数据库。

管理数据库

管理数据库是所有受管对象的通用数据存储库，基于描述管理数据的模型。管理数据库存储有关服务器、服务、规则、操作、虚拟平台对象、事件、报警以及这些对象之间的关系的信息。

CA Virtual Assurance 使用管理数据库存储以下信息：

- 服务器信息
- 服务关系
- 服务阈值

- 规则和操作
- 事件
- 其他组件的凭据

注意：有关配置管理数据库的详细信息，请参阅*《参考指南》*中的“命令行实用工具”一章，

性能数据库

性能数据库是一个存储库，用于存储从您的数据中心的服务器收集的所有度量标准。

CA Virtual Assurance 使用性能数据库存储以下信息：

- 从哪些服务器收集哪些度量标准
- 这些度量标准（随时间聚合）的值
- 服务器级别的记录间隔
- 服务器级别的阈值（整体服务器利用率）
- 数据中心级别的记录间隔
- 数据中心级别的阈值

存储在该数据库中的数据可用于各种功能。例如，该数据库是用于创建历史报告的数据的源。CA Virtual Assurance 还使用该数据库中的数据及用户创建的规则来制定逻辑业务决策。

注意：有关配置性能数据库的详细信息，请参阅“section dpmutil -perfdb 命令—配置性能数据库”一节。

用户界面

您可以使用 CA Virtual Assurance 基于 Web 的用户界面从中央位置管理数据中心。您可以在 CA Virtual Assurance 中使用嵌入式组件的功能，而无需分别打开组件界面。要自动化重复性工作，可以使用 AutoShell 界面。

例如，可以使用 CA SDM 进行问题管理，使用 JasperReports（默认报告引擎）从 CA Virtual Assurance 基于 Web 的用户界面中进行报告。还可以使用 CA EEM 功能来利用 Active Directory，以及从用户界面管理用户和权限，而无需打开 CA EEM。

您始终可以选择直接访问组件用户界面来执行更多高级功能。例如，您可能需要打开 CA EEM 以使用本地安全性。可以登录到安装有组件的服务器以直接访问其用户界面。或者，可以转到“管理”选项卡（CA Virtual Assurance UI 中的“配置”页面），选择组件，然后从“操作”下拉菜单中启动产品主页。

访问用户界面

访问用户界面可以发现并开通虚拟和物理系统、创建策略、排定作业等。“开始”菜单快捷方式只在 CA Virtual Assurance 服务器上可用。您必须直接访问管理器服务器，并使用“开始”菜单来使用一些产品功能，如 CLI 和 Autoshell。用户如果要从单独的服务器访问该界面，必须在 Web 浏览器中输入 URL。

访问用户界面

1. 选择“开始”、“程序”、“CA”、“CA Virtual Assurance”，从 CA Virtual Assurance 服务器启动 CA Virtual Assurance。

   将在以下 URL 显示 CA Virtual Assurance 登录页：

   ```
   https://servername:port/UI
   ```

   servername

   标识安装图形用户界面的服务器的名称。

   port

   指定服务器正在侦听的端口。

   默认：8443

2. 输入您的管理员登录凭据，然后单击“登录”。

   将出现“显示板”。

eHealth 集成概述

作为系统管理员，可将 eHealth 用于在物理 IT 基础架构中进行性能管理和报告。您希望将这些功能扩展到受管物理和虚拟服务器环境。

CA Virtual Assurance 使用 Application Insight Module (AIM) 管理和监控物理和虚拟系统环境。

注意：支持的环境因 CA Virtual Assurance 和 eHealth 版本而异。有关详细信息，请参阅 eHealth 文档。

下图提供了有关系统管理员如何设置 CA Virtual Assurance 以使 eHealth 能够监控 CA Virtual Assurance 受管环境的概述：

1. 安装 CA Virtual Assurance。

   注意：有关详细信息，请参阅*《CA Virtual Assurance 安装指南》*。

2. 在 CA Virtual Assurance 中配置 SNMP。

   验证 CA Virtual Assurance SNMP 配置是否与 eHealth 端口设置一致。如果将 CA Virtual Assurance 和 eHealth 安装在不同网络上，请验证相应防火墙端口是否已打开。

   注意：有关详细信息，请参阅*《CA Virtual Assurance 管理指南》*。

3. 从 CA Virtual Assurance 为您的环境部署 AIM。

   将相应的 AIM 和代理部署方法用于基础架构和环境。

   注意：有关详细信息，请参阅*《CA Virtual Assurance 管理指南》*。

4. （可选）发现带有 CA Virtual Assurance 的环境。

   发现环境的组件，从而在 CA Virtual Assurance 中启用服务器管理。

   注意：有关详细信息，请参阅*《CA Virtual Assurance 管理指南》*和*联机帮助*。

5. 发现带有 eHealth 的 AIM 服务器。

   AIM 对 eHealth 公开其支持的基础架构。

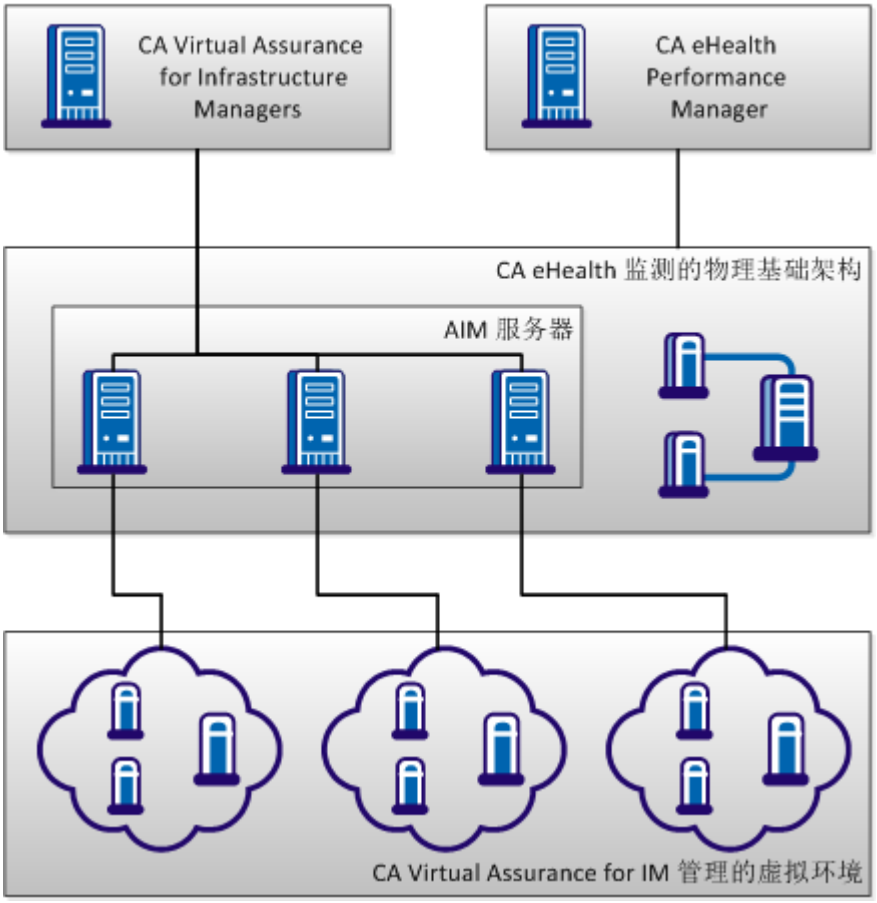
   注意：有关详细信息，请参阅 eHealth 文档。

eHealth 在其导航面板中显示发现的基础架构，并提供性能显示板以及环境组件的接近实时的性能和可用性报告。

使用 CA Virtual Assurance 管理环境组件并实施基于策略的管理。

下图表示有关集成基础架构的概述：

集成基础架构概览



Spectrum Infrastructure Manager 集成概述

作为系统管理员，可使用 Spectrum Infrastructure Manager 管理和监控物理 IT 基础架构，从而将故障隔离并找到原因。您希望将这些功能扩展到虚拟环境。

CA Virtual Assurance 使用 Application Insight Module (AIM) 管理和监控物理和虚拟系统环境。

注意：支持的环境因 CA Virtual Assurance 和 Spectrum Infrastructure Manager 版本而异。有关详细信息，请参阅 Spectrum Infrastructure Manager 文档。

下图提供了有关系统管理员如何设置 CA Virtual Assurance 以使 Spectrum Infrastructure Manager 能够建模和监控 CA Virtual Assurance 受管环境的概述：

1. 安装 CA Virtual Assurance。

   注意：有关详细信息，请参阅*《CA Virtual Assurance 安装指南》*。

2. 在 CA Virtual Assurance 中配置 SNMP。

   验证 CA Virtual Assurance SNMP 配置是否与 Spectrum Infrastructure Manager 端口设置一致。如果将 CA Virtual Assurance 和 Spectrum Infrastructure Manager 安装在不同网络上，请验证相应防火墙端口是否已打开。

   注意：有关详细信息，请参阅*《CA Virtual Assurance 管理指南》*。

3. 从 CA Virtual Assurance 为您的环境部署 AIM。

   将相应的 AIM 和代理部署方法用于基础架构和环境。

   注意：有关详细信息，请参阅*《CA Virtual Assurance 管理指南》*。

4. （可选）发现带有 CA Virtual Assurance 的环境。

   发现环境的组件，从而在 CA Virtual Assurance 中启用服务器管理。

   注意：有关详细信息，请参阅*《CA Virtual Assurance 管理指南》*和*联机帮助*。

5. 发现带有 Spectrum Infrastructure Manager 的 SystemEDGE 代理/AIM 主机。

   AIM 对 Spectrum Infrastructure Manager 公开其支持的基础架构。

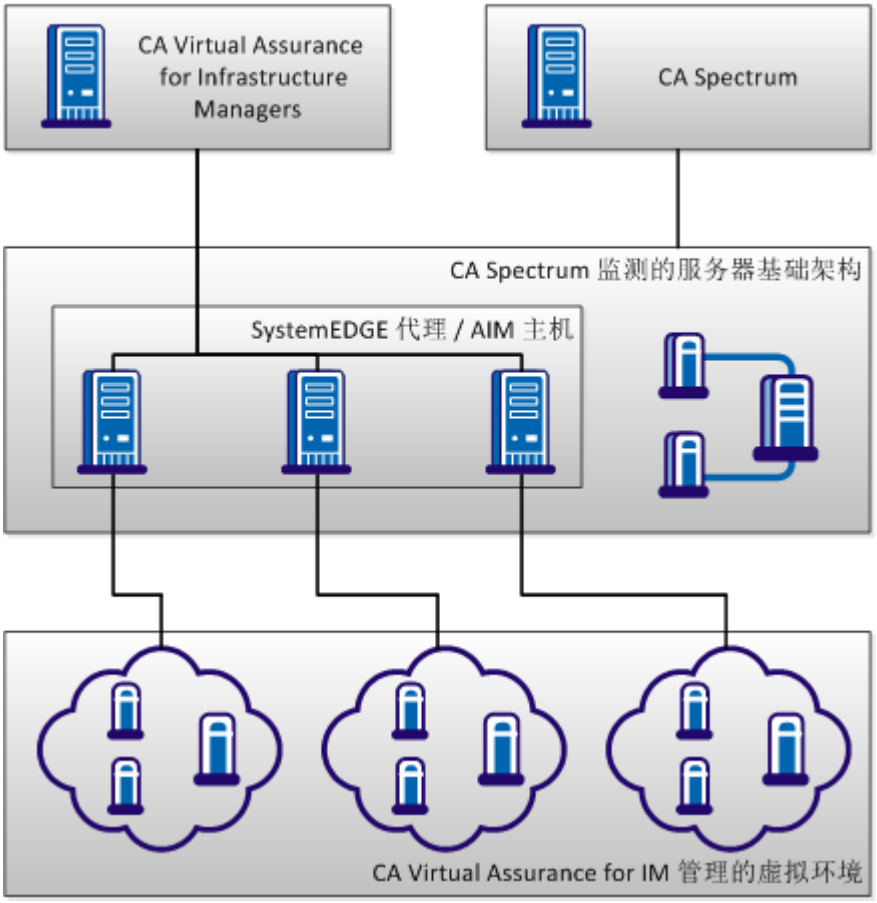
   注意：有关详细信息，请参阅 Spectrum Infrastructure Manager 文档。

Spectrum Infrastructure Manager 在其 OneClick 导航面板中显示发现的基础架构，并提供基础架构建模以及环境组件的可用性报告。

使用 CA Virtual Assurance 管理环境组件并实施基于策略的管理。

下图表示有关集成基础架构的概述：

集成基础架构概述



第 3 章： 管理用户和用户组

此部分包含以下主题：

用户访问控制

CA EEM 可保护 CA Virtual Assurance 组件之间的所有通信。您可以选择以下配置之一：

- Active Directory 用户
- 本地安全性

注意：有关配置外部目录的详细信息，请参阅 *《CA EEM 入门》*和*联机帮助*。可在安装 CA EEM 的计算机上从“开始”、“程序”、“CA”、“Embedded Entitlements Manager”、“文档”找到该文档，也可以在位于 http://ca.com/support 的 CA 在线支持网站上找到该文档。

Active Directory 用户

当您连接到现有的 Active Directory 配置时，预定义用户和用户组将与用户的中央存储库保持一致。CA Technologies 建议您在 Active Directory 中创建和修改用户，而不使用 CA Virtual Assurance 或 CA EEM。

CA Virtual Assurance 使用轻型目录访问协议 (LDAP) 对 Microsoft Active Directory 服务器进行读取和写入。默认情况下，LDAP 通信以不安全的方式进行传输。这将导致服务器与 Microsoft Active Directory 之间的通信不安全。要使 Microsoft Active Directory 安全，请使用通过安全套接字层 (SSL) 的 LDAP（即 LDAPS）。这种情况下，请安装来自 Microsoft 证书颁发机构或其他证书颁发机构的格式正确的证书。

注意：有关如何配置 Active Directory 以便安全传输数据的详细信息，请参阅 Microsoft 网站。请搜索知识库文章“如何在使用第三方证书颁发机构的情况下启用通过 SSL 的 LDAP”。在配置 Active Directory 以使用 LDAPS 之后，便可安全地传输数据。

Active Directory 的安全注意事项

轻型目录访问协议 (LDAP) 用于对 Microsoft Active Directory 服务器进行读写。默认情况下，LDAP 流量的传输是不安全的。这将导致服务器与 Microsoft Active Directory 之间的通信不安全。通过使用基于安全套接字层 (SSL) 的 LDAP (LDAPS)，可保证 Microsoft Active Directory 的安全。您必须从 Microsoft 证书颁发机构或非 Microsoft 证书颁发机构安装格式正确的证书。

一篇 Microsoft 知识库文章中介绍了相关要求。

注意：有关将 Active Directory 配置为安全传送数据的详细信息，请参阅 Microsoft 网站上的知识库文章“How to enable LDAP over SSL with a third-party certification authority”（如何对第三方证书颁发机构启用基于 SSL 的 LDAP）。在将 Active Directory 配置为使用 LDAPS 后，您可以安全地传输数据。

本地安全性

采用本地安全性，CA EEM 管理员可以专门针对 CA Virtual Assurance 创建用户、用户组和策略，因为这些信息都保存在本地存储中。本地安全性要求您手工定义自己的一套用户和用户组。这些用户和用户组与目录服务中当前定义的用户和用户组可能不一致。

CA EEM 与 CA Virtual Assurance 如何协作

CA EEM 包括以下关键对象：

- 身份（用户和用户组）
- 资源
- 策略

CA EEM 提供以下功能：

身份验证

对用户进行身份验证。经过身份验证的用户可在后续的授权处理中使用。

授权

允许用户访问特定资源。资源可以是任何逻辑或物理实体。在 CA Virtual Assurance 中，典型资源是用户界面组件（例如，选项卡、命令、下拉列表等）。与一个资源类关联的一组策略控制授权。这些策略是将 CA EEM 与 CA Virtual Assurance 集成的主要途径。

访问 CA EEM 用户界面

登录到 CA EEM 主页即可使用本地安全性。也可以从“开始”菜单中访问 CA EEM 文档，登录后可以在主页上访问联机帮助。

访问 CA EEM 用户界面

1. 选择“开始”、“程序”、“CA”、“Embedded Entitlements Manager”、“EEM UI”。

   此时将显示 CA EEM 登录窗口。

   注意：如果您收到安全证书请求，请绕过它，然后继续。要消除这些消息，可以通过您选择的供应商获取证书并将该证书应用于服务器。有关安装安全证书的信息，请访问 Apache Tomcat 网站。

2. 从“应用程序”下拉列表中选择“AIP”。

   “用户名”字段将填充为 EiamAdmin。

3. 在“密码”字段中输入密码，然后单击“登录”。

   此时将显示 CA EEM 主页，默认情况下会显示主页。

创建 CA EEM 用户

要向用户授予对 CA Virtual Assurance 的访问权限，请创建 CA EEM 用户。以下过程将介绍如何手工针对 CA Virtual Assurance 向 CA EEM 使用的通用数据存储添加 CA EEM 用户。还可以通过引用外部目录来添加用户。

注意：有关通过引用外部目录添加用户的详细信息，请参阅*《CA EEM 入门》*和*联机帮助*。

创建 CA EEM 用户

1. 单击 CA EEM 主页上的“管理身份”。

   默认情况下，“用户”页面处于选中状态。

2. 在“搜索用户”部分中选择“应用程序用户详细信息”选项。

3. 在“属性”下拉列表中让“用户名”保持选中状态，在“运算符”下拉列表中让“LIKE”保持选中状态，将“值”字段保持空白，然后单击“执行”。

   在“用户”窗格的分层树中，会列出所有 CA Virtual Assurance 用户。

4. 在左侧窗格中单击“新建用户”图标。

   右侧将显示“新建用户”窗格。

5. 在“用户名”字段中输入此用户的用户 ID，然后在“用户详细信息”窗格中单击“添加应用程序用户详细信息”。

6. 从“应用程序组成员身份”窗格的“可用用户组”框中选择应用程序组，然后单击向右箭头  。

   该应用程序组将添加到“选定的用户组”中。

   注意：还可以将该用户添加到一个或多个动态组或全局组中。有关详细信息，请参阅 CA EEM 文档。

7. 在“身份验证”窗格的“新密码”和“确认密码”字段中输入用户的密码，然后单击“保存”。

   在“用户”窗格下方将显示一条确认消息。

创建默认用户组

通过用户组，可按业务职能对用户进行逻辑分组。您可以通过创建用户组向多个用户授予相同的访问权限。尽管此过程仅介绍了如何创建应用程序组，但随后的过程会介绍如何为该应用程序组创建策略。您还可以为全局组、动态组和单个用户创建策略。

创建用户组

1. 单击 CA EEM 主页的“主页”选项卡上的“管理身份”。

   默认情况下，“用户”页面处于选中状态。

2. 单击“组”，选中“显示应用程序组”复选框，然后单击“执行”。

   “用户组”窗格中的“应用程序组”下将列出所有可用的应用程序组。

3. 在左侧窗格中单击“新建应用程序组”。

   右侧窗格中将显示“新建应用程序用户组”页面。

4. 输入新应用程序组的名称，然后单击“保存”。

   新应用程序用户组现已创建完成。

密码管理

用户凭据对 CA Virtual Assurance 组件之间的通信至关重要。CA Virtual Assurance 在内部存储用户和密码信息。在更改 CA Virtual Assurance 与之集成的外部组件的或应用程序的密码时，为保持一致性，请也在 CA Virtual Assurance 中更改这些密码。否则，CA Virtual Assurance 无法正常运行。

请考虑以下方面：

- Active Directory 安全性
- 本地安全性
- CA EEM 管理员
- 数据库 sa 用户（SQL 身份验证）

更改 CA EEM 管理员密码 (EiamAdmin)

如果您打算更改 CA EEM 管理员密码 (EiamAdmin)，请同时更改 CA EEM 和 CA Virtual Assurance 中的密码。

更改 CA EEM 中的管理员密码 (EiamAdmin)

1. 导航到“开始”、“程序”、“CA”、“Embedded Entitlements Manager”、“EEM UI”，打开用户界面。

   此时将显示“登录”对话框。

2. 使用当前 EiamAdmin 密码登录。

   用户界面将打开。

3. 单击“配置”和“EEM 服务器”。

   此时将显示“EEM 服务器”窗格。

4. 单击“EiamAdmin 密码”。

   此时将显示“新密码”和“确认密码”字段。

5. 输入您的密码，然后单击“保存”。

   现在可使用新的 EiamAdmin 密码登录 CA EEM。

更改 CA Virtual Assurance 中的管理员密码 (EiamAdmin)

1. 导航到“开始”、“程序”、“CA”、“CA Virtual Assurance”、“CA Virtual Assurance 命令提示符”。

   将显示命令提示符。

2. 输入以下命令：

   ```
   dpmutil -set -eiam
   ```

   dpmutil 命令提示您提供所需的凭据。

   完成命令。

3. 重新启动 CAAIPApache 和 CAIPTomcat 服务。

   凭据现已一致，CA Virtual Assurance 按预期运行。

注意：在两种情况下，可通过位于 *Install_path*\Apache\logs\error.log 的 Apache 日志文件确认产品是否正确启动。如果最后一个条目是“Validating EEM is available”，则仍存在凭据问题。验证用于“-set -eiam”和“-set -sysuser”的凭据是否可用于登录到 CA EEM UI。然后，使用有效凭据重试 dpmutil 命令。

更改数据库管理员 (sa) 密码

如果使用 Microsoft SQL 身份验证，且更改了 Microsoft SQL 用户（通常为“sa”用户）的密码，也请更改 CA Virtual Assurance 密码。

更改 Microsoft SQL Server 中的数据库管理员 (sa) 密码

1. 打开 Microsoft SQL Server Management Studio 并登录。
2. 在“对象资源管理器”中展开“安全”，然后登录。
3. 打开 sa 并在右侧窗格中更改密码。

注意：有关进一步的详细信息，请参阅 Microsoft SQL Server 文档。

更改 CA Virtual Assurance 中的数据库管理员 (sa) 密码

1. 导航到“开始”、“程序”、“CA”、“CA Virtual Assurance”、“CA Virtual Assurance 命令提示符”。

   将显示命令提示符。

2. 输入以下命令：

   ```
   dpmutil -set -mgmtdb
   ```

   dpmutil 命令提示您使用相应的凭据。

   完成命令。

3. 如果性能数据库使用同一服务器和数据库用户 (sa)，请输入以下命令：

   ```
   dpmutil -set -perfdb
   ```

   dpmutil 命令提示您使用相应的凭据。

   完成命令。

4. 重新启动 CAAIPApache 和 CAIPTomcat 服务。

   凭据现已一致，CA Virtual Assurance 按预期运行。

为本地安全性更改系统用户密码

CA Virtual Assurance 需要 *sys_service* 系统用户才能正常运行，例如，启动或停止 Apache 服务。您在使用本地安全性的安装期间指定 *sys_service* 系统用户及其密码。安装程序将 sys_service 凭据存储在 CA EEM 和 CA Virtual Assurance 中。如果以后在 CA EEM 中更改了 sys_service 的密码，也请在 CA Virtual Assurance 中更改该密码，以确保全部 CA Virtual Assurance 服务继续运行。

更改 CA EEM 中的 sys_service 密码

1. 导航到“开始”、“程序”、“CA”、“Embedded Entitlements Manager”、“EEM UI”，打开用户界面。

   此时将显示“登录”对话框。

2. 使用当前 EiamAdmin 密码登录。

   用户界面将打开。

3. 单击“管理身份并搜索用户”。

   用户将出现在“用户”窗格中。

4. 单击 sys_service 用户。

   用户属性将出现在右侧窗格中。

5. 向下滚动到“身份验证”部分，然后单击“重置密码”。

   此时将显示“新密码”和“确认密码”字段。

6. 输入您的密码，然后单击“保存”。

   新密码现存储在 CA EEM 中。

更改 CA Virtual Assurance 中的 sys_service 用户密码

1. 导航到“开始”、“程序”、“CA”、“CA Virtual Assurance”、“CA Virtual Assurance 命令提示符”。

   将显示命令提示符。

2. 输入以下命令：

   ```
   dpmutil -set -sysuser
   ```

   dpmutil 命令提示您提供所需的凭据。

   完成命令。

3. 重新启动 CAAIPApache 和 CAIPTomcat 服务。

   凭据现已一致，CA Virtual Assurance 按预期运行。

为 Active Directory 安全性更改系统用户密码

如果您的 CA Virtual Assurance 安装已配置为连接到 Active Directory，则安装 CA Virtual Assurance 的用户将自动注册到 CA EEM。注册之后，将允许 CA Virtual Assurance 对来自 Active Directory 域的用户进行身份验证。如果用户密码发生更改，用户将无法登录到 CA Virtual Assurance 用户界面，因为 CA EEM 无法继续对其进行身份验证。如下所示更改用户密码：

为 Active Directory 更改用户密码

1. 导航到“开始”、“程序”、“CA”、“Embedded Entitlements Manager”、“EEM UI”，打开用户界面。

   此时将显示“登录”对话框。

2. 使用当前密码登录。

   用户界面将打开。

3. 单击“配置”和“EEM 服务器”。

   此时将显示“EEM 服务器”窗格。

4. 单击左侧窗格中的“全局用户”/“全局组”，并将默认选项“外部目录的参考”保持选中。

5. 将 Microsoft Active Directory 保留为默认类型，并在“密码”和“确认密码”字段中输入新密码，然后单击“保存”。

6. 关闭 CA EEM

7. 导航到“开始”、“程序”、“CA”、“CA Virtual Assurance”、“CA Virtual Assurance 命令提示符”。

   将显示命令提示符。

8. 输入以下命令：

   ```
   dpmutil -set -sysuser
   ```

   Sysuser 是安装 CA Virtual Assurance 的同一用户。dpmutil 命令提示您使用第 5 步中指定的所需凭据。

   完成命令。

9. 重新启动 CAAIPApache 和 CAIPTomcat 服务。

   凭据现已一致，CA Virtual Assurance 按预期运行。

注意：在两种情况下，可通过位于 *Install_path*\Apache\logs\error.log 的 Apache 日志文件确认产品是否正确启动。如果最后一个条目是“Validating EEM is available”，则仍存在凭据问题。验证用于“-set -eiam”和“-set -sysuser”的凭据是否可用于登录到 CA EEM UI。使用有效凭据重试 dpmutil 命令。

用户组管理

“用户组”页提供了用户和用户组授权访问权限，以及对产品功能的用户访问控制。

详细信息：

搜索用户或用户组

您可以搜索要添加或删除的用户或用户组。

搜索用户或用户组

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 展开“用户组”并从列表中选择用户组。

   用户组页将出现在右侧窗格中。

4. 单击“成员身份”。

   将出现“用户/用户组”页面。

5. 在“身份”下拉列表中选择“用户”或“用户组”。在“属性”下拉列表中选择要搜索的属性，并使“LIKE”运算符保持选中状态。在“值”字段中输入值（或带通配符的部分值），然后单击“搜索”。

   匹配的用户或用户组名称的列表将出现在“可用用户/用户组”列表中。

创建用户组

通过用户组，可按业务职能对用户进行逻辑分组。您可以通过创建用户组向多个用户授予相同的访问权限。

创建用户组

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 键入用户组的“名称”。该名称可以基于业务职能或服务。

4. （可选）键入“说明”。

5. 单击“保存”。

   此时新用户组将出现在左侧窗格中。

详细信息：

将用户分配到组 (p. 41)

将用户分配到组

用户会继承分配给他们的用户组的访问权限。当您要将现有用户组的访问权限授予新用户时，可将这些用户添加到该用户组中。管理员用户组是预定义的组，默认情况下会出现在列表中。

将用户分配到组

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 展开“用户组”并从列表中选择用户组。

   将显示子菜单。

4. 选择“成员身份”子菜单。

   此时将出现一系列成员身份窗格。

5. 输入要在“值”文本框中添加的用户名，然后单击“搜索”。

   “可用用户/用户组”窗格中将显示搜索结果，或者显示一条消息，通知您找不到匹配项。如果您不确定用户名，可搜索用户或用户组 (p. 40)。

6. 从“可用用户/用户组”窗格中选择要添加的用户，然后单击向右箭头  。

   用户名将移至“选定的用户/用户组”窗格。

7. 单击“保存”完成用户添加操作。

   用户将被授予其用户组的访问权限。

将外部目录用户组分配给用户组

希望授予现有访问权限时，您可以将用户组从外部目录添加到现有 CA Virtual Assurance 用户组。管理员用户组是预定义的组，默认情况下会显示在列表中。

将外部目录用户组分配给用户组

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将在左侧窗格中显示“用户组”节点。

3. 展开“用户组”并从列表中选择用户组。

   将在右侧窗格中显示用户组页。

4. 选择“成员身份”子菜单。

   选项卡下将显示一系列成员身份窗格。

5. 从“身份”列表中选择“用户组”。

   搜索用户的条件显示在“属性”列表中。

6. 在“值”文本框中输入从外部目录添加的用户组名，然后单击“搜索”。

   如果找到用户，或者显示一条消息通知您未找到任何匹配项，则用户组显示在“可用用户/用户组”窗格中。用户组名称通过“可用用户/用户组”列表中的“[全局组]”标识。

7. 选择从“可用用户/用户组”窗格添加的用户组，然后单击向右箭头  。

   用户组将移动到“选定的用户/用户组”窗格。

8. 单击“保存”完成添加用户组。

   随即便授予用户分配给与其相关联的用户组的访问权限。

设置用户组权限

您可以使用“管理”页控制用户组对服务的访问。被授予管理员权限的用户有权访问所有服务。

注意：有关授予用户访问 CA Virtual Assurance 的权限的信息，请参阅*《管理指南》*。

设置用户组权限

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 选择要设置其权限的用户组，然后单击“权限”选项卡。

   此时将显示“权限”页面。

4. 单击要为其授予权限或限制其访问权限的选项卡和操作对应的复选框，然后单击“保存”。

   将会更新用户组权限。

   注意：如果限制某用户组访问特定页面，同时会限制该用户组对该页面执行任何操作。

设置用户组权限

您可以控制用户组对用户界面中的功能区域和特定功能的访问。默认情况下，AIPAdmins 用户组可以访问所有功能区域和功能。

设置用户组权限

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 选择要为其设置权限的用户组，然后单击“权限”。

   此时将显示“权限”页面。

4. 选择要允许或禁止访问的功能区域或特定功能，然后单击“保存”。

   此时用户权限将更新。

为服务设置用户组权限

您可以控制用户组对服务的访问。默认情况下，具有管理员权限的用户可以访问所有服务。

设置用户组权限

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 单击左侧窗格中的用户组。

4. 单击“服务访问”。

   右侧窗格将显示已启用或禁用服务的资源。

5. 根据需要启用或禁用服务访问的资源。

6. 单击“保存”。

   将更新“服务访问”列表。

设置运行命令脚本权限

您可以通过使用管理员对单个命令脚本操作授予或调用用户组访问权限。必须已经在“操作和规则”页面创建命令脚本操作（策略）。

设置运行命令脚本操作权限

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 展开“用户组”，并从列表中选择用户组。

   各选项卡将显示在右侧窗格中。

4. 选择“权限”选项卡。

   将会显示权限列表，其中包含选择或取消选择权限的复选框。

5. 展开“策略”文件夹，选择“运行命令脚本”，然后单击“保存”。

   将更新命令脚本权限。

导入外部目录

您可以导入提供用户名和密码身份验证的外部目录服务作为用户组。

导入外部目录

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 展开“用户组”并从列表中选择用户组。

4. 选择“成员身份”。

   此时将显示“用户/用户组”页。

5. 从“身份”下拉列表中选择“用户组”，在“值”文本框中键入外部目录的名称或部分名称，然后单击“搜索”。

   如果搜索未成功，将显示一条确认消息通知您；否则将使用找到的用户组填充“可用用户/用户组”部分。外部目录已导入 CA Virtual Assurance。

删除用户组

可以删除不再需要的用户组。

删除用户组

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 右键单击“用户组”，并选择“删除用户组”。

   用户组将删除。

为服务分配用户组访问权限

在具有多组用户的环境中，通常需要阻止一个组查看其他组的资源。管理员可将特定资源分配给用户组。有些管理员只能为其所属的组分配资源。但是，组 *AIPAdmins* 中的管理员拥有分配资源的完全访问权限。

为服务分配用户组访问权限

1. 单击“管理”。

   此时将显示“管理”页面。

2. 单击“用户组”。

   将出现“用户组”页面。

3. 在左侧窗格中，选择要为其设置权限的用户组，然后单击“服务访问”。

   此时将显示定义到系统的服务的树形列表。

4. 选择您要为其授予或限制访问权限的服务，然后单击“保存”。

   将向用户组授予为其关联服务分配的访问权限。

从用户组中删除用户或用户组

可以从现有的 CA Virtual Assurance 用户组中删除用户和用户组。管理员用户组是预定义的组，默认情况下会出现在列表中。

从用户组中删除用户或用户组

1. 依次单击“管理”、“配置”。

   将出现“配置”页面。

2. 选择“用户组”。

   此时“用户组”菜单将出现在左侧窗格中。

3. 展开“用户组”并从列表中选择用户组。

   此时子菜单将出现在右侧窗格中。

4. 选择“成员身份”子菜单。

   此时将出现一系列成员身份窗格。

5. 从“选定的用户/用户组”窗格中选择要删除的用户或用户组，然后单击向左箭头  。

   该用户或用户组将移至“可用用户/用户组”窗格。

6. 在完成删除用户和用户组的操作时，单击“保存”。

第 4 章： 管理系统性能

此部分包含以下主题：

系统管理

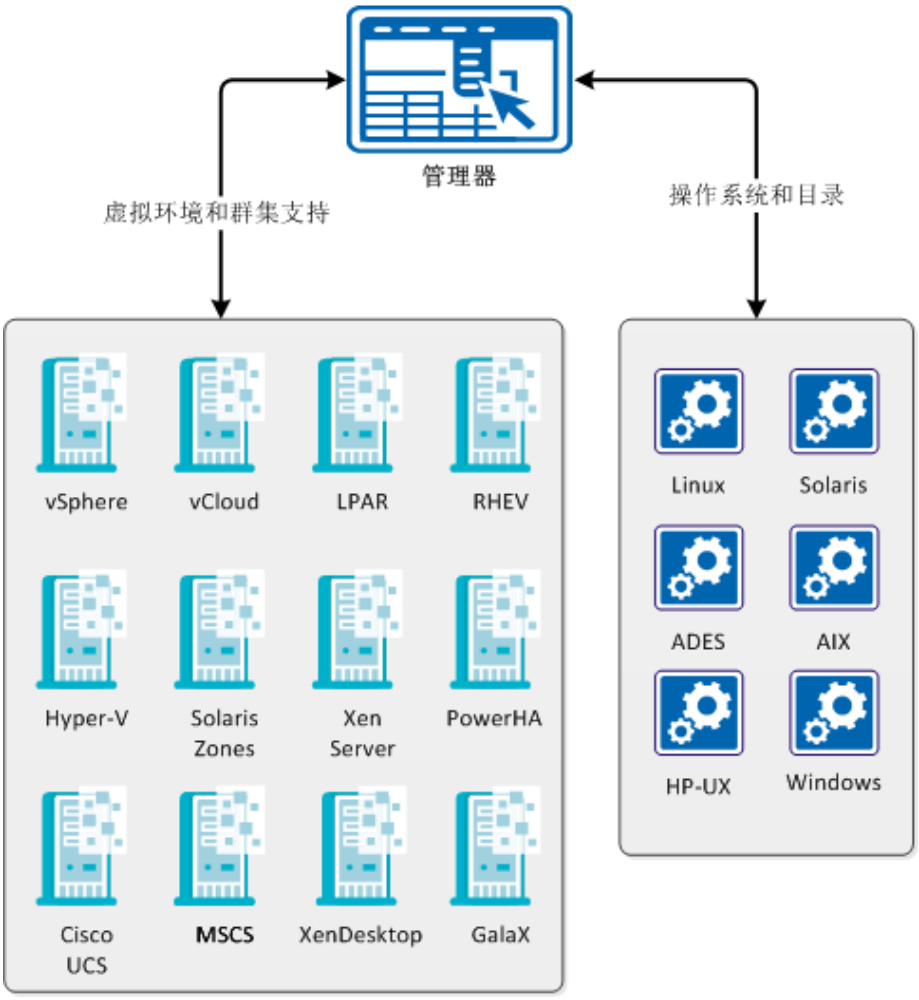
CA Virtual Assurance 旨在管理虚拟环境，但也可发现和管理系统（受管节点）。CA Virtual Assurance 在受管节点上支持以下操作系统：

- AIX
- HP-UX
- Linux、zLinux
- Solaris（Intel、SPARC）
- Windows

受管节点的可用管理组件有：

- SystemEDGE
- 高级加密 AIM
- 远程监控 AIM（仅适用于 Windows Server）
- 服务响应监控 (SRM) AIM
- CA Systems Performance LiteAgent

支持的虚拟环境和操作系统



SystemEDGE 是在 CA Virtual Assurance 中进行系统管理的基础，提供了以下优势：

- 对所有受管系统的集中式远程代理部署
- 集中式远程代理配置

- 可视化所有受监控度量标准，包括来自代理的对象模型的状态信息
- 服务响应监视器 AIM 的远程部署和配置
- 增强的代理安全选项

注意：有关 SystemEDGE 代理功能的详细信息，请参阅*《SystemEDGE 用户指南》*。

详细信息

SystemEDGE 功能 (p. 60)
服务响应监控 (p. 72)
远程监控组件之间的交互 (p. 552)
代理配置 (p. 68)
代理可视化 (p. 75)
安全和维护 (p. 70)

发现

您可以发现和添加要管理的服务器或整个子网，包括先前未受管的或最新添加的服务器。

注意：CA Virtual Assurance 发现过程需要解析主机名。如果更改了所发现服务器的 IP 地址，CA Virtual Assurance 将不会自动解析 IP 地址。因此，发现配置文件无法更新管理数据库。如果更改了 IP 地址，请重新发现服务器。

发现系统

您可以指定单个系统进行发现、管理，并且可以将该系统分配给服务。

发现系统

1. 依次选择“资源”、“管理”、“发现系统”。
2. 填写“系统名称”字段，以指定服务器的名称或 IP 地址。
3. （可选）单击“下一步”。

   此时将显示“增强的发现和 SNMP 信息”对话框。
4. （可选）启用“增强发现”以使用 SoftAgent 技术执行详细的发现。

5. （可选）启用“覆盖 SNMP 默认值”以使用 SNMP 信息执行详细的发现。
6. 单击“完成”。

   发现系统时，将显示成功消息。将自动管理发现的服务器，但不管理子网发现中的服务器。

删除系统

删除发现的系统会将该系统从 CA Virtual Assurance 中移除。

删除系统

1. 依次选择“资源”、“管理”、“管理系统”。
2. 从右侧窗格顶部的下拉菜单中，选择下列各项之一：
   - 裸机服务器
   - 受管服务器
   - 未受管服务器

   将显示已发现系统的列表。
3. 选择要删除的一个或多个系统，然后从“操作”下拉菜单中选择“删除”。

   注意：您还可以通过选择“全部删除”来删除“系统”页面上的所有系统。

   将出现一条消息提示您确认。
4. 单击“是”。

   系统将从“系统”页面中删除，并且在 CA Virtual Assurance 中不再显示为已发现。

发现网络

您可以指定要发现的一段网络。在用户界面中为网络发现指定 IP 地址时，使用 CIDR（无类别域间路由）表示法。这种表示法由地址和位数构成，用作子网前缀，如下面的示例所示：

172.24.143.0/24

还可以使用通配符和范围：

172.24.143.*

172.24.143.{1-255}

发现网络

1. 依次选择“资源”、“管理”、“发现网络”。
2. 填写下列字段。

   网络名称

   指定网络的名称。

   网络地址

   指定网络 IP 地址。将光标悬停在该字段上可显示地址示例。

   排除地址

   （可选）指定要从发现中排除的网络地址。
3. 选择“发现方式”的以下选项之一，并填写相应字段：

   Ping 扫射

   发现网络上的所有 IP 地址。

   DNS

   发现在域名系统 (DNS) 服务器中注册的主机名称。在字段中键入域名和 DNS 服务器名称。
4. （可选）单击“下一步”。

   此时将显示“增强的发现和 SNMP 信息”对话框。
5. （可选）启用“增强发现”以使用 SoftAgent 技术执行详细的发现。
6. （可选）启用“覆盖 SNMP 默认值”以使用 SNMP 信息执行详细的发现。
7. 单击“完成”。

   发现网络时，将显示成功消息。将自动管理发现的服务器，但不管理子网发现中的服务器。

增强的发现和 SNMP 信息

您可以指定凭据和 SNMP 信息以发现系统或网络。

使用增强的信息进行发现

1. 依次选择“资源”、“管理”、“发现网络”或“发现系统”。

   此时将显示“指定发现类型和目标”部分。

   在“发现类型”和“发现方法”部分中输入必需的详细信息之后，单击“下一步”。此时将显示“增强的发现和 SNMP 信息”部分。

2. 完成“增强的发现”部分中的以下字段：

   增强的发现

   选择该选项可为发现指定增强的凭据。

   发现凭据

   选择其中一个选项来指定凭据。

   指定凭据

   选择该选项可指定凭据，如用户名和密码。

   选择保存的凭据

   从“可用”列表中选择已保存的现有凭据。

3. 完成“SNMP 信息”部分中的以下字段，然后单击“下一步”：

   覆盖 SNMP 默认值

   选择该选项可为发现覆盖 SNMP 默认值。

   SNMP 设置

   选择其中一个选项来指定凭据。

   指定凭据

   选择该选项可指定凭据，如 SNMP 版本和团体字符串。

   选择保存的凭据

   从“可用”列表中选择已保存的现有凭据。

4. 单击“完成”。

   发现系统或网络时会显示成功消息。将自动管理发现的服务器，但不管理子网发现中的服务器。

取消网络发现

您可以取消正在进行的网络发现。

取消网络发现

1. 单击“资源”，然后打开“管理”窗格。
2. 在“管理”部分中，单击“管理已发现网络”。
3. 选择要取消发现的“正在进行中”网络，然后单击“网络列表”工具栏上的 —（取消）。

   将显示一条消息，确认选定网络的发现已取消。

重新发现网络

如果系统已添加到已发现的网络，或者自上次发现之后网络已通过其他方式进行了更改，可以重新发现该网络。

重新发现网络

1. 依次选择“资源”、“管理”、“管理已发现网络”。

   右侧窗格中将显示已发现网络的列表。
2. 选择要重新发现的网络，然后单击“网络列表”工具栏上的  （重新发现）。

   将在网络上启动发现。发现完成后，将反映对网络所做的所有更改（添加或删除系统）。

删除网络

您可以删除已发现的网络。但是，已发现的系统将保持原有的状态。

删除网络

1. 依次选择“资源”、“管理”、“管理已发现网络”。

   右侧窗格中将显示已发现网络的列表。
2. 选择要删除的网络，然后单击“网络列表”工具栏上的 -（删除）。

   将出现一条消息提示您确认。
3. 单击“确定”。

   相应的网络将从网络列表中删除。

服务

您可以将现有受管服务器分组到一项服务中并且监控该组。

详细信息：

创建服务

您可以将监控的服务器组织为逻辑服务，这些服务反映业务需求所要求的资源。

创建服务

1. 单击“资源”，然后打开“浏览”窗格。
2. 选择父服务节点，如“数据中心”或“CA Virtual Assurance 服务”。
3. 右键单击“管理”、“新服务”。

   将显示“服务: 新建”对话框。
4. 在“服务名称”字段中为新服务输入名称，在“服务优先级”字段中设置优先级。

   注意：服务名称不支持以下字符：% " “ ” ‘ ’ ' < > / \ : ` ~ ;

   服务优先级

   指定在单个轮询周期内运行操作的顺序。

   示例：

   服务 A：优先级 3

   服务 B：优先级 1

   服务 C：优先级 2

   在各自的所有规则都评估为 true 时，这些操作会按照以下顺序运行：服务 B、服务 C、服务 A。

5. 更改延迟发生设置或接受提供的默认值。

   延迟

   定义操作触发之前规则必须评估为 true 的频率。

6. 更改阈值上限和阈值下限百分比或接受默认值。

   阈值下限和阈值上限 %

   指定整个服务的阈值下限和阈值上限。

   限制：只能在服务级别评估总使用率度量标准。

7. 可以将服务分配给 CCA 服务器。将自动创建具有相同服务器列表的 CCA 服务。

   注意：不会将 CCA 服务器未发现的服务器添加到 CCA 服务中。查看“事件”表以查看可能出现的问题。

   另外，还可以选择要应用于服务内所有服务器的管理配置文件。

8. 从“服务器”部分的“可用服务器”列表中为新服务选择服务器，然后单击向右箭头。

   注意：如果可用服务器的列表冗长，请筛选列表以减少服务器集。要执行此操作，请单击“筛选”箭头，输入筛选条件，然后单击“搜索”。

   服务器将添加到“选定的服务器”部分。

9. 在“操作”下拉菜单上单击“保存”。

   新的服务将保存并显示在“浏览”窗格中。

   在服务级别上，可以抓取快照、查看组件、运行发现或变更检测等。右键单击服务，然后选择相关选项。

编辑服务

您可以编辑现有服务以对其进行重命名、更改设置或者在组中添加或删除资源。

修改服务

1. 单击“资源”，然后打开“浏览”窗格。
2. 选择服务，然后右键单击“管理”、“编辑服务”。

   此时将显示“服务: 编辑”对话框。

3. 根据需要，更改“服务优先级”字段中的优先级和阈值上限和阈值下限百分比。

   服务优先级

   指定在单个轮询周期内运行操作的顺序。

   示例：

   服务 A：优先级 3

   服务 B：优先级 1

   服务 C：优先级 2

   在各自的所有规则都评估为 true 时，这些操作会按照以下顺序运行：服务 B、服务 C、服务 A。

4. 更改延迟发生设置或接受默认值。

   延迟

   定义操作触发之前规则必须评估为 true 的频率。

   阈值下限和阈值上限 %

   指定整个服务的阈值下限和阈值上限。

   限制：只能在服务级别评估总使用率度量标准。

5. 从“服务器”部分的“可用服务器”列表中选择要添加到服务的服务器，然后单击向右箭头。

   注意：如果可用服务器的列表冗长，请筛选列表以减少服务器集。要执行此操作，请单击“筛选”箭头，输入筛选条件，然后单击“搜索”。

   服务器将添加到“选定的服务器”部分。

6. 从“服务器”部分的“选定的服务器”列表中选择要从服务删除的服务器，然后单击向左箭头。

   服务器将从“选定的服务器”部分移动到“可用服务器”部分。

7. 单击“保存”。

   “服务器”列表将更新。

从服务中删除服务器

您可能不再想让服务器属于某个特定的服务。可以从服务中删除服务器。

从服务中删除服务器

1. 单击“资源”。

   此时将显示“资源”页面。

2. 在“浏览”窗格中，展开“数据中心”文件夹和“CA Virtual Assurance 服务”文件夹。

   将显示数据中心中的已发现资源和受管资源。

3. 右键单击服务器并选择“管理”、“从服务删除”。

   将出现一条消息，提示您确认是否要删除服务器。

4. 单击“确定”。

   服务器将从服务中删除。

删除服务

删除服务时，其服务器集合也将被删除，但服务中的服务器在 CA Virtual Assurance 中仍然保持受管状态。

删除服务

1. 依次选择“资源”、“管理”、“管理服务”。

   右侧窗格中将显示服务列表。

2. 选择服务，然后单击“服务”工具栏上的 -（删除）。

   将出现一条消息提示您确认。

3. 单击“是”。

   服务将删除。

受管和未受管资源

通过更改监控状态，可以指定是否监控资源。如果将某个对象配置更改为“未受管”，PMM 会处理该请求并在 AIM 中将值设置为“未受管”。当前的监视器配置会保留在 MIB 属性中，子对象也会更改为“未受管”。父对象的配置和状态发生更改会生成陷阱。在随后的轮询和记录周期中，不会为父对象及其子对象生成陷阱。

如果选择某个对象并将其配置更改为“受管”，PMM 会处理该请求并在 AIM 中将值设置为“受管”。当前的监视器配置会保留在 MIB 属性中，子对象也会更改为“受管”。会为父对象生成配置更改陷阱。将在下一个轮询和记录周期中评估父对象及其子对象的状态，并且会根据需要生成状态更改陷阱。

重要信息！资源的受管或未受管状态与 SystemEDGE 的受管或未受管模式不同。将计算机系统设置为未受管可启用 SystemEDGE 维护模式（如果该系统上安装了此模式）。

详细信息：

取消管理受管资源 (p. 58)
管理未受管资源 (p. 59)
删除受管资源 (p. 59)

取消管理受管资源

您可以停止管理当前受管服务器。

遵循这些步骤:

1. 单击“资源”。

   此时将显示“资源”页面。

2. 在“浏览”窗格中，展开“数据中心”文件夹和“CA Virtual Assurance 服务”文件夹。

   将显示数据中心中的已发现资源和受管资源。

3. 右键单击服务器并选择“管理”、“取消管理”。

   将出现一条消息，提示您确认是否要取消管理服务器。

4. 单击“确定”。

   未受管理的服务器不会显示在受管资源列表中。要查看未受管理的服务器，请在“浏览”窗格中打开“未受管”文件夹。

管理未受管资源

您可以通过将已发现的资源添加到受管资源列表来监控这些资源的性能。

管理资源

1. 单击“资源”，然后打开“管理”窗格。
2. 在“管理”部分中，单击“管理系统”。
3. 从下拉列表中选择“未受管理的服务器”。

   将显示未受管理的资源列表。
4. 选择想要管理的资源，然后在“操作”下拉菜单中单击“管理”。

   将显示一条消息，确认资源已受管理。
5. 展开“受管”文件夹。

   资源显示在“受管”列表中，度量标准收集将开始下一个记录周期。

删除受管资源

您可以删除不想再管理的资源。

删除受管资源

1. 单击“资源”。
2. 此时将显示“资源”页面。
3. 在“浏览”窗格中，展开“数据中心”文件夹和“CA Virtual Assurance 服务”文件夹。

   将显示数据中心中的已发现资源和受管资源。
4. 右键单击服务器并选择“管理”、“从系统删除”。

   将出现一条消息，提示您确认删除。
5. 单击“确定”。

   已删除的服务器不会显示在受管或未受管服务器列表中。

SystemEDGE 功能

SystemEDGE 是一个轻量级代理，提供了对物理系统和虚拟系统的基于 SNMP 的监控。使用代理访问重要系统信息，如系统配置、性能、用户、文件系统等等。基于指定的阈值或条件监控此信息；并基于监视器创建对象以维持聚合对象状态。

SystemEDGE 支持在下列 MIB 中监控度量标准：

- MIB-II (RFC 1213)
- 主机资源 MIB (RFC 1514)
- 系统管理 MIB（CA 所有权）
- IF-MIB（部分）(RFC 2233)
- IP-MIB（部分）(RFC 4293)
- TCP-MIB（部分）(RFC 4022)
- UDP-MIB（部分）(RFC 4113)

您可以使用系统管理 MIB 中的监控表来启用以下类型的智能监控：

自主监控

提供对代理支持的任何基于整数的 MIB 对象的监控。在“自主监视器”表中创建条目，以指定要监控的对象、比较运算符、阈值和重要级别。代理根据这些条目自动监控对象。代理监控对象，根据指定的阈值和重要级别值维护当前状态。当超过阈值时，代理会发送状态更改陷阱。

进程和服务监控

提供对任何进程、Windows 服务或应用程序的监控。在“进程监视器”表中创建条目，以监控进程或服务是否正在运行，或者根据指定阈值监控进程表对象。代理监控进程，根据指定的阈值和重要级别值维护当前状态。当超出阈值或进程状态（正在运行或已停止）发生更改时，代理会发送状态更改陷阱。

进程组监控

提供定义一组进程并监控该组是否发生更改的功能。在定义进程组的“进程组监视器”表中创建条目，代理会监控这些组。如果进程组发生更改，代理会发送陷阱。

日志文件和目录监控

通过搜索指定为正则表达式的字符串，提供对任何 UTF-8 编码的系统或应用程序日志文件的监控。在“日志监视器”表中创建条目，代理会监控指定的日志文件以查找与用户定义的正则表达式匹配的行。出现匹配项时，代理会发送陷阱。可以将重要级别与监视器相关联，该关联关系包含在已发送的陷阱中。

Windows 事件监控

使用不同的筛选（如事件源）提供对 Windows 事件日志条目的监控。在“NT 事件监视器”表中创建条目，代理会监控事件日志以查找与用户定义的正则表达式匹配的事件。出现匹配项时，代理会发送陷阱。

历史记录收集

提供历史数据收集，以便进行管理器端基准制定和趋势分析。在“历史记录控制”表中创建条目，代理会随时间收集度量标准。使用度量标准可提供特定时间间隔内的平均系统性能。

有关监控功能和 SystemEDGE 体系结构的详细信息，请参阅 *《SystemEDGE 用户指南》*。

详细信息

系统管理 MIB (p. 61)
状态管理模型 (p. 64)
配置对象聚合 (p. 217)
无状态监控 (p. 65)
受管模式和未受管模式 (p. 65)

系统管理 MIB

系统管理 MIB 是私人企业 MIB，包括用于监控基础系统及其应用程序的运行状况和性能的对象。

具有可在系统管理 MIB 中监控的对象的组和表如下所示：

系统组 (sysedgeSystem)

包含基本系统信息，如主机名、CPU 类型和操作系统版本。

挂接设备表 (devTable)

包含挂接在主机上的设备和文件系统的相关信息。可以为诸如文件系统空间等值创建监视器，或通过在该表中设置列值来卸载挂接的设备。

内核配置组 (kernelConfig)

包含内核信息，例如 CPU 数目、虚拟内存量和时钟频率。可以使用该组监控内核的配置方式以及内核版本。

引导配置组 (bootconf)

包含根文件系统、转储文件系统和交换空间的相关信息。监控该表可跟踪诸如根文件系统名称、文件系统块和文件系统类型等值。

数据流组 (streams)

包含数据流 I/O 子系统的相关信息。可以通过监控该组中的对象（例如，正在使用的数据流数目、数据流分配失败次数以及队列中的数据流数目）来监控子系统的运行状况。

用户表 (userTable)

包含系统上用户帐户的相关信息。

组表 (groupTable)

包含系统上用户组的相关信息。

进程表 (processTable)

包含正在运行的进程的相关信息。可以监控该表来跟踪当前正在运行的进程，还可以通过设置特定属性来控制进程。例如，可以通过将 processkill 列的值设置为 9 来终止进程。

用户表 (whoTable)

包含当前登录到系统的用户的相关信息。可以监控该表中的属性，以跟踪在任何特定时刻正在使用系统的用户。

远程外壳组 (remoteshell)

包含用于在远程系统上运行外壳脚本和程序的属性。在该表中设置属性可指定命令及其参数以及输出文件的名称。

内核性能组 (kernelperf)

包含主机操作系统的运行状况和性能的相关信息。可以监控属性，例如当前进程和打开文件的数目、活动作业数目以及排定程序队列中的作业数目。

进程间通信表（msgqueTable、shmemTable、semTable）

在不同的表中包含消息队列、共享内存和信号的相关信息。监控这些表可协调进程间的通信。

消息缓冲区分配表 (mbufAllocTable)

包含系统使用消息缓冲区的方式的相关信息。监控该表中的属性可跟踪诸如缓冲区请求被拒绝或延迟的数目等信息。

数据流缓冲区分配表 (strbufAllocTable)

包含缓冲区分配以及数据流子系统使用的缓冲区的使用情况统计信息的相关信息。

I/O 缓冲区缓存组 (ioBufferCache)

包含基本磁盘 I/O 的 I/O 缓冲区分配和使用情况的相关信息。监控该表可跟踪诸如 I/O 缓冲区活动高峰期等信息。

目录名称查找缓存组 (dnlc)

包含目录和文件名缓存性能的相关信息。

AIX 逻辑分区组 (logicalPartition)

包含 IBM AIX 逻辑分区 (LPAR) 的相关信息。可以监控属性，例如每个分区的物理或逻辑 CPU 以及每个分区的 CPU 数目。

陷阱团体表 (trapCommunityTable)

包含 SNMP 信息，例如已配置的团体、用户和陷阱目标。

NT 系统组 (ntSystem)

包含特定于 Windows 系统的信息。该组包含系统、线程、注册表、服务、系统性能、缓存性能、内存性能、页面文件性能和事件监视器组，以便监控 Windows 系统上这些区域的属性。

RPC 统计信息组 (rpc)

包含内核远程过程调用的相关信息。监控该表可跟踪属性，例如用于检测 RPC 活动高峰期的计数器和统计信息。

NFS 统计信息组 (nfs)

包含内核的 NFS 工具的相关信息。监视该表可跟踪属性，例如用于检测 NFS 活动高峰期的统计信息和计数器。

磁盘统计信息表 (diskStatsTable)

包含磁盘 I/O 的相关信息。

CPU 统计信息表 (cpuStatsTable)

包含每个 CPU 的性能统计信息。可以监控属性，例如在空闲模式下所用的时间以及在等待模式下所用的时间。

系统管理 MIB 还包含监控表以及支持对象聚合的表。

状态管理模型

SystemEDGE 代理支持状态管理模型，这样自主监视器和进程监视器可以与总体 CA Virtual Assurance 管理模型完全集成在一起。代理将不同重要级别的多个监视器聚合为一个受管对象。该对象的状态对应于重要级别最高的被违反监视器。

代理根据分配的重要级别值计算各个监视器状态。结果状态可能为以下状态之一：

- 未知 (1)
- 正常 (2)
- 警告 (3)
- 轻微 (4)
- 重大 (5)
- 严重 (6)
- 致命 (7)
- 运行 (11)
- 关闭 (12)

注意：如果监视器的重要级别为“无”，则状态在“运行”和“关闭”之间进行切换。

系统管理 MIB 的“聚合”表使用对象类、实例和属性值，将具有相同值的监视器聚合为一个条目。该条目表示一个受监控对象，因此，该条目保持聚合状态。

注意：如果未在监视器中输入对象类、实例和属性的值，代理会向其中填充有意义的默认信息。默认自主监视器值基于使用 sysedge.oid 文件的受监控 OID，该文件可将受监控的 OID 映射到实例、类和属性值。默认进程监视器值基于进程正则表达式和受监控的属性。

“聚合”表会更新表中的当前状态，并且仅当阈值违规为某个对象创建了所有监视器的最差状态时，才发送状态更改陷阱。例如，假定您正在使用三个监视器监控 CPU 使用情况；一个监视器为 60%（分配了“警告”重要级别），一个监视器为 80%（“严重”重要级别），一个监视器为 100%（“致命”重要级别），则代理会返回 82% 的 CPU 使用情况。该值会导致 60% 和 80% 的监视器出现阈值违规问题。但是，代理仅向 80% 监视器发送一个状态更改陷阱，并将聚合状态更改为严重。

无状态监控

无状态监视器不获取对象状态信息，也不使用对象模型保持总体对象状态。这些监视器确实维护着一个重要级别值，但该重要级别用于跟踪单个监视器的重要性，而并非用于计算对象状态。下列各表支持无状态监控：

- 进程组监视器
- 日志文件监视器
- NT 事件监视器

您可以从 CA Virtual Assurance 用户界面中配置这些监视器，但无法使结果数据可视化。您必须依赖当基于定义的监视器检测到以下情况之一时代理发送的陷阱：

- 进程组更改
- 日志文件消息匹配指定的正则表达式
- 目录阈值违规
- 匹配指定条件的 Windows 事件日志事件

有关创建进程组、日志文件和 Windows 事件监视器的详细信息，请参阅*《SystemEDGE 用户指南》*。

受管模式和未受管模式

在部署 SystemEDGE（或在单机基础上进行安装）时，可以指定以受管模式运行该代理。在受管模式下，代理由从中部署了该代理的 CA Virtual Assurance 管理器节点进行管理，或由您在单机代理安装中指定的管理器节点进行管理。如果以受管模式运行代理，则会启用所有 CA Virtual Assurance 代理管理功能，例如 CA Virtual Assurance 用户界面的远程配置和高级可视化功能。受管模式还会将 CA Virtual Assurance 建立为代理配置的主要源。如果在 CA Virtual Assurance 外部修改了处于受管模式的代理，则 CA Virtual Assurance 管理员可以阻止或覆盖该更改。

您还能够以传统模式操作 SystemEDGE，或在没有 CA Virtual Assurance 管理器控制其配置的情况下操作 SystemEDGE。以传统模式运行的代理不限于传统监视器，也不限于那些不维护和计算状态的监视器。

当从 CA Virtual Assurance 部署代理时，可以使用“以受管模式运行”复选框，在软件包打包程序设置中指定是否以受管模式运行。当从 CA Virtual Assurance 单独安装代理时，请提供 CA Virtual Assurance 管理器节点，代理才能以受管模式运行。

Application Insight Module (AIM)

Application Insight Module (AIM) 新增了监控和管理特定于应用程序的事件和进程的功能。AIM 是 SystemEDGE 的功能扩展。

适用于 Cisco Unified Computing System (UCS) 的 AIM

CA Virtual Assurance 与 Cisco UCS 交互，以查询设备和收集统计信息。Cisco UCS 不将资源作为分散的系统进行管理，而是将网络、硬件、存储和虚拟化资源统一到一整个系统中。

适用于 Citrix XenDesktop 的 AIM

提供监控 Citrix XenDesktop 环境的功能。该 AIM 可在安装有 SystemEDGE 的任何 Windows 系统上运行。

适用于 Citrix XenServer 的 AIM

提供监控 Citrix XenServer 环境的功能。该 AIM 可在安装有 SystemEDGE 的任何 Windows 系统上运行。该 AIM 通过 XML RPC 直接与 XenServer 进行通信，以获取所有设置好的 XenServer 和资源池的整个视图。

适用于 Active Directory 和 Exchange Server 的 AIM

提供监控外部和内部基础架构上的 Active Directory 和 Exchange Server 的功能。AIM 启用了域和 Exchange 服务器管理、维护和升级。

AIM for Huawei GalaX

提供用于监控 Huawei GalaX 环境的功能。该 AIM 可在安装有 SystemEDGE 的任何 Windows 系统上运行。

适用于 IBM PowerHA 的 AIM

提供用于监测 IBM PowerHA（以前称为 High Availability Cluster Multiprocessing 系统）的功能。

适用于 IBM PowerVM (LPAR) 的 AIM

提供监控整个系统（包括 LPAR）的功能。该 AIM 可在安装有 SystemEDGE 的任何 Windows 系统上运行。该 AIM 通过安全外壳 (SSH) 连接与 HMC/IVM 进行通信，以便 AIM 可以通过关联的 HMC/IVM 系统与 POWER 系统上的 LPAR 进行通信。验证是否在 HMC/IVM 系统和运行该 AIM 的 Windows 服务器上启用了 SSH。

适用于 KVM 的 AIM

提供用于监控 RHEV 环境的功能。该 AIM 可在安装有 SystemEDGE 的任何 Windows 系统上运行。AIM 与 RHEV 管理器进行通信，以便获取注册到管理器的所有 KVM 服务器的整个视图。

适用于 Microsoft 群集服务的 AIM

提供监控 Microsoft 群集的功能。该 AIM 可在安装有 SystemEDGE 的任何 Windows 系统上运行。该 AIM 与 Microsoft 群集服务进行通信，以获取所监控的群集、节点、服务和应用程序的整个视图。

适用于 Microsoft Hyper-V 的 AIM

提供监控 Microsoft Hyper-V 环境的功能。适用于 Hyper-V 服务器的 SystemEDGE AIM 在 Hyper-V 服务器上运行。

适用于远程监控的 AIM

提供监控远程 Windows 系统的功能。远程监控也称为无代理监控。

适用于服务响应监视器的 AIM

提供对 Windows、UNIX 或 Linux 服务器上所运行服务的运行状况和响应能力进行监控的功能。

适用于 Solaris Zones 的 AIM

提供用于监控已配置为运行区域的 Solaris 系统的功能。该 AIM 可在安装有 SystemEDGE 的任何 Windows 系统上运行。该 AIM 通过 SSH 连接与管理的 Solaris Zones 服务器进行通信。验证是否在受管的 Solaris 服务器和运行该 AIM 的 Windows 服务器上启用了 SSH。

适用于 VMware vCenter 服务器的 AIM

提供对 VMware vCenter 服务器控制下的系统进行监控的功能。该 AIM 可在安装有 SystemEDGE 的任何 Windows 系统上运行。该 AIM 与 vCenter 服务器软件进行通信，以获取关联的 VMware vCenter 服务器管理的所有 ESX 服务器的整个视图。

适用于 VMware vCloud Director 的 AIM

提供对 VMware vCloud Director 控制下的虚拟系统进行监控的功能。该 AIM 可在安装有 SystemEDGE 的任何 Windows 系统上运行。

详细信息

NodeCfgUtil 概述 (p. 695)

代理配置

从 CA Virtual Assurance 用户界面中可以获得下列两种类型的 SystemEDGE 配置：

点配置

用于对代理做出单个临时更改，而不必部署策略。例如，可以更改自主监视器阈值，添加临时进程监视器，或为 SRM 测试创建自主监视器。策略部署会覆盖点配置更改。

策略配置

用于创建通过一次操作即可部署到一组受管计算机的代理配置策略。例如，可以定义包含一组通用监视器和 SRM 测试的策略，并将该策略部署到企业中的所有系统，以确保正在监控同样重要的系统度量标准。

从 CA Virtual Assurance 用户界面以受管模式配置代理优先于所有其他形式的配置。如果用户通过 sysedge.cf 配置文件或 SNMP 设置对本地代理进行手动更改，则 CA Virtual Assurance 策略配置会在应用策略之后覆盖这些更改。

详细信息

执行点代理配置 (p. 68)
配置概述 (p. 160)

执行点代理配置

CA Virtual Assurance 无需创建和应用策略，即可对单个代理做出单个或点配置更改。此功能用于对单个系统的监控配置进行临时更改。下列方案提供了点配置更改可能有用或有必要的情景示例：

- 特定于单个系统的临时更改
- 用于解决临时偏差的更改
- 在将不同监控重要级别和阈值提交到常规监控策略之前进行试验的更改

在进行点配置更改时，CA Virtual Assurance 会将更改应用于任何现有策略或本地配置上的系统。但是，下次对系统应用策略时，该策略会覆盖点配置更改。在点配置更改合并为基本策略或被策略应用覆盖之前，会将其报告为策略异常。

点配置可用于自主监视器和进程监视器。

执行点代理配置

1. 单击“资源”，并在“浏览”窗格中选择要配置的系统。

   将在右侧窗格中显示系统信息。

2. 单击右侧窗格中的“配置”，并选择“自主监视器”或“进程监视器”。

   将显示现有的自主监视器或进程监视器。

3. 单击工具栏上的 +（新建）。

   将显示用于新建自主监视器或进程监视器的字段。

4. 填写必需字段，然后单击“保存”。

   注意：有关详细信息，请参阅 *《SystemEDGE 用户指南》*。

   监视器将保存并显示在自主监视器或进程监视器的更新列表中。

您还可以修改、删除或复制现有的自主监视器或进程监视器。

监控软件设置

通过“监控软件”页面，您可以为单个服务器、服务器组或服务设置非策略相关信息。

遵循这些步骤:

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 选择一个系统或服务。

3. 单击“监控软件”。

   此时将显示“计算机详细信息”窗格。

4. 根据需要修改设置，然后单击“应用”：

   系统说明

   定义系统的说明。

   系统联系人

   定义系统的联系人。

系统位置

定义系统的位置。

SystemEDGE 记录级别

指定 SystemEDGE 记录级别。

设置将会更新。

安全和维护

CA Virtual Assurance 向 SystemEDGE 代理提供下列增强的安全和维护选项：

- 可从用户界面配置的维护模式
- SystemEDGE 代理的单点配置
- 阻止在 CA Virtual Assurance 外进行更改的能力
- 有关在 CA Virtual Assurance 外进行了更改的通知，以及忽略或拒绝不需要的更改的机会

详细信息

启用维护模式 (p. 70)

启用维护模式

可以在 CA Virtual Assurance 中启用 SystemEDGE 维护模式，在这种模式下代理将停止处理所有监视器条目和发送陷阱。如果代理的系统正处于计划停机状态，并且您想避免接收假警报陷阱，则维护模式很有用。

在维护模式下，代理将继续收集度量标准并响应 SNMP 请求，但会挂起对所有监视器和历史记录收集的处理。代理会保存维护开始时所有监视器的当前值，将其与维护结束时的当前值进行比较，并在必要时发送陷阱以响应当前值。

遵循这些步骤:

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 展开“受管”，并选择一个系统。

3. 单击“监控软件”。

   此时将显示“计算机详细信息”窗格。

4. 将“维护模式”选项设置为“已启用”，然后单击“应用”。

   代理将执行热启动并启用维护模式。

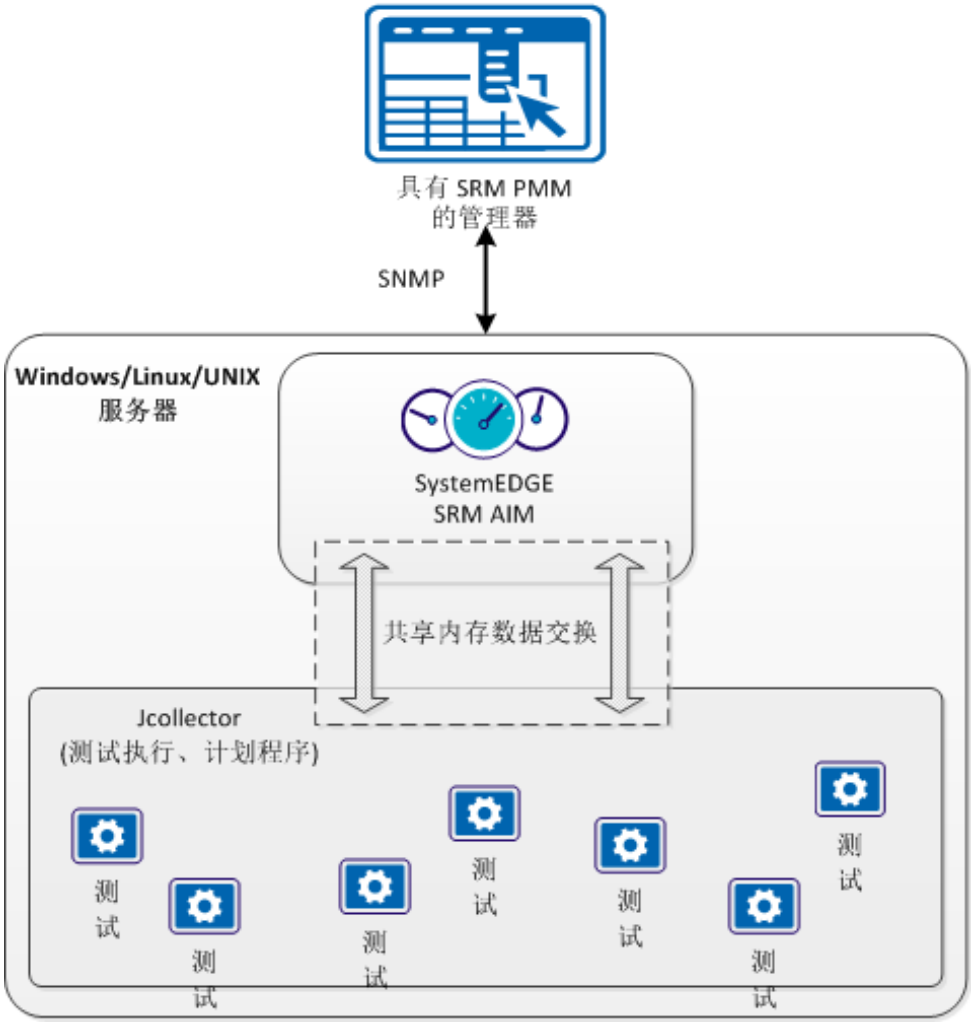
若要使代理退出维护模式，只需禁用“维护模式”复选框，并单击“应用”。

服务响应监控

服务响应监控应用程序审视模块 (SRM AIM) 是 SystemEDGE 的功能扩展（插件）。SRM 检索运行在本地或远程系统上的逻辑或物理服务的响应。SRM 基于 Java，是多线程的，可处理跨多个服务器的多个测试配置。SRM 执行预配置或自定义的测试，以测量执行所需的时间和吞吐量。

下图说明了这些关系。

服务响应监控组件之间的交互



svcrsp.cf 配置文件包含测试规格。SRM AIM 将读取该配置文件，并使测试规格在共享内存段中可用。SRM Jcollector 组件从共享内存中读取每个测试配置。Jcollector 执行测试，收集此计时进程的结果，然后将结果传播到 SRM AIM。SystemEDGE 将这些结果和关联的状态信息发送到 CA Virtual Assurance。

服务响应监视器 (SRM) AIM 监控关键系统服务的可用性和响应时间，例如 DNS、DHCP 或基于已定义阈值的 SQL。通过创建 SRM 测试来启用该功能。通过 SRM 测试，可以执行以下操作：

- 测试系统服务可用性和响应时间
- 获得对复杂的多层基础架构的可见性，以便在问题影响用户之前查明问题
- 获得有关延迟、断电和性能问题的实时通知
- 确认 DNS 和 DHCP 等服务根据服务级别协议运行良好
- 维护容量规划、故障排除或长期行为趋势分析的历史数据

CA Virtual Assurance 为 SRM AIM 提供了以下功能：

- 使用 SystemEDGE 代理远程部署
- 远程测试配置
- 测试可视化

有关 SRM AIM 体系结构的详细信息，请参阅 *《SRM 用户指南》*。

详细信息

SRM 测试 (p. 73)

SRM 测试

SRM AIM 提供了下列响应时间测试：

Active Directory 用户

确定 Windows Active Directory 服务运行正常，以管理共享文件和资源。

自定义

确定重要自定义服务或其他任务正在高效运行。

DHCP

确定动态主机配置协议服务器正在响应地址请求。

DNS

确定域名系统服务器正在处理主机名到地址解析请求。

文件 I/O

确定诸如读取、写入及比较操作可跨文件系统运行。

FTP 和 TFTP

确定用户可登录到指定服务器以上载和下载文件。

HTTP 和 HTTPS

确定用户可以连接到企业 Web 服务器，并确定网页上是否显示特定文本。

LDAP

验证与 LDAP 服务器的连接，以便验证用户请求和 LDAP 查询的访问权限。

NIS

验证正在处理 NIS 映射请求。

NNTP

验证用户可以连接到其 Usenet 新闻组服务器和公司布告栏。

Ping

确定网络设备存在并可在整个网络中访问。

电子邮件

确定电子邮件服务器可用并可有效地处理电子邮件。SRM 支持对 IMAP、MAPI、POP3、SMTP 以及从 SMTP 服务器发起的往返电子邮件的测试。

SNMP

确定 SNMP 代理正在响应 SNMPv1 GET 请求。

SQL 查询

确定 SQL 数据库服务器可用并正在处理短查询。

TCP

确定系统正在侦听并处理连接请求。

虚拟用户

获得实际用户事务（键盘输入和鼠标单击）的连续响应时间和可用性数据，可以对这些事务进行记录（通常使用 WinTask）以确认业务任务成功运行。

代理可视化

CA Virtual Assurance 用户界面显示代理处于受管模式的系统的监控信息。平台管理模型 (PMM) 解释和转变代理信息，从而使这些信息适合基础 CA Virtual Assurance AIP 体系结构，并可以在 AOM 数据库中显示。PMM 可用于基础 SystemEDGE 代理和 SRM AIM。

在 CA Virtual Assurance 用户界面中可以可视化的代理数据包括以下内容：

- 使用状态管理模型创建的受管对象
- 所有受管对象的状态
- 单个监视器
- SRM 测试

详细信息

查看受管对象状态 (p. 76)
查看 SystemEDGE 监视器 (p. 75)
查看服务响应测试 (p. 77)

查看 SystemEDGE 监视器

对于以受管模式运行 SystemEDGE 的系统，CA Virtual Assurance 用户界面可显示所有定义的自主监视器和进程监视器。您可以查看有关每个监视器的详细信息以及 执行点配置， (p. 68)如添加、删除、修改或复制监视器。

查看 SystemEDGE 监视器

1. 单击“资源”、展开“受管”，然后选择系统。

   右侧窗格中将显示系统“摘要”页面。

2. 单击“配置”，然后单击“自主监视器”或“进程监视器”。

   将显示“自主监视器”或“进程监视器”窗格。

“自主监视器”和“进程监视器”窗格包含列出以下监视器属性的表：

- 索引
- 状态
- 状态

注意：该状态可能与监视器相关联的任何受管对象的状态不一样。受管对象状态是构成对象的所有监视器的当前最差状态。

- 对象的类别、实例和属性

  注意：这些列中具有相同值的监视器是同一受管对象的组成部分。
- 当前监控的对象的值、运算符和阈值
- 重要级别
- 陷阱数
- 最后陷阱

查看受管对象状态

CA Virtual Assurance 用户界面显示了受管系统的所有 SystemEDGE 受管对象。

查看受管对象状态

1. 单击“资源”，在浏览树中展开适当的文件夹，并且选择运行 SystemEDGE 的受管系统。

   右侧窗格中将显示系统“摘要”页面。

“系统状态信息”窗格包含受管对象的总数和最高对象重要级别。

“受管对象”表包含关于每个受管对象的以下信息：

- 运行状况
- 操作状态（活动、维护中、销毁）
- 对象类别、实例和属性
- 当前监控值、操作符、阈值和监控计算机名。

从该表中可选择受管对象，然后单击“操作”，转到“定义”来查看构成受管对象的监视器。

查看服务响应测试

CA Virtual Assurance 用户界面显示使用服务响应监测 AIM 以受管模式运行 SystemEDGE 的系统的服务响应测试。

查看服务响应测试

1. 单击“资源”、展开“受管”，然后选择系统。

   右侧窗格中将显示系统“摘要”页面。

2. 单击“详细信息”，然后单击“服务回应”。

   将显示“服务响应测试”窗格。

“服务响应测试”窗格包含一个表，列出以下测试属性：

- 索引号
- 对象类名
- 测试名称和类型
- 测试目标
- 间隔
- 状态
- 最后的结果
- 错误总数

第 5 章：管理 SystemEDGE 和 Application Insight Module (AIM)

本章介绍了如何在您的环境中安装和配置监控软件。另外，本章还提供了有关适当的用户权限，以及如何将 SystemEDGE 更改为受管模式或未受管模式的详细信息。

此部分包含以下主题：

用户权限和访问要求参考

以下部分概述安装 CA Virtual Assurance 组件和使用 CA Virtual Assurance 监控环境的访问要求。每个部分包括有关所需通信端口的信息。如果分布式管理器安装范围跨越防火墙，可使用该列表验证所需通信端口是否已打开。

此文档适用于：

- 安装、配置和使用 CA Virtual Assurance 管理虚拟环境的管理员。
- 使用 CA Virtual Assurance 监控虚拟环境的操作员。

详细信息：

Active Directory 和 Exchange Server (ADES)

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

(Exchange 2007) 需要域管理员或 Exchange 管理员角色。

(Exchange 2010) 需要 Exchange 组织管理角色。

通信端口

PowerShell 端口：80、443、5985 和 5986

ADSI 端口：3268 和 389

Cisco UCS

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

要求具有足够权限的 UCS 管理器用户帐号来运行以下 UCS 操作：刀片服务器电源操作、服务配置文件操作、池操作、策略操作、导入/导出操作。

注意：我们建议给 UCS 用户授予管理员权限。

如果无法授予管理员权限，请将以下角色分配给 UCS 用户：

- Ext-lan-config
- Ext-san-config
- Service-profile-config
- Service-profile-config-policy
- Service-profile-ext-access
- Service-profile-network
- Service-profile-network-policy
- Service-profile-qos
- Service-profile-qos-policy
- Service-profile-security
- Service-profile-security-policy
- Service-profile-server
- Service-profile-server-oper
- Service-profile-server-policy
- Service-profile-storage
- Service-profile-storage-policy
- 操作
- Server-equipment

通信端口

HTTP 端口：80

HTTPS（端口：443）

Citrix XenDesktop

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

Citrix XenDesktop 5.6 版要求在 XenDesktop 中至少具有只读管理员角色的 Active Directory 帐户。

通信端口

WinRM 端口：5985、5986

SNMP 端口：161

WMI 端口：135

Citrix XenServer

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

（XenServer 6.0 和更高版本）要求具有只读角色的 root 使用者或 Active Directory 使用者。

通信端口

HTTPS（端口：443）

SNMP 端口：161

Huawei GalaX

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

Huawei GalaX 监控要求使用管理员用户凭据和来自 GalaX 环境的相应 p12 文件。

通信端口

HTTP 端口：8773

Hyper-V

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

要求本地管理员帐户。

SCVMM 监控

要求 System Center Virtual Machine Monitoring (SCVMM) 管理员角色。

通信端口

Windows RPC 端点映射程序端口：135

DCOM/WMI 端口：在 RPC 端点协调期间动态分配

IBM PowerHA

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控 PowerHA

要求帐户具有执行以下 CLI 命令的权限：

- clstat
- clRGinfo -s
- cldump
- cllsnw
- cltopinfo
- cllsif
- clshowsrv -v
- vmstat

通信端口

安全外壳 TCP 端口：22

IBM PowerVM

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

以下要求取决于您要使用 CA Virtual Assurance 监控的现有环境：

监控硬件管理控制台 (HMC)

要求 hmcsuperadmin 任务角色帐户。我们建议对资源角色仅包括您希望用户管理的 P 服务器的用户进行定义。

注意：HMC 监控需要 HMC *和* VIOS 配置。

监控虚拟 IO 服务器 (VIOS)

需要您要监控的 VIOS 上的 padmin 用户帐号。

监控集成的虚拟化管理器 (IVM)

需要您要监控的 IVM 上的 padmin 用户帐号。

注意：IVM 监控需要 IVM 配置。

通信端口

安全外壳 TCP 端口：22

Microsoft 群集服务器

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

需要域管理员帐户或群集节点本地帐户。如果使用域用户，其必须在域管理员组中。如果使用群集节点本地帐户，该用户必须是管理员组的成员。

重要信息！在所有节点上设置相同群集节点本地凭据。如果群集服务移至不同节点，并且该节点具有不同凭据，则 AIM 将无法连接。

通信端口

Windows RPC 端点映射程序端口：135

DCOM/WMI 端口：在 RPC 端点协调期间动态分配

Oracle Solaris Zones

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

需要 root 用户访问权限。

通信端口

安全外壳 TCP 端口：22

Red Hat Enterprise Virtualization

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

需要具有超级用户权限的相应 Red Hat Enterprise 管理员角色。

注意：可以使用 Microsoft Active Directory (AD) 用户或 Red Hat Enterprise IPA 用户。

通信端口

REST API 端口：8443

远程部署代理

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

在 Windows 上安装

要求 Windows 系统管理员权限。

在 Linux 上安装

要求 root 访问权限或使用 sudo 或 pfexec。

跨平台远程部署

使用基础架构部署 (ID)。

ID 管理器组件

（Windows 目标）要求目标计算机上的 Windows 共享 Admin$ 的映射。

（Unix 或 Linux 目标）要求管理器和目标之间的 SSH 连接成功。

远程部署 (Windows)

CIFS UDP 端口：137（入站/出站）

CIFS UDP 端口：138（入站/出站）

TCP 端口：135（入站）

CIFS TCP 端口：139（入站/出站）

CIFS TCP 端口：445（入站/出站）

CAM UDP 端口：4104（入站/出站）

CAM TCP 端口：4105（可配置）的通信端口

远程部署（UNIX、Linux）

CAM UDP 端口：4104（入站/出站）

安全外壳 TCP 端口：22（入站）

TCP 端口：135（入站）

CAM TCP 端口：4105（可配置）的通信端口

远程监控

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

远程监控

需要访问 Windows Management Instrumentation (WMI) 的凭据。

通信端口

Windows RPC 端点映射程序端口：135

DCOM/WMI 端口：在 RPC 端点协调期间动态分配

作为最佳实践，远程监控系统必须是 AD 域的成员。通过该成员身份，您可以使用域帐户，并且不需要在每个 RM 系统上定义本地用户帐户。创建作为 AD 域的 Domain Admins 组成员的 CARMuser 域帐户。

在 RM 安装期间提示进行用户凭据设置时，向域帐户提供密码。对于该域的任何系统成员，无需其他配置。

注意：如有需要，可以限制 CARMuser 访问权限，使用户不是 Domain Admins 组的成员。在这种情况下，配置 WMI 命名空间访问和 DCOM 访问。有关定义 WMI 命名空间访问和 DCOM 访问的详细信息，请参阅 Microsoft 网站。

SystemEDGE 和高级加密

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

在 Linux 或 UNIX 上安装

要求 root 访问权限或为非特权用户帐户使用 sudo 配置。

监控

编辑和加载 cf 文件的权限，或使用远程配置的权限。

通信端口

UDP 端口：161（SNMP Get/Set 请求）；备用端口：1691

UDP 陷阱端口：162（出站）

受管模式中的 SystemEDGE 使用 CAM：

CAM UDP 端口：4104

CAM TCP 端口：4105

VMware vCenter

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

（对 AIM 有效）要求在 VC 中，对 AIM 组件具有只读用户访问权限。

（对 PMM 有效）要求为 vSphere vCenter 服务器指定的权限集。

重要信息！用户角色必须与正在执行的操作的类型匹配，否则操作无法运行。

通信端口

HTTPS（端口：443）

VMware vCloud

本节列出了安装和监控环境所需的访问权限以及必需的通信端口。确认列出的通信端口处于打开状态。

AIM 安装

在 AIM 主机上需要 Windows 系统管理员权限。

监控

（对 AIM 有效）要求系统管理员角色。

（对 VMware WS 有效）操作局限于用户角色。

系统管理员@System

授予完全访问权限。

组织访问@org_name

限制组织级别操作和角色分配。

通信端口

REST API 端口：8443

如何配置 SNMP 和访问控制列表

本节介绍了全局和服务器级别的 SNMP 设置之间的区别、如何应用“访问控制列表”以及如何配置 SNMP 以成功发现系统。

详细信息：

SNMP 一致性 (p. 90)
全局和服务器级别的 SNMP 设置 (p. 91)
如何配置 SNMPv1/v2 设置和访问控制列表 (p. 93)
如何管理服务器级别的 SNMP 设置 (p. 103)
如何配置 SNMPv3 (p. 107)
配置 CA Virtual Assurance 以转发事件 (p. 113)

SNMP 一致性

一致的 SNMP 设置是正确发现系统和网络所必需的。如果 CA Virtual Assurance 管理器上不存在远程系统上的 SystemEDGE 的任何 SNMP 设置，则 CA Virtual Assurance 无法在该系统上发现所需的资源。CA Virtual Assurance 至少需要有效的只读 SNMP 凭据来发现系统。

如果您远程部署 SystemEDGE 代理，并且通过“策略配置”配置代理，则会自动实现管理器和受管系统之间的 SNMP 一致性条件。

如果您在本地配置远程服务器上的 SNMP 设置，请验证 SNMP 设置的一致性。如果在管理器上未指定远程服务器上的任何 SNMP 设置，请指定缺少凭据作为 CA Virtual Assurance 中的全局 SNMP 对象，并发现远程系统。

本章中的 SNMP 方案和过程假定 SystemEDGE 代理以受管模式运行。在受管模式下，SystemEDGE 在 CA Virtual Assurance 中通过“策略配置”进行配置。

详细信息：

全局和服务器级别的 SNMP 设置 (p. 91)

全局和服务器级别的 SNMP 设置

服务器级别或全局 SNMP 设置之类的类别仅存在于 CA Virtual Assurance 管理器上。“策略配置”通过策略向受管服务器提供了这些设置的集合。这些 SNMP 设置最终显示在每个受管目标服务器上的 sysedge.cf 配置文件中。SystemEDGE 不区分服务器级别或全局 SNMP 设置。该信息仅存储在管理器上。管理器了解已应用到特定受管服务器的策略的版本。

如有必要，可将自己的全局或服务器级别的 SNMP 设置添加到 CA Virtual Assurance 管理器中。

在大多数情况下，全局 SNMP 设置机制为您提供了管理服务器上 SNMP 设置的适当灵活性。在特定情况下，可能需要使用服务器级别的 SNMP 设置。创建策略的 SNMP 设置集合时，“策略配置”提供了充分的灵活性。可根据具体情况选择全局或服务器级别的 SNMP 设置。

全局 SNMP 设置填充适用于“远程部署”的 SystemEDGE 软件包打包程序中的下列字段的下拉列表：

- 端口
- 读团体
- 读写团体

或者，您可以以内联方式编辑字段。

可用的 SNMPv1 团体字符串取决于端口设置。在您先选择端口号后，您将在该端口的下拉列表中自动获得有效的团体字符串。如果未在软件包打包程序中指定凭据，安装程序将默认为公开的只读字符串。软件包打包程序中的凭据自 SystemEDGE 安装后有效，直到受管服务器上的 SystemEDGE 注册到“策略配置”以进入受管模式。SystemEDGE 通过策略加载设置。

注意： SystemEDGE 的安装需要至少一个 SNMPv1 团体。在 CA Virtual Assurance 在服务器上发现 SystemEDGE 之后，CA Virtual Assurance 可以将这些 SNMPv1 设置视为服务器级别的 SNMP 设置。

“管理”、“配置”、“部署与配置”下的以下选项，可控制软件包打包程序中的 SNMP 设置是否成为服务器级别的 SNMP 设置。

- 注册 SystemEDGE 代理时创建服务器特定的 SNMP 设置。

如果启用此选项，CA Virtual Assurance 将使用安装的 SNMPv1 设置作为服务器级别 SNMP 凭据。

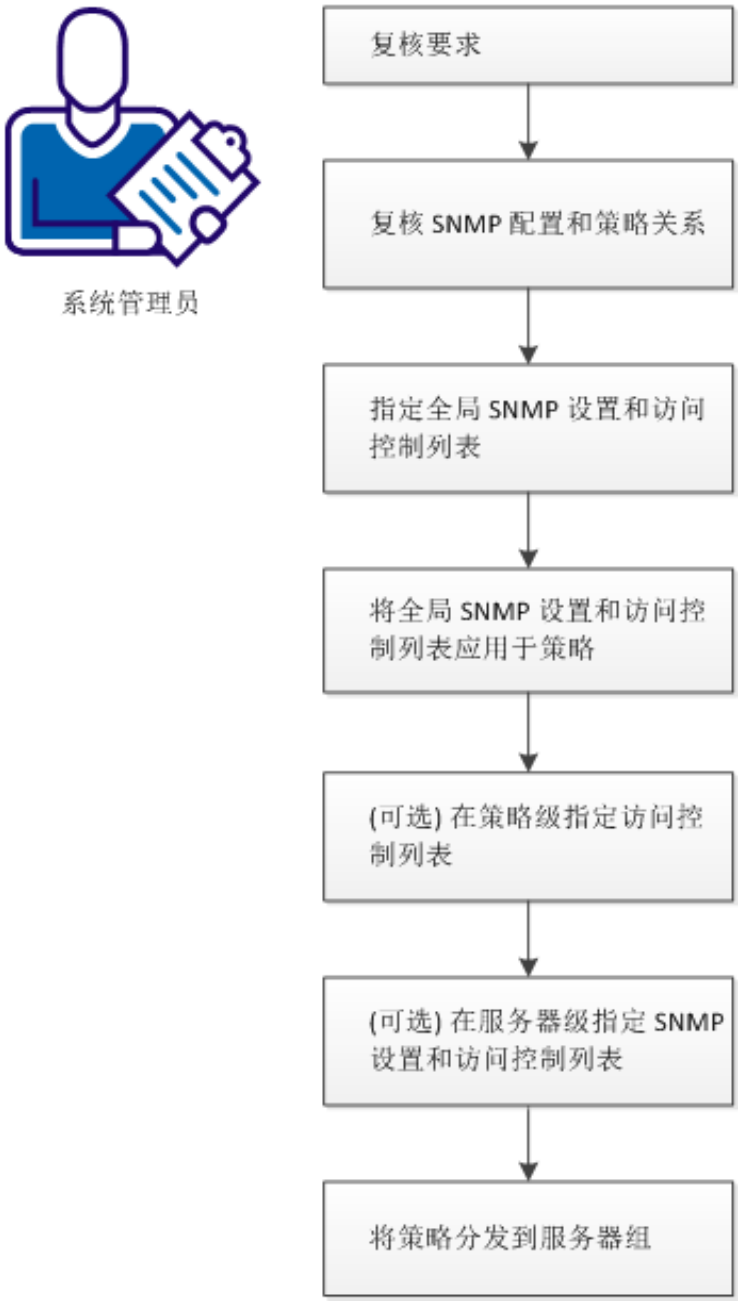
对于每个远程部署作业，您可以指定在部署过程中应用于目标系统的策略。如果您未指定特定策略，CA Virtual Assurance 将使用 SystemEDGE 默认策略。如果已经定义多个 SystemEDGE 策略，您可以在 SystemEDGE 的“策略”窗格中从现有策略的列表确定默认策略。

详细信息：

如何配置 SNMPv1/v2 设置和访问控制列表 (p. 93)
如何管理服务器级别的 SNMP 设置 (p. 103)
如何配置 SNMPv3 (p. 107)

如何配置 SNMPv1/v2 设置和访问控制列表

下图提供了有关为环境指定 SNMP 设置时所需要的操作的概述。该图包括适用于常见情况和特殊情况的策略。特殊情况在该图中表示为可选。



请执行以下步骤：

查看要求 (SNMPv1/2)

在开始配置 CA Virtual Assurance 上的 SNMP 设置之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP 以及 Windows Server 操作系统。
- 您对 CA SystemEDGE 有基本了解。
- 可以访问包括监控代理 (CA SystemEDGE) 的 CA Virtual Assurance 管理器安装。
- 可以在受管节点上访问监控代理 (CA SystemEDGE)。
- 您可以访问 CA Virtual Assurance 用户界面。
- CA Virtual Assurance 已发现所有相关系统。
- SystemEDGE 在要配置的所有系统上以受管模式运行。

详细信息：

查看 SNMP 配置和策略关系 (p. 94)

查看 SNMP 配置和策略关系

SNMPv1/v2 的 SNMP 设置对象由名称、团体字符串、操作类型（只读或读写）、SNMP 版本、端口、超时，重试限制和访问控制列表 (ACL) 组成。

ACL 可指定运行 SystemEDGE 的一组受管系统的管理器系统列表。CA Virtual Assurance 管理器可通过策略配置将 SNMP 设置和 ACL 分发到受管系统。这些受管系统仅会接受 ACL 中列出的管理器系统发出的 SNMP 请求。如果未指定任何 ACL，则受管系统会接受任何系统发出的 SNMP 请求。

如果已定义 ACL，则还会自动将 CA Virtual Assurance 管理器添加到 ACL 列表。始终连接 CA Virtual Assurance 管理器。

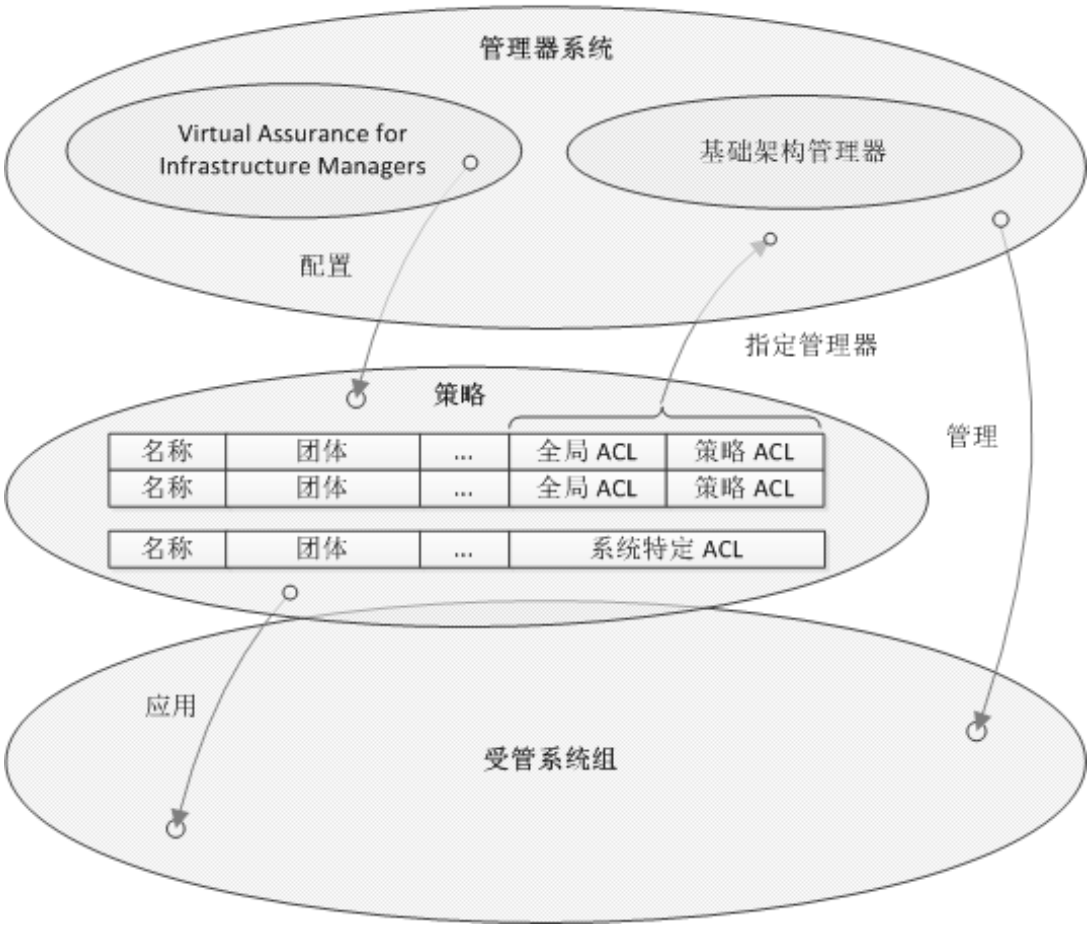
在大多数情况下，可跨许多或所有系统使用相同的 SNMP 凭据。要适当管理和应用这些凭据，可以在全局级别指定 SNMP 凭据和 ACL。要合理发现和管理系统，管理器和代理系统上需要具有一致的 SNMP 凭据和 ACL 设置。可在“管理”、“配置”、“SNMP”下指定全局 SNMP 设置对象。

在特殊情况下，可以在策略级别添加 ACL，或可以在系统级别完全指定 SNMP 凭据和 ACL。如果要在系统级别修改 SNMP 设置，请更改每个受影响系统的设置。

仅将这些 SNMP 设置应用于目标系统，这些设置与目标系统使用相同端口。

下图说明了策略体系结构：

策略体系结构



可以在全局、策略或系统级别配置 SNMP 设置，并可以将这些设置分配给策略（左上角箭头）。可通过 CA Virtual Assurance 将策略应用于一组受管系统。访问控制列表 (ACL) 可指定管理受管系统组的管理器系统名称。如果将所有所需管理器系统添加到 ACL，则受管系统仅会响应这些管理器发出的 SNMP 请求。

详细信息：

指定全局 SNMP 设置和访问控制列表 (p. 96)
将全局 SNMP 设置和访问控制列表应用于策略 (p. 97)
（可选）在策略级别指定访问控制列表 (p. 98)
（可选）在服务器级别指定 SNMP 设置和访问控制列表 (p. 99)
将策略分发给服务器组 (p. 100)
三个服务器组的示例 (p. 101)

指定全局 SNMP 设置和访问控制列表

可以在全局、策略和系统级别指定 SystemEDGE SNMP 凭据的访问控制列表 (ACL)。可以通过将 ACL 与全局 SNMP 对象关联来最大限度地减少与特定于系统的 SNMP 对象的依存关系。

使用用户界面中的“管理”、“配置”、“SNMP”在全局级别编辑 ACL。

遵循这些步骤:

1. 在用户界面中导航到“管理”、“SNMP”。

   此时将显示“SNMP 设置”页面。

2. （可选）单击“操作”、“新建”以创建 SNMP 设置对象。

   此时将显示“新建 SNMP 设置”对话框。SNMP 设置对象由名称、团体字符串、操作类型（只读或读写）、SNMP 版本、端口、超时、重试限制和访问控制列表 (ACL) 组成。使用要应用 SNMP 设置的受管节点上指定的端口号。

3. 指定所需数据以创建 SNMP 设置对象，然后单击“确定”。

4. 选择要添加 ACL 的 SNMP 设置对象，然后单击“编辑”图标。

   此时将显示带有 ACL 面板“编辑 SNMP 设置”对话框。

5. 在“策略配置 SystemEDGE 访问控制列表”面板下指定管理器系统的名称或 IP 地址，然后单击“确定”。

   将指定特定的全局 SNMP 设置对象的 ACL。

可以将带有访问控制列表的全局 SNMP 设置对象应用于策略。

详细信息：

将全局 SNMP 设置和访问控制列表应用于策略 (p. 97)
（可选）在策略级别指定访问控制列表 (p. 98)
（可选）在服务器级别指定 SNMP 设置和访问控制列表 (p. 99)
将策略分发给服务器组 (p. 100)

将全局 SNMP 设置和访问控制列表应用于策略

在完成带有相应 ACL 的全局 SNMP 设置之后，请将 SNMP 设置应用于策略。

遵循这些步骤:

1. 在用户界面中导航到“资源”、“配置”。

   此时将显示“策略”页面。

2. 在导航窗格中展开“策略”、“策略”、“SystemEDGE”。

   此时将显示 SystemEDGE 页面，其中列出了可用策略。

3. （可选）单击 以创建策略。

   此时将显示“新建 SystemEDGE 策略”对话框。

4. 指定所需数据以创建策略，然后单击“确定”。

5. 打开要应用于一个或多个受管系统的策略，然后单击“陷阱及团体”。

   此时将显示“团体”页面，其中包含 SNMP 设置表和以下选项：

   - 仅包括服务器团体
   - 包括服务器团体和所有默认团体（全局团体）
   - 自定义选择

   注意：表中唯一包括在配置中的默认（全局）SNMP 设置是所带有的端口匹配代理端口的那些设置。

6. 选择三个选项之一，并验证您是否至少具有一个配有为每个目标系统指定的相应端口的团体。

   如果选择第一个选项 *“仅包括服务器团体”*，请验证目标系统中是否存在相应服务器级别的 SNMP 设置。可选择的可用服务器团体为常规团体：

   - 服务器读取
   - 服务器写入

   它们表示服务器级别的现有读写凭据。

如果选择第二个选项，则表中的所有全局 SNMP 设置和服务器级别的设置将应用于目标系统。

如果选择第三个选项，则仅表中选定的 SNMP 应用于目标系统。此选项仅允许您选择全局设置。

7. 单击“保存策略”。

可以将策略分发给相应的服务器组，或在策略或服务器级别指定其他 ACL（如有必要）。

详细信息：

（可选）在策略级别指定访问控制列表 (p. 98)
（可选）在服务器级别指定 SNMP 设置和访问控制列表 (p. 99)
将策略分发给服务器组 (p. 100)

（可选）在策略级别指定访问控制列表

在为策略指定带有可选全局 ACL 的全局 SNMP 设置之后，可以在策略级别定义 ACL。

遵循这些步骤:

1. 从策略页面中选择第二个或第三个选项，从而应用表中的全局 SNMP 设置：
   - 包括服务器团体和所有默认团体（全局团体）
   - 自定义选择
2. 从表中选择全局 SNMP 设置对象，然后单击*“视图”*或*“未定义”*链接。

   此时将打开 ACL 对话框。
3. 将管理器系统的名称或 IP 地址添加到*“特定于策略的 SNMP 访问控制列表”*字段，然后单击“确定”。

   要应用此策略的服务器组中的服务器将接受这些管理器系统发出的 SNMP 请求。
4. 单击“保存策略”。

可以将策略分发给相应的服务器组，或在系统级别指定其他 ACL（如有必要）。

详细信息：

（可选）在服务器级别指定 SNMP 设置和访问控制列表 (p. 99)
将策略分发给服务器组 (p. 100)

（可选）在服务器级别指定 SNMP 设置和访问控制列表

在特殊情况下，可以为特定受管系统指定 SNMP 设置和访问控制列表。

遵循这些步骤:

1. 在用户界面中导航到“资源”、“浏览”。

   此时将显示“浏览”窗格。

2. 展开“浏览”树，并右键单击要指定 SNMP 凭据和访问控制列表的系统。

3. 从弹出菜单中选择“策略”、“配置 SNMP 设置”。

   “SNMP 设置”对话框将列出该系统的有效 SNMP 设置。

4. 单击“添加”。

   此时将显示“新建 SNMP 设置”对话框。

5. 指定名称、端口、团体字符串、操作类型（只读或读写）、SNMP 版本、超时和重试限制。使用服务器上已安装的 SystemEDGE 的端口号。单击“确定”。

6. 关闭对话框，转到选定系统页面，然后单击“监控软件”、“SNMP 访问控制”选项卡。

   将列出指定的且特定于系统的 SNMP 团体设置。

7. 从“访问控制列表”列单击“编辑”链接。

   此时将显示特定于系统的“访问控制列表”对话框。

8. 在“SNMP 访问控制列表”字段中输入管理器系统名称，然后单击“确定”。

   受管系统将接受 ACL 中列出的管理器系统发出的 SNMP 请求。

9. 单击“保存”。

将策略分发给相应的服务器组。

详细信息：

将策略分发给服务器组 (p. 100)

将策略分发给服务器组

在完成带有相应 ACL 的 SNMP 设置之后，请将策略应用于网络中的系统。

遵循这些步骤:

1. 在用户界面中导航到“资源”、“配置”。

   此时将显示“策略”页面。

2. 在导航窗格中展开“策略”、“策略”、“SystemEDGE”。

   此时将显示 SystemEDGE 页面，其中列出了可用策略。

3. 选择先前使用相应 SNMP 设置保存的策略。

   此时将打开策略页面。

   注意：如果不希望通过策略配置将现有服务器级别的 SNMP 设置和 ACL 应用于受管系统，请清除“服务器团体”窗格中的“服务器读取”和“服务器写入”条目。

4. 单击“操作”、“应用”。

   此时将显示“选择计算机”页面。

5. 选择要使用该策略配置的所有系统，然后单击“应用”。

   可以查看交付状态，或返回到“策略”页面。

   新设置将应用于目标系统。

详细信息：

三个服务器组的示例 (p. 101)

三个服务器组的示例

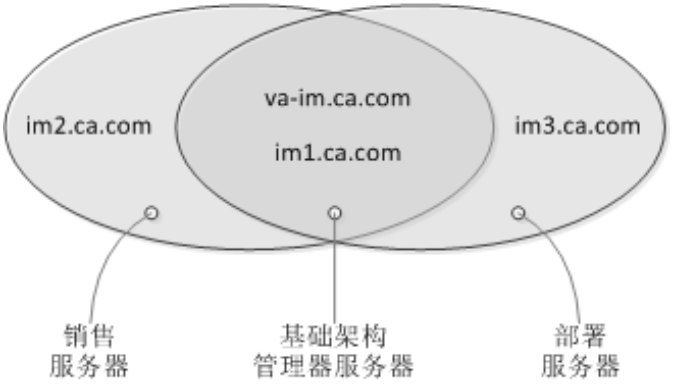
以下示例说明了一个用例，其中包括在全局和策略级别指定的三个服务器组、全局 SNMP 设置和 ACL。

数据中心包括以下服务器组：

- 基础架构管理器服务器：CA Virtual Assurance 系统、SQL Server 系统、CA EEM 系统、一个或多个分发服务器、三个基础架构管理器系统（im1.ca.com、im2.ca.com、im3.ca.com）。通过 va-im.ca.com、im1.ca.com 管理这些系统。
- 销售服务器：通过 va-im.ca.com、im1.ca.com、im2.ca.com 管理所有属于销售部门的服务器。
- 开发服务器：通过 va-im.ca.com、im1.ca.com、im3.ca.com 管理所有属于开发部门的服务器。

服务器组	全局团体设置	全局访问控制列表	策略级别访问控制列表
基础架构管理器服务器	_public_	va-im.ca.com、im1.ca.com	-
	admin	va-im.ca.com、im1.ca.com	-
销售服务器	_public_	va-im.ca.com、im1.ca.com	im2.ca.com
	admin	va-im.ca.com、im1.ca.com	im2.ca.com
开发服务器	_public_	va-im.ca.com、im1.ca.com	im3.ca.com
	admin	va-im.ca.com、im1.ca.com	im3.ca.com

访问控制列表关系



遵循这些步骤:

1. 在“管理”、“SNMP”下指定下列全局 SNMP 对象：

   infrastructure-read：端口 161，只读访问权限，团体 _public_，ACL：va-im.ca.com、im1.ca.com

   infrastructure-write：端口 161，读写访问权限，团体 _admin_，ACL：va-im.ca.com、im1.ca.com

   sales-read：端口 161，只读访问权限，团体 _public_，ACL：va-im.ca.com、im1.ca.com

   sales-write：端口 161，读写访问权限，团体 _admin_，ACL：va-im.ca.com、im1.ca.com

   development-read：端口 161，只读访问权限，团体 _public_，ACL：va-im.ca.com、im1.ca.com

   development-write：端口 161，读写访问权限，团体 _admin_，ACL：va-im.ca.com、im1.ca.com

2. 根据默认策略创建三种策略（每种策略针对一个服务器组）：基础架构、销售和开发
3. 切换到基础架构策略页，从表中选择第三个选项以应用全局 SNMP 设置：
   - 自定义选择
4. 将 infrastructure-read 和 infrastructure-write 全局 SNMP 对象添加到基础架构策略中。
5. 保存该策略。
6. 切换到销售策略页，从表中选择第三个选项以应用全局 SNMP 设置：
   - 自定义选择
7. 将 sales-read 和 sales-write 全局 SNMP 对象添加到销售策略中。

8. 对于 sales-read 和 sales-write 对象，请单击“查看”链接。

   此时将打开相应的 ACL 对话框。

9. 将 im2.ca.com 添加到 sales-read 和 sales-write 对象（策略特定的 SNMP 访问控制列表），然后单击“确定”。
10. 保存该策略。
11. 切换到开发策略页，从表中选择第三个选项以应用全局 SNMP 设置：
    - 自定义选择
12. 将 development-read 和 development-write 全局 SNMP 对象添加到开发策略中。
13. 对于 development-read 和 development-write 对象，请单击相应的“查看”链接。

    此时将打开相应的 ACL 对话框。

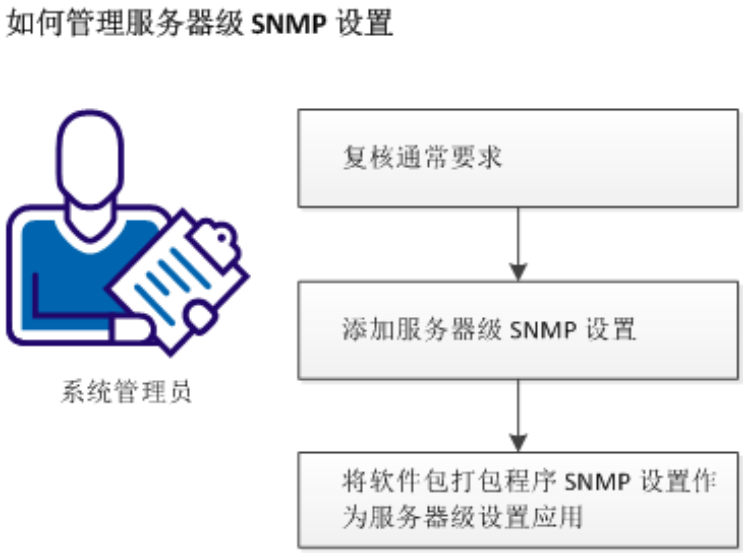
14. 将 im3.ca.com 添加到 development-read 和 development-write 对象，然后单击“确定”。
15. 保存该策略。
16. 将每个策略（基础架构、销售、开发）应用到与其相关联的服务器组。

详细信息：

查看 SNMP 配置和策略关系 (p. 94)

如何管理服务器级别的 SNMP 设置

下图提供了管理服务器级别的 SNMP 设置时所需操作的概述。



请执行以下步骤：

查看要求（服务器级别） (p. 104)
添加服务器级别的 SNMP 设置 (p. 104)
将软件包打包程序 SNMP 设置应用为服务器级别的设置 (p. 106)

查看要求（服务器级别）

在开始管理 CA Virtual Assurance 上服务器级别的 SNMP 设置之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP 以及 Windows Server 操作系统。
- 您对 CA SystemEDGE 有基本了解。
- 已阅读“如何配置 SNMPv1/v2 设置和访问控制列表”方案。
- 可以访问包括监控代理 (CA SystemEDGE) 的 CA Virtual Assurance 管理器安装。
- 可以在受管节点上访问监控代理 (CA SystemEDGE)。
- 您可以访问 CA Virtual Assurance 用户界面。
- CA Virtual Assurance 已发现所有相关系统。
- SystemEDGE 在要配置的所有系统上以受管模式运行。

添加服务器级别的 SNMP 设置

CA Virtual Assurance 通过 SNMP 请求从 SystemEDGE 收集性能度量标准。您可以为各个服务器配置 SNMP 设置。

遵循这些步骤:

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。
2. 展开“数据中心”文件夹及任何子文件夹，然后选择要配置的服务器。
3. 右键单击并选择“策略”。

   此时将显示“策略”子菜单。
4. 单击“配置 SNMP 设置”。

   此时将打开“配置 SNMP 设置”对话框，显示服务器级别的设置。

5. 执行以下操作之一：
   - 选中列表中现有度量标准对应的复选框，然后单击工具图标（编辑）以修改现有条目。
   - 单击“添加”，在服务器级别创建 SNMP 条目。

   此时将显示“新建 SNMP 设置”对话框。
6. 填写下列字段，然后单击“确定”：

   名称

   描述定义的 SNMP 凭据。

   端口

   定义在要使用这些凭据进行管理的系统上为 SystemEDGE 配置的端口。

   SNMP 版本

   指定正在使用的 SNMP 版本。如果选择 SNMP v3 陷阱，将显示其他配置参数的面板。

   团体字符串（针对 SNMP v1/v2）

   指定 SNMP 团体字符串。

   安全用户（针对 SNMP v3）

   为定义的 SNMP 凭据指定 SNMP 安全用户。

   访问类型

   指定访问权限类型。有效选项为“只读”或“读写”。

   超时

   指定超时前等待通知发送确认消息的时间（秒）。

   默认值：10 秒

   重试限制

   指定超时后重试发送通知的次数。

   身份验证（针对 SNMP v3）

   指定要使用的身份验证协议。从“类型”下拉列表中选择“MD5”或“SHA”，然后指定密码。

   隐私（针对 SNMP v3）

   指定要使用的隐私协议。从“类型”下拉列表中选择“DES”、“AES”或“3DES”，然后指定密码。

SNMP 设置将会得到保存，并出现在“服务器设置”表中。

将软件包打包程序 SNMP 设置应用为服务器级别的设置

SystemEDGE 注册到“策略配置”后，可指示 CA Virtual Assurance 使用软件包打包程序 SNMP 设置作为服务器级别的 SNMP 设置。否则，直到 SystemEDGE 注册到“策略配置”后，才会使用软件包打包程序 SNMP 设置。

遵循这些步骤:

1. 切换到“管理”、“配置”、“部署与配置”。

   以下选项控制软件包打包程序中的 SNMP 设置是否成为服务器级别的 SNMP 设置。

   - 注册 SystemEDGE 代理时创建服务器特定的 SNMP 设置。

2. 根据需求启用或禁用该选项。

   如果禁用该选项，软件包打包程序 SNMP 设置将不存储在管理器上，并且不能用于分发。

   如果启用该选项，软件包打包程序 SNMP 设置将在 CA Virtual Assurance 管理器上存储为服务器级别的 SNMP 设置。

3. 切换到“资源”、“配置”，然后打开要应用到受管节点的 SystemEDGE 策略。

   此时将显示“策略”窗格。

4. 在“陷阱和社区”、“服务器社区”下选择适当的项。

   “服务器读取”和“服务器写入”表示服务器级别 SNMP 设置，可用于要应用该策略的受管节点。

5. 在“默认团体”下选择适当的项。

   “默认团体”表示全局 SNMP 设置。

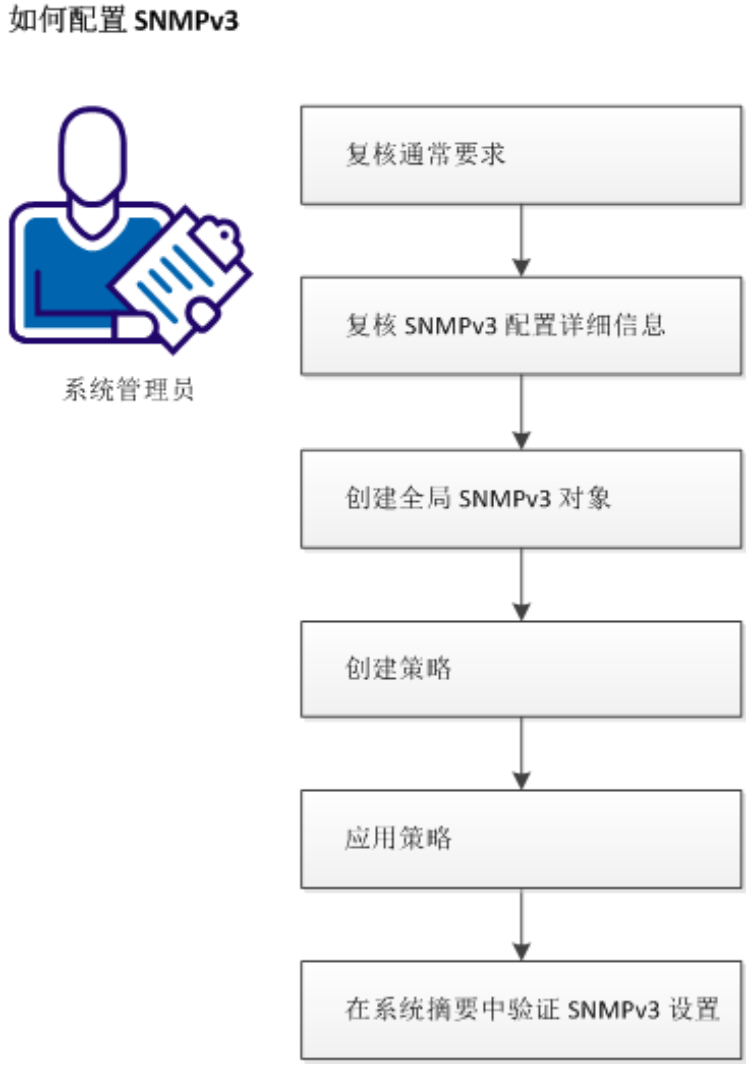
6. 切换到“资源”、“部署”、“软件包”，然后打开 SystemEDGE 软件包打包程序。

7. 设置 SNMP 凭据，选择要在受管节点上安装后应用到 SystemEDGE 代理的策略，然后保存打包程序。

8. 创建“部署作业”，并使用其策略将 SystemEDGE 软件包部署到受管节点。

如何配置 SNMPv3

下图提供了指定适用于您的环境的 SNMPv3 设置时所需的操作概述。此用例介绍适用于 CA Virtual Assurance 的 SNMPv3 配置。



请执行以下步骤：

查看通用要求 (SNMPv3) (p. 108)
查看 SNMPv3 配置详细信息 (p. 108)
创建全局 SNMPv3 对象 (p. 109)
创建策略 (p. 110)
应用策略 (p. 112)
验证系统摘要中的 SNMPv3 设置 (p. 112)

查看通用要求 (SNMPv3)

在开始配置 CA Virtual Assurance 上的 SNMP 设置之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP 以及 Windows Server 操作系统。
- 您对 CA SystemEDGE 有基本了解。
- 已阅读“如何配置 SNMPv1/v2 设置和访问控制列表”方案。
- 已阅读“如何管理服务器级别的 SNMP 设置”方案。
- 可以访问包括监控代理 (CA SystemEDGE) 的 CA Virtual Assurance 管理器安装。
- 可以在受管节点上访问监控代理 (CA SystemEDGE)。
- 您可以访问 CA Virtual Assurance 用户界面。
- CA Virtual Assurance 已发现所有相关系统。
- SystemEDGE 在要配置的所有系统上以受管模式运行。

查看 SNMPv3 配置详细信息

在您打算使用 SNMPv3 在 CA Virtual Assurance 管理器和环境中的受管节点之间进行通信时，请考虑以下详细信息。

- 要安装 SystemEDGE，至少需要一个 SNMPv1 团体。CA Virtual Assurance 发现服务器后，CA Virtual Assurance 会将这些 SNMPv1 设置视为服务器特定的 SNMP 设置。
- 验证您的基础架构管理器是否支持 SNMPv3。
- 创建全局 SNMPv3 凭据。
- 创建将 SNMPv3 设置应用到远程服务器的策略。
- 如果需要纯 SNMPv3 配置，请禁止“策略配置”应用服务器特定的 SNMPv1 设置。

创建全局 SNMPv3 对象

可创建对某一特定服务器有效的全局 SNMP 设置或服务器特定的 SNMP 设置。可通过策略将全局设置应用到服务器组。

遵循这些步骤:

1. 在用户界面中导航到“管理”、“SNMP”。

   此时将显示全局对象的 SNMP 设置页。

2. 单击“操作”、“新建”以创建 SNMP 设置对象。

   此时将显示“新建 SNMP 设置”对话框。

3. 将 SNMP 版本设置为 SNMPv3。

   此时对话框中将显示与 SNMPv3 相关的字段。

4. 填写下列字段，然后单击“确定”：

   名称

   为要定义的 SNMP 凭据指定名称。

   端口

   定义为使用这些凭据进行管理的系统上的 SystemEDGE 配置的端口。

   SNMP 版本

   指定 SNMPv3（已在上一步骤中设置）。

   安全用户

   为定义的 SNMP 凭据指定 SNMP 安全用户。

   访问类型

   指定访问权限类型。有效选项为“只读”或“读写”。

   超时

   指定超时前等待通知发送确认消息的时间（秒）。

   默认值：10 秒

   重试限制

   指定超时后重试发送通知的次数。

   身份验证

   指定要使用的身份验证协议。从“类型”下拉列表中选择“MD5”或“SHA”，然后指定密码。

隐私

指定要使用的隐私协议。从“类型”下拉列表中选择“DES”、“AES”或“3DES”，然后指定密码。

SNMP 设置将会得到保存，并出现在“服务器设置”表中。

创建策略

完成全局 SNMPv3 设置后，将 SNMPv3 设置应用到策略。

遵循这些步骤:

1. 在用户界面中导航到“资源”、“配置”。

   此时将显示“策略”页面。

2. 在导航窗格中展开“策略”、“策略”、“SystemEDGE”。

   此时将显示 SystemEDGE 页面，其中列出了可用策略。

3. 单击  以创建策略。

   此时将显示“新建 SystemEDGE 策略”对话框。

4. 指定所需数据以创建策略，然后单击“确定”。

5. 打开要应用于一个或多个受管系统的策略，然后单击“陷阱及团体”。

   此时将显示“团体”页面，其中包含 SNMP 设置表和以下选项：

   - 仅包括服务器团体
   - 包括服务器团体和所有默认团体
   - 自定义选择

   注意：表中唯一包括在配置中的默认（全局）SNMP 设置是所带有的端口匹配代理端口的那些设置。

6. 选择“自定义选择”。

   此选项仅允许您选择全局 SNMPv3 对象，并清除任何服务器特定的 SNMP 设置。

7. 选择至少一个 SNMPv3 设置对象，并为每个目标系统指定适当的端口，然后单击“保存策略”。

   选择的 SNMPv3 对象与该策略相关联。

8. 单击“陷阱目标”选项卡。

   此时将显示“陷阱目标”页面。可配置 SNMPv3 陷阱目标。

9. 在“陷阱类型”字段中，选择“SNMPv3 陷阱信息”或“SNMPv3 通知信息”（也称为通知请求和已确认陷阱）。

   根据选择的不同，将显示以下字段：

   目标

   指定要向其发送陷阱的主机。您可以指定一个主机名或 IP 地址。

   端口

   在要发送陷阱的目标主机上指定端口号。

   用户名

   指定要用来发送陷阱的 SNMPv3 用户。

   编码

   指定发送陷阱时使用的编码类型。

   默认值：000

   此编码类似于在 SNMPv1 中配置的陷阱编码。另请参阅 *《SystemEDGE 用户指南》* 中的“配置 SNMPv1 陷阱目标”。

   上下文

   *（星号）是该字段唯一支持的值。该值为必填项。

   超时

   （仅限通知）指定超时前等待通知发送确认消息的时间（秒）。

   重试次数

   （仅限通知）指定超时后重试发送通知的次数。

10. 填写各个字段并单击“添加”。

    新条目将显示在“陷阱目标”表中。

    可重复最后一个步骤向表中添加更多条目。

11. 选择“陷阱目标”之一，然后单击“保存策略”。

    策略将与适当的陷阱目标一起保存。

可将策略分配给适当的服务器组。

应用策略

完成 SNMPv3 设置后，可将策略应用到网络中的系统。

遵循这些步骤:

1. 在用户界面中导航到“资源”、“配置”。

   此时将显示“策略”页面。
2. 在导航窗格中展开“策略”、“策略”、“SystemEDGE”。

   此时将显示 SystemEDGE 页面，其中列出了可用策略。
3. 选择先前与适当的 SNMPv3 设置一起保存的策略。

   此时将打开策略页面。
4. 单击“操作”、“应用”。

   此时将显示“选择计算机”页面。
5. 选择要使用该策略配置的所有系统，然后单击“应用”。

   可以查看交付状态，或返回到“策略”页面。

   新设置将应用于目标系统。

备选方案

如果要将 SystemEDGE 部署到远程系统并使用 SNMPv3 凭据，可将策略应用到软件包打包程序，并运行部署作业。

验证系统摘要中的 SNMPv3 设置

要确认 SNMPv3 设置已正确应用到目标系统，请切换到 CA Virtual Assurance 用户界面中的“浏览”窗格。

遵循这些步骤:

1. 在“浏览”窗格中展开组件树。
2. 选择已应用 SNMPv3 设置的受管系统，然后打开“摘要”。

   此时将显示“计算机状态信息”。
3. 确认“活动 SNMP 凭据”字段显示 SNMPv3 全局对象。

注意：如果已在受管服务器上应用纯 SNMPv3 配置，并打开该服务器上的 SystemEDGE“控制面板”（仅限 Windows），则团体和陷阱字段将为空。SystemEDGE“控制面板”在这些字段中显示 SNMPv1 信息。

配置 CA Virtual Assurance 以转发事件

配置产品以将事件转发到 CA 或第三方 SNMP 事件管理器。过程包含以下两个部分：

1. 配置事件管理器以接收 CA Virtual Assurance 陷阱或事件。
2. 配置 CA Virtual Assurance 以转发事件。

以下过程假设您已配置事件管理器控制台来接收事件。

遵循这些步骤:

1. 打开 CA Virtual Assurance 用户界面。
2. 单击“管理”。

   此时将显示“管理”页面。
3. 单击“配置”。

   将出现“配置”页面。
4. 在左侧窗格中单击“事件”。

   此时将显示“事件”窗格。
5. 单击 +（添加）。

   “转发”和“类型”字段将自动填充。

   注意：如果这些字段未填充，请重新启动 Apache Tomcat。
6. 在“服务器”字段中输入管理服务器名称。
7. 输入 SNMP 的其他端口号，或保留自动填充的默认端口 162。
8. 单击“确定”。

   即会出现一条确认消息。
9. 单击“保存”以保存更新的事件转发记录。

   您的设置已更新，将出现配置信息。CA Virtual Assurance 现已配置为转发事件。

如何部署 SystemEDGE 和 AIM

本节说明了如何设置和管理作业以成功部署您的监控软件。

详细信息：

概述

CA Virtual Assurance 提供了将 SystemEDGE 及其他代理远程部署到所有受管系统的综合解决方案。您可以基于提供的包含定制安装参数的软件包创建部署模板，并同时将这些模板部署到许多受管系统。该自动化部署解决方案提供了一个可在整个企业中部署和配置代理的位置。

远程部署提供以下功能：

部署配置

允许创建、编辑和删除定义如何在目标系统上部署软件包的配置。这些配置称为软件包打包程序。

部署作业管理

允许创建、启动、取消和筛选部署作业，也允许使用多个分发服务器将多个软件包同时部署到多个目标。

部署作业报告

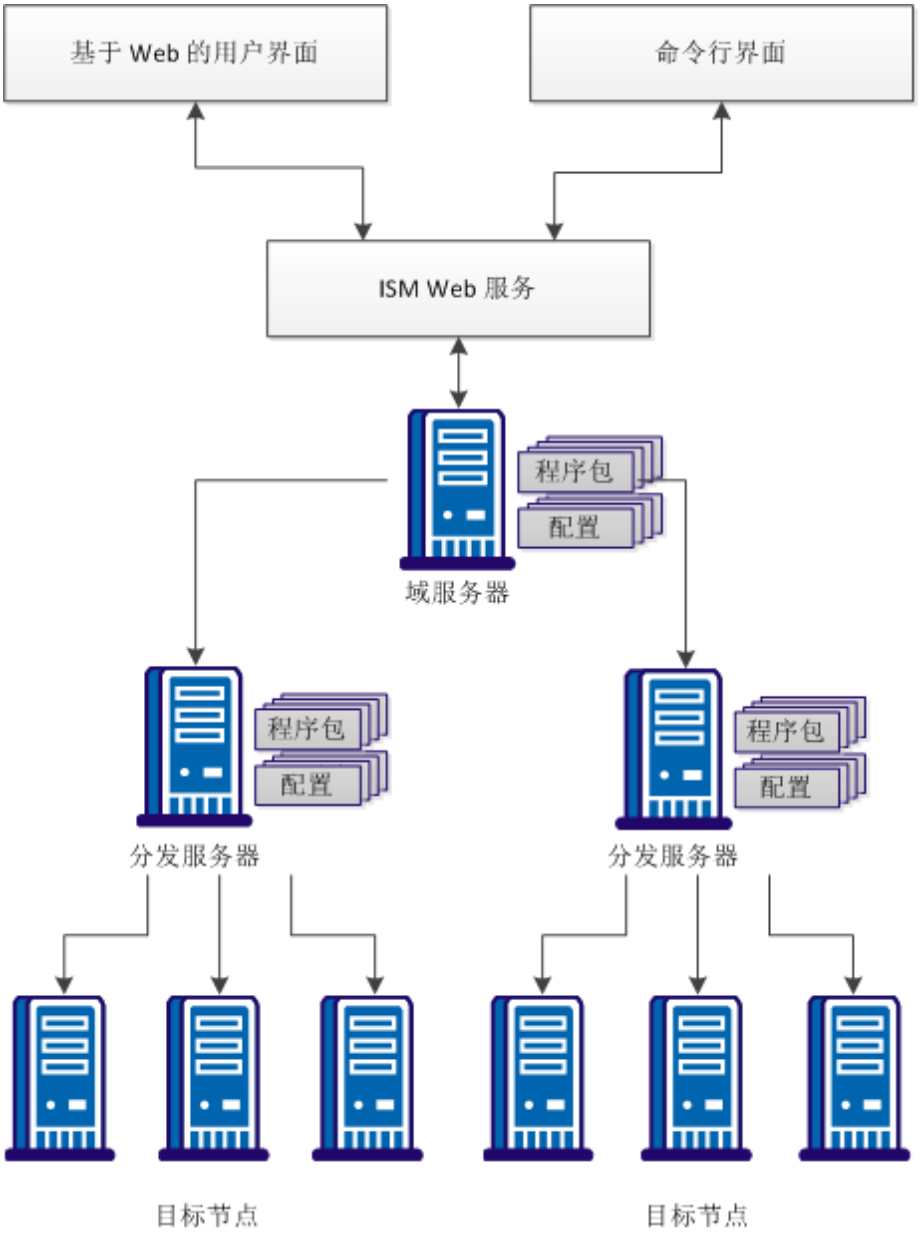
允许查询部署作业的状态。

部署事件

提供跟踪受管节点状态的部署相关事件的源。

远程部署体系结构

部署解决方案的总体体系结构由域服务器和分发服务器组件驱动。下图表示部署相关组件的概述：



关于软件包

部署软件包提供了将监控软件部署到整个企业内的系统所必需的材料。部署软件包被分割成多个软件包打包程序，它们是特定于平台的。软件包打包程序将安装代理软件所需的安装参数封装在一起，并且适用于支持部署的所有平台。

注意：默认软件包打包程序名称未本地化，并将在所有支持的语言中标识为“默认名称”。自定义软件包打包程序名称已本地化。

部署组件

该部分列出并简要介绍了部署关键组件：

域服务器

域服务器是所有配置和控制数据的存储库。服务器负责管理部署操作所需的配置和软件包数据，并管理所有配置操作。在部署过程中，详细的事件数据在域服务器和分发服务器之间传递。单个域服务器负责维护所有分发服务器作业的状态。

分发服务器

分发服务器控制位于同一计算机上的基础架构部署管理器 (IDManager) 服务器。该体系结构允许多个分发服务器提供部署服务。

基础架构部署

基础架构部署启动并管理部署作业。在部署过程中，基础架构部署管理器 (IDManager) 提供对远程系统的访问权限，基础架构部署初级步骤 (ID Primer) 为远程安装代理软件包提供机制。IDPrimer 用于将部署包数据传输到目标计算机并运行安装。可使用现有 IDPrimer 安装进行同一目标计算机的所有后续部署。IDManager 控制所有部署操作并处理作业状态。

配置

本节提供有关远程部署用户界面配置和分发服务器连接的详细信息。

详细信息：

部署显示板视图 (p. 117)
增强的远程部署搜索功能 (p. 118)
作业状态筛选 (p. 118)
更改分发服务器连接到的域服务器 (p. 119)

部署显示板视图

显示板上提供下列视图，用于跟踪部署度量标准：

部署任务摘要

显示一个饼形图和一个列表，其中显示已完成、活动、未决和失败部署任务的数目。

未解决部署任务

显示未成功完成的部署的列表。可以单击作业 ID 来查看关于为何未解决任务的详细信息。

活动部署任务

显示当前处于活动状态的部署任务的列表。详细信息包括关联的部署作业、目标、软件包及当前状态。可以单击任务 ID 以获取当前状态的详细信息。

部署软件包摘要

显示条形图，其中显示每种部署软件包类型的部署数目。

已完成部署作业

显示成功完成的部署的列表。可以单击作业 ID 来查看关于作业的详细信息。

增强的远程部署搜索功能

增强的搜索功能提供与远程部署有关的关键词的搜索结果，并且也可用于从搜索结果快速访问远程部署操作。优势如下所示：

优势如下所示：

- 快速访问远程部署组件。
- 将远程部署软件包部署到服务器和服务。
- 管理远程部署软件包和模板。
- 快速创建和管理部署作业，并且授予对可用软件包和打包程序的访问权限。

遵循这些步骤:

1. 在“值”字段中输入关键字（或带通配符的部分值），然后单击“搜索”。

   示例：

   部署或远程或远程部署。

   将显示远程部署链接的列表。
2. 选择适当的远程部署操作。

   执行远程部署操作。

作业状态筛选

筛选作业状态数据以仅显示每个作业的相关详细信息。您可以对列进行排序和自定义，并且按一列或多列筛选。

遵循这些步骤:

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”文件夹。
2. 单击“作业”。

   将在右侧窗格中显示作业详细信息。
3. （可选）选择/取消选择“作业状态”列的复选框。

   将显示自定义列。
4. 选择/取消选择列的筛选。

   作业将按筛选选择进行显示。

更改分发服务器连接到的域服务器

在最初安装后域服务器计算机的网络地址发生更改的情况下，有必要重新配置分发服务器，以连接到新的网络地址。

在进行以下所示的配置更改之前，请务必确保可从分发服务器连接到新的网络地址。如果分发服务器无法使用新地址连接到域服务器，则部署功能将无法正常工作。

更改分发服务器连接到的域服务器

1. 从“开始”菜单中，打开“管理工具”、“服务”。

   将出现“服务”用户界面，列出了已安装的服务。

2. 右键单击“CA SM 分发服务器”并选择“属性”。

   将显示“属性”对话框。

3. 单击“停止”以停止服务。

4. 在“开始”参数字段中输入以下参数：

   -m *domainserver*

   domainserver 参数指定域服务器的 IP 地址或 DNS 名称。

5. 单击“开始”。

   分发服务器现在将尝试连接到输入的域服务器地址。

可扩展性

部署系统使用多个分发服务器作为可扩展性层来提供一定程度的可扩展性。每个分发服务器与一个 IDManager 实例进行通信。IDManager 可以对多个组件部署到多个目标计算机进行管理。因为该联合模型，CA Virtual Assurance 支持许多同步部署。

部署大小调整关键因素

许多关键因素对基础架构规模调整和系统性能有相当大的影响，包括：

- 要传送的软件包大小。
- 要传送的软件包数目。
- 软件包的传送频率。
- 部署组件和目标计算机之间的网络延迟。
- 网络带宽管理。

注意：向目标计算机的初始部署安装了 IDPrimer，一个小型安装代理。安装了 IDPrimer 后，对同一个目标的后续部署会节约一些时间。

部署建议：

- 验证目标服务器通常能否满足远程部署软件的要求。
- 安装目标位置本地的其他分发服务器。
- 尽量使用目标位置本地的分发服务器进行部署。
- 尽量安排在网络通信低谷期间启动部署。

注意：有关 CA Virtual Assurance 可扩展性的详细信息，请参阅“可扩展性最佳实践”。

多个分发服务器

虽然通过远程部署解决方案，可以用单个中央服务器（管理器）管理所有部署，但如果有任何以下要求，CA Technologies 建议您安装指向中央域服务器的远程分发服务器：

- 您有两个或多个远程地理位置，您需要将代理程序软件部署到这些位置，但需要使用单个管理器集中管理这些位置。

  在此类情况下，CA Technologies 建议每个位置至少有一台连接到中央域服务器的分发服务器。
- 您有一个位置，但需要部署到几百台计算机。

  在此情况下，可以跨子网逻辑分布安装多个分发服务器，这些分发服务器将连接到中央域服务器。

部署软件包

部署软件包提供了将监控软件部署到整个企业内的系统所必需的材料。部署软件包根据具体平台细分为各种类别，软件包打包程序可用于所有支持部署的平台。

重要信息！ AIM 依存于 SystemEDGE 和高级加密软件包。要部署任何这些软件包，系统上必须已存在 SystemEDGE 和高级加密软件包，或者必须在部署作业中包括这些软件包。

提供了下列部署软件包：

性能代理 (CA Systems Performance LiteAgent)

提供一个轻量级监控代理，用于在 Windows、UNIX 或 Linux 上监控和收集性能度量标准。

SystemEDGE

提供核心 SystemEDGE 代理。

SystemEDGE ADES

提供适用于 Active Directory 和 Exchange Server 的 AIM。

SystemEDGE 高级加密

提供适用于 SystemEDGE 的 FIPS 140 兼容加密软件包。

SystemEDGE AIX LPAR

提供适用于 IBM PowerVM (LPAR) 的 AIM。

SystemEDGE CXEN

提供适用于 Citrix XenServer 的 AIM。

SystemEDGE Citrix XenDesktop

提供适用于 Citrix XenDesktop 的 AIM。

SystemEDGE GalaX

提供用于 Huawei GalaX8800 的 AIM。

SystemEDGE Hyper-V

提供适用于 Microsoft Hyper-V 的 AIM。

SystemEDGE IBM PowerHA

提供用于 IBM PowerHA （以前称为 High Availability Cluster Multiprocessing ）的 AIM。

SystemEDGE KVM

提供基于 KVM 技术适用于 Red Hat Enterprise Virtualization (RHEV) 的 AIM。

SystemEDGE MSCS

提供适用于 Microsoft 群集支持 (MSCS) 的 AIM。

SystemEDGE RM

提供远程监控 AIM。

SystemEDGE Solaris Zones

提供适用于 Oracle Solaris Zones 的 AIM。

SystemEDGE SRM

提供服务响应监视器 AIM。

SystemEDGE UCS

提供适用于 Cisco UCS 的 AIM。

SystemEDGE VC

提供适用于 VMware vCenter 的 AIM。

SystemEDGE VCLOUD

提供适用于 VMware vCloud Director 的 AIM。

默认软件包打包程序

向可使用远程部署进行部署的软件包提供现成的默认软件包打包程序。这些软件包打包程序包含安装程序参数，这些参数的一系列默认值适用于选中的软件包。如果软件包需要必需参数，请在您部署该软件包之前，指定这些参数并保存设置。

除非需要修改软件包的安装程序参数值，否则您不必再次编辑参数。如果您继续部署软件包而未指定必需参数，则部署进程将停止。软件包打包程序将不处于可部署状态。

可用软件包打包程序将提供以下参数。用户界面中指示了必需参数：

SystemEDGE

在“管理”、“配置”、“SNMP”下指定的全局 SNMP 设置可在 SystemEDGE 软件包打包程序中填充以下字段的下拉列表：

- 端口
- 读团体
- 读写团体

或者，您可以以内联方式编辑字段。

可用的团体字符串取决于端口设置。在您先选择端口号后，您将在该端口的下拉列表中自动获得有效的团体字符串。

安装路径

定义软件包的根安装目录。

数据路径

定义软件包的数据目录。

共享路径

定义用于 CA 共享组件的根安装目录。

端口

定义 SystemEDGE 端口号。

默认值：161

说明

定义 SNMP 系统描述。

位置

定义 SNMP 系统位置。

联系人

定义 SNMP 系统联系人。

读团体

定义 SNMP 只读团体字符串。

默认值：public

读写团体

定义 SNMP 读写团体字符串

陷阱团体

定义 SNMP 陷阱团体字符串

陷阱目标

定义 SNMP 陷阱目标主机名。

陷阱端口

定义 SNMP 陷阱端口。

默认值：162

权限分隔用户 (UNIX/Linux)

指定用户名，在 SNMP 通信期间代理使用其凭据运行。

该条目可指示代理使用其他用户帐户运行 SNMP 通信。此代理还会将该用户的默认组用作有效组。

默认值：代理使用 root 帐户运行。

“启动代理”复选框

指定是否在安装结束时自动启动 SystemEDGE。

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

注意：“停止重新启动”复选框仅用于 Windows 软件包。

“禁用本地代理”复选框

指定是否替换本地 SNMP 代理。

“使用本地设置”复选框

指定是否使用本地的 SNMP 代理设置（如果替换本地的 SNMP 代理）。

“以受管模式运行”复选框

指定是否以受管模式运行 SystemEDGE。

“受管策略名称”下拉列表

指定可用 SystemEDGE 策略的列表。

注意：在从 4.3 版或 4.2 版修补程序级别 3 升级 SystemEDGE 时，安装程序将仅使用以下参数：

CASE_PUBDATADIR
CASE_MANAGER_HOSTNAME
CASE_MANAGER_POLICY_NAME
CASE_START_AFTER_INSTALL
CASE_LEGACY_MODE
CASE_SNMP_PORT
CASE_INSTALL_DOCS
CASE_SNMP_TRAP_COMMUNITY (1)
CASE_SNMP_TRAP_DESTINATION (1)
CASE_SNMP_TRAP_PORT (1)
CASE_SNMP_READ_COMMUNITY (1)
CASE_SNMP_WRITE_COMMUNITY (1)
CASE_SNMP_READ_ALLOWED_MANAGERS (1)
CASE_SNMP_WRITE_ALLOWED_MANAGERS (1)

忽略其他参数。

(1) 这些参数很特殊。它们的设置已附加到现有的 SystemEDGE 4.x 设置，允许 SystemEDGE 4.x 管理器和 SystemEDGE 5.x 管理器运行。

注意：有关参数的详细信息，请参阅*《SystemEDGE 用户指南》*中的*“安装和部署”*一章。

CA SystemEDGE ADES

Windows 域

指定要监控的 Windows 域。

域用户

指定用于连接到域服务器或 Exchange Server 的域管理员用户。

域用户密码

指定用于连接到域服务器或 Exchange Server 的域管理员用户的密码。

管理实体

指定受管实体。

0

指定要监控 Active Directory。

1

指定要监控 Exchange Server。

2

指定要监控 Active Directory 和 Exchange Server。

管理模式

指定用于提供管理的选项。

0

指定要监控整个域。

1

指定要监控域的特定主机。

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

SystemEDGE 高级加密

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE AIX LPAR

LPAR 主机

指定用于连接到 IBM LPAR 服务器的主机名。指定 IBM LPAR 主机名，以便部署该软件包。

用户名

指定用于连接到 IBM LPAR 服务器的用户名。指定 IBM LPAR 用户名，以便部署该软件包。

密码

指定用于连接到 IBM LPAR 服务器的密码。指定 IBM LPAR 密码，以便部署此软件包。

CA SystemEDGE CXEN

CXEN 主机名

指定用于 Citrix XenServer 集成的主机名。

CXEN 用户名

指定用于 Citrix XenServer 集成的用户名。

CXEN 密码

指定用于 Citrix XenServer 集成的密码。

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE CXenDesktop

主机名

指定用于 Citrix XenDesktop 集成的主机名。

用户名

指定用于 Citrix XenDesktop 集成的用户名。

密码

指定用于 Citrix XenDesktop 集成的密码。

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE GalaX

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE PowerHA

主机名

指定用于连接 IBM PowerHA 的主机名。指定 PowerHA 主机名，以便部署该软件包。

用户名

指定用于连接 IBM PowerHA 的用户名。指定 PowerHA 用户名，以便部署该软件包。

密码

指定用于连接 IBM PowerHA 的密码。指定 PowerHA 密码，以便部署该软件包。

端口

定义 PowerHA 端口号。

默认值：22

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE Hyper-V

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE KVM (RHEV)

KVM 主机名

指定用于连接到 Red Hat Enterprise Virtualization (RHEV) 的主机名。

KVM 用户名

指定用于连接到 RHEV 的用户名。

KVM 密码

指定用于连接到 RHEV 的密码。

KVM 端口

指定用于连接到 RHEV 的端口。

默认值：8443

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE MSCS

MSCS 主机名

指定用于连接到群集的主机名。

MSCS 用户名

指定用于连接到群集的用户名。

MSCS 密码

指定用于连接到群集的密码。

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE RM

默认 WMI 用户名

定义用于连接到远程计算机的默认用户名。指定用户名，以便部署该软件包。

默认 WMI 密码

定义用于连接到远程计算机的默认密码。指定密码，以便部署该软件包。

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE SRM

“允许脚本”复选框

指定是否允许作为测试运行脚本。

“允许文件 I/O 测试”复选框

指定是否允许作为测试运行文件 I/O。

“允许不受信任 SSL”复选框

指定是否允许使用未经验证的证书访问 SSL 站点。

“禁用用户 TOS”复选框 (Windows)

指定是否禁止应用程序在传出 IP 数据包中设置服务位类型。

“停止重新启动”复选框 (Windows)

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE Solaris Zone

Zones 主机

指定用于连接到 Solaris Zone 服务器的主机名。指定 Solaris Zone 主机名，以便部署该软件包。

用户名

指定用于连接到 Solaris Zone 服务器的用户名。指定 Solaris Zone 用户名，以便部署该软件包。

密码

指定用于连接到 Solaris Zone 服务器的密码。指定 Solaris Zone 密码，以便部署该软件包。

CA SystemEDGE UCS

UCS 主机名

指定用于连接到 UCS 的主机名。指定 UCS 主机名，以便部署该软件包。

UCS 用户名

指定用于连接到 UCS 的用户名。指定 UCS 用户名，以便部署该软件包。

UCS 密码

指定用于连接到 UCS 的密码。指定 UCS 密码，以便部署该软件包。

UCS 协议

指定要使用的协议：HTTP 或 HTTPS。

端口

定义 UCS 端口号。

默认值：80 (HTTP) 或 443 (针对 HTTPS)。

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE VC

主机名

指定用于连接到 vCenter 的主机名。指定 vCenter 主机名，以便部署该软件包。

用户名

指定用于连接到 vCenter 的用户名。指定 vCenter 用户名，以便部署该软件包。

密码

指定用于连接到 vCenter 的密码。指定 vCenter 密码，以便部署该软件包。

端口

定义 vCenter 端口号。

默认值：443

协议

指定要使用的协议：HTTP 或 HTTPS。

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA SystemEDGE VCLOUD

VCLOUD 主机名

指定用于连接到 vCloud 的主机名。

VCLOUD 用户名

指定用于连接到 vCloud 的用户名。

VCLOUD 密码

指定用于连接到 vCloud 的密码。

VCLOUD 端口

定义 vCloud 端口号。

默认值：443

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

CA Systems Performance LiteAgent

共享路径

定义用于 CA 共享组件的根安装目录。

安装路径

定义软件包的根安装目录。

“停止重新启动”复选框

指定是否在安装结束时停止自动重新启动。

详细信息

创建新的软件包打包程序 (p. 137)
修改软件包打包程序 (p. 138)

部署软件包库

软件包库包含一组可配置的可安装软件包，您可以在这个库中控制哪些产品、版本和平台可供部署使用。可通过创建标准软件包配置来控制安装这些产品的方式，标准软件包配置定义了以无人看管方式安装所配置的软件包时所需的参数。

每个软件包必须有关联的软件包配置文件。配置文件提供了软件包的详细描述，以及软件包安装的具体配置。有关详细信息，请参阅部署软件包配置文件 (p. 135)一节。

软件包库位于以下目录中：

%AllUsersProfile%\CA\SM\domainserver\Deployment\Packages\SM

目录树布局是按照 IDManager 组件的要求定义的。软件包库本身包含一个顶级软件包目录，该目录包含两个子目录，即“Public”和“Private”。“Public”目录包含所有可部署的软件包。

```
..
└──────SM
    ├──────CA_LiteAgent
    ├──────CA_ProcProbe_Utility
    ├──────CA_SystemEDGE_AdvancedEncryption
    ├──────CA_SystemEDGE_Core
    |    └──────5.8.0
    |        └──────ENU
    |            ├──────AIX_aix
    |            ├──────HPUX_hp
    |            ├──────HPUX_ia64
    |            ├──────Linux_ia64
    |            ├──────Linux_ppc
    |            ├──────Linux_x86
    |            ├──────Solaris_sparc
    |            ├──────Solaris_x86
    |            ├──────Windows_ia64
    |            ├──────Windows_x64
    |            └──────Windows_x86
    ├──────CA_SystemEDGE_CXEN
    ├──────CA_SystemEDGE_CXENDESKTOP
    ├──────CA_SystemEDGE_ESAD
    ├──────CA_SystemEDGE_GALAX
    ├──────CA_SystemEDGE_HACMP
    ├──────CA_SystemEDGE_HyperV
    ├──────CA_SystemEDGE_KVM
    ├──────CA_SystemEDGE_LPAR
    ├──────CA_SystemEDGE_MSCS
    ├──────CA_SystemEDGE_RM
    ├──────CA_SystemEDGE_SRM
    ├──────CA_SystemEDGE_UCS
    ├──────CA_SystemEDGE_VCLOUD
    ├──────CA_SystemEDGE_Zone
    └──────CA_VMVCAIM
```

顶级“Public”目录有五个子目录：

组件名称

必须是 IDManager 实例名，CA Virtual Assurance 的组件名称为 SM。

软件包

包含单个可部署软件包的所有版本、本地化和体系结构，例如 CA_SystemEDGE_Core，CA_SystemEDGE_SRM

版本

包含的软件包版本。

语言

软件包安装语言。

示例：-ENU

体系结构

体系结构特定的安装材料，例如 Windows_ia64、Solaris_x86。

注意：体系结构目录名称必须是 IDManager 支持的平台之一。

在分发服务器计算机内运行时，IDManager 组件使用分发服务器下的目录。这包含供内部使用的加密软件包临时缓存。作业完成时应删除这些软件包。

私有的 IDPrimer 安装材料包含在其他目录内。默认情况下，这些安装材料存储在 IDManager 组件自身的安装目录下，如下所示：

<CA Shared Components>/IDMgrApi/packages/private/idprimer

该目录包含基础架构部署组件支持的所有平台的 IDPrimer 安装材料。

软件包筛选

如果服务器已升级，远程部署可显示越来越多的软件包版本。该版本的默认设置是仅显示最新可用的软件包。因此，还会对“软件包 - 详细信息”选项卡中的数据进行筛选，以便仅显示每个软件包的最新版本。从该面板中选择打包程序，在选定的打包程序位置展开目录树。

如果想查看所有软件包，可以通过选择“软件包信息”面板中的“仅显示最新软件包版本”复选框覆盖默认的筛选行为。启用（默认）后，将从左侧目录树和“软件包详细信息”选项卡中筛选出任何较旧的软件包版本。

更改筛选行为：

1. 选择/取消选择“软件包信息”面板中的“仅显示最新软件包版本”复选框。
2. 刷新用户界面中的“部署”视图。

   将出现最新的软件包版本。

注意：UI 中显示软件包版本的所有其他位置不受影响。

部署软件包配置文件

除了软件包安装材料，可通过附加的软件包配置文件 pkginfo_PLATFORM.xml 引用各个可部署的软件包。软件包配置文件说明了安装软件包和配置流程。

配置文件提供了以下内容：

- 安装软件包的可本地化描述。
- 一种软件包依存关系可以机读格式编码所依据的机制。
- 记录可公开访问的安装参数类型。
- 参数类型的其他上下文，以便可以在 UI 内执行一种级别的验证。
- 参数名称与标记之间的映射，用于以独立于平台的方式表示软件包安装程序中的参数。
- 指定应如何在目标计算机上执行安装材料。
- 安装程序退出代码与部署系统识别的那些代码之间的映射。

可使用特定于区域设置的并列文件有选择地提供 pkginfo.xml 文件的本地化元素，或将这些元素内嵌在单个文件中。可加载名称与 pkginfo_PLATFORM.xml 匹配的文件，以获得本地化的消息数据。

部署系统需要将软件包配置文件与针对具体平台的子目录平行放在软件包树中。有关示例，请参阅以下目录：

%AllUsersProfile%\CA\SM\domainserver\Deployment\Packages\SM\CA_SystemEDGE_Core\5.7.1\ENU

```
pkginfo_AIX.xml
pkginfo_HPUX.xml
pkginfo_Linux.xml
pkginfo_LinuxPPC.xml
pkginfo_Solaris_sparc.xml
pkginfo_Solaris_x86.xml
pkginfo_Windows.xml
```

使用远程部署

您可以从 CA Virtual Assurance 用户界面中使用集中式远程部署，通过一次操作将监控代理部署到多个系统中。通过 CA Virtual Assurance 进行软件包部署是安全且可靠的解决方案，该解决方案使您可以从中央界面配置安装在整个企业中的监控软件。

部署限制

在执行部署之前考虑以下限制：

- 如果想在 CA Virtual Assurance 管理器系统上安装代理，必须执行手工单机代理安装。不支持在 CA Virtual Assurance 管理器系统上部署代理。
- 部署过程取决于现有主机操作系统服务的可用性，以便能够远程访问目标系统。当目标节点上不提供这些服务时，必须在目标系统上安装 IDPrimer 客户端软件包和相应的密钥。

  注意：有关安装的详细信息，请参阅 *手工安装远程部署初级步骤软件* 一节。
- 大多数（但不是全部）受支持的代理平台都支持部署。

  注意：有关部署支持的详细信息，请参阅 *《CA Virtual Assurance 版本说明》*。

部署凭据限制

UI 将用户名和密码字段的输入内容限制为 64 个字符。

审核跟踪

作业和任务是部署系统的两个基本概念。*部署作业*指定要在一个或多个目标系统上提供的一个或多个软件包。*部署任务*表示目标系统上软件包的各个部署。部署作业报告允许您查询部署作业的状态。

您可以创建、控制和查询部署作业的状态。启动作业之后，会将其各个部署任务委派给执行实际部署的可用分发服务器。发生这种情况时，您可以跟踪作业的进度，以验证部署进展是否正常并标识和解决所有问题。

远程部署能够提供以下信息：

- 当前部署作业为：
  - 非活动（尚未开始）
  - 活动
  - 已完成，其为：
    - 成功
    - 部分成功
    - 不成功

- 部署作业为：
  - 与特定目标计算机相关联
  - 与特定软件包/软件包组相关联
- 已将哪些软件包部署到特定目标计算机
- 哪个用户创建/启动了特定软件包的部署
- 特定部署作业以哪个计算机为目标
- 活动部署作业以哪个计算机为目标

注意：远程部署支持将软件部署到 UNIX/Linux 系统，这些系统具有使用 noexec 标志安装的 /tmp 文件系统。

创建新的软件包打包程序

软件包打包程序可在部署特定软件包时为要遵循的部署机制提供特定于平台的说明。每个软件包都包含支持远程部署的所有平台的默认软件包打包程序。如果某些系统需要与默认设置不同的设置，您可以创建新的软件包打包程序。

遵循这些步骤:

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”文件夹。

2. 展开“软件包”。

   “部署”窗格中将显示可用软件包列表。

3. 右键单击“部署”窗格中的某个软件包名称，然后选择“创建新打包程序”。也可以单击“可用打包程序”工具栏上的 +（新建）。

   此时将显示“新建打包程序”对话框。

4. 输入打包程序的名称及可选说明，指定打包程序应支持的平台，然后单击“确定”。

   打包程序现已创建完成，并在右侧窗格中显示详细信息。

   注意：如果创建 SystemEDGE 软件包打包程序，请注意“陷阱端口”、“陷阱目标”和“陷阱团体”字段之间的依存关系。要么不设置任何字段，要么设置所有字段。如果设置部分字段，安装程序会显示错误消息。

修改软件包打包程序

软件包打包程序为部署软件包定义了一组特定于平台的安装设置，如安装路径、端口、陷阱团体等。您可以编辑用户创建的或默认的软件包打包程序以更改该组安装设置。可用属性因软件包类型而有所不同。

修改软件包打包程序

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”文件夹。

2. 展开“软件包”、特定软件包类型和打包程序平台，并选择要修改的打包程序。

   将在右侧窗格中显示该打包程序的详细信息。

3. 根据需要修改软件包属性，然后单击“保存”。“属性”窗格中显示的选项因选择的软件包类型而有所不同。

复制软件包打包程序

您可以复制软件包打包程序并根据需要编辑属性。

遵循这些步骤:

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”。

2. 展开软件包、特定软件包类型和平台。

3. 选择打包程序。

   将在右侧窗格中显示该打包程序的详细信息。

4. 右键单击打包程序名称。选择“复制”。还可以从“操作”下拉菜单中选择“复制”。

   此时将显示“复制”对话框。

5. 输入软件包打包程序的新名称以及说明（可选），然后单击“确定”。

   将在部署窗格中显示新的软件包打包程序。

6. 根据需要编辑属性，然后单击“保存”。

   左侧窗格中将显示新的软件包打包程序。

删除软件包打包程序

您可以删除不再需要的软件包打包程序。

遵循这些步骤:

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”。

2. 展开软件包、特定软件包类型和平台。
3. 选择打包程序。

   将在右侧窗格中显示该打包程序的详细信息。

4. 右键单击打包程序名称。选择“删除”。还可以从“操作”下拉菜单中选择“删除”。

   将出现一条警告消息。

5. 单击“是”确认删除。

   软件包打包程序即已删除。

重命名软件包打包程序

您可以重命名软件包打包程序。

遵循这些步骤:

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”。

2. 展开软件包、特定软件包类型和平台。
3. 选择打包程序。

   将在右侧窗格中显示该打包程序的详细信息。

4. 右键单击打包程序名称。
5. 选择“重命名”。还可以从“操作”下拉菜单中选择“重命名”。

   此时将显示“重命名”对话框。

6. 输入新名称，然后单击“确定”。

   已重命名软件包打包程序。

创建部署作业

要将代理部署到系统，请创建部署作业。部署作业包含 CA Virtual Assurance 将部署软件包适时传送给相应系统所需的详细信息。

遵循这些步骤:

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”。

2. 在“管理资源”窗格中右键单击“作业”文件夹，然后选择“创建新作业”。还可以选择“作业”文件夹，然后单击“作业状态”工具栏上的 +（新建）。

   此时将显示“作业设置”页面。

3. 在“作业名称”窗格中输入名称，可以选择使该作业基于现有的模板，然后单击“下一步”。

   此时将显示“软件包选择”页面。

4. 选择平台和希望部署的软件包。

5. （可选）单击“详细信息”选项卡。

   此时将显示“软件包打包程序详细信息”对话框，您可以使用该对话框以内联方式编辑软件包属性。如果软件包打包程序处于不完整或无效状态，可以通过内联编辑修改字段。

   a. 单击“编辑”并修改软件包打包程序属性。

   b. 单击“保存”，然后单击“确定”。

      软件包打包程序属性即已更新。

6. 单击向下箭头将软件包打包程序添加到作业中，然后单击“下一步”。

   此时将显示“计算机选择”页面。

7. 选择要部署到的系统，然后单击“下一步”。如果您的环境中有许多服务器，则需要多个包含一些条目的页面才能列出所有服务器。在页面上选择服务器并滚动到下一页时，在前一页上选择的所有服务器仍是有效的。

   此时将显示“已选择计算机”页面。

8. 单击“设置凭据”，设置建立连接所需的系统凭据，然后单击“下一步”。

   注意：使用域凭据部署到 Windows 目标系统必须采用“域\用户名”形式。

   此时将显示“高级”页。

9. （可选）设置分发服务器来管理部署。如果不设置，则将进行自动选择。
10. 为该作业选择排定选项：

    立即交付

    在创建新部署作业后立即启动作业。“立即交付”是默认选项。

    交错交付

    在特定时间段内交付软件包。

    排定交付

    排定未来特定时间的部署。
11. （可选）如果先前已使用该部署基础架构将某个软件包成功部署到系统，您可以强制是否再次运行。
12. 单击“下一步”。

    此时将显示“摘要”页面。
13. 检查作业的详细信息，然后单击“部署”。

    部署作业创建完成。

注意：在创建作业之后，您可以将该作业另存为模板。模板可以省去软件包和机器的选择，因此可以在后续作业中轻松复用。

在部署之前指定读写团体

为了获得完全 SystemEDGE 监控和管理功能，您必须为 SystemEDGE 代理指定有效的读写 SNMP 团体。您可以在部署之前在远程部署软件包打包程序中为 SystemEDGE 配置读/写团体字符串。

在部署之前指定读写团体

1. 依次选择“资源”、“部署”。
2. 打开“部署”窗格。

   将出现可用的部署组。
3. 展开“软件包”、特定软件包类型和打包程序平台，并选择要修改的打包程序。

   将在右侧窗格中显示该打包程序的详细信息。
4. 在“读写团体”字段中指定读写参数，然后单击“保存”。

   注意：如果在用户界面中指定的团体字符串中包含空格字符或分号(;)，代理将无法正常运行。

详细信息：

添加服务器级别的 SNMP 设置 (p. 104)
将策略应用于计算机 (p. 257)

指定读写团体后继安装

为了获得完全 SystemEDGE 监控和管理功能，您必须为 SystemEDGE 代理指定有效的读写 SNMP 团体。如果您已部署了 SystemEDGE 代理，则可以添加读/写团体字符串后继安装。您可以通过创建可用于监控和管理多个系统的全局 SNMP 条目，或创建服务器特定的 SNMP 条目来实现此操作。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。
2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。
3. 单击“陷阱和团体”选项卡。

   此时将显示“团体”页面。
4. 选择“仅包括服务器特定 SNMP 设置”。
5. 单击“保存策略”。

   将保存策略。

创建全局 SNMP 条目

1. 单击“管理”。

   此时将显示“管理”页面。
2. 单击“配置”。

   将出现“配置”页面。
3. 单击 SNMP。
4. 选中希望从列表中编辑的 SNMP 设置对应的复选框，然后单击工具图标（编辑）。

   此时将显示“编辑 SNMP 设置”对话框。
5. 从“访问类型”下拉菜单中选择“读写”，在“团体字符串”字段中指定参数，然后单击“确定”。

6. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

7. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

8. 单击“陷阱和团体”选项卡。

   此时将显示“团体”页面。

9. 选择“包括服务器特定 SNMP 设置和选定的默认设置”。

10. 单击“保存策略”。

    将保存策略。

注意：有关详细信息，请参阅“将策略应用到计算机”一节。

详细信息：

添加服务器级别的 SNMP 设置 (p. 104)

跟踪部署作业状态

启动用于将一组代理软件包部署到一组计算机的作业之后，您可以跟踪其进度和状态。“作业”选项卡显示一个包含创建的所有部署作业的表，该表列出了作业名称、包括的软件包、作业状态等。从该表中，您可以下钻以查看有关特定作业的更多详细信息，包括作业失败的原因。

注意：在“作业状态”窗格中，您可以通过选择筛选来筛选出特定作业任务。

遵循这些步骤:

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”。

2. 单击“作业”文件夹。

   此时将显示“作业状态”页面。

3. 单击要查看的作业。

   此时将显示“作业信息”页面。

4. 在“任务状态”窗格中，通过使用任何可用的筛选器，筛选出特定作业任务。或者，使用分页界面来识别所需任务。
5. 单击“扩展状态”以查看有关任务的扩展信息。

   此时将显示“扩展状态信息”对话框，其中显示有关任务的详细信息：

   信息

   显示有关任务的常规信息。

   消息

   显示有关任务的消息，例如“软件包交付失败”。

   原因

   显示失败的原因。

   示例：

   - 缺乏计算机可用性
   - 系统凭据无效
   - 无法解析系统主机名
   - 未满足软件包依存关系

   操作

   显示改正相应问题要执行的操作。

重新提交部署作业

您可以重新提交失败或部分失败的部署作业。

遵循这些步骤：

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”。
2. 单击“作业”文件夹。

   此时将显示“作业状态”页面。
3. 单击要重新提交的作业。

   此时将显示“作业信息”页面。
4. 单击“操作”，并选择“重新提交”。

   将在“软件包选择”屏幕中出现“部署”向导。
5. 根据需要选择要被部署的软件包打包程序，然后单击“下一步”。

   此时将显示“已选择计算机”页面。

6. （可选）删除不希望在其上进行部署的计算机。

   注意：先前已在其上成功部署了所有软件包的计算机将处于未选中状态。

7. 单击“设置凭据”，根据需要修改所有选定的计算机的凭据，从已重新启动的作业中移除计算机（可选），然后单击“下一步”。

   此时将显示“高级”页。

8. （可选）修改作业的排定选项。

   立即交付

   在创建新部署作业后立即启动作业。“立即交付”是默认选项。

   交错交付

   在特定时间段内交付软件包。

   排定交付

   排定未来特定时间的部署。

9. 选择“重新部署以前已部署的软件包”以强制部署所有软件包（包括先前成功部署的软件包），然后单击“下一步”。

   此时将显示“摘要”页面。

10. 检查作业的详细信息，然后单击“部署”。

    已重新提交作业。

查看已部署软件包

通过“监控软件”页面，您可以查看部署到单台计算机或一组计算机的软件包的列表。

查看已部署软件包

1. 选择“资源”。

   此时将显示“浏览”窗格。

2. 选择一个系统或服务。

   此时将显示“摘要”页面。

3. 依次选择“监控软件”、“部署”。

   此时将显示“部署历史记录”页面，其中列出了该计算机的所有部署作业。该表显示了选定系统的所有部署作业的详细信息：

   - Task ID
   - 作业 ID

- 目标
- 软件包
- 平台
- 打包程序
- 打包程序版本
- 启动者
- 开始时间
- 结束时间
- 状态
- 扩展状态

查看部署历史记录

可从以下位置获得部署历史记录信息：

“部署”窗格

显示已完成的、活动的、未决的和失败的部署任务的计数和成功部署的摘要。单击顶级的“部署”文件夹来访问该视图。

“作业”窗格

显示一个包含所有创建的部署作业的表，该表列出了作业名称、包含的软件包和作业状态。从该表中，您可以下钻以查看有关特定作业的更多详细信息，包括作业失败的原因。部署失败的常见原因包括以下情况：

- 系统凭据无效
- 无法解析系统主机名
- 未满足软件包依存关系

注意：您可以从该窗格中重新提交作业，以改正失败的原因并重新部署。单击“作业”文件夹访问该视图。

特定远程部署用例

正在使用自定义端口部署/安装 SystemEDGE 代理

向非标准端口部署 SystemEDGE 代理需要配置大量设置。为确保部署系统后，管理器可以发现和管理该系统，请执行以下操作：

1. 更新软件包打包程序：
   - 如果要使用远程部署解决方案，则必须先配置软件包打包程序来指定要使用的端口。导航到用户界面中的“开通”、“部署”并更改“端口”字段。写团体字符串也可在此处更新。
2. 更新 CA Virtual Assurance 中的 SNMP 团体字符串：
   - 为了让管理器成功监控和管理使用非标准端口的计算机，管理器必须知道要用于进行监控和管理的相应端口/写团体字符串组合。通过创建可用于监控和管理多个系统的全局 SNMP 条目，或者创建服务器特定的 SNMP 条目，能够达到这一目的：
     - 更新全局 SNMP 设置：导航到用户界面中的“管理”、“SNMP”，并使用相应的 SNMP 团体字符串/端口组合来添加新条目。
     - 更新特定于服务器的 SNMP 设置：导航到“策略”、“浏览”、“*Machine_Name*”、“度量标准”、“SNMP 设置”，并为必需的端口/写团体字符串添加新条目。

这些设置更新后，可按通常的方式部署/安装该代理。SystemEDGE 平台管理模块则会使用自定义端口/写团体字符串组合来发现、监控和管理服务器。

为 SystemEDGE 代理重新配置端口

可以通过重新安装代理为 SystemEDGE 代理重新配置端口。重新安装代理后，设置保持不变，有一个开通用来编辑要重新配置的端口的详细信息。

重新配置 SystemEDGE 代理端口

可以从标准（默认）端口 161 到 1691 重新配置 SystemEDGE 代理端口。例如，可以在默认端口 161 上安装实施 MIB-II 代理的 Microsoft SNMP 服务。重新配置代理端口不支持 sysedge.cf 文件。变更端口应通过重新安装代理完成。这可通过使用指定不同端口的远程部署来重新部署代理的方式完成。在 Windows 系统上，还可以使用 SystemEDGE 控制面板小程序重新配置代理。

使用控制面板重新配置 SystemEDGE 代理

1. 单击“开始”、“控制面板”，选择“添加或删除程序”，在列表中选择“SystemEDGE Core”，单击“更改”。

   将打开 SystemEDGE 安装向导。

2. 单击“下一步”。

   将打开“重新安装类型”页面。

3. 选择“重新安装”，然后单击“下一步”。

   “应用程序配置”页面打开，允许您更改安装文档设置。

4. 单击“下一步”。

   将打开“SystemEDGE SNMP 端口号”页面。

5. 指定 SystemEDGE 端口号 1691，然后单击“下一步”。

6. 检查设置并单击“重新安装”。

   SystemEDGE 代理即被重新配置为使用端口号 1691。

使用远程部署/策略配置重新配置 SystemEDGE 代理端口。

1. 遵循“创建部署作业” (p. 140)一章中的步骤。在向导的第 5 步，选择“重新部署以前已部署的软件包”。

   注意：重新安装时，将忽略所有提供的安装参数（端口号除外）。

   重新安装代理以更改端口后，需要在管理器上完成部分手动步骤，以确保代理配置了正确的团体字符串。

2. 执行以下操作之一：

为服务器创建服务器特定的 SNMP 条目：

1. 在 CA Virtual Assurance UI 中，单击“资源”选项卡，打开“浏览”窗格，选择计算机名称。

   将选择“Machine_Name”。

2. 右键单击“Machine_Name”，并依次选择“策略”、“配置 SNMP 设置”。

   此时将显示“SNMP 设置”页面。

3. 单击“添加”为所需端口创建新条目。

   此时将显示“新建 SNMP 设置”页面。

4. 输入所需的详细信息，然后单击“确定”。

   将为服务器创建服务器特定的 SNMP 条目。

确保全局 SNMP 设置存在并更新策略：

在 CA Virtual Assurance UI 中，导航到“管理”、“SNMP”，然后为需要的端口添加一个新条目。当设置正确时，可通过导航至“资源”选项卡，打开“配置”窗格，然后选择策略来编辑策略。然后单击“陷阱及团体”>“团体”，并选择中间选项“包括服务器特定 SNMP 设置和所有默认设置”。单击“保存策略”以保存该策略。您应该立即将该策略应用于系统 (p. 257)。您可以在目标计算机上使用 SystemEDGE 控制面板小程序来检查由代理使用的团体字符串。

注意：有关详细信息，请参阅*《管理指南》*中的“使用自定义端口部署/安装 SystemEDGE 代理”一章。

详细信息：

添加服务器级别的 SNMP 设置 (p. 104)

使用非特权用户帐号远程部署到 UNIX/Linux

如果想使用非特权用户帐号，请考虑下列关于 sudo 配置的要求：

- sudo 不得强制执行的程序附有有效的伪终端。要对特定用户禁用这种验证（如果已全局启用），请将代码行“Defaults:$username !requiretty”添加到 /etc/sudoers 文件。将 $username 替换为远程部署使用的实际用户名。

  编辑文件的标准方式是使用 visudo 命令。visudo 命令调用 $EDITOR。在编辑完成时，会验证文件的语法。如果结果无效，visudo 会阻止保存该文件。

- 在运行升级的程序之前，sudo 不得向用户询问密码。为了实现这一点，向用户授予特权的行中必须出现 NOPASSWD: 关键字。

- 必须允许 Sudo 运行必要的命令或全部命令。满足之前要求的配置条目（/etc/sudoers 中的行）如下：

  ```
  $username ALL=(ALL) NOPASSWD: ALL
  ```

  或

  ```
  $username ALL = NOPASSWD: /usr/bin/id,/bin/sh /tmp/idprimer/PifInst *
  ```

  注意：将 $username 替换为远程部署使用的实际用户名。如果“id”和“sh”的路径与 /usr/bin/id 或 /bin/sh 不同，请相应地调整配置条目中的路径。

在 Solaris 上，考虑 pfexec 的以下要求：

- 可使用以下命令将配置文件“Primary Administrator”分配给任何本地用户

  ```
  usermod -P “Primary Administrator” {user}
  ```

- 可以通过手工在文件 /etc/user_attr 中增加条目，将配置文件“Primary Administrator”分配给任何非本地用户：

  ```
  user::::type=normal;profiles=Primary Administrator
  ```

没有写团体的代理配置

虽然并不强制为 SystemEDGE 软件包打包程序提供写团体，但仍需考虑以下信息：

- 即使仅为代理配置 SNMP 读团体而无写团体，仍可通过 SystemEDGE PMM 发现 SystemEDGE 代理。但是，无法对未配置 SNMP 写团体的代理进行点配置更改。
- 如果为代理配置写团体，则仅支持完全 vCenter 和远程监控功能。若不为代理配置 SNMP 写团体，则无法从 CA Virtual Assurance UI 配置和管理 AIM。
- 可以在后继安装中使用“策略配置”从 CA Virtual Assurance UI 配置无写团体的代理。使用“策略配置”，也可配置代理使用 SNMP v3。与 SNMP v1/2 相比，SNMP v3 更安全。

部署到运行防火墙软件的 Windows Vista™、Windows 2008 和 Windows XP 计算机

要使代理能够部署到运行防火墙软件的计算机，请考虑以下内容：

- 如果运行 Windows Vista™ 或 Windows,2008 操作系统的目标计算机的防火墙已*关闭*（禁用）且部署到计算机失败，则创建或设置下列注册表变量，以使它成为具有值 0x1 的 DWORD 类型：

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy
  ```

  因为 Windows Vista™ 或 Windows 2008 中的用户帐户控制 (UAC) 不自动将管理权限授予本地用户，所以必须进行该操作。即使本地用户是管理员组的成员，也要进行该操作。

  注意：设置该值将导致禁用远程 UAC 访问令牌筛选。

  仅当用户在运行 Windows Vista™ 或 Windows 2008 的计算机上拥有本地管理员帐户时，才有必要设置该值。域管理员不会得益于此项更改。

- 如果运行 Windows Vista™ 或 Windows 2008 的目标计算机的防火墙已*打开*（已启用），则应当打开下列除文件共享端口外的端口，以对该计算机启用部署：

  UDP 端口

  CAM：4104

  文件和打印机共享等：137、138

  TCP 端口

  IDManager：135

  文件和打印机共享等：139、445

- 如果部署仍然失败，则应当完全启用 Windows Vista™ 或 Windows 2008 防火墙中的下列出站规则：
  - 远程协助
  - 网络发现
  - 文件和打印机共享
  - 核心网络
- 要对运行防火墙软件的 Windows XP 计算机启用代理部署，必须手工执行以下操作：
  1. 更改安全策略网络访问：共享并且本地帐户的安全模型从“仅限来宾－将本地用户作为来宾进行验证”更改为“经典－将本地用户作为其自身验证”。

     使用经典模型，能很好地控制对资源的访问，并防止使用本地帐户进行的网络登录映射到“来宾”帐户，这些“来宾”帐户对给定的资源通常只有“只读”权限。
  2. 配置以下防火墙设置：
     - 允许文件和打印机共享
     - 打开 UDP 端口 4104
     - 打开 TCP 端口 135

部署作业

要将代理部署到目标系统，请先创建部署作业。部署作业包含 CA Virtual Assurance 将部署软件包按排定时间交付给相应系统所需的详细信息。您可以使用可从多个位置访问的远程部署作业向导来创建新作业。选择以下方式之一：

- 使用显示板快速启动面板中的“部署作业”链接
- 从“资源”、“部署”选项卡中的“作业”面板，使用 +（新建）按钮
- 从“资源”、“浏览”选项卡中的受管节点的上下文菜单
- 从“资源”、“浏览”选项卡中当前选定的受管节点的“监控软件”、“部署”选项卡，使用 +（新建）按钮

在创建部署作业时，请指定以下信息：

作业信息

包括作业名，以及是否以现有模板为基础创建作业。

部署软件包

包括平台、要部署的软件包和每个软件包的特定打包程序。

计算机信息

包括要部署软件包的系统以及建立连接所需的系统凭据。

IP 地址

指定您部署作业所在接口的 IP 地址。如果系统具有多个 IP 地址，则带有管理属性的 IP 地址将被设置为默认地址。

注意：无法选择未启用管理属性的 IP 地址。

部署时间

指定执行部署的时间：立即、特定时期内、或安排在将来的具体时间。

创建作业后，也可将作业保存为模板。模板可以省去软件包和机器的选择，因此可以在后续作业中轻松复用。

基础架构部署过程

在执行部署时，过程的主要步骤如下所示：

1. 从管理员计算机中，基础架构部署客户端组件向 IDManager 发出请求，以在一列中的一个或多个目标计算机上安装代理。部署管理器可能正在客户端的远程计算机上运行。目标计算机列表可包括明确计算机名或 IPv4 地址。

   注意：仅可部署已发现的资源。

   要在每个目标计算机上继续部署，请务必验证其名称（无论是明确输入还是从容器中获得）是否适合解析为部署管理器计算机上显示的目标地址。例如，如果从目录中检索的目标的列表不完全满足网络域名条件，部署可能无法在某些网络配置中进行。

2. 检查目标计算机上是否已安装 IDPrimer。如果未安装，IDPrimer 将首先安装在目标计算机上。IDManager 试图传递 IDPrimer 安装软件包。使用的传递方式取决于目标操作环境以及该环境中启用的安全性。将 IDPrimer 映像复制到目标计算机后，便会开始安装。

   因为一些操作系统没有远程调用 IDPrimer 安装的方法，在这种情况下，必须手动执行 IDPrimer 安装。

3. IDPrimer 安装程序在目标计算机上安装自身和 CA Messaging (CAM) 组件。IDPrimer 已安装，且 IDManager 接收到来自目标计算机的“安装完成”信号后，即可开始部署软件包。先前已安装 IDPrimer 且已经使用 IDPrimer 进行身份验证的 IDManager 可以部署软件包，而无需重新提供用户名和密码。在后续的部署中，IDPrimer 使用不对称加密密钥进行身份验证，并限制对我们有权访问的管理器进行访问。

详细信息

自动部署 CA Virtual Assurance 基础架构的先决条件

通过基础架构部署组件，可以将代理软件远程安装到目标计算机。只能使用源计算机和目标计算机上的基础操作系统的功能完成安装。安装会受制于企业网络配置产生的所有限制。

部署软件的第一步是将小型初级步骤应用程序 IDPrimer 远程安装到目标计算机上。*该 IDPrimer* 软件负责软件组件安装映像的后续转移，及其安装的调用。在将 IDPrimer 安装到目标计算机时，部署管理器必须提供在目标计算机上有效的用户凭据。

使用以下某种机制，将 IDPrimer 转移到目标系统。如果目标操作系统为部署管理器所知，说明选择了正确的转移机制。如果无法确定目标操作系统，则会依次尝试下列各个机制。

- 打开网络共享

  部署管理器试图连接到目标系统上的 Windows 网络共享。默认情况下，使用的共享名是 ADMIN$。IDManager 配置选项控制该默认共享名。此机制仅适用于在基于 Windows 的环境上运行的部署管理器。Windows XP Home 等 Windows 操作系统不支持该部署机制。

- 使用 SSH 协议打开到目标计算机的网络连接，并使用 SFTP 传输初级步骤安装软件包

  该机制在任何运行 SSH 服务器的计算机上运行，不过在使用 Linux 或 UNIX 计算机作为目标计算机时有用。

  注意：在部署到 Solaris 系统时，建议您使用 SunSSH v1.1 （或更高版本）或者 OpenSSH 的最新版本。有关适用于 Solaris 平台和版本的修补程序的详细信息，请参阅以下网站：http：//opensolaris.org/os/community/security/projects/SSH。

  如果您正在目标计算机上运行防火墙，请验证满足以下条件：

  - SSH 端口 (22) 已启用以允许来自部署管理器的连接
  - 目标计算机上的 SSH 服务器已配置为使用具有 3DES 加密密码和 HMAC-SHA1 消息身份验证代码 (MAC) 的 RSA 密钥。

  注意：大多数 SSH 服务器默认支持该配置，但如果不支持，请参考 SSH 服务器文档查看详细说明。

  要部署到 UNIX 或 Linux 代理，请配置最近 SSH 实现的 /etc/ssh/sshd_config 配置文件，如下所示：

  - 将 PasswordAuthentication 设置为“Yes”
  - 将 PermitRootLogin 设置为 Yes，或按照使用非特权用户帐户远程部署到 UNIX/Linux (p. 150) 一节中所述配置 sudo/pfexec。
  - 确认已启用 SFTP 子系统

  远程部署支持将软件部署到系统，这些系统具有使用 noexec 标志安装的 /tmp 文件系统。

  在部署到一些同时运行 IPv4 和 IPv6 堆栈的 IBM AIX 系统，且使用 IPv6 地址时，将目标计算机 SSH 服务器配置为使用 IPv4 的端口 22。要配置 SSH，请编辑 sshd_config 配置文件并将 ListenAddress 设置为“::”。

  注意：如果希望部署管理器与目标计算机之间的 SSH 通信符合 FIPS 标准，请确认除了在部署管理器上设置仅 FIPS 模式外，在目标计算机上运行的 SSH 服务器还使用符合 FIPS 标准的加密模块。

重要信息！一些现代的操作系统不鼓励，甚至有时主动禁止远程安装软件。如果尝试将软件部署到这些系统，部署将失败，状态为“无初级步骤传输”。在这种情况下，会以其他方法安装软件组件，例如，使用物理分发介质（如 DVD）。

或者，您可以预装或为计算机开通 IDPrimer 软件。这样就不必依赖基础操作系统提供的设施进行部署。如果未执行身份验证，请在授权部署之前提供有效凭据。

要确定环境中是否可进行自动部署，可以通过运行下列标准操作系统操作，来执行一些简单的检查：

- 要使用 Windows 共享传送 IDPrimer 映像，请将共享从部署管理器主机映射到每个部署目标计算机。使用在部署请求中提供的目标用户凭据。

  默认共享：ADMIN$

- 要使用 SSH 传送 IDPrimer 映像，必须能使用 SSH 从部署管理器连接到部署目标计算机。

详细信息

使用非特权用户帐号远程部署到 UNIX/Linux (p. 150)

使用 IPv6 地址的基础架构部署的说明

如果要使用 IPV6 环境中的 CA Virtual Assurance 部署服务，应注意以下先决条件：

1. 需要在管理器机器（和各个部署（分发）服务器）上将下列注册密钥设为 1：
   - HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)
2. 必须将下面列出的三个热修订更新应用于 Windows 2003 管理器计算机：
   - http://support.microsoft.com/kb/947369/en-us
   - http://support.microsoft.com/kb/950092/en-us
   - http://support.microsoft.com/kb/974927/en-us
3. 目标计算机的主机名必须解析为全局 IPv6 地址，而 IPv6 地址的反向查找必须解析为相同的主机名。
4. 基础架构部署配置策略选项，每个管理器计算机上的 usehostnames 值必须为 1。默认情况下该文件位于以下目录中：

   C:\Program Files\CA\SC\IDMgrApi\config\SM\idconfig.xml

IDManager 采用的用于传输软件包的协议

在使用分发服务器部署时，IDManager 使用以下协议将软件包传输到目标计算机：

Windows 网络共享

如果分发服务器和目标计算机在 Windows 上，则使用该机制。

SSH/SFTP

如果分发服务器或目标计算机在 Linux 或 Unix 上，则使用该机制。

有关这些传输机制的详细信息，请参阅自动部署 CA Virtual Assurance 基础架构的先决条件 (p. 154)。

基础架构部署初级步骤软件的手工安装

即使由于某种原因而无法自动部署到目标计算机，如果在目标计算机上手工安装初级步骤软件，仍可以部署软件。通过物理安装初级步骤软件包或通过登录脚本运行安装，即可完成此操作。

除了安装初级步骤软件外，您必须安装安全密钥，该密钥由用来部署到目标计算机的部署管理器生成。

Windows 上的部署初级步骤安装

在运行 Windows 的目标计算机上安装部署初级步骤需要以下操作：

- 在目标计算机上提供 CA Virtual Assurance 安装介质 (DVD)，或将初级步骤设置文件手工复制到目标计算机。初级步骤设置文件存储在安装介质上的以下目录中：

  在 32 位 Windows 上有效

  %PROGRAMFILES%\CA\SC\IDMgrApi\packages\private\idprimer\Windows_x86

  在 64 位 Windows 上有效

  %PROGRAMFILES(X86)%\CA\SC\IDMgrApi\packages\private\idprimer\Windows_x86

- 在目标计算机上运行 IDPrimer_Setup.exe 以安装初级步骤。

Linux 或 UNIX 上的部署初级步骤安装

在 Linux 或 UNIX 目标计算机上安装部署初级步骤需要以下操作：

- 在目标计算机上提供 CA Virtual Assurance 安装介质 (DVD)，或将初级步骤安装映像手工复制到目标计算机。初级步骤安装映像存储在安装介质上的以下目录中：

  %PROGRAMFILES%\SC\IDMgrApi\packages\private\idprimer\Linux_x86

- 切换至目标计算机上包含初级步骤安装映像的目录，并运行以下安装命令来安装初级步骤：

  ```
  # sh installidp
  ```

向初级步骤安装提供部署管理证书

在目标计算机上的初级步骤接受部署软件包前，部署管理器生成需要传输到目标计算机的证书。部署证书文件名为 dmkeydat.cer

安装时可配置证书的位置。如果要将证书存储在更安全的区域或提供故障切换解决方案的两个管理器之间共享的位置，则可以配置其他文件位置。在后一种情况下，共享证书使部署管理器能够与任意管理器提供的 IDPrimer 组件通信，而无需重新提供身份验证凭据。

Windows 上的部署管理证书

在 Windows 上，部署证书位于以下目录中：

C:\Program Files\CA\SC\IDMgrApi\config\SM

必须将证书文件（后缀为 .PMR，例如 MANAGER1 SM.PMR）复制到目标计算机上的初级步骤安装文件夹中，默认如下：

\Program Files\CA\SC\IDPrimer

Linux 或 UNIX 上的部署管理证书

在 Linux 和 UNIX 上，必须将部署证书复制到目标计算机上的初级步骤安装文件夹中，默认如下：

/opt/CA/SharedComponents/ID/primer/bin

Linux 的兼容性库

IDPrimer 安装程序假定某些 32 位库依赖关系存在。在安装 IDPrimer 之前，这些 32 位库必须存在于 Linux 主机上。

多数 32 位 Linux 发行版本已默认安装。发出以下命令可满足 64 位 Linux 上的依赖关系：

- 适用于 RedHat、CentOS 和 SuSE（32 位和 64 位操作系统）：

  ```
  yum install libstdc++.i686
  ```

  此命令总共安装 4 个 RPM 软件包：glibc、libstdc++、nss-softokn-freebl 和 libgcc。

- 适用于 Debian（64 位）：

  ```
  apt-get install ia32-libs
  ```

  此命令安装以下所需的 32 位库：libc、libstd++、libgcc。

注意：有关所需兼容性库和其他系统软件包的更多信息，请访问 Linux 供应商的支持网站。

详细信息：

基础架构部署过程 (p. 153)

如何通过策略和模板配置 SystemEDGE 和服务响应监视器

本节说明了如何通过 CA Virtual Assurance（中央控制点）管理环境中的监控软件配置。

详细信息：

配置概述 (p. 160)
如何将策略和分层模板应用到服务器 (p. 162)
如何创建自动监测器并将其应用于系统 (p. 196)
如何监控特定于用户的度量标准（MIB 扩展） (p. 202)
如何监控特定的 Windows 性能注册表度量标准 (p. 205)
如何创建 SRM 策略 (p. 208)
发现代理 (p. 209)
策略配置功能的常见用法 (p. 209)

配置概述

通过从 CA Virtual Assurance 用户界面使用集中式策略配置，可以配置受管代理，并通过一次操作将配置应用于多个系统。策略配置使您可以在集中位置配置 SystemEDGE 和 SRM AIM，并且以一致、可靠和安全的方式在企业内分布策略。

使用 CA Virtual Assurance 的远程策略配置具有以下优点：

- 可以创建跨监控平台使用的平台独立监控策略
- 可以创建能够组合成一个策略的监控模板
- 可以创建能够组合成一个策略的监控模板
- 配置事件和操作的审核记录
- 可以通过事件和报告跟踪企业内的策略遵从性
- 与部署解决方案集成，并且类似于部署，目标系统上的内存占用量很少
- 可扩展到数千并发配置
- 支持多个代理配置源（CA Virtual Assurance、、SystemEDGE 等），并可通过 CA Virtual Assurance 接受或拒绝更改
- 可以远程控制由 SystemEDGE 加载的 AIM
- 可以导入现有 SystemEDGE 配置供未来策略配置使用
- 配置多个监视器定义时提供选项表，无需输入单个 OID 编号
- 自动监控索引分配，无需手动定义索引并可避免冲突

详细信息

如何创建 SystemEDGE 策略 (p. 209)
如何创建 SRM 策略 (p. 208)
将策略应用于计算机 (p. 257)
查看策略应用进度 (p. 258)
配置和查看已应用的策略 (p. 259)
代理策略显示板视图 (p. 161)
如何监控特定于用户的度量标准（MIB 扩展） (p. 202)
如何监控特定的 Windows 性能注册表度量标准 (p. 205)

代理策略显示板视图

显示板上提供了以下视图，可用于跟踪代理策略分配：

策略状态摘要

显示表示策略数量的饼图和列表。系统可能处于以下五种不同的状态：

未配置

已安装 SystemEDGE 代理，但未配置策略。

已安装代理

已安装 SystemEDGE 代理。

已配置

已安装 SystemEDGE 代理且已配置策略。

配置错误

已安装 SystemEDGE 且已配置策略，但最后一个配置失败。

已安装但未受管

SystemEDGE 已安装，但是在策略配置无法管理的模式下运行。

策略明细

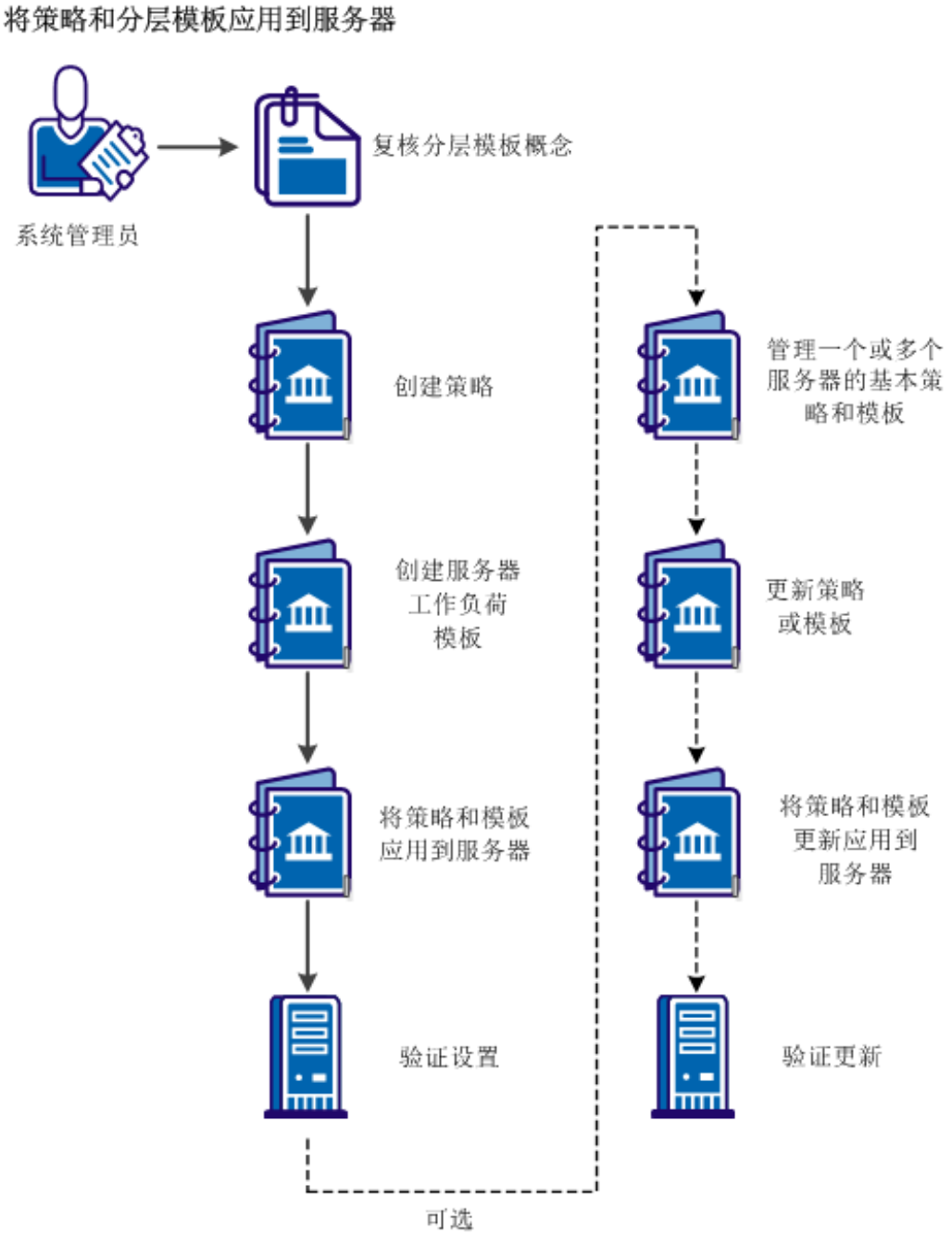
显示一个饼图和列表，其中显示所有策略以及每个策略所包含的系统数。

具有不标准策略的计算机

显示包含已应用策略的非标准更改的系统。

如何将策略和分层模板应用到服务器

从 CA Virtual Assurance 用户界面，可以通过创建基本策略并将模板作为层添加到该策略来控制 SystemEDGE 代理监控。该图说明了如何使用基本策略和分层模板：

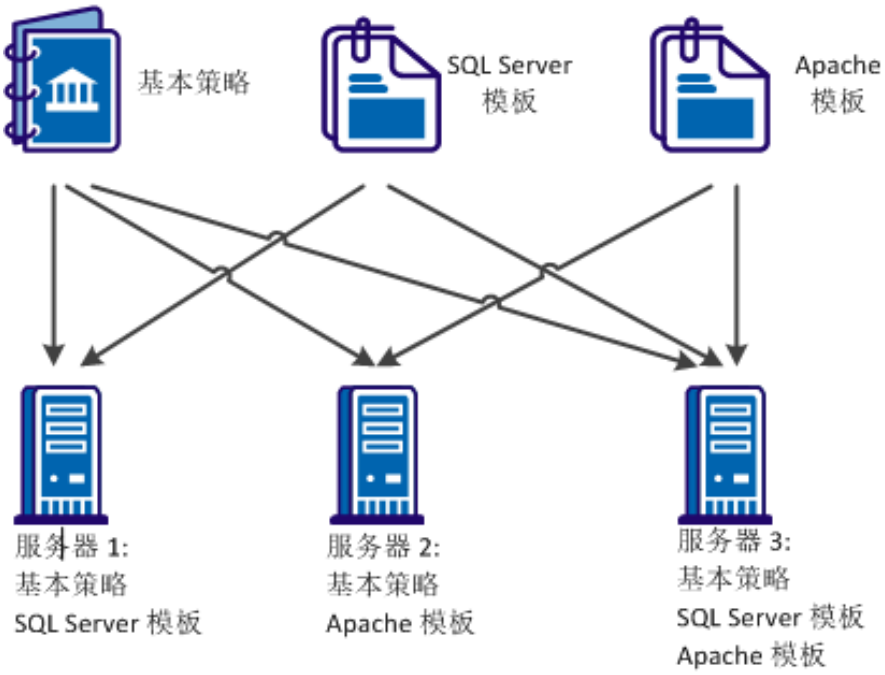


请执行以下步骤：

分层模板概念

在企业中，每个服务器或服务器组所处理的工作负荷有所不同。可以创建多个特定于服务器或服务器组所处理的工作负荷的策略。要协助创建策略，可以使用模板创建特定于应用程序的监视器。会将基本策略和分层模板组合以形成一个配置文件，并将其应用于需要监控的服务器。可以添加或删除分层模板。可以直接将模板更新应用于服务器，而无需更改基本策略，或将更新的模板重新导入到基本策略中。

示例: 将基本策略和模板应用到服务器



可以在以下方案中使用分层模板：

不同应用程序

为运行不同应用程序集的每个服务器创建模板库。可以直接将模板更新应用于每个服务器。

动态环境

在动态环境中，服务器的工作负荷频繁变更。可以使用分层模板将监视器划分到各个逻辑组中。可以根据工作负荷的变更，直接将逻辑组应用于系统或从系统中删除。

共享服务器

在企业设置中，跨多个部门共享服务器。每个部门管理和监控共享服务器上的应用程序。可以使用分层模板分别管理模板并将模板应用于各个部门的系统。

应用程序维护

可将监控拆分到多个模板中。在服务器中，可删除不使用的应用程序的模板，而不影响对其余系统的监控。

开箱即用模板

可以将开箱即用模板应用于受管节点。使用受管节点上的模板配置配置策略。这些模板可用于以下操作系统：

对于所有操作系统：

CPU 使用率－自动监测

交换容量

对于 Windows：

应用程序监控－CA eTrust Antivirus

进程崩溃

系统错误

系统进程

用户活动

Windows 服务－自动监测

对于 UNIX（AIX、HPUnix、Linux、Solaris）：

系统消息

系统进程

用户活动

创建策略

创建基本策略，以定义一组监视器、MIB 扩展、陷阱和团体以及控制设置来控制代理监控。

“陷阱和团体”和“控制设置”中的通用设置仅可用于策略。如果使用分层模板，那么通用设置是在基本策略中指定的。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”工具栏上单击 +（新建）。

   将显示“新建 SystemEDGE 策略”对话框。

3. 输入策略的名称和可选说明、系统类型和是否将其基于现有策略，然后单击“确定”。

   将创建策略，并在右侧窗格中显示配置屏幕。

4. 单击“保存策略”。

   将创建并保存策略。

注意：如有必要，还可以将现有默认策略用作基本策略。

详细信息：

复制 SystemEDGE 策略 (p. 210)
重命名 SystemEDGE 策略 (p. 210)
删除 SystemEDGE 策略 (p. 211)

定义 SystemEDGE 策略控制设置

通过使用 SystemEDGE 策略控制设置，可以控制下列代理行为：

- 安全设置
- SNMP 设置
- MIB 表填充
- UNIX 设置
- 性能监控设置

通过将这些通用控制设置添加到基本策略中，可以将它们与特定服务器工作负荷配置隔离开。

可以将策略中定义的控制设置应用到希望使用该配置监控的所有系统。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“控制设置”。

   此时将显示“控制”页面。

4. （可选）单击“使用默认值”。

   将显示默认选项窗格。您可以更改默认设置。

5. 配置以下控制设置：

   SNMP

   可以定义以下基本 SNMP 属性：

   绑定地址

   指定代理绑定到的接口，代理在该接口上侦听传入 SNMP 请求。有效地址是 IPv4 或 IPv6 地址。

   注意：相应的默认 _port 在安装期间指定。

   绑定端口

   指定代理绑定到以发送 SNMP 陷阱的陷阱端口。如果没有指定 bind_address，代理将绑定到所有可用的 UDP 地址。

   默认值：由系统选择的端口

   IP 族

   指定代理通信方法：仅 IPv4、仅 IPv6 或两者。默认情况下，代理首先尝试使用 IPv4，然后尝试使用 IPv6。

FIPS 模式

指定代理使用符合 FIPS 标准的加密。选择“非 FIPS 模式”可启用 CA eTrust 公钥基础构架库，如果该方法失败，则退回到内部最小安全解决方案。选择“FIPS 共存模式”可启用符合 FIPS 标准的加密，如果该方法失败，则退回到 CA eTrust 公钥基础构架库。如果这些方法失败，请选择“仅 FIPS 模式”来启用 RSA BSAFE Crypto-C Micro Edition 符合 FIPS 标准的库，且不执行加密。

默认值：非 FIPS 模式

陷阱源

指定用于发送陷阱的源地址。有效地址是 IPv4、IPv6 地址或主机名。

默认值：代理的主机名

安全设置

可以定义以下安全首选项：

身份验证陷阱

当代理收到具有代理无法识别的团体名称的 SNMP 消息时，发送身份验证失败陷阱。

默认：禁用

进程集

在“进程”表和“运行软件”表中允许访问在代理系统上运行的进程和其他软件。在这些表上允许 SNMP Set 可能会引起安全问题。

远程外壳组

允许管理系统远程指示代理通过远程 Shell 组在代理系统上运行 Shell 脚本和程序。泄漏此类信息可能会产生潜在的安全风险。

执行操作

超过阈值时，通过监控表执行操作命令。运行操作命令和脚本的功能可能导致安全问题。

MIB 表填充

在系统管理 MIB 中填充以下表：

- 进程表
- 用户组表
- 用户表
- 陷阱团体表
- 监视器镜像表
- 聚合镜像表
- 顶端进程表

每个表包含可以在 MIB 中公开的敏感信息，或者可以将其禁用以节省磁盘空间的不必要信息。默认设置可以填充除进程表之外的所有表。

杂项

可以定义以下杂项设置：

允许代理使用 SNMP 更新

允许代理使用 SNMP Set 更新（例如，删除写团体）。如果在代理上允许 SNMP Set，那么通过该方法进行的任何更新会导致生成 SNMP Set 更改通知。查看系统的策略详细信息时，这些更新还会导致异常。

向管理器通知配置更新

使代理能够将通知发送给管理器，以便代理处理任何 SNMP Set 请求。

热启动发现

使代理在每次热启动配置更新之后重新发现所有设备。如果管理具有许多设备的系统，则每次热启动之后进行发现可能会消耗太多时间和太多资源。

使用 Perl 兼容的正则表达式

Perl 兼容的正则表达式 (PCRE) 使您可以指定 i18n 兼容的正则表达式，同时定义支持正则表达式的监视器。正则表达式的示例包括日志文件、进程、进程组、Windows 服务和 Windows 事件。您也可以使用该选项来创建更复杂的正则表达式。SystemEDGE 代理 5.1.0 及更高版本中提供该选项。

自动解决索引冲突

使您能够解决索引冲突。将分层模板应用于所有系统时，会为添加到模板中的监视器分配索引。如果在基本策略或其他模板中分配的索引与现有索引冲突，该选项会重新分配唯一索引值。

注意：基本策略中包含的索引始终在已交付的配置中维护。如果已禁用该选项，则无法解决冲突索引。然而，将分层模板应用于系统时，冲突的索引在引起冲突索引的分层模板上显示为错误。

历史性能监控

可以为性能多维数据集 AIM 定义以下设置，性能多维数据集 AIM 将历史信息收集到系统性能多维数据集中，以用于历史性能管理：

收集间隔

指定将信息从“历史记录”表收集到性能多维数据集中的频率。

索引范围开始

指定保留的索引范围的开始，其中默认情况下代理将为性能多维数据集数据的收集创建历史记录控制条目。例如，如果 SRM（服务响应监控）配置为收集性能数据，则使用此保留的范围。

索引范围结束

指定保留的索引范围的结束，其中默认情况下代理将为性能多维数据集数据的收集创建历史记录控制条目。例如，如果 SRM（服务响应监控）配置为收集性能数据，则使用此保留的范围。

UNIX 控制设置

可以为在 UNIX 系统上运行的代理定义以下设置：

子程序组

指定除根之外的在其中运行子程序的组名称。

子程序用户

指定除根之外的在其中运行子程序的用户名。

Linux Freemem 包括

指定在可用内存计算中包括系统缓冲区、磁盘已缓存内存还是两者。

查询系统设备

可以查询以下系统设备度量标准：

- 串行设备状态
- 软盘状态
- 磁盘大小、容量、说明以及其他属性（探测磁盘）
- NFS 文件系统状态
- HP-UX 图形状态

查询这些度量标准会引起潜在的代理阻塞问题。默认设置可以仅查询串行设备状态和 NFS 文件系统状态。

6. 单击“插件”。

   此时将显示“插件”窗格。该窗格控制哪些 AIM 随代理一起加载。

7. 执行以下操作之一：

   - 选择“加载所有可用插件”，加载代理系统上所有可用的 AIM。
   - 选择“加载表中选择的插件”。
   - 单击“外部插件”工具栏上的 +（新添加），将 AIM 添加到“外部插件”表中。

   注意：有关可用 AIM 的详细信息，请参阅*《SystemEDGE 用户指南》*。

   将配置 AIM 加载。

8. 单击“聚合监视器”。

   按照配置对象聚合 (p. 171)中所述配置聚合监视器。

   将定义控制设置。

9. 单击“保存策略”。

   将保存策略。

详细信息：

配置对象聚合 (p. 217)

配置对象聚合

默认情况下，SystemEDGE 将监视器聚合到一个受管对象中，该受管对象包含对象类、实例和属性特性的相同值。例如，将所有具有 SysHealth 类、CPU 实例及 SysTime 属性的监视器合并到聚合受管对象中。

您可以在定义 SystemEDGE 策略时将代理配置为在较高级别上聚合对象。也可以配置与对象聚合及状态管理模型相关的代理行为的其他方面。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“控制设置”。

   将显示“控制”页面。

4. 单击“聚合监视器”。

   将显示“聚合监视器”页面。

5. 选中一个或多个复选框以指定聚合级别。

   这些聚合级别比默认值更高，高到能够将所有监视器聚合到一个顶级的代理对象中。通过指定聚合级别，可以创建分层对象体系结构，将状态传播到比指定高的级别。

6. 配置以下其他设置，然后单击“保存策略”：

   发送所有聚合监视器的遗留陷阱

   指定是否发送构成受管对象的所有监视器的传统陷阱。默认情况下，即使对象中的其他监视器违反了阈值，代理也仅发送最高重要级别的监视器的状态变更陷阱。

   执行所有聚合监视器的命令

   指定是否执行构成受管对象的所有监视器的操作命令。默认情况下，即使对象中的其他监视器违反了阈值，代理也仅运行最高重要级别的监视器的操作命令。

   聚合设置现已配置完成。应用或重新应用策略以使更改生效。

详细信息：

定义 SystemEDGE 策略控制设置 (p. 212)

定义陷阱和团体

SNMP 设置定义代理使用的团体和它将陷阱发送到的目标。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“陷阱和团体”选项卡。

   此时将显示“团体”页面。

4. 选择下列项之一，单击“操作”，然后选择“应用”：
   - 仅包括服务器特定 SNMP 设置
   - 包括服务器特定 SNMP 设置和所有默认设置
   - 包括服务器特定 SNMP 设置和选定的默认设置

   SNMP 设置将更新，且“团体”表中的团体页面将显示以下内容：

   名称

   指定团体字符串的名称。

   端口

   指定 SNMP 的端口。

   SNMP 版本

   指定团体使用的 SNMP 版本。

   访问权限

   指定团体应该具有读写权限还是只读权限。

   注意：请至少添加一个只读团体和一个读写团体。

   Community/User

   指定社区名称。

   身份验证协议

   指定用于对 SNMPv3 数据进行身份验证的协议。

   隐私协议

   指定用于对 SNMPv3 数据进行身份验证的协议。

   访问控制列表

   指定 IP 地址的空格分隔列表以将团体使用仅限于那些地址。如果保留列表为空，代理将授予对任何使用关联团体名称的系统的访问权限。访问列表仅供使用 SNMPv1 的团体使用。

   注意：有关定义 SNMPv2c 和 SNMPv3 访问列表的信息，请参阅*《SystemEDGE 用户指南》*。

5. （可选）根据需要添加、更新或删除其他团体。
6. 单击“保存策略”。

   将保存策略。

7. 单击“陷阱目标”。

   此时将显示“陷阱目标”页面。

8. 使用以下控件定义陷阱目标，然后单击“添加”：

陷阱类型

根据 SNMP 版本，指定要发送的陷阱的类型。

目标

指定向其发送陷阱的 IPv4 或 IPv6 地址。

端口

指定向其发送陷阱的 UDP 端口。

社区

指定随陷阱发送的团体名称。

编码

（可选）指定如何将在“控件设置”窗格的“陷阱源”字段中定义的源地址包含到陷阱中。如果陷阱源转换为 IPv6 地址，则该参数十分重要。以三位数的格式 XYZ 输入编码参数，假定起始为零。

默认值：000

X

控制扩展四字节 IPv4 源地址字段（仅 SNMPv1 陷阱）。输入 0 将不扩展源地址字段以包括 16 字节 IPv6 地址，输入 1 将扩展源地址字段。

Y、Z

控制将源信息包含到陷阱的 varbind (Y) 或 UDP 数据包（Z；仅 SNMPv1 陷阱）。为这些数字输入以下内容之一：

0：不修改陷阱的 varbind 或外部 UDP 数据包。

1：如 varbind 或数据包中一样包含 trap_source 参数（IPv4/IPv6 地址或主机名）。

2：最好将 trap_source 参数作为 IPv4 地址包含在内（然后依次是 IPv6 地址、主机名）。

3：最好将 trap_source 参数作为 IPv6 地址包含在内（然后依次是 IPv4 地址、主机名）。

4：最好将 trap_source 参数作为主机名包含在内（然后依次是 IPv4、IPv6）。

5：遵循 2 的首选项并包含主机名。

6：遵循 3 的首选项并包含主机名。

7：遵循 1 的首选项并包含主机名（如果 trap_source 是 IPv6 地址）。

陷阱源

（可选）指定 IPv4 或 IPv6 地址或者主机名以用作陷阱源。

默认值：全局陷阱

陷阱目标在“定义的陷阱目标”表中显示。

9. （可选）根据需要添加、更新或删除其他陷阱目标。
10. 单击“保存策略”。

    将保存策略。

注意：有关详细信息，请参阅 *《SystemEDGE 用户指南》*。

为服务器工作负荷创建模板

创建特定于服务器的工作负荷的模板。可以指定监视器和 MIB 扩展。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后单击“SystemEDGE”。

   将显示“模板列表”页面。
2. 在“模板列表”工具栏上单击“+ (新建)”。

   将显示“新建 SystemEDGE 监控模板”对话框。
3. 输入模板的名称和可选说明、系统类型以及是否使其基于现有模板，然后单击“确定”。

   将创建模板并显示“摘要”页面。
4. 模板是监视器和 MIB 扩展的集合。要将监视器添加到模板，请参阅将监视器添加到模板或策略 (p. 176)部分。要将 MIB 扩展添加到模板，请参阅定义 MIB 扩展 (p. 188)部分。
5. 单击“保存模板”。

   将创建并保存模板。

将监视器添加到模板或策略

将监视器添加到特定于服务器或服务器组所处理的工作负荷的模板。对于将监视器添加到策略，以下程序是类似的。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”和相应的子类别。

   将显示“模板列表”页面。

2. 在“模板”列表中选择模板。

   将显示模板的“摘要”页面。

3. 单击“监视器”并选择要添加的监视器。

   要创建监视器，请定义为以下监视器指定阈值和重要级别值的设置：

   - 创建阈值监视器 (p. 177)
   - 创建进程监视器 (p. 179)
   - 创建日志文件监视器 (p. 181)
   - 创建 Windows 事件监视器 (p. 183)
   - 创建历史记录监视器 (p. 185)
   - 创建进程组监视器 (p. 186)

4. （可选）对任何其他监视器重复该过程。
5. 单击“保存”。

   会将监视器加载到策略或模板中。

详细信息：

定义阈值监视器 (p. 227)
定义进程监视器 (p. 229)
定义日志文件监视器 (p. 231)
定义 Windows 事件监视器 (p. 233)
定义历史记录监视器 (p. 234)
定义进程组监视器 (p. 236)

创建阈值监视器

创建阈值监视器，该监视器允许代理针对指定阈值监控服务器或服务器组。当超过阈值时，代理会发送陷阱。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”和相应的子类别。

   将显示“模板列表”页面。

2. 在“模板”列表中选择模板。

   将显示模板的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“阈值”。

   此时将显示“阈值监视器”页面。

5. 在“阈值监视器”工具栏上单击“+ (新建)”。

   此时将显示“阈值监视器详细信息: 新建”对话框。

6. 配置以下阈值设置：

   索引

   定义要使用的表索引。

   平台

   指定平台。

   说明

   定义可选说明。

   对象类

   指定要监控的对象类。值是指可用的 MIB 表。

   对象类名

   定义要用于对象状态模型的对象类名。值是一个任意字符串（例如 FileSystems）。

对象属性

指定要监控的对象属性。值是指选为对象类的表的可用属性。属性（例如，devCapacity = 1.3.6.1.4.1.546.1.1.1.7.1.14）指定要使用该阈值监视器监视的 MIB 对象 (OID) 的初始部分。

对象属性名称

定义要用于对象状态模型的对象属性名称。这是一个任意字符串（例如 PercentUsed）。

对象实例

指定要监控的对象实例。该值（例如，.3 监视设备表（devTable）的第三行）指定了使用该阈值监视器进行监视的 MIB 对象 (OID) 的索引部分。对于一些对象类，可以给出实例本身的名称（例如，对于 Unix 计算机，使用 C: 而不是 .3 或 /var）。

对象实例名称

定义要用于对象状态模型的对象实例名称。值是一个任意字符串（例如 SysVol_C）。

间隔

将监视器的评估间隔定义为 30 秒的倍数。

“阈值配置”页面使您可以定义以下设置：

重要级别

指定用于对象状态模型的重要级别。

运算符

指定要使用的运算符。

值

定义要使用的值。

抽样类型

指定要使用的抽样类型。

“维护窗口”页面使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态。

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

“可选设置”子选项卡使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

7. 单击“保存”

   会保存“阈值监视器”设置。

8. 单击“保存模板”。

   会将阈值监视器加载到模板中。

创建进程监视器

创建进程监视器，该监视器允许代理针对指定阈值监控进程、服务或进程表对象。当超出阈值或进程状态（正在运行或已停止）发生更改时，代理会发送陷阱。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”和相应的子类别。

   将显示“模板列表”页面。

2. 在“模板”列表中选择模板。

   将显示模板的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“处理”。

   此时将显示“进程监视器”页面。

5. 在“进程监视器”工具栏上单击“+ (新建)”。

   此时将显示“进程监视器详细信息: 新建”对话框。

6. 配置以下进程设置：

索引

定义要使用的表索引。

平台

指定平台。

说明

定义可选说明。

对象类名

指定要用于对象状态模型的对象类名。值是一个任意字符串（例如 Process）。

对象属性

指定要监控的对象属性。值定义了进程监控的可用属性。

对象属性名称

定义要用于对象状态模型的对象属性名称。值是一个任意字符串（例如 MemUsedPercent）。

对象实例

指定要监控的对象实例。这是用来按名称、Solaris Zones 中的进程（使用 ZoneRegExpr/ProcRegExpr）匹配进程或按名称匹配 Windows 服务的正则表达式（依赖于可选设置）。模式应唯一匹配单个进程（服务）。可以包括参数（请参阅可选设置）。

对象实例名称

指定要用于对象状态模型的对象实例名称。值是一个任意字符串（例如 ApacheServer）。

间隔

将监视器的评估间隔定义为 30 秒的倍数。

“阈值配置”页面使您可以定义以下设置：

重要级别

指定用于对象状态模型的重要级别。

运算符

指定要使用的运算符。

值

定义要使用的值。

抽样类型

指定要使用的抽样类型。

“维护窗口”页面使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态。

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

“可选设置”子选项卡使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

7. 单击“保存”

   会保存“进程监视器”设置。

8. 单击“保存模板”。

   会将进程监视器加载到策略中。

创建日志文件监视器

创建日志文件监视器，该监视器允许代理通过搜索指定为正则表达式的字符串来监控任何 UTF-8 编码的系统或应用程序日志文件。出现匹配项时，代理会发送陷阱。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”和相应的子类别。

   此时将显示“模板列表”页面。

2. 在“模板”列表中选择模板。

   此时将显示模板的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“日志文件”。

   此时将显示“日志文件监视器”页面。

5. 在“日志文件监视器”工具栏上单击“+ (新建)”。

   此时将显示“日志文件监视器详细信息: 新建”对话框。

6. 配置以下进程设置：

   索引

   定义要使用的表索引。

   监视器类型

   指定要使用的监视器类型。

   平台

   指定平台。

   说明

   定义可选说明。

   日志文件/目录名称

   定义要监控的文件或目录的路径。

   搜索筛选器

   指定搜索筛选器。

   间隔

   定义监视器的评估间隔（分钟）

   重要级别

   指定匹配监视器的重要性。

   “维护窗口”页面使您可以定义以下设置：

   状态

   指定监视器维护条目是否处于活动状态。

   开始时间

   在监视器关闭时定义开始时间，维护窗口启动。

   终止时间

   在监视器再次打开时定义终止时间，维护窗口关闭。

   “可选设置”页面使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

7. 单击“保存”

   会保存“日志文件监视器”设置。

8. 单击“保存模板”。

   会将日志文件监视器加载到策略中。

创建 Windows 事件监视器

创建 Windows 事件监视器，该监视器允许代理使用不同的筛选（事件源）监控 Windows 事件日志条目。出现匹配项时，代理会发送陷阱。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”和相应的子类别。

   将显示“模板列表”页面。

2. 在“模板”列表中选择模板。

   将显示模板的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“Windows 事件”。

   此时将显示“Windows 事件监视器”页面。

5. 在“Widows 事件监视器”工具栏上单击“+ (新建)”。

   此时将显示“Windows 事件详细信息: 新建”对话框。

6. 配置以下进程设置：

   索引

   定义要使用的表索引。

   平台

   指定平台。

   说明

   定义可选说明。

事件日志

指定要读取的事件日志。

事件类型

指定要匹配的事件类型。

源筛选

定义要使用的源筛选。

说明筛选

定义要使用的说明筛选。

重要级别

指定匹配监视器的重要性。

“维护窗口”子选项卡使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态。

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

“可选设置”子选项卡使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

7. 单击“保存”

   会保存“Windows 事件监视器”设置。

8. 单击“保存模板”。

   会将 Windows 事件监视器加载到策略中。

创建历史记录监视器

创建历史记录监视器，该监视器允许代理提供历史数据收集，以便进行管理器端基准制定和趋势分析。代理使用度量标准提供特定时间间隔内的平均系统性能。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”和相应的子类别。

   此时将显示“模板列表”页面。

2. 在“模板”列表中选择模板。

   此时将显示模板的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“历史记录”。

   此时将显示“历史记录监视器”页面。

5. 在“历史记录监视器”工具栏上单击“+ (新建)”。

   此时将显示“历史记录详细信息: 新建”对话框。

6. 配置以下进程设置：

   索引

   定义要使用的表索引。

   平台

   指定平台。

   说明

   定义可选说明。

   对象类

   指定要监控的对象。值是指可用的 MIB 表值。

   对象属性

   指定要监控的对象属性。值是指选为对象类的表的可用属性。属性（例如，devCapacity = 1.3.6.1.4.1.546.1.1.1.7.1.14）指定要使用该历史记录条目监视的 MIB 对象 (OID) 的初始部分。

   对象实例

   定义要监控的对象实例。该值（例如，0.3 监视设备表 (devTable) 的第三行）指定了使用该历史记录条目进行监控的 MIB 对象 (OID) 的索引部分。

间隔

将收集间隔定义为 30 秒的倍数。

存储段

定义要收集的抽样数。

“添加到性能多维数据集”复选框

指定是否为该条目收集性能多维数据。

“维护窗口”页面使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

7. 单击“保存”

   会保存“历史记录监视器”设置。

8. 单击“保存模板”。

   会将历史记录监视器加载到策略中。

创建进程组监视器

创建进程组监视器，该监视器允许代理定义一组进程并监控该组是否发生更改。如果进程组发生更改，代理会发送陷阱。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”和相应的子类别。

   将显示“模板列表”页面。

2. 在“模板”列表中选择模板。

   将显示模板的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“进程组”。

   此时将显示“历史记录监视器”页面。

5. 在“进程组监视器”工具栏上单击“+ (新建)”。

   此时将显示“进程组详细信息: 新建”对话框。

6. 配置以下进程设置：

   索引

   定义要使用的表索引。

   平台

   指定平台。

   说明

   定义可选说明。

   进程名称

   定义进程名称。这是用来按名称

   间隔

   将监视器的评估间隔定义为 30 秒的倍数。

   用户名

   除任何进程名正则表达式之外，定义要匹配的用户名。

   组名称

   除任何进程名正则表达式之外，定义要匹配的组名称。

   重要级别

   指定组变更监视器的重要性

   “维护窗口”页面使您可以定义以下设置：

   状态

   指定监视器维护条目是否处于活动状态

   开始时间

   在监视器关闭时定义开始时间，维护窗口启动。

   终止时间

   在监视器再次打开时定义终止时间，维护窗口关闭。

   “可选设置”页面使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

7. 单击“保存”

   会保存“进程组监视器”设置。

8. 单击“保存模板”。

   会将进程组监视器加载到策略中。

定义 MIB 扩展

定义 MIB 扩展提供了通过本地文件操作无法实现的功能优点。策略配置功能提供了字段名称和主要属性（如对象类型）列表。

配置策略或监控模板时，单击“MIB 扩展”选项卡以添加以下对象：

- MIB 扩展
- Windows 性能
- Windows 注册表

注意：要将 MIB 扩展添加到模板或策略中，请参阅将 MIB 扩展添加到模板或策略 (p. 188)。出于将 MIB 扩展直接应用于所监控系统的目的，会支持模板内的 MIB 扩展。应该直接在“策略”本身中创建用于在策略内使用的 MIB 扩展。

将 MIB 扩展添加到模板或策略

使用策略配置功能为模板或策略定义 MIB 扩展。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，然后展开“监控模板”或“监控策略”。
2. 从“模板”列表或“可用策略”页面中，单击模板名称或策略名称。

   此时将出现“摘要”页。
3. 单击“MIB 扩展”选项卡。

   此时将显示“MIB 扩展”页面。
4. 使用以下控件定义 MIB 扩展属性，然后单击“添加”：

   索引

   定义属性叶编号。

   类型

   指定属性类型。

   扩展命令

   定义要执行的脚本或二进制文件的完整路径或名称（包括参数）。

   访问权限

   指定属性访问权限。
5. 单击“Windows 性能”选项卡。

   此时将显示“Windows 性能”窗格。

6. 使用以下控件定义 Windows 性能属性，然后单击“添加”：

   索引

   定义属性叶编号。

   类型

   指定属性类型。

   对象

   指定性能注册表对象。

   计数器

   指定性能注册表计数器。

   实例

   定义性能注册表实例。

7. 单击“Windows 注册表”选项卡。

   此时将显示“Windows 注册表”窗格。

8. 使用以下控件定义 Windows 注册表属性，然后单击“添加”：

   索引

   定义属性叶编号。

   类型

   指定属性类型。

   按键

   在 HKEY_LOCAL_MACHINE 中定义注册表项。

   值

   定义属性值。

   注意：有关详细信息，请参阅 *《SystemEDGE 用户指南》*。

9. 单击“保存模板”或“保存策略”。

   配置已保存。

（可选）从模板或策略中重新索引监视器

可以在“阈值”、“进程”、“日志文件”、“Windows 事件”、“历史记录”和“进程组”选项卡上重新索引监视器。重新索引会将连续值分配给现有索引。

注意：重新索引监视器后，此功能可确保未来索引会从下一个逻辑基本索引开始。

要重新索引监视器，请考虑以下内容：

- 验证监视器是否存在。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，然后展开“监控模板”或“监控策略”。
2. 从“模板”列表或“可用策略”页面中，单击模板名称或策略名称。

   此时将显示“摘要”页面。
3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中包含监视器的列表。
4. 依次单击相应的监视器选项卡和“操作”，然后选择“重新索引”。

   此时将显示新的基本索引对话框。
5. 输入数字值作为基本索引

   示例：1000
6. 选择“使索引连续”

   使索引连续

   选择“使索引连续”选项，以使现有索引是连续的。

   示例：1001、1002、1003、1004 等。

   注意：如果不选择此选项，则索引之间的差距会保留。

   示例：1001、1010、1020、1030 等。
7. 单击“确定”以确认重新索引。

   此时将重新索引监视器。

从模板或策略中删除监视器

可以从策略或模板中删除监视器。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，然后展开“监控模板”或“监控策略”。
2. 从“模板”列表或“可用策略”页面中，单击模板名称或策略名称。

   此时将显示“摘要”页面。
3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。
4. 单击相应的监视器选项卡并选择要删除的一个或多个监视器。
5. 单击“操作”，然后选择“删除”。

   将出现一条警告消息。
6. 单击“确定”确认删除。
7. （可选）对任何其他监视器重复该过程。
8. 单击“保存策略”。

   将从策略中删除监视器。

   注意：无法删除模板，也无法删除服务器或服务器组使用其模板的策略。

（可选）更新策略或模板

如有必要，可以通过向策略或模板添加监视器或者从策略或模板中删除监视器，更新现有策略或模板。更新过程类似于创建过程。

遵循这些步骤:

1. 添加或删除特定于服务器工作负荷的监视器。要将监视器添加到模板或策略中，请参阅将监视器添加到模板或策略 (p. 176)。要从策略中删除监视器，请参阅从模板或策略中删除监视器 (p. 191)。
2. 定义 MIB 扩展 (p. 188)。
3. 定义 SystemEDGE 策略控制设置 (p. 165)。

   策略或模板将更新。

将策略和模板应用到服务器并验证设置

在创建模板之后，可以将具有该模板的策略直接应用于整个企业中的服务器或服务器组。

遵循这些步骤:

1. 在“可用策略”表中选择策略，或从“模板”列表中选择模板。

   此时将显示策略或模板的“摘要”页面。

2. 选择“受管计算机”选项卡。

   将显示受管计算机列表。

3. 单击“操作”，然后选择“应用”。

   此时将出现用于选择要在其中应用策略的系统的选项卡。

   更新运行该策略/模板的计算机

   用于将策略应用于已正在运行策略或模板的系统。

   应用于未运行该策略/模板的计算机

   用于将策略或模板应用于系统。

4. （策略选项）从“更新运行该策略的计算机”选项卡，执行以下选项之一：

   - 选择“使用该策略更新所有计算机”，在当前运行该策略的所有计算机上部署该策略。如果进行了希望全局应用的配置策略更改，则该选项十分有用。
   - 选择“更新所选的计算机组”，仅更新满足以下任意条件的计算机：
     - 运行该策略过期版本的计算机
     - 已应用策略例外的计算机
     - 运行该策略当前版本的计算机
     - 该策略存在配置错误的计算机

     当用户将点配置更改应用于不在应用的策略中表示的代理时，将发生策略异常。
   - 选择“高级(手动选择计算机)”，以在“选择计算机”窗格中手工添加要将策略重新应用到的计算机。

5. （模板选项）从“更新运行该模板的计算机”选项卡，选择以下选项之一：

   在“现有计算机”下，选择以下选项之一：

   - 更新应用该模板的所有计算机。
   - 仅更新没有应用该模板最新更改的计算机。
   - 仅更新未成功应用模板的计算机。
   - 高级(手动选择计算机)
   - 从计算机中删除该模板。

6. （可选）从“应用于未运行该策略/模板的计算机”选项卡中选择要应用策略或模板的系统。
7. 单击“应用策略”或“应用模板”。

   此时将启动应用程序。
8. 验证服务器行为是否和预期一样。如有必要，可以更新和应用已更新的策略和模板。

（可选）管理一个或多个服务器的基本策略和模板

管理单个或多个服务器的模板和基本策略。您可以替换当前基本策略、添加模板或删除模板。

遵循这些步骤:

1. 单击“资源”选项卡，打开“浏览”窗格，然后选择要更改策略配置的服务器。

   此时将显示服务器的“资源”页面。
2. 选择“监控软件”、“策略”。

   该表将显示应用于服务器的策略和模板的列表。
3. 单击  （修改策略），将该服务器的当前基本策略替换为其他可用基本策略。

   此时将显示“修改策略”对话框，列出所有可用的基本策略。
4. 选择适当的策略，然后单击“应用”。

   已应用选定服务器的新基本策略。策略的状态从“已请求交付”、“已交付”更改为“已配置”。

5. 单击  （修改模板），向选定服务器的配置添加模板或从选定服务器的配置中删除模板。

   此时将显示“修改模板”对话框，在左侧窗格中列出可用模板，在右侧窗格中列出应用的模板。

6. 选择要添加或删除的模板，使用箭头进行分配，然后单击“应用”。

   一组新模板已应用于配置。模板的状态从“已请求交付”、“已交付”更改为“已配置”。

   已应用新配置。

也可以将多个服务器作为一组进行管理。

遵循这些步骤:

1. 在指定服务器组的数据中心级别创建服务。

   此时新服务将显示在“浏览”窗格中。

2. 选择服务。

   此时将显示“服务”页面。

3. 选择“监控软件”、“策略”。

   该表将显示应用于服务器的策略和模板的列表。

   以下步骤与单个服务器的步骤相同。

4. 完成配置。

（可选）更新策略或模板

如有必要，可以通过向策略或模板添加监视器或者从策略或模板中删除监视器，更新现有策略或模板。更新过程类似于创建过程。

遵循这些步骤:

1. 添加或删除特定于服务器工作负荷的监视器。要将监视器添加到模板或策略中，请参阅将监视器添加到模板或策略 (p. 176)。要从策略中删除监视器，请参阅从模板或策略中删除监视器 (p. 191)。
2. 定义 MIB 扩展 (p. 188)。
3. 定义 SystemEDGE 策略控制设置 (p. 165)。

   策略或模板将更新。

（可选）将策略和模板更新应用到服务器并验证更新

在更新模板之后，将模板更新直接应用于整个企业中的服务器或服务器组。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后选择“SystemEDGE”。

   “摘要”页面显示 SystemEDGE 监控模板的列表。

2. 选择模板名称。

   此时将显示包含模板信息的“摘要”页面。

3. 单击“操作”，然后选择“应用”。

   此时将显示用于选择要在其中应用监控模板的计算机的选项卡。使用“更新运行该模板的计算机”选项卡可以将监控模板应用于已经使用该模板的计算机。使用“应用于未运行该模板的计算机”选项卡可将监控模板应用于未使用任何模板的计算机。

4. （可选）在“现有计算机”下，从“更新运行该模板的计算机”选项卡选项中选择计算机。

5. （可选）在“已选择计算机”下，选择要将模板重新应用到的计算机。

6. （可选）从“应用于未运行该模板的计算机”选项卡中选择要向其应用模板的计算机。

7. 单击“应用”。

   将启动模板应用程序，并显示“查看状态”链接。

8. 单击“查看状态”链接以验证 SystemEDGE 监控模板更新是否应用于服务器。

   该页面将显示应用了 SystemEDGE 监控模板更新的服务器列表。

   分层模板更新已成功应用于服务器或服务器组。

9. 验证服务器行为是否和预期一样。如有必要，可以再次更新和应用已更新的策略和模板。

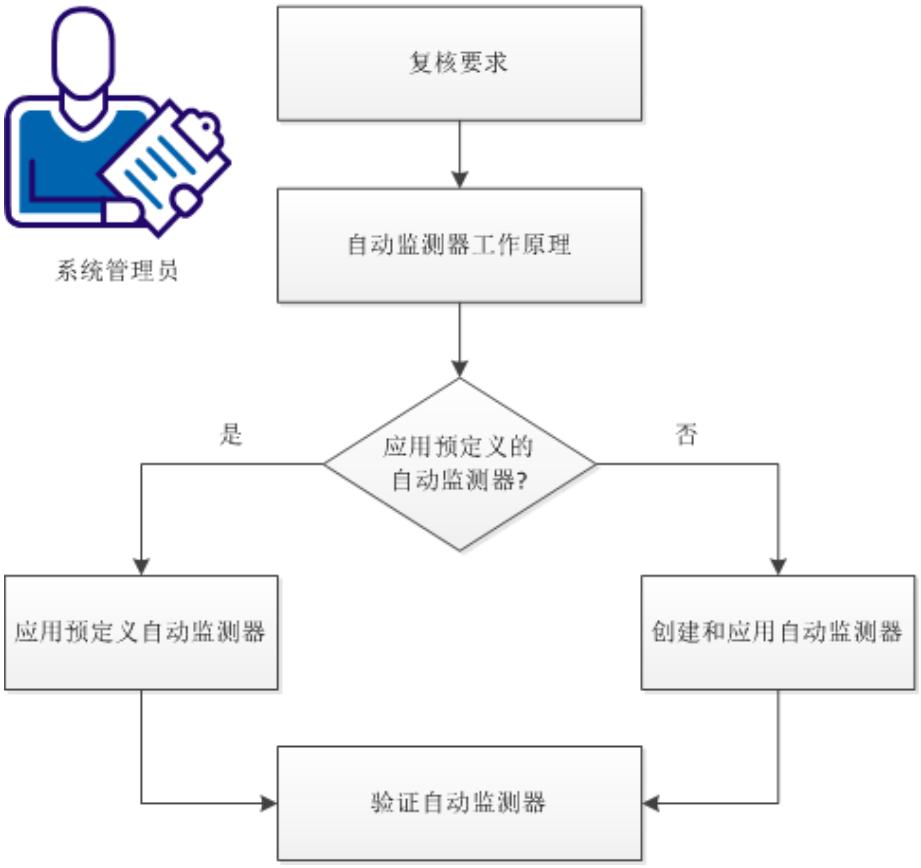
如何创建自动监测器并将其应用于系统

此方案介绍系统管理员如何使用自动监测器来动态监控受管系统上的资源。

您可以使用自动监测器来发现在受管系统上添加或删除的资源。如果资源已添加，自动监测器将创建相应的监视器。如果资源已删除，自动监测器将执行“丢失操作”。

下图提供了有关如何创建自动监测器并将其应用于受管系统的概述。

如何创建自动监测器并将其应用于系统



请执行以下步骤：

查看要求 (p. 197)
自动监测器的工作方式 (p. 197)
应用预定义的自动监测器 (p. 200)
创建自动监测器并将其应用于系统 (p. 201)
验证自动监测器 (p. 202)

查看要求

在为 SystemEDGE 创建自动监测器之前，请查看以下要求：

- 您熟悉 TCP/IP 和 SNMP。
- 您对 CA Virtual Assurance 和 SystemEDGE 有基本了解。
- 您可以访问 CA Virtual Assurance 用户界面。
- 确认受影响的 SystemEDGE 代理正在以受管模式运行。

详细信息：

应用预定义的自动监测器 (p. 200)
创建自动监测器并将其应用于系统 (p. 201)

自动监测器的工作方式

自动监测器使用正则表达式作为模式运行定期发现过程，以匹配自动监测器为其创建监视器的资源的名称。自动监测器允许 SystemEDGE 在新资源处于联机状态时自动为其创建监视器。自动监测器在保留的索引范围 (1000000 - 1999999) 内创建监视器。

资源消失时，SystemEDGE 会向 CA Virtual Assurance 发送陷阱，并应用已在自动监测器中配置的“丢失操作”。如果监控的资源丢失，“丢失操作”可删除监视器，或将资源状态设置为特定状态：

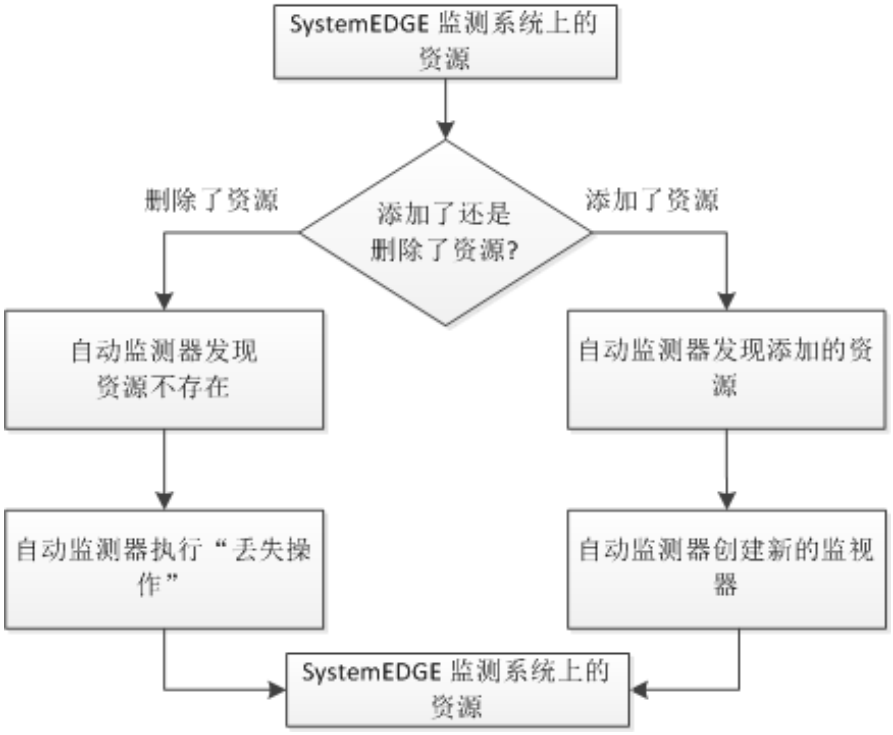
正常、警告、轻微、重大、严重、致命、运行或关闭

通过自动监测器，可在不了解受管系统上所存在资源的情况下创建灵活的策略或分层模板。资源可能是设备、服务或受管系统上运行的进程。

可使用下列自动监测器类型：

- 常规自动监测器－为受管系统上的各种资源（例如设备、接口、文件系统或文件）创建监视器。
- 进程和服务自动监测器－为受管系统上运行的进程和服务创建监视器。

自动检测器的进程工作流



配置“丢失操作”时，可使用下列指导原则：

- 如果丢失的资源影响系统的运行状况，可配置“丢失操作”以将相应资源的状态更改为严重状态。
- 如果丢失的资源不影响系统的运行状况，可配置“丢失操作”以删除相应的监视器。

详细信息：

常规自动监测器 (p. 199)
进程和服务自动监测器 (p. 199)

常规自动监测器

常规自动监测器可以为受管系统上的各种资源（例如设备、接口、文件系统或文件）创建监视器。

以下列表提供了常规自动监测器的一些示例：

- 所有已发现设备的容量
- 所有已发现磁盘上的磁盘服务时间
- 所有 cmd 进程上的驻留集大小
- 所有隧道网络接口的操作状态
- 所有设备的设备状态

详细信息：

自动监测器的工作方式 (p. 197)

进程和服务自动监测器

使用进程和服务自动监测器可动态地创建进程和服务监视器。

无论何时服务满足自动监测器条件（服务名称、启动类型等等）时，服务自动监测器均会在进程表中创建多个服务监视器。例如，可以监控所有启动类型为“自动”的已安装 SQL 服务。

进程自动监测器采用两种方式创建进程监视器：

- 使用进程名（默认）－进程名与自动监测器条件相匹配时。

  例如，当进程符合进程名为“sql”或“svchost”的条件时，将创建进程监视器。自动监测器创建的进程监视器跟踪当前在受管系统上运行的匹配进程，而不管 PID 为何。

  - 自动监测器创建的进程监视器与手动创建的进程监视器具有相同的语义。
  - 可单独监控名称相同但参数不同的一组进程。例如，“java.exe”。
  - 可以为一组相关的进程创建监视器。

- 使用 PID－PID 符合自动监测器条件时。自动监测器允许监视器进程在用户界面中使用 PID 标记，或在 sysedge.cf 文件中指定 watch 标记 0x1000。

  每个自动监测器创建的监视器均跟踪进程的所有匹配实例。

  - 为特定的进程实例创建监视器。
  - 监控不具有区分参数的进程的多个实例。

详细信息：

自动监测器的工作方式 (p. 197)

应用预定义的自动监测器

策略配置在模板和 SystemEDGE 默认策略中提供以下预定义的自动监测器：

- CPU 使用率（独立于操作系统的模板）
- CA ARCserve（Windows 模板）
- Windows 服务（Windows 模板）
- Microsoft Exchange（Windows 模板）
- 所有文件系统（SystemEDGE 默认策略）
- 所有磁盘（SystemEDGE 默认策略）

验证您是否可以使用预定义的自动监测器。

遵循这些步骤：

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”或“监控模板”，然后单击“SystemEDGE”。

   “可用策略”窗格或“模板列表”将打开并显示预定义的自动监测器。

2. 在“可用策略”窗格或“模板列表”中，单击预定义的自动监测器。

   将打开“自动监测器详细信息”窗格。

3. 单击“操作”、“应用”。

   将打开“计算机选择”页面。

4. 选择适当的系统，然后单击“应用”。

   已将自动监测器添加到选定的系统的 SystemEDGE 配置中。

   SystemEDGE 将根据自动监测器设置自动创建监视器。

   注意：对于处于未受管模式的 SystemEDGE，请在 sysedge.cf 文件中指定自动监测器。当 SystemEDGE 更改为受管模式时，在 SystemEDGE 注册到 CA Virtual Assurance 之前定义的自动监测器可以被导入到策略中。

详细信息：

创建自动监测器并将其应用于系统 (p. 201)

创建自动监测器并将其应用于系统

对于处于受管模式的 SystemEDGE，您可以在策略中或在模板中指定自动监测器。集中式配置提供在所有服务器之间进行一致监控。在策略或模板中配置自动监测器，并且应用自动监测器来监控受管系统上的资源。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”或“监控模板”，然后单击“SystemEDGE”。

   将打开“可用策略”窗格或“模板列表”。

2. 打开策略或模板，然后单击“自动监测器”。

   将打开“常规自动监测器”窗格。

3. 如果您要添加进程或服务自动监测器，请选择“进程/服务”选项卡。

4. 在工具栏上单击 （添加）。

   将打开“自动监测器详细信息”窗格。

5. 指定所需值，然后单击“保存”。

   自动监测器已保存。

6. 单击“操作”、“应用”。

   将打开“计算机选择”页面。

7. 选择适当的系统，然后单击“应用”。

   已将自动监测器添加到选定的系统的 SystemEDGE 配置中。

   SystemEDGE 将根据自动监测器设置自动创建监视器。

   注意：对于处于未受管模式的 SystemEDGE，请在 sysedge.cf 文件中指定自动监测器。当 SystemEDGE 更改为受管模式时，在 SystemEDGE 注册到 CA Virtual Assurance 之前定义的自动监测器可以被导入到策略中。

详细信息：

验证自动监测器 (p. 202)

验证自动监测器

在 CA Virtual Assurance 用户界面中，您可以验证自动监测器是否已经创建资源的相应监视器。自动监测器在保留的索引范围 (1000000-1999999) 内创建监视器。

遵循这些步骤:

1. 单击“资源”选项卡。

   此时将显示“资源”页面。

2. 在“浏览”窗格中，展开“数据中心”文件夹和“CA Virtual Assurance Services”文件夹。

   将显示数据中心中的已发现资源和受管资源。

3. 选择您要验证其相应监视器的资源。

   将显示选定的资源的快速启动任务。

4. 单击“配置”选项卡。

   “自我监视器”页面将出现并显示自动监测器在保留的索引范围内创建的监视器。

详细信息：

自动监测器的工作方式 (p. 197)

如何监控特定于用户的度量标准（MIB 扩展）

此分步示例介绍了如何监控特定于用户的度量标准。

如何监控特定于用户的度量标准（MIB 扩展）

1. 创建返回所需数据的程序。例如，代理系统上可返回一些固定数据的简单 DOS 批处理脚本。

   ```
   @echo off
   echo 99
   ```

2. 打开文本编辑器，然后将这两行存储在 C: 驱动器的 data.bat 中。

3. 创建引用此批处理文件的 MIB 扩展。
   a. 从用户界面单击*“策略”*，在导航窗格中打开*“配置”*，展开“策略”树，然后打开 SystemEDGE 策略。

      将在右侧窗格中显示策略详细信息。
   b. 单击“MIB 扩展”选项卡。

      将打开“MIB 扩展”窗格。
   c. 将以下数据添加到字段中：

      索引：1（如果这是第一个 MIB 扩展）

      类型：整数

      扩展命令：C:\data.bat

      访问权限：只读
   d. 单击“*添加*”。

      MIB 扩展将添加到策略中。
   e. 单击*“保存策略”*。

      将保存策略。
4. 创建阈值监视器以检查新监视器的值。
   a. 单击*“监视器”*，然后单击*“阈值”*。

      此时将显示“阈值监视器详细信息编辑”窗格。
   b. 将以下数据添加到字段中：

      索引：（已自动添加）

      平台：独立于操作系统

      对象类：extensionGroup [通过添加新的标量变量来扩展 MIB]

      对象属性：1

      对象实例名称：MyData

      间隔：60

      重要级别：重大报警

      运算符：大于或等于

      值：50

      比例：1

      抽样类型：绝对值

c. 单击“*保存*”。

将保存策略。已添加阈值为“50”的“重大”报警。由于之前创建的脚本始终返回值“99”，将立即违反此阈值。

d. 单击*“操作”*，然后单击*“应用”*以将策略应用于计算机。

此时将显示“已选择计算机”窗格。

e. 验证选定的计算机是否正确，然后单击*“应用”*。

具有 MIB 扩展的策略将应用于选定的计算机。

单击*“返回策略”*。

此时将显示“策略详细信息”窗格。

配置代理后，您可以从“资源”选项卡中查看此阈值监视器的状态。您可以看到已违反“重大”阈值。

如何监控特定的 Windows 性能注册表度量标准

此分步示例介绍了如何监控特定于用户的度量标准。Windows 性能对象和计数器中使用的名称必须与 perfmon.exe 中的名称匹配。

如何监控特定于用户的度量标准（MIB 扩展）：

1. 为 Windows 性能注册表度量标准创建 MIB 扩展。
   a. 从用户界面，单击“资源”选项卡，打开“配置”窗格，展开“策略”树，然后单击相应的子类别。

      将在右侧窗格中显示策略详细信息。

   b. 单击*“MIB 扩展”*选项卡。

      将打开“MIB 扩展”窗格。

   c. 单击*“Windows 性能”*。

      此时将显示“Windows 性能已定义扩展”窗格。

   d. 将以下数据添加到字段中：
      示例：

      索引：1（如果此扩展是第一个扩展）。

      类型：整数

      对象：系统

      计数器：进程（提供运行进程的总数）。

      系统度量标准没有“实例”，因此该字段保留为空。

      注意：创建策略时，您可以为对象和计数器指定自定义条目。创建其他策略时，将保存相同的度量标准以供将来使用。

   e. 单击*“添加”*。

      MIB 扩展将添加到策略中。

   f. 单击*“保存策略”*。

      将保存策略。

2. 创建阈值监视器以检查新监视器的值。
   a. 单击*“监视器”*，然后单击*“阈值”*。

      此时将显示“阈值监视器详细信息编辑”窗格。

   b. 单击 +（新建）以创建监视器。

      此时将显示“阈值监视器详细信息: 新建”对话框。

c. 配置以下阈值设置：

索引

定义要使用的表索引。

平台

指定平台。

说明

定义可选说明。

对象类

指定要监控的对象类。值是指可用的 MIB 表。

对象类名

定义要用于对象状态模型的对象类名。值是一个任意字符串（例如 FileSystems）。

对象属性

指定要监控的对象属性。值是指选为对象类的表的可用属性。属性（例如，devCapacity = 1.3.6.1.4.1.546.1.1.1.7.1.14）指定要使用该阈值监视器监视的 MIB 对象 (OID) 的初始部分。

对象属性名称

将要用于对象状态模型的对象属性名称定义为任意字符串，例如 PercentUsed。

对象实例

指定要监控的对象实例。该值（例如，.3 监视设备表（devTable）的第三行）指定了使用该阈值监视器进行监视的 MIB 对象 (OID) 的索引部分。对于一些对象类，可以给出实例本身的名称（例如，对于 Unix 计算机，使用 C: 而不是 .3 或 /var）。

对象实例名称

定义要用于对象状态模型的对象实例名称。值是一个任意字符串（例如 SysVol_C）。

间隔

将监视器的评估间隔定义为 30 秒的倍数。

“阈值配置”页面使您可以定义以下设置：

重要级别

指定用于对象状态模型的重要级别。

运算符

指定要使用的运算符。

值

定义要使用的值。

抽样类型

指定要使用的抽样类型。

“维护窗口”页面使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态。

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

“可选设置”子选项卡使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

d. 单击*“保存”*。

监视器已添加到策略中。

3. 单击*“操作”*，然后单击*“应用”*以将策略应用于计算机。

此时将显示“已选择计算机”窗格。

a. 验证选定的计算机是否正确，然后单击*“应用”*。

具有 MIB 扩展的策略将应用于选定的计算机。

b. 单击*“返回策略”*。

此时将显示“策略详细信息”窗格。

配置代理后，您可以从“资源”选项卡的“浏览”、“摘要”选项卡下查看此阈值监视器的状态。

如何创建 SRM 策略

可创建 SRM 策略来定义要执行的测试、要监控的阈值、配置首选项和控制代理运行方式及其监控内容的其他设置。创建策略之后，可将其应用于任意数量的通过 SRM AIM 以受管模式运行 SystemEDGE 代理的系统。通过策略可以执行所有配置操作，您可以利用合并界面、选项表以及到远程系统的动态部署的优点来在本地手动配置这些配置操作。

以下过程描述了如何创建 SRM 策略：

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“服务响应”窗格。

2. 在“可用策略”工具栏上单击 +（新建）。

   将显示“新建服务响应监控策略”对话框。

3. 输入策略的名称和描述，以及该策略是否基于现有策略，然后单击“确定”。

   将创建策略，并在右侧窗格中显示配置屏幕。

4. 定义要包括的测试。
5. 定义测试阈值。
6. 定义控制设置 (p. 248)。
7. 单击“保存策略”。

   将保存策略。

发现代理

当代理有多个 NIC（网络接口控制器）时，策略配置将发现该代理的所有名称或地址。为了避免发现不需要的名称和地址，策略配置支持发现具有管理名称或地址的代理以部署作业。

注意：系统每 30 分钟刷新发现代理列表。

遵循这些步骤:

1. 登录到 CA Virtual Assurance 应用程序，然后单击“资源”选项卡。
2. 从“资源管理器”选项卡，右键单击“域服务器”并选择“策略”、“SystemEDGE”、“发现代理”。

   将打开确认对话框。
3. 单击“确定”。

   注意:要查看该列表，请单击“监控软件”选项卡，然后单击“策略”选项卡。将显示具有管理名称或地址的可用代理的列表。

策略配置功能的常见用法

本节介绍常见策略配置功能。

如何创建 SystemEDGE 策略

可创建 SystemEDGE 策略来定义一组监视器、要加载的 AIM、配置首选项和控制代理运行方式及其监控内容的其他设置。创建策略之后，可将其应用于任意数量的以受管模式运行 SystemEDGE 代理的系统。通过策略可以执行所有配置操作，您可以利用合并界面、选项表以及到远程系统的动态部署的优点来在本地手动配置这些配置操作。

以下过程描述如何创建 SystemEDGE 策略：

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“SystemEDGE”窗格。
2. 在“可用策略”工具栏上单击 +（新建）。

   将显示“新建 SystemEDGE 策略”对话框。
3. 输入策略的名称和描述，以及该策略是否基于现有策略，然后单击“确定”。

   将创建策略，并在右侧窗格中显示配置屏幕。

4. 定义要包括的监视器。
5. 定义控制设置 (p. 212)。
6. 定义 SNMP 设置 (p. 172)。
7. 定义 MIB 扩展。
8. 单击“保存策略”。

   将保存策略。

复制 SystemEDGE 策略

您可以复制现有的 SystemEDGE 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。
2. 在“可用策略”表中选择要复制的策略，单击“操作”并选择“复制”。您也可以右键单击“配置”窗格中的策略并选择“复制”。

   此时将显示“复制”对话框。
3. 输入策略的新名称，然后单击“确定”。

   将复制策略，并在右侧窗格中显示一个“配置”屏幕。
4. 单击“保存策略”。

   将保存策略。

重命名 SystemEDGE 策略

您可以重命名现有的 SystemEDGE 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。
2. 在“可用策略”表中选择要重命名的策略，单击“操作”并选择“重命名”。您也可以右键单击“配置”窗格中的策略，然后选择“重命名”。

   此时将显示“重命名”对话框。

   注意：如果该策略正在使用中，则会显示一条错误消息，表示无法重命名策略。

3. 输入策略的新名称，然后单击“确定”。

   会出现一条确认消息，通知您已重命名策略。

4. 单击“保存策略”。

   将保存策略。

删除 SystemEDGE 策略

您可以删除现有的 SystemEDGE 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择要删除的策略，单击“操作”并选择“删除”。您也可以右键单击“配置”窗格方中的策略，然后选择“删除”。

   注意：如果策略正在使用中，则会显示一条错误消息，指示无法删除该策略。

   将出现一条警告消息。

3. 单击“确定”确认删除。

   即会出现一条确认消息。将删除策略。

将 SystemEDGE 配置导入策略中

将 SystemEDGE 升级到当前版本后，导入先前的 SystemEDGE 配置，并将其转换为 SystemEDGE 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”工具栏上单击 +（新建）。

   此时将显示“新建 SystemEDGE 策略”对话框。

3. 单击“导入”。

   此时将显示“SystemEDGE 代理计算机”窗口。

4. 选择要从中导入 SystemEDGE 配置的计算机，然后单击“确定”。

   注意：计算机列表显示所有从原始配置文件升级的计算机（定义了监视器）。发现 SystemEDGE 5.x 并在策略配置中注册后，计算机将显示在列表中。如果未列出计算机，验证是否已在先前的 SystemEDGE 版本级别定义其监视器，且是否已配置“策略配置”。

5. 在“新建 SystemEDGE 策略”对话框中输入名称和可选说明，并单击“确定”以完成导入过程。

6. 单击“保存策略”。

   将保存策略。

定义 SystemEDGE 策略控制设置

通过使用 SystemEDGE 策略控制设置，可以控制下列代理行为：

- 安全设置
- SNMP 设置
- MIB 表填充
- UNIX 设置
- 性能监控设置

您可以将策略中定义的控制设置应用于所有计算机。

遵循这些步骤：

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“控制设置”。

   此时将显示“控制”页面。

4. （可选）单击“使用默认值”。

   将显示默认选项窗格。您可以更改默认设置。

5. 配置以下控制设置：

SNMP

可以定义以下基本 SNMP 属性：

绑定地址

指定代理绑定到的接口，代理在该接口上侦听传入 SNMP 请求。有效地址是 IPv4 或 IPv6 地址。

注意：相应的默认 _port 在安装期间指定。

绑定端口

指定代理绑定到以发送 SNMP 陷阱的陷阱端口。如果没有指定 bind_address，代理将绑定到所有可用的 UDP 地址。

默认值：由系统选择的端口

IP 族

指定代理通信方法：仅 IPv4、仅 IPv6 或两者。默认情况下，代理首先尝试使用 IPv4，然后尝试使用 IPv6。

FIPS 模式

指定代理使用符合 FIPS 标准的加密。选择“非 FIPS 模式”可启用 CA eTrust 公钥基础构架库，如果该方法失败，则退回到内部最小安全解决方案。选择“FIPS 共存模式”可启用符合 FIPS 标准的加密，如果该方法失败，则退回到 CA eTrust 公钥基础构架库。选择“仅 FIPS 模式”可启用 RSA BSAFE Crypto-C Micro Edition 符合 FIPS 标准的库，如果库失败，则不执行加密。

默认值：非 FIPS 模式

陷阱源

指定用于发送陷阱的源地址。有效地址是 IPv4、IPv6 地址或主机名。

默认值：代理的主机名

安全设置

可以定义以下安全首选项：

身份验证陷阱

当代理收到具有代理无法识别的团体名称的 SNMP 消息时，发送身份验证失败陷阱。

默认：禁用

进程集

在“进程”表和“运行软件”表中允许访问在代理系统上运行的进程和其他软件。在这些表上允许 SNMP Set 可能会引起安全问题。

远程外壳组

允许管理系统远程指示代理通过远程 Shell 组在代理系统上运行 Shell 脚本和程序。泄漏此类信息可能会产生潜在的安全风险。

执行操作

超过阈值时，通过监控表执行操作命令。运行操作命令和脚本的功能可能导致安全问题。

MIB 表填充

在系统管理 MIB 中填充以下表：

- 进程表
- 用户组表
- 用户表
- 陷阱团体表
- 监视器镜像表
- 聚合镜像表
- 顶端进程表

每个表包含可以在 MIB 中公开的敏感信息，或者可以将其禁用以节省磁盘空间的不必要信息。默认设置可以填充除进程表之外的所有表。

杂项

可以定义以下杂项设置：

允许代理使用 SNMP 更新

允许代理使用 SNMP Set 更新（例如，删除写团体）。如果在代理上允许 SNMP Set，则通过此方式进行的任何更新会导致生成 SNMP Set 更改通知，并且在查看系统的策略详细信息时还会导致异常。

向管理器通知配置更新

使代理能够将通知发送给管理器，以便代理处理任何 SNMP Set 请求。

热启动发现

使代理在每次热启动配置更新之后重新发现所有设备。如果管理具有许多设备的系统，则每次热启动之后进行发现可能会消耗太多时间和太多资源。

使用 Perl 兼容的正则表达式

Perl 兼容的正则表达式 (PCRE) 使您可以指定 i18n 兼容的正则表达式，同时定义支持正则表达式的监视器。正则表达式的示例包括日志文件、进程、进程组、Windows 服务和 Windows 事件。您也可以使用该选项来创建更复杂的正则表达式。SystemEDGE 代理 5.1.0 及更高版本中提供该选项。

自动解决索引冲突

使您能够解决索引冲突。将分层模板应用于所有计算机时，会为添加到模板中的监视器分配索引。如果在基本策略或其他模板中分配的索引与现有索引冲突，该选项会重新分配唯一索引值。

注意：基本策略中包含的索引始终在已交付的配置中维护。如果已禁用该选项，则无法解决冲突索引。然而，将分层模板应用于计算机时，冲突的索引在引起冲突索引的分层模板上显示为错误。

历史性能监控

可以为性能多维数据集 AIM 定义以下设置，性能多维数据集 AIM 将历史信息收集到系统性能多维数据集中，以用于历史性能管理：

收集间隔

指定将信息从“历史记录”表收集到性能多维数据集中的频率。

索引范围开始

指定保留的索引范围的开始，其中默认情况下代理将为性能多维数据集数据的收集创建历史记录控制条目。例如，如果 SRM（服务响应监控）配置为收集性能数据，则使用此保留的范围。

索引范围结束

指定保留的索引范围的结束，其中默认情况下代理将为性能多维数据集数据的收集创建历史记录控制条目。例如，如果 SRM（服务响应监控）配置为收集性能数据，则使用此保留的范围。

UNIX 控制设置

可以为在 UNIX 系统上运行的代理定义以下设置：

子程序组

指定除根之外的在其中运行子程序的组名称。

子程序用户

指定除根之外的在其中运行子程序的用户名。

Linux Freemem 包括

指定在可用内存计算中包括系统缓冲区、磁盘已缓存内存还是两者。

查询系统设备

可以查询以下系统设备度量标准：

- 串行设备状态
- 软盘状态
- 磁盘大小、容量、说明以及其他属性（探测磁盘）
- NFS 文件系统状态
- HP-UX 图形状态

查询这些度量标准会引起潜在的代理阻塞问题。默认设置可以仅查询串行设备状态和 NFS 文件系统状态。

6. 单击“插件”。

   此时将显示“插件”窗格。该窗格控制哪些 AIM 随代理一起加载。

7. 执行以下操作之一：

   - 选择“加载所有可用插件”，加载代理系统上所有可用的 AIM。
   - 选择“加载表中选择的插件”。
   - 单击“外部插件”工具栏上的 +（新添加），将 AIM 添加到“外部插件”表中。

   注意：有关可用 AIM 的详细信息，请参阅*《SystemEDGE 用户指南》*。

   将配置 AIM 加载。

8. 单击“聚合监视器”。

   按照配置对象聚合 (p. 217)中所述配置聚合监视器。

   将定义控制设置。

9. 单击“保存策略”。

   将保存策略。

详细信息：

配置对象聚合 (p. 217)

配置对象聚合

默认情况下，SystemEDGE 将监视器聚合到一个受管对象中，该受管对象包含对象类、实例和属性特性的相同值。例如，将所有具有 SysHealth 类、CPU 实例及 SysTime 属性的监视器合并到聚合受管对象中。

您可以在定义 SystemEDGE 策略时将代理配置为在较高级别上聚合对象。也可以配置与对象聚合及状态管理模型相关的代理行为的其他方面。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“控制设置”。

   此时将显示“控制”页面。

4. 单击“聚合监视器”。

   此时将显示“聚合监视器”页面。

5. 选中一个或多个复选框以指定聚合级别。

   这些聚合级别比默认值更高，高到能够将所有监视器聚合到一个顶级的代理对象中。通过指定聚合级别，可以创建分层对象体系结构，将状态传播到比指定高的级别。

6. 配置以下其他设置，然后单击“保存策略”：

   发送所有聚合监视器的遗留陷阱

   指定是否发送构成受管对象的所有监视器的传统陷阱。默认情况下，即使对象中的其他监视器违反了阈值，代理也仅发送最高重要级别的监视器的状态变更陷阱。

   执行所有聚合监视器的命令

   指定是否执行构成受管对象的所有监视器的操作命令。默认情况下，即使对象中的其他监视器违反了阈值，代理也仅运行最高重要级别的监视器的操作命令。

   聚合设置现已配置完成。应用或重新应用策略以使更改生效。

详细信息：

定义 SystemEDGE 策略控制设置 (p. 212)

定义新的 SystemEDGE 监控模板

可以使用不同的策略配置 SystemEDGE。通过监控模板，可以配置多个策略，并将这些策略传送给共享服务器上的同一代理。

通过“监控模板”页面，可以查看和更新应用于特定服务器或服务器组的策略。可以创建 SystemEDGE 监控模板（分层模板）并导入到策略中。这样可以在多个策略中重复使用监视器，而无需多次设置监视器。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后单击“SystemEDGE”。

   此时将显示 SystemEDGE 页面。

2. 在“模板列表”工具栏上单击“+ (新建)”。

   此时将显示“新建 SystemEDGE 监控模板”对话框。

3. 输入模板的名称和可选说明、系统类型和是否将其基于现有模板，然后单击“确定”。

   将创建模板并显示“摘要”页面。要将监视器添加到模板中，请参阅将监视器添加到 SystemEDGE 策略 (p. 226)部分。

4. 单击“保存模板”。

   将保存模板。

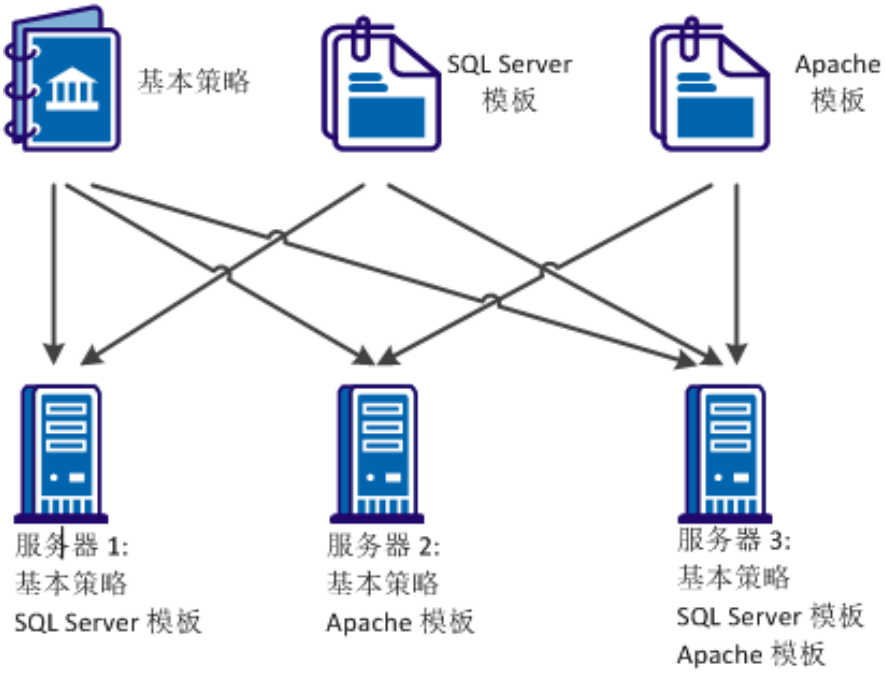
详细信息：

分层模板 (p. 220)
将监控模板导入 SystemEDGE 策略 (p. 221)
复制 SystemEDGE 监控模板 (p. 222)
修改 SystemEDGE 监控模板 (p. 222)
重命名 SystemEDGE 监控模板 (p. 223)
删除 SystemEDGE 监控模板 (p. 223)
查看监控模板应用程序进度 (p. 224)
将模板应用于计算机 (p. 224)
分层模板 (p. 220)
修改 SystemEDGE 监控模板 (p. 222)
重命名 SystemEDGE 监控模板 (p. 223)
查看监控模板应用程序进度 (p. 224)
将模板应用于计算机 (p. 224)

分层模板

在企业中，每个服务器或服务器组所处理的工作负荷有所不同。可以创建多个特定于服务器或服务器组所处理的工作负荷的策略。要协助创建策略，可以使用模板创建特定于应用程序的监视器。会将基本策略和分层模板组合以形成一个配置文件，并将其应用于需要监控的服务器。可以添加或删除分层模板。可以直接将模板更新应用于服务器，而无需更改基本策略，或将更新的模板重新导入到基本策略中。

示例: 将基本策略和模板应用到服务器



可以在以下方案中使用分层模板：

不同应用程序

为运行不同应用程序集的每个服务器创建模板库。可以直接将模板更新应用于每个服务器。

动态环境

在动态环境中，服务器的工作负荷频繁变更。可以使用分层模板将监视器划分到各个逻辑组中。可以根据工作负荷的变更，直接将逻辑组应用于系统或从系统中删除。

共享服务器

在企业设置中，跨多个部门共享服务器。每个部门管理和监控共享服务器上的应用程序。可以使用分层模板分别管理模板并将模板应用于各个部门的系统。

应用程序维护

可将监控拆分到多个模板中。在服务器中，可删除不使用的应用程序的模板，而不影响对其余系统的监控。

开箱即用模板

可以将开箱即用模板应用于受管节点。使用受管节点上的模板配置配置策略。这些模板可用于以下操作系统：

对于所有操作系统：

CPU 使用率－自动监测

交换容量

对于 Windows：

应用程序监控－CA eTrust Antivirus

进程崩溃

系统错误

系统进程

用户活动

Windows 服务－自动监测

对于 UNIX（AIX、HPUnix、Linux、Solaris）：

系统消息

系统进程

用户活动

将监控模板导入 SystemEDGE 策略

您可以将监控模板导入 SystemEDGE 策略。这会通过一次操作将所有系统的现有策略替换为一致策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“操作”，然后选择“导入”。

   此时将显示“导入模板向导”。

5. 从下拉列表选择要导入的系统类型和监控模板。
6. （可选）为每个导入的监视器定义新的基本索引。
7. 从下拉列表中选择“冲突解决选项”，然后单击“下一步”。

   此时将显示“解决冲突”页面。

8. 查看监视器冲突并进行索引调整，然后单击“下一步”。

   此时将显示“摘要”页面。

9. 查看将要导入的监视器，然后单击“完成”完成导入过程。
10. 单击“保存策略”。

    将保存策略。

复制 SystemEDGE 监控模板

您可以复制现有的 SystemEDGE 监控模板。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后单击“SystemEDGE”。

   “摘要”页面显示 SystemEDGE 监控模板的列表。

2. 选择要复制的监控模板，单击“操作”，然后选择“复制”。您也可以右键单击“配置”窗格中的监控模板，然后选择“复制”。

   此时将显示“复制”对话框。

3. 输入监控模板的新名称，然后单击“确定”。

   此时将复制监控模板，并在右侧窗格中显示一个“配置”屏幕。

修改 SystemEDGE 监控模板

可以修改 SystemEDGE 监控模板。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后单击“SystemEDGE”。

   “摘要”页面显示 SystemEDGE 监控模板的列表。

2. 选择模板名称。

   此时将显示包含模板信息的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击相应的监视器选项卡并选择要修改的监视器。

   此时将显示“编辑”对话框。

5. 根据您的需求修改设置，然后单击“保存”。
6. （可选）对任何其他监视器重复该过程。
7. 单击“保存”。

   此时将保存监控模板。

重命名 SystemEDGE 监控模板

您可以重命名现有的 SystemEDGE 监控模板。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后单击“SystemEDGE”。

   “摘要”页面显示 SystemEDGE 监控模板的列表。

2. 选择要重命名的监控模板，单击“操作”，然后选择“重命名”。您也可以右键单击“配置”窗格中的监控模板，然后选择“重命名”。

   此时将显示“重命名”对话框。

3. 输入监控模板的新名称，然后单击“确定”。

   此时将重命名监控模板，并在右侧窗格中显示一个配置屏幕。

删除 SystemEDGE 监控模板

您可以删除不再需要的现有 SystemEDGE 监控模板。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后单击“SystemEDGE”。

   “摘要”页面显示 SystemEDGE 监控模板的列表。

2. 单击“受管计算机”选项卡

   此时将显示“摘要”页面，其中显示应用于模板的受管计算机列表。

3. 选择要删除的监控模板，然后单击“删除”图标。

   即会出现一条确认消息。

4. 单击“确定”确认删除。

   将删除监控模板。

查看监控模板应用程序进度

可以逐个详细查看每个模板的监控模板应用程序操作的进度。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后选择“SystemEDGE”。

   “摘要”页面显示 SystemEDGE 监控模板的列表。

2. 选择模板名称。

   此时将显示包含模板信息的“摘要”页面。

3. 单击“受管计算机”选项卡。

   此时将显示“受管计算机”页面，其中显示当前运行监控模板的计算机的列表，您可以查看配置状态。

4. （可选）单击“查看配置”。

   此时将显示“SystemEDGE 配置”窗格，通过该窗格可以查看策略和模板以及为代理交付的配置文件。

将模板应用于计算机

更新监控模板之后，可将其应用于企业内的计算机。

遵循这些步骤:

1. 单击“资源”窗格，打开“配置”窗格，展开“监控模板”，然后选择“SystemEDGE”。

   “摘要”页面显示 SystemEDGE 监控模板的列表。

2. 选择模板名称。

   此时将显示包含模板信息的“摘要”页面。

3. 单击“操作”，然后选择“应用”。

   此时将显示用于选择要在其中应用监控模板的计算机的选项卡。使用“更新运行该模板的计算机”选项卡可以将监控模板应用于已经使用该模板的计算机。使用“应用于未运行该模板的计算机”选项卡可将监控模板应用于未使用任何模板的计算机。

4. （可选）在“现有计算机”下，选择以下选项之一：
   - 更新应用该模板的所有计算机。
   - 仅更新没有应用该模板最新更改的计算机。
   - 仅更新未成功应用模板的计算机。
   - 高级(手动选择计算机)
   - 从计算机中删除该模板。
5. （可选）在“已选择计算机”下，选择要将模板重新应用到的计算机。
6. （可选）从“应用于未运行该模板的计算机”选项卡中选择要向其应用模板的计算机。
7. 单击“应用”。

   此时将启动模板应用程序。

将 SystemEDGE 配置导入模板中

将 SystemEDGE 升级到当前版本后，导入先前的 SystemEDGE 配置，并将其转换为 SystemEDGE 监控模板。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后单击“SystemEDGE”。

   此时将显示“可用 SystemEDGE 监控模板”页面。

2. 单击“可用 SystemEDGE 监控模板”工具栏上的 +（新建）。

   此时将显示“新建 SystemEDGE 监控模板”对话框。

3. 单击“导入”。

   此时将显示“SystemEDGE 代理计算机”窗口。

4. 选择要从中导入 SystemEDGE 配置的计算机，然后单击“确定”。

   注意：计算机列表显示所有从原始配置文件升级的计算机（定义了监视器）。发现 SystemEDGE 5.x 并在策略配置中注册后，计算机将显示在列表中。如果未列出计算机，验证是否已在先前的 SystemEDGE 版本级别定义其监视器，且是否已配置“策略配置”。

5. 在“新建 SystemEDGE 监控模板”对话框中输入名称和可选说明，并单击“确定”以完成导入过程。

6. 单击“保存模板”。

   将保存模板。

将监视器添加到 SystemEDGE 策略

您可以将监视器添加到 SystemEDGE 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”并选择要添加的监视器。

   - 定义阈值监视器 (p. 227)
   - 定义进程监视器 (p. 229)
   - 定义日志文件监视器 (p. 231)
   - 定义 Windows 事件监视器 (p. 233)
   - 定义历史记录监视器 (p. 234)
   - 定义进程组监视器 (p. 236)

4. （可选）对任何其他监视器重复该过程

5. 单击“保存策略”。

   监视器将加载到策略，并保存该策略。

注意：有关监视器的信息，请参阅 *《SystemEDGE 用户指南》*。

详细信息：

定义阈值监视器 (p. 227)
定义进程监视器 (p. 229)
定义日志文件监视器 (p. 231)
定义 Windows 事件监视器 (p. 233)
定义历史记录监视器 (p. 234)
定义进程组监视器 (p. 236)

定义阈值监视器

您可以定义 SystemEDGE 策略的阈值设置。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“阈值”。

   此时将显示“阈值监视器”页面。

5. 在“阈值监视器”工具栏上单击“+ (新建)”。

   此时将显示“阈值监视器详细信息: 新建”对话框。

6. 配置以下阈值设置：

   索引

   定义要使用的表索引。

   平台

   指定平台。

描述

定义可选说明。

对象类

指定要监控的对象类。下拉列表中的值是指可用的 MIB 表。

对象类名

定义要用于对象状态模型的对象类名。这是一个任意字符串（例如 FileSystems）。

对象属性

指定要监控的对象属性。下拉列表中的值是指选为对象类的表的可用属性。属性（例如，devCapacity = 1.3.6.1.4.1.546.1.1.1.7.1.14）指定要使用该阈值监视器监视的 MIB 对象 (OID) 的初始部分。

对象属性名称

定义要用于对象状态模型的对象属性名称。这是一个任意字符串（例如 PercentUsed）。

对象实例

指定要监控的对象实例。该值（例如，.3 监视设备表（devTable）的第三行）指定了使用该阈值监视器进行监视的 MIB 对象 (OID) 的索引部分。对于一些对象类，可以给出实例本身的名称（例如，对于 Unix 计算机，使用 C: 而不是 .3 或 /var）。

对象实例名称

定义要用于对象状态模型的对象实例名称。这是一个任意字符串（例如 SysVol_C）。

间隔

将监视器的评估间隔定义为 30 秒的倍数。

“阈值配置”页面使您可以定义以下设置：

重要级别

指定用于对象状态模型的重要级别。

运算符

指定要使用的运算符。

值

定义要使用的值。

抽样类型

指定要使用的抽样类型。

“维护窗口”页面使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态。

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

“可选设置”子选项卡使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

注意：有关详细信息，请参阅*《SystemEDGE 用户指南》*。

7. 单击“保存”

   会保存“阈值监视器”设置。

8. 单击“保存策略”。

   会将阈值监视器加载到策略中。

定义进程监视器

您可以定义 SystemEDGE 策略的进程设置。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“处理”。

   此时将显示“进程监视器”页面。

5. 在“进程监视器”工具栏上单击“+ (新建)”。

   此时将显示“进程监视器详细信息: 新建”对话框。

6. 配置以下进程设置：

索引

定义要使用的表索引。

平台

指定平台。

描述

定义可选说明。

对象类名

指定要用于对象状态模型的对象类名。这是一个任意字符串（例如 Process）。

对象属性

指定要监控的对象属性。下拉列表中的值定义进程监视的可用属性。

对象属性名称

定义要用于对象状态模型的对象属性名称。这是一个任意字符串（例如 MemUsedPercent）。

对象实例

指定要监控的对象实例。这是用来按名称、Solaris Zones 中的进程（使用 ZoneRegExpr/ProcRegExpr）匹配进程或按名称匹配 Windows 服务的正则表达式（依赖于可选设置）。模式应唯一匹配单个进程（服务）。可以包括参数（请参见可选设置）。

对象实例名称

指定要用于对象状态模型的对象实例名称。这是一个任意字符串（例如 ApacheServer）。

间隔

将监视器的评估间隔定义为 30 秒的倍数。

“阈值配置”页面使您可以定义以下设置：

重要级别

指定用于对象状态模型的重要级别。

运算符

指定要使用的运算符。

值

定义要使用的值。

抽样类型

指定要使用的抽样类型。

“维护窗口”页面使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态。

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

“可选设置”子选项卡使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

注意：有关详细信息，请参阅*《SystemEDGE 用户指南》*。

7. 单击“保存”

   会保存“进程监视器”设置。

8. 单击“保存策略”。

   会将进程监视器加载到策略中。

定义日志文件监视器

您可以定义 SystemEDGE 策略的日志文件设置。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“日志文件”。

   此时将显示“日志文件监视器”页面。

5. 在“日志文件监视器”工具栏上单击“+ (新建)”。

   此时将显示“日志文件监视器详细信息: 新建”对话框。

6. 配置以下进程设置：

   索引

   定义要使用的表索引。

   监视器类型

   指定要使用的监视器类型。

   平台

   指定平台。

   描述

   定义可选说明。

   日志文件/目录名称

   定义要监控的文件或目录的路径。

   搜索筛选器

   指定搜索筛选器。

   间隔

   定义监视器的评估间隔（分钟）

   重要级别

   指定匹配监视器的重要性。

   “维护窗口”页面使您可以定义以下设置：

   状态

   指定监视器维护条目是否处于活动状态。

   开始时间

   在监视器关闭时定义开始时间，维护窗口启动。

   终止时间

   在监视器再次打开时定义终止时间，维护窗口关闭。

“可选设置”页面使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

注意：有关详细信息，请参阅 *《SystemEDGE 用户指南》*。

7. 单击“保存”

   会保存“日志文件监视器”设置。

8. 单击“保存策略”。

   会将日志文件监视器加载到策略中。

定义 Windows 事件监视器

您可以定义 SystemEDGE 策略的 Windows 事件设置。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“Windows 事件”。

   此时将显示“Windows 事件监视器”页面。

5. 在“Widows 事件监视器”工具栏上单击“+ (新建)”。

   此时将显示“Windows 事件详细信息: 新建”对话框。

6. 配置以下进程设置：

   索引

   定义要使用的表索引。

   平台

   指定平台。

   描述

   定义可选说明。

事件日志

指定要读取的事件日志。

事件类型

指定要匹配的事件类型。

源筛选

定义要使用的源筛选。

说明筛选

定义要使用的说明筛选。

重要级别

指定匹配监视器的重要性。

“维护窗口”子选项卡使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态。

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

“可选设置”子选项卡使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

注意：有关详细信息，请参阅*《SystemEDGE 用户指南》*。

7. 单击“保存”

   会保存“Windows 事件监视器”设置。

8. 单击“保存策略”。

   会将 Windows 事件监视器加载到策略中。

定义历史记录监视器

您可以定义 SystemEDGE 策略的历史记录设置。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“历史记录”。

   此时将显示“历史记录监视器”页面。

5. 在“历史记录监视器”工具栏上单击“+ (新建)”。

   此时将显示“历史记录详细信息: 新建”对话框。

6. 配置以下进程设置：

   索引

   定义要使用的表索引。

   平台

   指定平台。

   描述

   定义可选说明。

   对象类

   指定要监控的对象。下拉列表中的值指可用的 MIB 表。

   对象属性

   指定要监控的对象属性。下拉列表中的值是指选为对象类的表的可用属性。属性（例如，devCapacity = 1.3.6.1.4.1.546.1.1.1.7.1.14）指定要使用该历史记录条目监视的 MIB 对象 (OID) 的初始部分。

   对象实例

   定义要监控的对象实例。该值（例如，.3 监视设备表（devTable）的第三行）指定了使用该历史记录条目进行监视的 MIB 对象 (OID) 的索引部分。

   间隔

   将收集间隔定义为 30 秒的倍数。

   存储段

   定义要收集的抽样数。

   “添加到性能多维数据集”复选框

   指定是否为该条目收集性能多维数据。

“维护窗口”页面使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

注意：有关详细信息，请参阅*《SystemEDGE 用户指南》*。

7. 单击“保存”

   会保存“历史记录监视器”设置。

8. 单击“保存策略”。

   会将历史记录监视器加载到策略中。

定义进程组监视器

您可以定义 SystemEDGE 策略的进程组设置。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击“进程组”。

   此时将显示“历史记录监视器”页面。

5. 在“进程组监视器”工具栏上单击“+ (新建)”。

   此时将显示“进程组详细信息: 新建”对话框。

6. 配置以下进程设置：

索引

定义要使用的表索引。

平台

指定平台。

描述

定义可选说明。

过程名称

定义进程名称。这是用来按名称

间隔

将监视器的评估间隔定义为 30 秒的倍数。

用户名

除任何进程名正则表达式之外，定义要匹配的用户名。

组名称

除任何进程名正则表达式之外，定义要匹配的组名称。

重要级别

指定组变更监视器的重要性

“维护窗口”页面使您可以定义以下设置：

状态

指定监视器维护条目是否处于活动状态

开始时间

在监视器关闭时定义开始时间，维护窗口启动。

终止时间

在监视器再次打开时定义终止时间，维护窗口关闭。

“可选设置”页面使您可以对可用于不同的监视器条目或历史记录控制条目的标志进行定义。

注意：有关详细信息，请参阅*《SystemEDGE 用户指南》*。

7. 单击“保存”

会保存“进程组监视器”设置。

8. 单击“保存策略”。

会将进程组监视器加载到策略中。

查看 SystemEDGE 策略内的监视器

您可以查看 SystemEDGE 策略内包含的监视器。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。您可以单击“监视类”子选项卡来查看策略内包含的不同监视器。

详细信息

修改 SystemEDGE 策略内包含的监视器 (p. 239)
从 SystemEDGE 策略中删除监视器 (p. 239)

复制 SystemEDGE 策略内包含的监视器

您可以复制 SystemEDGE 策略内包含的监视器。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击相应的监视器选项卡并选择要复制的监视器。
5. 单击“操作”，然后选择“复制”。

   此时将显示“编辑”对话框。

6. 根据您的需求修改设置，然后单击“保存”。
7. （可选）对任何其他监视器重复该过程。

8. 单击“保存策略”。

   将保存策略。

修改 SystemEDGE 策略内包含的监视器

您可以修改 SystemEDGE 策略内包含的监视器。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击相应的监视器选项卡并选择要修改的监视器。
5. 单击“操作”，然后选择“修改”。

   此时将显示“编辑”对话框。

6. 根据您的需求修改设置，然后单击“保存”。
7. （可选）对任何其他监视器重复该过程。
8. 单击“保存策略”。

   将保存策略。

从 SystemEDGE 策略中删除监视器

您可以从 SystemEDGE 策略中删除监视器。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。

4. 单击相应的监视器选项卡并选择要删除的监视器。
5. 单击“操作”，然后选择“删除”。

   将出现一条警告消息。
6. 单击“确定”确认删除。
7. （可选）对任何其他监视器重复该过程。
8. 单击“保存策略”。

   将保存策略。

在 SystemEDGE 策略中修改现有模板

您可以修改现有监控模板并将其导入到 SystemEDGE 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。
2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。
3. 单击“监视器”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的监视器列表。
4. 单击“操作”，然后选择“导入”。

   此时将显示“导入模板向导”。
5. 使用所需的信息更新监控模板。
6. 从下拉列表中选择要导入的系统类型和更新的监控模板。
7. （可选）为每个导入的监视器定义新的基本索引。
8. 选择“冲突解决选项”为“将现有监视器替换为导入的实体”，然后单击“下一步”。

   此时将显示“解决冲突”页面。
9. 复查监视器冲突并进行索引调整，然后单击“下一步”。

   此时将出现“摘要”页。
10. 复查将要导入的监视器，然后单击“完成”完成导入过程。

11. 单击“保存策略”。

    将保存策略。

12. 从“操作”下拉列表中选择“应用”。

    已保存的策略将应用于期望的计算机。

定义新 SRM 策略

您可以创建 SRM 策略，以定义要执行的测试、要监控的阈值、配置首选项和控制代理如何运行及其监控内容的其他设置。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”工具栏上单击 +（新建）。

   将显示“新建服务响应监控策略”对话框。

3. 输入策略的名称和可选说明、系统类型和是否将其基于现有策略，然后单击“确定”。

   将创建策略，并在右侧窗格中显示配置屏幕。

4. 单击“保存策略”。

   将保存策略。

详细信息：

复制 SRM 策略 (p. 241)
重命名 SRM 策略 (p. 242)
删除 SRM 策略 (p. 242)

复制 SRM 策略

可以复制现有的 SRM 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择要复制的策略，单击“操作”并选择“复制”。您也可以右键单击“配置”窗格中的策略并选择“复制”。

   将显示“复制”对话框。

3. 输入策略的新名称，然后单击“确定”。

   将复制策略，并在右侧窗格中显示一个“配置”屏幕。

4. 单击“保存策略”。

   将保存策略。

重命名 SRM 策略

可以重命名现有的 SRM 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择要重命名的策略，单击“操作”并选择“重命名”。您也可以右键单击“配置”窗格中的策略，然后选择“重命名”。

   将显示“重命名”对话框。

   注意：如果该策略正在使用中，则会显示一条错误消息，表示无法重命名策略。

3. 输入策略的新名称，然后单击“确定”。

   会出现一条确认消息，通知您已重命名策略。

4. 单击“保存策略”。

   将保存策略。

删除 SRM 策略

可以删除现有的 SRM 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择要删除的策略，单击“操作”并选择“删除”。您也可以右键单击“配置”窗格方中的策略，然后选择“删除”。

   注意：如果策略正在使用中，则会显示一条错误消息，表示无法删除该策略。

3. 将出现一条警告消息。单击“确定”确认删除。
4. 单击“保存策略”。

   将保存策略。

将测试添加到 SRM 策略中

可以将测试添加到 SRM 策略中。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“测试”并在“测试监视器”工具栏上单击“+ (新建)”。

   将显示“新建”对话框。

4. 在“测试名称”字段中，指定测试的唯一名称。名称必须小于等于 64 个字符。测试名称区分大小写。
5. （可选）输入测试的说明。
6. （可选）定义测试类别。
7. 在“测试类别”列表中单击所需的测试类型：

   Active Directory 用户

   确定 Windows Active Directory 服务运行正常，以管理共享文件和资源。

   自定义

   确定重要自定义服务或其他任务正在高效运行。

   DHCP

   确定动态主机配置协议服务器正在响应地址请求。

   DNS

   验证域名系统服务器是否正在处理主机名以处理解析请求。

文件 I/O

确定诸如读取、写入及比较操作可跨文件系统运行。

FTP 和 TFTP

确定用户可登录到指定服务器以上载和下载文件。

HTTP 和 HTTPS

确定用户可以连接到企业 Web 服务器，并确定网页上是否显示特定文本。

LDAP

验证与 LDAP 服务器的连接，以便验证用户请求和 LDAP 查询的访问权限。

NIS

验证正在处理 NIS 映射请求。

NNTP

验证用户可以连接到其 Usenet 新闻组服务器和公司布告栏。

Ping

确定网络设备存在并可在整个网络中访问。

电子邮件

确定电子邮件服务器可用并可有效地处理电子邮件。SRM 支持对 IMAP、MAPI、POP3、SMTP 以及从 SMTP 服务器发起的往返电子邮件的测试。

SNMP

确定 SNMP 代理正在响应 SNMPv1 GET 请求。

SQL 查询

确定 SQL 数据库服务器可用并正在处理短查询。

TCP

确定系统正在侦听并处理连接请求。

虚拟用户

获得实际用户事务（键盘输入和鼠标单击）的连续响应时间和可用性数据，可以对这些事务进行记录（通常使用 WinTask）以确认业务任务成功运行。

注意：有关每个测试类型的更多信息和定义，请参阅*《SRM 用户指南》*。

8. 在“测试间隔”字段中指定测试间的间隔（以秒为单位）。间隔必须是 30 秒的倍数。使用该选项来调整测试的性能。
9. 在“测试超时”字段中，指定经过多长时间后测试超时（以秒为单位）。选择一个小于间隔但是大于执行测试所需时间的数字。
10. 通过从“轮询间隔”列表中选择以下内容之一，设置轮询间隔：
    - 正常
    - 关
    - 慢放

    注意：有关详细信息，请参阅 *《SRM 用户指南》*
11. （可选）选中“保留历史数据”复选框
12. 单击“保存”将测试添加到策略中。

    将保存测试。
13. （可选）对任何其他测试重复该过程。
14. 单击“保存策略”。

    将保存策略。

详细信息：

修改 SRM 测试 (p. 245)
将阈值定义添加到 SRM 策略中 (p. 247)
修改 SRM 阈值定义 (p. 248)
定义 SRM 控制设置 (p. 248)

修改 SRM 测试

可以修改现有的 SRM 测试。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。
2. 在“可用策略”表中选择包含要修改的测试的策略。

   此时将出现“摘要”页。
3. 单击“测试”选项卡。

   此时将显示“测试监视器”页面。

4. 选择要修改的测试，单击“操作”，然后选择“修改”。

   将显示“编辑”对话框。

5. 根据需求修改测试，然后单击“保存”。

   将更新测试。

6. 单击“保存策略”。

   将保存策略。

复制 SRM 测试

您可以复制现有的 SRM 测试。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择包含要复制的测试的策略。

   此时将出现“摘要”页。

3. 单击“测试”选项卡。

   此时将显示“测试监视器”页面。

4. 选择要复制的测试，单击“操作”，然后选择“复制”。

   此时将显示复制对话框。

5. 输入 SRM 测试名称。

   将复制 SRM 测试。

删除 SRM 测试

可以删除现有的 SRM 测试。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择包含要删除的测试的策略。

   此时将显示“摘要”页面。

3. 单击“测试”选项卡。

   此时将显示“测试监视器”页面。

4. 选择要修改的测试，单击“操作”，然后选择“删除”。
5. 确认您的操作。

   将删除 SRM 测试。

将阈值定义添加到 SRM 策略中

可以将阈值定义添加到 SRM 策略中。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。
2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。
3. 单击“阈值”选项卡，然后单击“阈值监视器”工具栏上的“+ (新建)”。

   此时将显示“阈值监视器详细信息”对话框。
4. 配置以下阈值监视器设置：

   名称

   定义阈值监视器名称。

   属性

   指定要使用的属性。

   运算符

   指定要使用的运算符。

   警告值

   定义要使用的警告值。

   轻微值

   定义要使用的轻微值。

   重大值

   定义要使用的重大值。

   严重值

   定义要使用的严重值。

   致命值

   定义要使用的致命值。

5. 单击“保存”将阈值定义添加到策略中。

   将保存阈值定义。

6. 单击“保存策略”。

   将保存策略。

修改 SRM 阈值定义

可以修改现有的 SRM 阈值定义。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择包含要修改的阈值定义的策略。

   此时将出现“摘要”页。

3. 单击“阈值”选项卡。

   此时将显示“阈值监视器”页面。

4. 选择要修改的阈值定义，单击“操作”，然后选择“修改”。

   将显示“编辑”对话框。

5. 根据需求修改阈值定义，然后单击“保存”。

   将更新阈值定义。

6. 单击“保存策略”。

   将保存策略。

定义 SRM 控制设置

SRM 控制设置定义了通常在 svcrsp.cf 文件中控制的 AIM 行为的各方面，包括以下内容：

- 安全设置
- 日志级别
- 索引保留

在 SRM 策略中定义的控制设置会应用于向其应用策略的所有计算机。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击策略页面上的“控制设置”选项卡。

   此时将显示“控制”窗格。

4. 配置以下控制设置：

   最大线程数

   指定 jcollector 应用于执行测试的线程数

   日志级别

   指定 SRM AIM 的日志级别。默认值为“警告”。

   允许外部脚本

   指定是否允许执行外部脚本。

   允许执行文件 I/O 测试

   指定是否允许执行文件 I/O 测试。

   允许不信任的 SSL 证书

   指定是否允许没有信任 SSL 证书的站点的 SSL 测试。

   Java bin 位置

   定义 Java 可执行文件的位置。

   注意：在 AIX 上指定完整路径和二进制文件。

   覆盖环境中的 CLASSPATH

   定义要额外加载的类。如果已定义，覆盖环境中的 CLASSPATH。

   无收集器

   指定 SystemEDGE 是否应当启动 jcollector。

   绕过 JRE 内部缓存

   指定是否绕过 JRE 内部缓存。

   无 TOS 用于 IPv4 (HP-UX)

   指定是否禁用 TOS。

共享内存名称

定义共享内存的 ID。

保留的测试索引

定义保留的测试索引范围。

将定义控制设置。

5. 单击“保存策略”。

   将保存策略。

定义新的 SRM 测试定义模板

可以创建可导入到策略中的 SRM 测试定义模板。这使您可以在多个策略中重复使用测试，而无需多次设置测试。

定义新的 SRM 测试定义模板

1. 单击“资源”选项卡，打开“配置”窗格，展开“监控模板”，然后单击“服务响应”。

   此时将显示“服务响应”页面。

2. 在“测试模板列表”工具栏上单击“+ (新建)”。

   此时将显示“新建服务响应测试定义模板”对话框。

3. 输入测试定义模板的名称和可选说明和是否将基于现有模板，然后单击“确定”。

   将创建测试定义模板并显示“摘要”页面。要将测试添加到模板中，请参阅将测试添加到 SRM 策略中 (p. 243)部分。

4. 单击“保存模板”。

   将保存模板。

详细信息：

将测试定义模板导入到 SRM 策略中 (p. 250)
修改 SRM 测试定义模板 (p. 251)
复制 SRM 测试定义模板 (p. 252)
重命名 SRM 测试定义模板 (p. 252)
删除 SRM 测试定义模板 (p. 253)

将测试定义模板导入到 SRM 策略中

可以将测试定义模板导入到 SRM 策略中。

遵循这些步骤：

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“测试”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的测试监视器列表。

4. 单击“操作”，然后选择“导入”。

   此时将显示“导入模板向导”。

5. 从下拉列表中选择要导入的测试模板。
6. （可选）为每个导入的测试定义定义新的基本索引。
7. 从下拉列表中选择“冲突解决选项”，然后单击“下一步”。

   此时将显示“解决冲突”页面。

8. 复查所有测试定义冲突并调整索引，取消选中所有不应导入的测试定义，然后单击“下一步”。

   此时将出现“摘要”页。

9. 复查将要导入的测试定义，然后单击“完成”完成导入过程。
10. 单击“保存策略”。

    将保存策略。

修改 SRM 测试定义模板

可以修改 SRM 测试定义模板。

修改 SRM 测试定义模板

1. 打开“配置”窗格，展开“监控模板”，单击“服务响应”，然后展开“测试定义模板”。

   此时将显示“测试模板列表”，其中包含一列测试模板。

2. 选择要修改的“服务响应”测试模板。

   此时将显示该测试模板的“摘要”页面。

3. 单击“测试”选项卡，选择要修改的测试监视器，单击“操作”并选择“修改”。

   将显示“编辑”对话框。

4. 根据您的需求修改设置，然后单击“保存”。

5. 单击“保存模板”。

   将保存模板。

复制 SRM 测试定义模板

可以复制 SRM 测试定义模板。

复制 SRM 测试定义模板

1. 打开“配置”窗格，展开“监控模板”，单击“服务响应”，然后展开“测试定义模板”。

   此时将显示“测试模板列表”，其中包含一列测试模板。

2. 选择要复制的“服务响应”测试模板。

   此时将显示该测试模板的“摘要”页面。

3. 单击“测试”选项卡，选择要复制的测试，单击“操作”并选择“复制”。您也可以右键单击“配置”窗格中的测试模板，然后选择“复制”。

   将显示“复制”对话框。

4. 输入测试定义模板的新名称，然后单击“确定”。

   将复制该测试定义模板并将其显示在“测试模板”列表中。

重命名 SRM 测试定义模板

可以重命名 SRM 测试定义模板。

重命名 SRM 测试定义模板

1. 打开“配置”窗格，展开“监控模板”，单击“服务响应”，然后展开“测试定义模板”。

   此时将显示“测试模板列表”，其中包含一列测试模板。

2. 选择要重命名的“服务响应”测试模板。

   此时将显示该测试模板的“摘要”页面。

3. 单击“测试”选项卡，选择要重命名的测试，单击“操作”并选择“重命名”。您也可以右键单击“配置”窗格中的测试模板，然后选择“重命名”。

   将显示“重命名”对话框。

4. 输入测试定义模板的新名称，然后单击“确定”。

   此时将显示一条确认消息，通知您已重命名测试定义模板。

删除 SRM 测试定义模板

可以删除 SRM 测试定义模板。

删除 SRM 测试定义模板

1. 打开“配置”窗格，展开“监控模板”，单击“服务响应”，然后展开“测试定义模板”。

   此时将显示“测试模板列表”，其中包含一列测试模板。

2. 选择要删除的“服务响应”测试模板。

   此时将显示该测试模板的“摘要”页面。

3. 单击“测试”选项卡，选择要删除的测试，单击“操作”并选择“删除”。您也可以右键单击“配置”窗格中的测试模板，然后选择“删除”。

   将出现一条警告消息。

4. 单击“确定”确认删除。

   即会出现一条确认消息。此时将删除测试模板。

定义新的 SRM 阈值定义模板

可以创建可导入到策略中的 SRM 阈值定义模板。这使您可以在多个策略中重复使用阈值，而无需多次设置阈值。

定义新的 SRM 阈值定义模板

1. 打开“配置”窗格，展开“监控模板”，然后单击“服务响应”。

   此时将显示“服务响应”页面。

2. 在“阈值模板列表”工具栏上单击“+ (新建)”。

   此时将显示“新建服务响应阈值定义模板”对话框。

3. 输入阈值定义模板的名称和可选说明和是否将基于现有模板，然后单击“确定”。

   将创建阈值定义模板并显示“摘要”页面。要将阈值定义添加到模板中，请参阅将阈值定义添加到 SRM 策略中 (p. 247)部分。

4. 单击“保存模板”。

   将保存模板。

详细信息：

将阈值定义模板导入到 SRM 策略中

可以将阈值定义模板导入到 SRM 策略中。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“阈值”选项卡。

   此时将显示“摘要”页面，其中显示一个由策略管理的阈值监视器列表。

4. 单击“操作”，然后选择“导入”。

   此时将显示“导入模板向导”。

5. 从下拉列表中选择要导入的阈值模板。

6. 选择如何处理索引冲突，然后单击“下一步”。

   此时将显示“解决冲突”页面。

7. 复查所有阈值定义冲突，调整阈值定义名称，并取消选中所有不应导入的阈值定义，然后单击“下一步”。

   此时将出现“摘要”页。

8. 复查将要导入的阈值定义，然后单击“完成”完成导入过程。

9. 单击“保存策略”。

   将保存策略。

修改 SRM 阈值定义模板

可以修改 SRM 阈值定义模板。

修改 SRM 阈值定义模板

1. 打开“配置”窗格，展开“监控模板”，单击“服务响应”，然后展开“阈值定义模板”。

   此时将显示“阈值模板列表”，其中包含一列测试模板。

2. 选择要修改的“服务响应”阈值模板。

   此时将显示该测试模板的“摘要”页面。

3. 单击“阈值”，选择要修改的阈值监视器，单击“操作”并选择“修改”。

   此时将显示“阈值监视器详细信息”对话框。

4. 根据您的需求修改设置，然后单击“保存”。

5. 单击“保存模板”。

   将保存模板。

复制 SRM 阈值定义模板

可以复制 SRM 阈值定义模板。

复制 SRM 阈值定义模板

1. 打开“配置”窗格，展开“监控模板”，单击“服务响应”，然后展开“阈值定义模板”。

   此时将显示“阈值模板列表”，其中包含一列测试模板。

2. 选择要复制的“服务响应”阈值模板。

   此时将显示该阈值模板的“摘要”页面。

3. 单击“阈值”选项卡，选择要复制的阈值监视器，单击“操作”并选择“复制”。您也可以右键单击“配置”窗格中的阈值模板，然后选择“复制”。

   将显示“复制”对话框。

4. 输入阈值定义模板的新名称，然后单击“确定”。

   此时将复制阈值定义模板并将其显示在“阈值模板”列表中。

重命名 SRM 阈值定义模板

可以重命名 SRM 阈值定义模板。

重命名 SRM 阈值定义模板

1. 打开“配置”窗格，展开“监控模板”，单击“服务响应”，然后展开“阈值定义模板”。

   此时将显示“阈值模板列表”，其中包含一列阈值模板。

2. 选择要重命名的“服务响应”阈值模板。

   此时将显示该阈值模板的“摘要”页面。

3. 单击“阈值”选项卡，选择要重命名的阈值监视器，单击“操作”并选择“重命名”。您也可以右键单击“配置”窗格中的测试模板，然后选择“重命名”。

   将显示“重命名”对话框。

4. 输入阈值定义模板的新名称，然后单击“确定”。

   此时将显示一条确认消息，通知您已重命名阈值定义模板。

删除 SRM 阈值定义模板

可以删除 SRM 阈值定义模板。

删除 SRM 阈值定义模板

1. 打开“配置”窗格，展开“监控模板”，单击“服务响应”，然后展开“阈值定义模板”。

   此时将显示“阈值模板列表”，其中包含一列测试模板。

2. 选择要删除的“服务响应”阈值模板。

   此时将显示该阈值模板的“摘要”页面。

3. 单击“阈值”选项卡，选择要删除的阈值监视器，单击“操作”并选择“删除”。您也可以右键单击“配置”窗格中的阈值模板，然后选择“删除”。

   将出现一条警告消息。

4. 单击“确定”确认删除。

   即会出现一条确认消息。将删除阈值模板。

导入现有的 SRM 配置

将现有的 Service Availability (SA) 2.0 AIM 升级到 SRM 3.1.0 后，可以导入之前的 SA 2.0 配置，并将其转换为 SRM 3.1.0 策略。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”工具栏上单击 +（新建）。

   此时将显示“新建服务响应策略”对话框。

3. 单击“导入”，从列表中选择要导入策略的计算机，然后单击“确定”。

4. 输入名称和可选的说明，并且单击“确定”来完成导入过程。

5. 单击“保存策略”。

   将保存策略。

将策略应用于计算机

创建配置策略之后，将该策略应用于企业内的计算机。应用配置策略时，CA Virtual Assurance 将包含所有策略设置的已编译配置文件推送到所有指定的代理计算机。新策略将在自动代理热启动之后实施。

如果发生以下情况之一，可以将策略重新应用于计算机：

- 已更新策略。
- 收到通知，告知代理计算机上的配置已更改。

遵循这些步骤:

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后选择“SystemEDGE”或“服务响应”。

   此时将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 选择要应用的策略。

   将在右侧窗格中显示策略详细信息。

4. 单击“操作”，然后选择“应用”。

   此时将出现用于选择要在其中应用策略的计算机的选项卡。使用“更新运行该策略的计算机”选项卡可以将策略应用于已经运行该策略的计算机。使用“应用于未运行该策略的计算机”选项卡，可以将策略应用于不使用任何策略或使用其他策略的计算机。

5. （可选）从“更新运行该策略的计算机”选项卡，执行以下选项之一：

   - 选择“使用该策略更新所有计算机”，在当前运行该策略的所有计算机上部署该策略。如果进行了希望全局应用的配置策略更改，则该选项十分有用。
   - 选择“更新所选的计算机组”，仅更新满足以下任意条件的计算机：
     - 运行该策略过期版本的计算机
     - 已应用策略例外的计算机
     - 运行该策略当前版本的计算机
     - 该策略存在配置错误的计算机

     选择这些选项中的任意一个。当用户将点配置更改应用于不在应用的策略中表示的代理时，将发生策略异常。
   - 选择“高级(手动选择计算机)”，以在“选择计算机”窗格中手工添加要将策略重新应用到的计算机。

6. （可选）从“应用于未运行该策略的计算机”选项卡中选择要向其应用策略的计算机。

7. 单击“应用策略”。

   此时将启动策略应用程序。

查看策略应用进度

可以逐个详细查看每个策略的策略应用操作的进度。

遵循这些步骤:

1. 选择“资源”选项卡，打开“配置”窗格，展开“策略”，然后选择“SystemEDGE”或“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“受管计算机”选项卡。

   将出现“受管计算机”页面，其中显示当前运行该策略的计算机的列表，您可以查看配置状态。

4. （可选）单击“查看例外”。

   此时将显示“策略例外”窗格，通过该窗格可以查看自上次应用策略以来已应用于系统的 SNMP 集。

   注意：该屏幕仅可用于 SystemEDGE 策略。

5. （可选）单击“查看配置”。

   此时将显示“策略配置”页面，通过该页面可以查看为代理交付的配置文件。

6. （可选）单击“查看错误”。

   将显示“策略错误”窗格。如果无法成功应用策略，则可在策略被拒绝时查看代理返回的错误列表。

配置和查看已应用的策略

通过“策略”功能，您可以管理应用于单个服务器、服务器组或服务的策略和模板。可以执行以下操作：

- 更新策略和模板
- 查看自上一策略或模板应用程序以来的异常。
- 查看策略配置
- 查看策略错误
- 批量更新策略
- 删除模板

遵循这些步骤:

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 选择一个系统或服务。单击“资源”页面，然后单击“监控软件”。

   此时将显示“计算机详细信息”页面。

3. 单击“策略”。

   “策略”页面显示 SystemEDGE 和 SRM 策略以及 SystemEDGE 模板的列表。

   注意：“筛选”将显示处于“挂起”、“已交付”（成功）、“已配置”和“失败”状态的分层模板的列表。

4. 您可以批量更新策略和模板。在“策略和模板”表中，选择要批量更新的策略或模板并单击“操作”，然后选择以下选项之一：

   - 批量更新 SystemEDGE 策略。
   - 批量更新服务响应策略。
   - 批量更新 SystemEDGE 模板。
   - 批量删除模板

   注意：如果要将策略应用于单个服务器，则系统会提示您输入策略名称。

   策略的批量更新：

   在选定的策略应用于服务组时，您可以选择要应用策略的计算机。

   模板的批量更新：

   通过某个对话框可以从“可用的模板”中选择模板。在选择模板之后，单击下列选项之一：

   将现有配置替换为选定模板

   删除应用于所有计算机的现有模板，并将选定模板应用于所有计算机。

   将选定模板附加于现有配置

   添加选定模板。如果任何选定模板已经作为计算机配置的一部分被应用，则重新应用这些模板。

   批量删除模板：

   删除应用于计算机的现有模板。

5. 单击“应用策略”以将策略或模板应用于计算机。

   在“策略”页面上，您可以查看应用于计算机的策略或模板的进度。

6. （可选）单击“查看配置”图标。

   此时将显示“策略配置”页面。对于配有模板的计算机，它会显示“策略和模板”以及 SystemEDGE 配置文件。对于配有服务响应监视器的计算机，它还显示服务响应监视器配置文件。

7. 单击“保存策略”。

   将保存策略。

将策略还原回早期的版本

可以将策略还原回早期的版本。

遵循这些步骤：

1. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后选择“SystemEDGE”或“服务响应”。

   将显示“可用策略”页面。

2. 在“可用策略”表中选择策略。

   将显示策略的“摘要”页面。

3. 单击“版本”选项卡。

   此时将显示“版本”页面。

4. 在表中选择要还原到的版本并单击“使其成为当前版本”。

   将显示一条消息。单击“确定”。将创建新版本的策略并显示“摘要”页面。

5. （可选）您可以获得该版本的新副本。在“可用策略”表中选择版本，然后单击“复制”。

   将显示“复制”对话框。

6. 输入策略的新名称，然后单击“确定”。

   将复制策略并将其添加到“配置”窗格中的策略树中。此时将显示新副本的摘要页面。

7. 单击“保存策略”。

   将保存策略。

指定新实例的默认策略

可以为所有新发现的实例设置一个默认策略。如果未在 SystemEDGE 或 SRM 的安装或部署期间指定策略，或如果指定的策略不可用，将传送策略。

指定默认策略

1. 打开“配置”窗格，展开“策略”，然后选择“SystemEDGE”或“服务响应”。

   将显示“可用策略”页面。

2. 在“默认策略”部分中，从“默认策略”下拉列表中选择要使用的策略，然后单击“应用”

   将应用默认策略。

如何更改 SystemEDGE 的配置模式

在某些情况下，可能需要更改 SystemEDGE 的配置模式。下图提供了更改配置模式所需操作的概述。

如何更改 SystemEDGE 的配置模式

请执行以下步骤：

查看要求

在更改 SystemEDGE 的配置模式之前，请查看以下要求。

- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您对 CA SystemEDGE 有基本了解。
- 可以访问包括监控代理 (CA SystemEDGE) 的 CA Virtual Assurance 管理器安装。
- 可以在受管节点上访问监控代理 (CA SystemEDGE)。
- 您可以访问 CA Virtual Assurance 用户界面。
- CA Virtual Assurance 已发现所有相关系统。

查看受管模式和未受管模式详细信息

考虑以下术语：在此方案中，在 SystemEDGE 配置的上下文中使用术语“未受管模式”和“受管模式”。

未受管模式

不通过 CA Virtual Assurance“策略配置”管理特定服务器上的 SystemEDGE 配置。可编辑 sysedge.cf 文件以修改配置。

受管模式

通过 CA Virtual Assurance“策略配置”管理特定服务器上的 SystemEDGE 配置。在 CA Virtual Assurance 管理器上的“策略配置”中指定 SystemEDGE 配置，并将其分配到网络中适当的服务器。如果在本地编辑 sysedge.cf 文件，CA Virtual Assurance 将使用下一个策略分发覆盖更改。

考虑将影响 SystemEDGE 配置模式的以下情况：

- 如果从产品介质运行典型 SystemEDGE 安装，SystemEDGE 将配置为在安装后以未受管模式运行。
- 如果从产品介质运行自定义 SystemEDGE 安装，则可以指定用于受管模式的管理器系统。如果已指定管理器系统，且 CA Virtual Assurance 在安装后发现 SystemEDGE，SystemEDGE 将自动注册到“策略”配置，并且 SystemEDGE 将以受管模式运行。
- 如果使用“远程部署”在远程系统上安装 SystemEDGE，则可以在部署作业中指定 SystemEDGE 的配置模式。默认值为受管模式。

重要信息！ “浏览”窗格显示“受管”和“未受管”文件夹，其中列出了 CA Virtual Assurance 已轮询（受管）或未轮询（未受管）的已发现服务器。该属性与 SystemEDGE 配置的受管或未受管模式不同。“浏览”窗格中服务器的受管或未受管状态对 SystemEDGE 的配置模式没有影响。SystemEDGE 配置文件中的特定条目表示 SystemEDGE 的配置模式。

验证 SystemEDGE 的当前配置模式

下列步骤介绍了确定 SystemEDGE 配置模式的方法。

下列术语用于所有这些用例：

静态 sysedge.cf 文件

标识安装程序规定的文件，位于 *Installed_Dir*\SystemEDGE\config 目录中。

默认值:

Windows：C:\Program Files\CA\SystemEDGE\config

UNIX/Linux：/opt/CA/SystemEDGE/config

动态 sysedge.cf 文件

标识正在进行的 SystemEDGE 配置文件，位于 *Data_Dir*\port<*number*> 目录中。

默认值:

Windows：C:\Users\Public\CA\SystemEDGE\port161

UNIX/Linux：/opt/CA/SystemEDGE/config/port161

遵循这些步骤:

1. 登录到运行要确定其配置模式的 SystemEDGE 的服务器。
2. 切换到 SystemEDGE 的“data”目录，然后打开 port<*number*> 目录。在 Windows 上，可以从 SystemEDGE“控制面板”的“data”目录中打开 sysedge.cf 文件。

   注意：“data”目录中的动态 sysedge.cf 文件与“config”目录中的静态 sysedge.cf 文件不同。
3. 在 port<*number*> 目录中打开动态 sysedge.cf 文件。

   如果 SystemEDGE 以受管模式运行，则第一行指定控件值 (ctrl_value)。

   示例：

   ```
   ctrl_value 0x9e30d00e

   # Generated file - DO NOT EDIT
   #
   # Configuration file generated on 2012:03:27 05:37
   #
   # Generated from default.generic.0.prof
   #
   版本 5.7
   ```

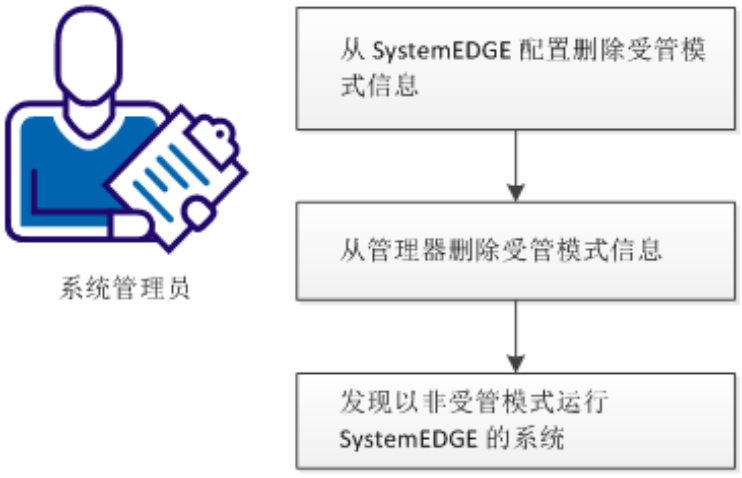
   如果 SystemEDGE 以未受管模式运行，则第一行指定版本。

   示例：

   ```
   版本 5.7
   ```

如何将 SystemEDGE 从受管模式更改为未受管模式

下图提供了更改为未受管模式所需操作的概述。



请执行以下步骤：

从 SystemEDGE 配置删除受管模式信息 (p. 266)
从管理器删除受管模式信息 (p. 267)
发现运行处于未受管模式的 SystemEDGE 的系统 (p. 267)

从 SystemEDGE 配置删除受管模式信息

以下过程介绍了如何从特定服务器上的 SystemEDGE 配置删除受管模式信息。

遵循这些步骤:

1. 登录到要在其上更改 SystemEDGE 配置模式的服务器。
2. 在方便的位置创建下列备份目录：

   ```
   data.backup
   config.backup
   ```

3. 使用正常机制停止 SystemEDGE。
4. 导航到 SystemEDGE 的“data”目录，然后打开 port<*number*> 目录。默认目录为 port161。

   列出了目录内容。

5. 将以下文件移动到 data.backup 目录，以使其不再显示在 port<*number*> 目录中：

   ```
   .sysedge.id
   sysedge.cf
   ```

6. 更改到 SystemEDGE 的“config”目录。

   列出了目录内容。

7. 将以下文件复制到 config.backup 目录：

   ```
   sysedge.cf
   ```

8. 导航到“config”目录，在文本编辑器中打开 sysedge.cf 文件，并向下滚动到文件底部。
9. 删除以下行：

   ```
   manager_name <hostname of the manager>
   ```

10. 保存文件并启动 SystemEDGE。

    SystemEDGE 将在“data”目录中创建不具有任何受管模式信息的 sysedge.cf 文件。

从管理器删除受管模式信息

以下过程介绍了如何从特定服务器上的 SystemEDGE 配置删除受管模式信息。

遵循这些步骤:

1. 登录到 CA Virtual Assurance 用户界面，并转到“管理”。

   此时将打开“资源”选项卡，并显示“浏览”窗格。

2. 在“搜索”字段中输入已在其上修改了 SystemEDGE 配置的服务器的名称，然后单击  （搜索）。

   此时将打开“搜索”窗口，并列出搜索结果。

3. 单击搜索结果之一。

   此时将打开该特定服务器的资源页，并显示“快速启动”面板。

4. 单击“从系统删除”。

   服务器将从“浏览”窗格消失。将在管理器上删除所有与服务器相关的对象，包括受管模式信息。

发现运行处于未受管模式的 SystemEDGE 的系统

以下过程介绍了如何重新发现在未受管模式下运行的服务器。

遵循这些步骤:

1. 登录到 CA Virtual Assurance 用户界面，并转到“管理”。

   此时将打开“资源”选项卡，并显示“浏览”窗格。

2. 右键单击“数据中心”，并依次选择“管理”、“发现”、“服务器”。

   此时将打开“发现”窗口。

3. 输入已在上一步骤中删除的服务器名称，然后单击“完成”。

   CA Virtual Assurance 发现 SystemEDGE 以未受管模式运行的服务器。

   CA Virtual Assurance 完成发现后，已发现的服务器上的 SystemEDGE 尚未在“策略配置”中注册。SystemEDGE 以未受管模式运行。

4. 双击“浏览”窗格中的服务器名称。

   将打开该服务器的资源页。

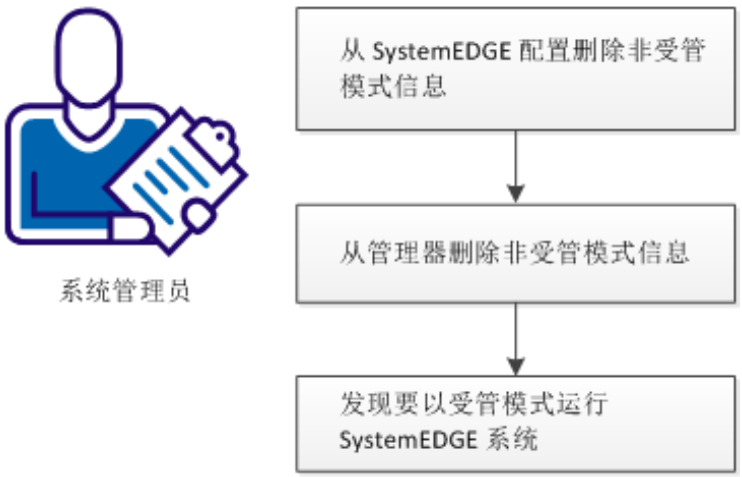
5. 切换到“摘要”选项卡以确认 CA Virtual Assurance 是否已正确发现服务器。如有必要，可选择 CA Virtual Assurance 用来监控服务器的不同 SNMP 团体。

   现在，可通过编辑 sysedge.cf 配置文件配置该服务器上的 SystemEDGE。

如何将 SystemEDGE 从未受管模式更改为受管模式

下图提供了更改为受管模式所需操作的概述。

如何将 SystemEDGE 从非受管模式更改受管模式



请执行以下步骤：

从 SystemEDGE 配置删除未受管模式信息 (p. 268)
从管理器删除未受管模式信息 (p. 269)
发现要在受管模式下运行 SystemEDGE 的系统 (p. 270)

从 SystemEDGE 配置删除未受管模式信息

以下过程介绍了如何从特定服务器上的 SystemEDGE 配置删除未受管模式信息，并准备服务器以更改为受管模式。

遵循这些步骤:

1. 登录到要在其上更改 SystemEDGE 配置模式的服务器。
2. 在方便的位置创建下列备份目录：

   ```
   data.backup
   config.backup
   ```

3. 使用正常机制停止 SystemEDGE。

4. 导航到 SystemEDGE 的“data”目录，然后打开 port<*number*> 目录。默认目录为 port161。

   列出了目录内容。

5. 将以下文件移动到 data.backup 目录，以使其不再显示在 port<*number*> 目录中：

   ```
   sysedge.cf
   ```

6. 更改到 SystemEDGE 的“config”目录。

   列出了目录内容。

7. 将以下文件复制到 config.backup 目录：

   ```
   sysedge.cf
   ```

8. 导航到“config”目录，在文本编辑器中打开 sysedge.cf 文件，并向下滚动到文件底部。

9. 添加以下行：

   ```
   manager_name <hostname of the manager>
   ```

10. 保存文件并启动 SystemEDGE。

    SystemEDGE 将在“data”目录中创建 sysedge.cf 文件。

从管理器删除未受管模式信息

以下过程介绍了如何从特定服务器上的 SystemEDGE 配置删除未受管模式信息。

遵循这些步骤:

1. 登录到 CA Virtual Assurance 用户界面，并转到“管理”。

   此时将打开“资源”选项卡，并显示“浏览”窗格。

2. 在“搜索”字段中输入已在其上修改了 SystemEDGE 配置的服务器的名称，然后单击  （搜索）。

   此时将打开“搜索”窗口，并列出搜索结果。

3. 单击搜索结果之一。

   此时将打开该特定服务器的资源页，并显示“快速启动”面板。

4. 单击“从系统删除”。

   服务器将从“浏览”窗格消失。将在管理器上删除所有与服务器相关的对象。

发现要在受管模式下运行 SystemEDGE 的系统

以下过程介绍了如何重新发现导致 SystemEDGE 在受管模式下运行的服务器。

遵循这些步骤:

1. 登录到 CA Virtual Assurance 用户界面，并转到“管理”。

   此时将打开“资源”选项卡，并显示“浏览”窗格。
2. 右键单击“数据中心”，并依次选择“管理”、“发现”、“服务器”。

   此时将打开“发现”窗口。
3. 输入已在上一步骤中删除的服务器名称，然后单击“完成”。

   CA Virtual Assurance 发现服务器。

   CA Virtual Assurance 完成发现后，已发现的服务器上的 SystemEDGE 已在“策略配置”中注册。SystemEDGE 以受管模式运行。
4. 双击“浏览”窗格中的服务器名称。

   将打开该服务器的资源页。
5. 切换到“摘要”选项卡以确认 CA Virtual Assurance 是否已正确发现服务器。如有必要，可选择 CA Virtual Assurance 用来监控服务器的不同 SNMP 团体。

验证 SystemEDGE 配置模式

基本上可以重复“验证当前配置模式” (p. 264)中的步骤。

如果 SystemEDGE 以未受管模式运行，则“data”目录中动态 sysedge.cf 文件的第一行指定版本。

示例

```
release 5.7.1
```

如果 SystemEDGE 以受管模式运行，则第一行指定控件值 (ctrl_value)。

示例

```
ctrl_value 0x9e30d00e

# Generated file - DO NOT EDIT
#
# Configuration file generated on 2012:03:27 05:37
#
# Generated from default.generic.0.prof
#
release 5.7.1
```

在发现过程中，其他元信息已添加到动态 sysedge.cf 文件的末尾。

示例

```
template data_directory <path>
data_directory "C:\Users\Public\CA\SystemEDGE\"
template default_port CA Portal
default_port 161
template manager_name <name>
manager_name manager_server.mycompany.com
template manager_policy_name <policy>
manager_policy_name default.generic
template manager_policy_version <version>
manager_policy_version 1
```

详细信息：

验证 SystemEDGE 的当前配置模式 (p. 264)

第 6 章： 管理虚拟环境

此部分包含以下主题：

Cisco UCS

Cisco Unified Computing System (Cisco UCS) 是 Cisco 数据中心解决方案。该解决方案将两个互联结构交换机与多达两个交换机、40 个机箱和 320 个刀片服务器相集成。在交换机上运行的 Cisco UCS 管理器向网络、存储和刀片服务器提供管理功能，同时也支持虚拟化。CA Virtual Assurance 与 Cisco UCS 交互作用，以便查询包括硬件资源、运行状况和设备统计信息在内的 UCS 设备信息。CA Virtual Assurance 支持使用 UCS AIM 和 PMM 的 Cisco UCS。有关 Cisco UCS 界面及其操作的信息，请参阅 Cisco UCS 文档。

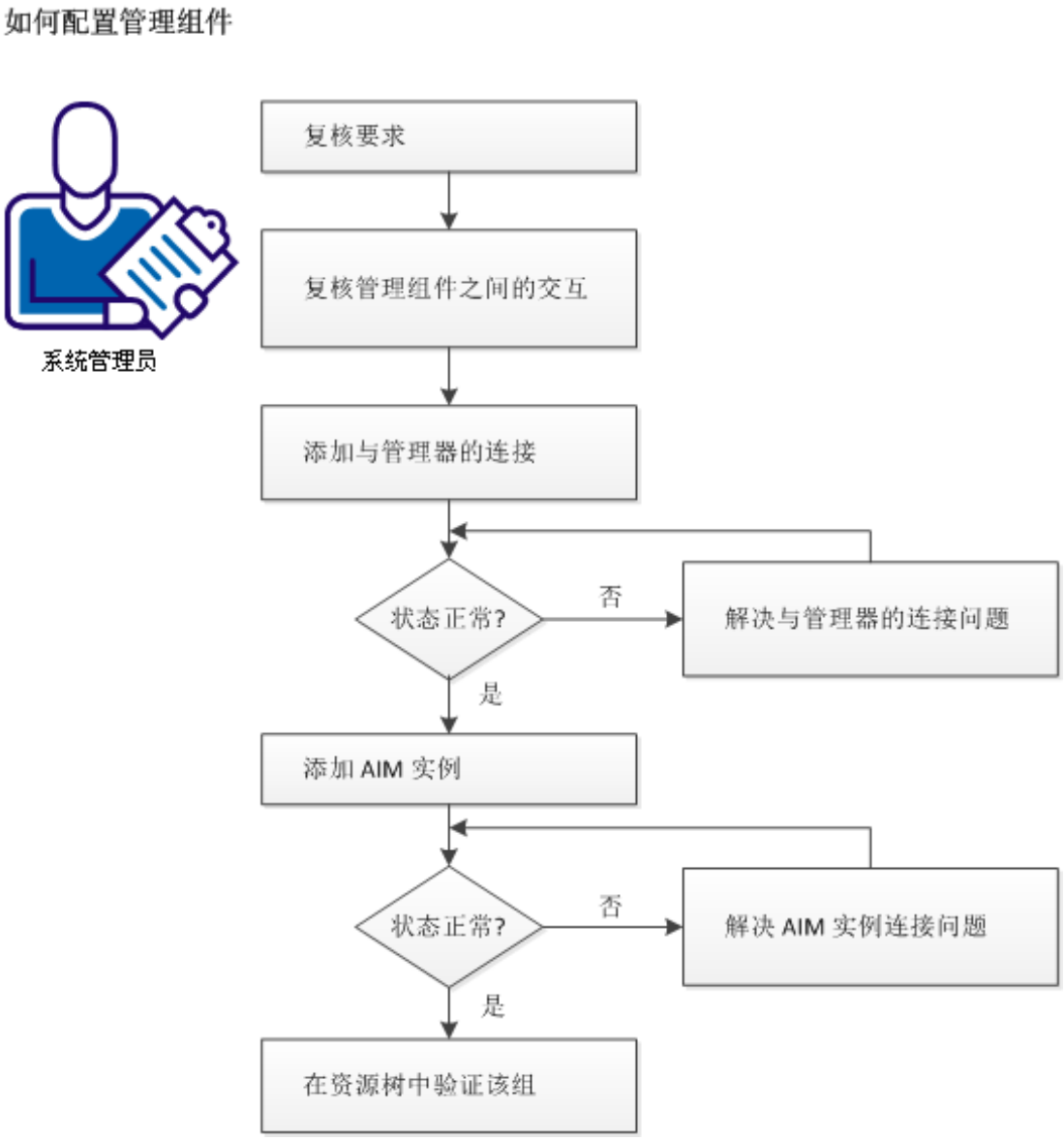
管理员可使用“管理”用户界面或 dpmutil CLI 命令注册 UCS 管理器。如果 dpmutil 已使用，则运行 nodecfgutil.exe 来配置 UCS AIM。

注意：有关 CLI 命令的信息，请参阅 *《参考指南》*。

详细信息：

如何配置 Cisco UCS 管理组件

下图提供了有关配置管理组件所需操作的概述。该图包括针对连接问题的相应故障排除策略。



在交换机上运行的 Cisco UCS 管理器向网络、存储和刀片服务器提供管理功能，同时也支持虚拟化。

CA Virtual Assurance 与 Cisco UCS 交互作用，以便查询包括硬件资源、运行状况和设备统计信息在内的 UCS 设备信息。CA Virtual Assurance 支持使用 UCS AIM 和 PMM 的 Cisco UCS。

请执行以下步骤：

查看要求

在配置 CA Virtual Assurance 的管理组件之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您熟悉 CA Virtual Assurance 和 SystemEDGE。
- 您可以访问包括以下内容的 CA Virtual Assurance 管理器安装：
  - 平台管理模块 (PMM)
  - Application Insight Module (AIM)
  - 监控代理 (SystemEDGE)
- 您可以访问 CA Virtual Assurance 用户界面。
- 您具有有效的凭据（用户名和密码），可访问要管理的环境中的服务器。
- 您知道使用哪个协议（HTTP 或 HTTPS）和端口，以通过 Web 服务访问环境中的服务器。默认：HTTPS，端口：443。
- 您已验证环境中的服务器运行正常。
- 如果将 PMM 和 AIM 安装在不同系统上，请确认 PMM 和 AIM 系统上的 SNMP 设置一致。读和写团体字符串以及 SNMP 端口号必须是相同的。
- 您已验证 CA Virtual Assurance 管理器已发现您要使用的远程 AIM 服务器。

详细信息：

Cisco UCS 服务器 (p. 276)

Cisco UCS 服务器

验证 Cisco UCS 管理的以下条件：

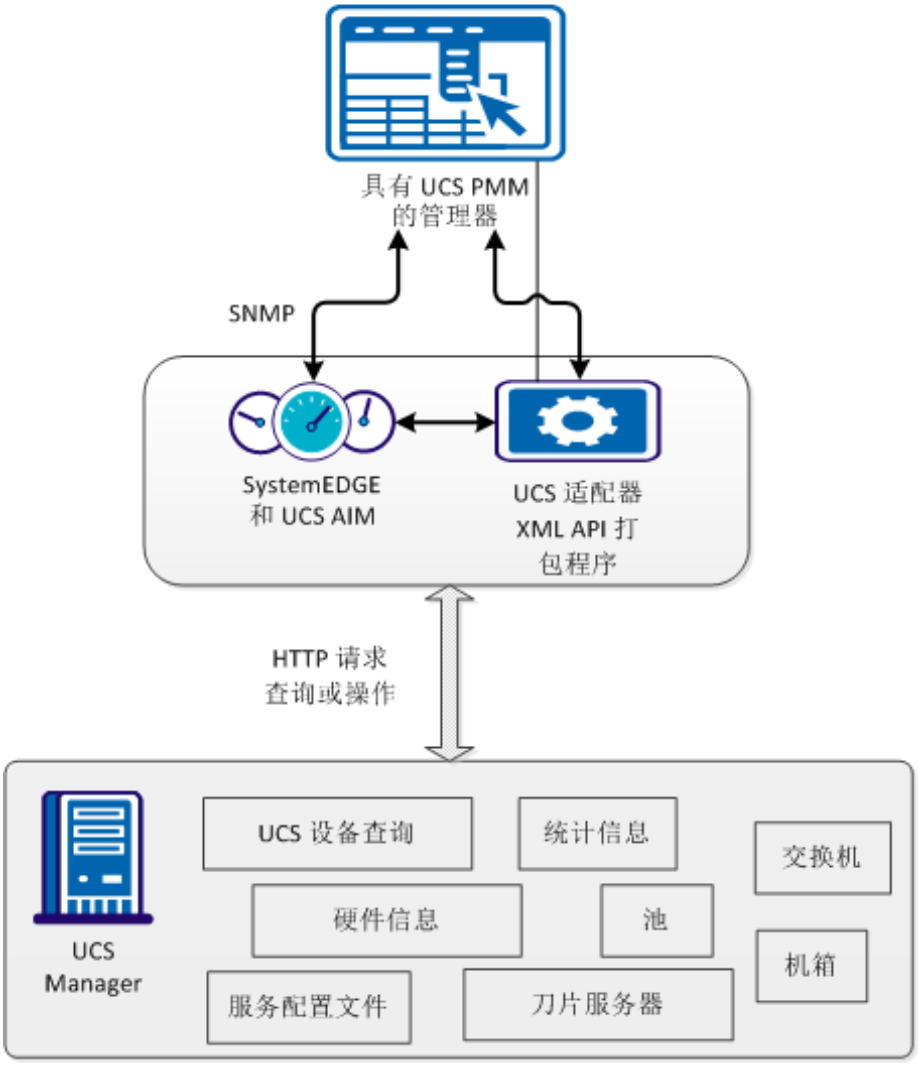
- 启动 Cisco Java 用户界面，以验证 Cisco UCS 管理器是否正在运行。启动 Cisco Java 用户界面的链接是 http://<UCS_Manager_name> 或 https://<UCS_Manager_name>。

Cisco UCS 管理组件之间的交互

Cisco UCS 集成要求适用于 SystemEDGE 的 UCS AIM 提供 SNMP Get/Set 请求，从而检索 UCS 设备和统计数据，然后配置设备。此外，UCS 平台管理模块 (PMM) 也查询 UCS 设备和统计信息，并且将数据存储在管理数据库中。Cisco 提供了 XML API 以便与 Cisco UCS 管理器进行交互。

通过 API，CA Virtual Assurance 可以访问硬件、统计信息、池（UUID、MAC、WWPN、WWNN）以及 UCS 管理器的服务配置文件信息。

Cisco UCS 管理组件之间的交互



上图显示了 Cisco UCS 的集成组件。UCS 适配器和 Cisco UCS 管理器之间的通信协议是 HTTP 或 HTTPS。

此外，XML API 还提供配置特定设备属性和执行池和服务配置文件管理的功能。池和服务配置文件管理是 CA Virtual Assurance 跨多个 UCS 管理器管理以检测池范围冲突的用例之一。

将 Cisco UCS 添加到管理器

可以使用用户界面的“管理”页面添加 Cisco UCS 管理器服务器。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“Cisco UCS”。
3. 在 Cisco UCS 窗格工具栏上单击 （添加）。

   此时将显示“添加 Cisco Unified Computing System 服务器”对话框。

4. 输入所需的连接数据（服务器名称、用户、密码、端口），指定首选 AIM，并启用“受管状态”（复选框）。
5. 输入必要的服务器标识信息，然后单击“确定”。

   如果网络连接已成功建立，服务器会添加到右上角的窗格并带有绿色状态图标。

   注意：如果连接失败，将显示“验证失败”对话框。单击“是”，CA Virtual Assurance 将服务器添加到列表中并带有红色状态图标。如果您单击“否”，将不添加任何内容。

管理器到服务器的连接失败

症状：

在“管理”、“配置”下添加服务器连接后，对服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的服务器连接数据是否仍然有效。如有必要，请更新连接数据。
- 验证服务器系统是否正在运行并且可以访问。
- 验证连接所需的所有服务是否在服务器系统上运行良好。

更新服务器连接数据：

1. 单击与失败的连接关联的 （添加）或 （编辑）。
2. 添加连接详细信息，启用“受管状态”，然后单击“确定”。

   将更新连接数据。
3. 单击右上角的 （验证）以验证新设置。

   如果无法建立与服务器的连接，请继续执行下一步骤。

验证服务器系统是否正在运行并且可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```
2. 要确定服务器是否具有有效的 DNS 条目和 IP 地址，请检查这些命令的输出。

   如果服务器不在 DNS 中，请将服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。
3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress <Server Name>
   ```

   输入正确的 IP 地址和服务器名称并保存文件。例如：

   ```
   192.168.50.50 myServer
   ```
4. 切换到 CA Virtual Assurance 用户界面、“管理”选项卡、“配置”、“服务器”窗格，并单击右上角的 （验证）。

   即使服务器凭据和连接数据正确并且您可以 ping 服务器，连接仍然可能失败。在这种情况下，可能是服务器引起该问题。如果无法建立与服务器的连接，请继续执行下一步骤。

验证连接所需的所有服务是否在服务器系统上运行良好。

1. 要访问服务器，请联系系统管理员。
2. 登录到服务器系统。
3. 验证连接所需的所有服务是否运行良好。
4. 如有必要，请启动或重新启动服务。
5. 切换到管理器系统上的 CA Virtual Assurance 用户界面、服务器窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证服务器连接。

   如果与服务器的连接失败，请验证根据该方案的要求收集的数据是否有效。

   与管理员或技术支持合作，解决服务器连接问题。

注册 UCS AIM 服务器

将 Cisco UCS 组件添加到 CA Virtual Assurance 管理器后，使用用户界面的“管理”页面添加 AIM 实例，以管理 Cisco UCS 环境。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“Cisco UCS”。
3. 在“UCS AIM 服务器”窗格工具栏上单击 （添加）。

   此时将显示“添加 Cisco Unified Computing System AIM 服务器”对话框。

4. 从下拉列表中选择“UCS AIM 服务器”。

   此时将显示 UCS AIM 服务器的列表。

5. 从下拉列表中选择“Cisco UCS 服务器”。

   CA Virtual Assurance 使用 Cisco UCS 窗格中列出的服务器填充“Cisco UCS 服务器”下拉列表。您只能管理 CA Virtual Assurance 管理器为之建立了有效连接的 UCS 服务器。

   注意：如果 AIM 位于远程系统中，则 CA Virtual Assurance 一定会首先发现该系统。发现之后，AIM 服务器将显示在下拉列表中。

6. 单击“确定”。

   将注册选定服务器的新 AIM 实例。

   注意：如果实例未处于错误或已停止状态，CA Virtual Assurance 将开始发现关联的环境。发现过程完成后，您可以开始管理 Cisco UCS 环境。

排除 AIM 实例连接的故障

如果 AIM 连接处于未就绪状态，将出现以下状态图标之一：

 发现正在进行

 无轮询

 错误

 警告

 已禁用

 未知

有关 AIM 实例状态的详细信息，请参阅工具提示。以下故障排除部分提供了用于解决该问题的详细信息和步骤。

AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为服务器添加 AIM 实例后，状态图标显示  （发现正在进行）。

解决方案：

等到环境的发现过程完成。发现持续时间取决于与环境中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示指示未完成发现请求数量的工具提示。发现作业完成时，CA Virtual Assurance 会向资源树中添加一个服务器文件夹。然后，您可以开始管理您的环境。

AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （无轮询）。

解决方案：

关联实例不需要特定的操作。此图标表示 CA Virtual Assurance 管理器不轮询此 AIM。AIM 不是首选。

如果多个 AIM 已配置为管理特定服务器，PMM 将选择其中一个 AIM 作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决可能导致与 AIM 连接失败的最常见问题：

- 验证是否可以访问 AIM 服务器。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 确认命令的输出对于 AIM 服务器有有效的 DNS 条目和 IP 地址。

   如果 AIM 服务器不在 DNS 中，则将 AIM 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ipaddress servername

   输入正确的 IP 地址和 AIM 服务器名称。例如：

   192.168.50.51 myAIM

4. 在“AIM 服务器”窗格的右上角，单击 （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“AIM 服务器”窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证 AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否有效。

AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 AIM 实例之后，几个实例的状态图标显示 （已禁用）。该 AIM 实例未受管理。

如果 CA Virtual Assurance 发现具有以下关系的 AIM，则显示该状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的服务器配置了 AIM。
- AIM 连接到未配置的服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的服务器连接并将其受管状态更改为已启用。

验证资源树中的 Cisco UCS

在成功配置和发现之后，新发现的资源将在“资源”、“浏览”窗格中的相应组下列出。

遵循这些步骤:

1. 单击“资源”，然后打开“浏览”窗格。
2. 扩展 Cisco UCS 组。

   此时将显示受管的 Cisco UCS 资源。

CA Virtual Assurance 现在已准备好管理配置的 Cisco UCS 环境。

Cisco UCS 管理

通过与 Cisco UCS 的 CA Virtual Assurance 集成，您可以从一个集中的用户界面来管理 UCS 交换机、机箱和刀片服务器。您可以从交换机上运行的 UCS 管理器中查看 UCS 资源并执行管理操作（如克隆、快照、电源操作等）。

本节介绍可以在“资源”页面的 Cisco UCS 资源上执行的资源管理操作。“资源”页面显示有关以下 UCS 对象的基本信息：

- Cisco UCS 服务器
- UCS 管理器服务器
- 机箱
- 刀片服务器
- 构造互连
- 组织

通过“摘要”页面，您可以查看与该对象相关联的信息（例如，机箱摘要可以显示其刀片服务器，刀片服务器摘要可以显示其存储），以及与资源相关联的事件。

如果可用，“详细信息”页面使您可以查看其他资源信息，如系统属性、软件、硬件、性能等。在此处指定自动化源之后，将自动为系统创建默认的访问和管理配置文件并运行发现。

其他页面可用来执行资源管理任务。也可以通过“浏览”窗格对象的右键单击菜单来执行 UCS 管理任务。

详细信息：

如何使用集中式服务配置文件

驻留在 CA Virtual Assurance 管理数据库 中的中央服务配置文件提供了跨多个 UCS 域管理配置信息的有效方式。使用 CA Virtual Assurance 用户界面，将服务配置文件从 UCS 管理器导入到 管理数据库 中，或在 管理数据库 中创建中央服务配置文件。

在 管理数据库 中，可以将中央服务配置文件导出到任意 UCS 管理器。

管理中心服务配置文件

您可以从“资源”页面中管理中心服务配置文件。要进行访问，请在“浏览”窗格中选择“Cisco UCS 服务器”，然后单击右侧窗格中的“中心服务配置文件”。

从 UCS 管理器导入服务配置文件

1. 单击空心三角形（导入）图标。
2. 使用“导入服务配置文件”对话框选择 UCS 管理器。单击“刷新”以填充“服务配置文件”列表，然后选择“导入所有服务配置文件”，或者从列表中选择一个或多个服务配置文件。要在导入之后从 UCS 管理器中删除导入的配置文件，请选择“删除源服务配置文件”。
3. 单击“确定”。

   选定的服务配置文件将导入到 管理数据库 中。

在 管理数据库 中创建或更新中心服务配置文件

1. 单击 +（创建）图标或选择中心服务配置文件，然后单击工具（编辑）图标。
2. 使用向导页面创建或更新中心服务配置文件。

   注意：在 管理数据库 中创建服务配置文件时无法指定池和策略；此信息仅供参考。将中央服务配置文件导出到 UCS 管理器后，可以指定此信息。
3. 创建或更新服务配置文件后，单击“完成”。

将服务配置文件导出到 UCS 管理器

1. 选择一个或多个中心服务配置文件
2. 单击蓝色三角形（导出）图标。

   此时将显示“导出服务配置文件”对话框。
3. 在“可用 UCS 管理器”列表中，选择一个 UCS 管理器，然后单击向右箭头，将其传输到“选定的 UCS 管理器”列表。单击双右箭头可传输所有管理器。
4. 单击“确定”。

   注意：不会导出池和策略；它们必须已驻留在目标 UCS 管理器上。

从 管理数据库 中删除服务配置文件

1. 选择要删除的服务配置文件。
2. 单击 -（删除）图标。

服务配置文件

*服务配置文件*包含 Cisco UCS 硬件方面的配置信息，包括接口、光纤连接及网络和服务器身份。您可以为特定 UCS 管理器创建服务配置文件或者在 CA Virtual Assurance 管理数据库 中集中创建。可将 UCS 管理器上的服务配置文件*导入*到 管理数据库，也可从中将服务配置文件*导出*到其他 UCS 管理器。

使用服务配置文件，可从操作系统提取支持的 Cisco UCS 硬件。通过添加或删除服务配置文件，可使服务联机或脱机。通过将服务配置文件从一个刀片服务器再分配到另一个刀片服务器，可将一组服务（操作系统和应用程序）移动到其他服务器。

服务配置文件信息可包括：

- 按设备 UUID 或虚拟 UUID 池划分的刀片服务器
- 本地存储、RAID 或 SAN（HBA、WWNN 和 WWNN 池）的任意配置中的存储空间
- 网络（MAC、vNIC 0、vNIC 1 及 MAC 池）
- 服务器启动顺序或其他策略
- 服务器分配类型（稍后分配、预先开通插槽、开通现有服务器、从池中选择服务器）

如何创建或更新服务配置文件

CA Virtual Assurance 提供了一个向导，管理员可以使用该向导创建服务配置文件，您可以使用预定义的策略选项更新服务配置文件。系统、网络和存储管理员可以协作来使用唯一身份特征以及必要的连接特征创建服务配置文件。

服务配置文件向导提供了 Cisco UCS 管理器接口的子集，以便利用 Cisco 环境中的知识和经验。

示例：创建服务配置文件

使用 CA Virtual Assurance 用户界面选择“创建服务配置文件”选项，然后指定要创建的服务器配置文件名称以及选择服务器配置文件是否满足以下条件：

- 基于硬件
- 具有默认网络和存储连接的简单服务器配置文件
- 基于现有服务配置文件模板
- 必须是明确创建的自定义服务配置文件

基于选定的选项，向导将引导您完成访谈过程以获得必要的身份和连接信息。您可以接受默认信息或明确指定身份 (UUID)、网络 (MAC/VLAN)、存储 (WWN/vHBA) 和引导策略信息。

将服务配置文件与刀片服务器关联

服务配置文件可以与刀片服务器关联、取消关联或设置为在故障切换时应用。

调整 UCS 服务配置文件

1. 右键单击并选择“策略”。

   此时将显示“策略”子菜单。
2. 右键单击并依次选择“策略”、“操作和规则”。

   将出现“操作和规则”页面。
3. 单击“操作”。

   将出现“操作”页面。
4. 单击 +（添加新操作）。

   将显示“操作定义: 新操作”页面。
5. 在“类型”下拉列表上单击操作类型“配置服务配置文件”。

   将显示“配置服务配置文件”表单。
6. 指定要对其应用服务配置文件的 UCS 资源详细信息。选择配置文件操作。

   注意：如果需要服务台核准，请输入所需信息。
7. 在“操作”下拉菜单上单击“保存”。

   此时将修改服务配置文件关系。

详细信息：

配置服务配置文件：Cisco UCS (p. 624)

如何管理端口配置文件

使用以下过程来使用 CA Virtual Assurance 管理端口配置文件。

1. 导出插件。

   要在 Cisco UCS 管理器和 vCenter 之间建立通信，请按如下方式在目标 vCenter 中生成并安装一个或多个扩展 XML 文件：

   - 对于 vCenter 4.0，需要多个扩展文件。
   - 对于 vCenter 4.0 更新 1 版本及更高版本，从 Cisco UCS 管理器导出单个扩展文件。

   导出所需的文件后，使用 vSphere Client 将这些文件作为新插件导入到 vCenter 中。这是每个 UCS 管理器和 vCenter 组合的一时需求，Cisco UCS 管理器无法使用从不同 UCS 管理器导出的文件。

2. 将 .vib 文件导出到 ESX 服务器。

   根据 ESX 版本，通过安装 Cisco Nexus 1000V 虚拟以太网模块软件中的相应 .vib 文件组件来配置 ESX 服务器。此软件包（由 Cisco 和 VMware 联合设计）提供与 VMware 虚拟基础架构完全集成的分布式虚拟交换机解决方案。

3. 创建端口配置文件网络拓扑结构 (p. 291)
4. 创建端口配置文件和端口配置文件客户端 (p. 291)

创建端口配置文件网络拓扑结构

要将端口配置文件推送到 VMware，Cisco UCS 管理器必须已定义 vCenter、数据中心、DVS 文件夹、DVS 和配置文件客户端对象。这些对象的拓扑结构必须与 VMware 中的拓扑结构匹配。通过 CA Virtual Assurance，您可以创建所需的拓扑结构。

遵循这些步骤:

1. 单击“资源”，然后打开“浏览”窗格。
2. 在“浏览”树中右键单击 UCS 管理器，然后单击 VMware 以启动“vCenter 布局”对话框
3. 展开 vCenter 并突出显示 vCenter、数据中心、DVS 文件夹、DVS 或配置文件客户端对象。
4. 在“操作”下拉菜单中选择“新建”。
5. 输入所需的信息，然后单击“完成”。在“DVS”面板上选择“启用”会自动将关联的端口配置文件推送到 vCenter。

   将添加 vCenter、数据中心、DVS 文件夹、DVS 或配置文件客户端对象。

注意：要使用该对话框来删除拓扑结构对象，请选择“操作”下拉菜单上的“删除”。

创建端口配置文件和端口配置文件客户端

可以使用“CA Virtual Assurance vCenter 布局”对话框来创建端口配置文件和端口配置文件客户端。

遵循这些步骤:

1. 在“浏览”树中右键单击 UCS 管理器，然后单击 VMware 以启动“vCenter 布局”对话框。
2. 突出显示端口配置文件以创建端口配置文件，或突出显示现有端口配置文件以创建端口配置文件客户端。
3. 在“操作”下拉菜单中选择“新建”。
4. 输入所需的信息，然后单击“确定”。

   将创建端口配置文件或端口配置文件客户端。

注意：也可以使用该程序来编辑或删除端口配置文件和端口配置文件客户端。突出显示现有端口配置文件或端口配置文件客户端，然后选择“操作”下拉菜单上的“编辑”或“删除”。

配置 SNMP 数据轮询器

SNMP 数据轮询器从 UCS AIM 中检索 CISCO 设备信息。轮询元素包括：

- 交换机
- 机箱（风扇、PSU）
- 刀片服务器（主要逻辑板、内存）
- 电源使用情况
- 温度

设置轮询时间间隔

1. 如下所示编辑 \conf\caucsconf.cfg 文件：

   ```
   <property name="CONFIG_KEY_UCS_AIM_POLL_INTERVAL">
       <!-- UCS AIM polling interval -->
       <value>300</value>
       <displayName>UCS AIM Polling Interval</displayName>
       </property>
   ```

2. 保存文件。

配置服务轮询器

*服务轮询器*直接从 UCS 管理器检索池和服务配置文件信息。轮询元素包括：

- UUID 池
- MAC 池
- 全球节点名称 (WWNN) 池
- 全球端口名称 (WWPN) 池
- 服务器池
- 服务配置文件

默认服务轮询间隔为 300 秒。

重置轮询间隔

1. 如下所示编辑 \conf\caucsconf.cfg 文件：

   ```
   <property
   name="CONFIG_KEY_UCS_SERVICE_POLL_INTERVAL">
       <!-- UCS service interval in seconds -->
       <value>300</value>
       <displayName>UCS Manager Polling Interval</displayName>
       </property>
   ```

2. 保存文件。

查看 Cisco UCS 资源

通过“资源”页面，您可以在 UCS 对象树中查看任何级别的 UCS 资源。例如，您可以检查以下要确定的对象：

- Cisco UCS 服务器－按类别、刀片服务器分配和导入的服务配置文件分类的 UCS 资源
- 集中式服务配置文件－UCS 管理器任务、导入和导出
- UCS 管理器－构造互连、机箱和组织
- 机箱－已安装的刀片服务器数目、风扇数目（及其状态）及输入/输出模块
- 刀片服务器－刀片服务器数目（无论打开还是关闭，也无论是否与服务配置文件关联）和 OS 主机名

  注意：在“浏览”树中展开刀片服务器可看到 OS 主机。在开通和发现完成后，用于刀片服务器的 OS 主机名将可用。
- 单个刀片服务器－高级清单，包括主板、CPU、内存及存储
- 构造互连－高级硬件和风扇
- 组织－池、服务配置文件和服务配置文件模板

查看 Cisco UCS 资源

1. 单击“资源”。

   此时将显示“资源”页面。
2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。
3. 查找并选择 Cisco UCS 资源。

   此时资源页面会出现在右侧窗格中。

将服务配置文件与刀片服务器关联

服务配置文件可以与刀片服务器关联、取消关联或设置为在故障切换时应用。

调整 UCS 服务配置文件

1. 右键单击并选择“策略”。

   此时将显示“策略”子菜单。
2. 右键单击并依次选择“策略”、“操作和规则”。

   将出现“操作和规则”页面。
3. 单击“操作”。

   将出现“操作”页面。
4. 单击 +（添加新操作）。

   将显示“操作定义: 新操作”页面。
5. 在“类型”下拉列表上单击操作类型“配置服务配置文件”。

   将显示“配置服务配置文件”表单。
6. 指定要对其应用服务配置文件的 UCS 资源详细信息。选择配置文件操作。

   注意：如果需要服务台核准，请输入所需信息。
7. 在“操作”下拉菜单上单击“保存”。

   此时将修改服务配置文件关系。

详细信息：

配置服务配置文件：Cisco UCS (p. 624)

备份 UCS 管理器配置

CA Virtual Assurance 支持备份以下类型的 UCS 管理器配置信息：

- 完全状态
- 所有配置
- 系统配置
- 逻辑配置

导出/导入功能模仿 Cisco UCS 功能，并允许您创建和重新运行备份作业。

导出 UCS 管理器配置

1. 单击“资源”。

   此时将显示“资源”页面。
2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。
3. 选择 Cisco UCS 管理器。

   “UCS 管理器”页面会出现在右侧窗格中。
4. 单击“导出/导入”。

   此时将显示“导出/导入”页。
5. 在“导出作业”部分，单击 +（创建）。

   将出现“创建备份操作”对话框。
6. 输入导出信息，然后单击“确定”。

   导出作业启动并显示在“导出”列表中。

导入 UCS 管理器配置

1. 单击“资源”。

   此时将显示“资源”页面。
2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。
3. 选择 Cisco UCS 管理器。

   “UCS 管理器”页面会出现在右侧窗格中。
4. 单击“导出/导入”。

   此时将显示“导出/导入”页。
5. 在“导入作业”部分，单击 +（创建）。

   将出现“创建备份操作”对话框。

6. 输入导入信息，然后单击“确定”。

   导入作业启动并显示在“导入”列表中。

vNIC 模板

CA Virtual Assurance 支持创建和管理 vNIC 模板。您可以指定模板目标作为服务配置文件或 VM。

要创建 vNIC 模板，在“服务配置文件”向导中选择“使用 vNIC 模板”，启动“创建 vNIC 模板”对话框。您也可以在“浏览”窗格中右键单击 UCS 组织。

UCS 组织

您可以使用组织分组相关的 UCS 资源，从而为 UCS 资源管理创建一个包括池、服务配置文件和服务配置文件模板的嵌套的分级结构。可以创建和删除组织及子组织。

详细信息：

创建子组织 (p. 297)

创建子组织

您可以在 UCS 根树上创建组织或子组织。

添加组织

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

   导航到根，或打开根并单击子组织

3. 右键单击根或子组织以选择“管理”、“创建子组织”。
4. 使用“创建子组织”对话框创建新的子组织。

   子组织已创建。

UCS 池

CA Virtual Assurance 使您可以创建池，从而更高效地管理 UCS 资源。

注意：如果池范围发生冲突，则会显示一个警告。

提供以下类型的池：

- UUID 池
- MAC 池
- 全球节点名称 (WWNN) 池
- 全球端口名称 (WWPN) 池
- 服务器池

WWNN 和 WWPN 池可以用于配置刀片服务器，以使用远程存储 (SAN)。

详细信息：

查看 UCS 池 (p. 298)
创建 UCS 池 (p. 299)
对 UCS 池进行重命名 (p. 300)
删除 UCS 池 (p. 301)

查看 UCS 池

通过“资源”页面，您可以查看 UCS 池。

查看 UCS 池

1. 单击“资源”。
   此时将显示“资源”页面。
2. 打开“浏览”窗格。
   将出现可用的组、服务和系统。
3. 单击 UCS 组织树顶端的根，并导航到所需的组织。
4. 单击“摘要”。
   此时将出现“摘要”页。
5. 在“组件”部分中，单击下拉菜单中所需的池类型。
6. 选择要查看的池，然后单击工具（视图）图标。
7. 单击“取消”返回到“池”列表。

创建 UCS 池

通过“资源”页面，您可以创建 UCS 池，以更高效地管理 UCS 资源。

创建资源池

1. 单击“资源”。

   此时将显示“资源”页面。
2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。
3. 单击 UCS 组织树顶端的根，并导航到所需的组织。
4. 单击“摘要”。

   此时将出现“摘要”页。
5. 在“组件”部分中，单击下拉菜单中所需的池类型。
6. 单击 +（添加新池）。

   将出现“创建池”对话框。
7. 使用该对话框完成定义。

   已将池添加到池列表。

注意：您可以自定义“快速启动”菜单以提供相应的功能。

对 UCS 池进行重命名

通过“资源”页面，您可以对 UCS 池进行重命名。

对 UCS 池进行重命名

1. 单击“资源”。

   此时将显示“资源”页面。
2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。
3. 单击 UCS 组织树顶端的根，并导航到所需的组织。
4. 单击“摘要”。

   此时将出现“摘要”页。
5. 在“组件”部分中，单击下拉菜单中所需的池类型。
6. 选择要重命名的池。
7. 单击双箭头图标 (>>)。

   “重命名池”对话框出现。
8. 使用该对话框对池进行重命名。

   列表中的池已重命名。

删除 UCS 池

通过“资源”页面，您可以删除 UCS 池。

删除 UCS 池

1. 单击“资源”。

   此时将显示“资源”页面。
2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。
3. 单击 UCS 组织树顶端的根，并导航到所需的组织。
4. 单击“摘要”。

   此时将出现“摘要”页。
5. 在“组件”部分中，单击下拉菜单中所需的池类型。
6. 选择要删除的池。
7. 单击 -（删除）图标。

   将出现“删除”确认信息。
8. 单击“是”。

   池即被删除。

UCS 操作类型

Cisco UCS 资源可以使用 CA Virtual Assurance 操作类型创建新的操作，这些新的操作可在满足分配的规则条件时自动进行 UCS 电源、资源分配和其他操作。还可以排定这些操作在特定时间发生。

UCS 陷阱管理

UCS PMM 侦听 UCS 陷阱指示。所有 UCS 陷阱都作为事件转发。

要将 UCS 陷阱转发到默认端口 162 上的陷阱接收器，请配置 SystemEDGE。

创建刀片服务器电源操作

您可以定义执行刀片服务器电源操作的操作。

创建刀片服务器电源操作

1. 单击“资源”，然后打开“浏览”窗格。
2. 选择“数据中心”节点，然后单击“策略”。
3. 单击“操作”。

   将出现“操作”页面。
4. 单击 +（添加新操作）。

   将显示“操作定义: 新操作”页面。
5. 在“类型”下拉列表上单击“配置电源”。
6. 在“环境”下拉列表上单击“Cisco UCS”。

   将显示“配置电源”表单。
7. 通过选择包含刀片服务器的 UCS 管理器和机箱指定要执行电源操作的刀片服务器。
8. 选择电源操作，然后在“操作”下拉菜单上单击“保存”。

   此时将创建刀片服务器电源操作。

详细信息：

配置电源：Cisco UCS (p. 616)

删除 UCS 服务器

可以使用用户界面的“管理”页面删除 Cisco UCS 服务器。

删除 UCS 服务器

1. 单击“管理”。
   此时将显示“管理”页面。
2. 在“配置”窗格的“开通”部分中，单击“Cisco UCS”。
   此时将显示“Cisco UCS”页面。
3. 选择要删除的服务器。
4. 单击服务器工具栏上的 -（删除）。
   将出现一条确认提示消息。
5. 单击“确定”。
   服务器已删除。

删除 UCS AIM

您可以使用用户界面的“管理”页面删除 UCS AIM。

删除 UCS 服务器

1. 单击“管理”。
   此时将显示“管理”页面。
2. 在“配置”窗格的“开通”部分中，单击“Cisco UCS”。
   此时将显示“Cisco UCS”页面。
3. 选择要删除的 UCS AIM 服务器。
4. 单击服务器工具栏上的 -（删除）。
   将出现一条确认提示消息。
5. 单击“确定”。
   UCS AIM 服务器已删除。

Citrix XenServer

Citrix XenServer 是一个虚拟化平台，该平台为虚拟化服务器和客户端操作系统提供接近裸机的虚拟化性能。XenServer 使用 Xen 管理程序来虚拟化装有该管理程序的每个服务器，以便每个服务器可以使用保证的性能同时托管多个虚拟机 (VM)。XenServer 使用其自身的操作系统来管理 XenServer 主机的物理和虚拟资源，因此，不需要特定的操作系统。XenServer 支持 Linux 和 Windows 来宾操作系统。

XenServer 资源可分为以下三个级别进行管理：

主机管理

*XenServer 主机*对象代表运行 XenServer 及其 VM 的物理主机。XenServer 主机可以是独立主机，也可以与 XenServer 池关联。您可以监控 XenServer 主机上可用的虚拟和物理资源、管理包含虚拟磁盘映像的存储库、管理任务，或以维护模式运行 XenServer 主机。

资源池管理

*资源池*是最多为 16 台 XenServer 主机的连接组。与共享存储以及动态控制的内存、CPU 和网络资源结合，资源池中的 XenServer 主机提供 VM 运行所在的操作环境。您可以管理池中 XenServer 主机的成员身份或角色，并且可以允许 XenServer 监控池成员的运行状况以获得高可用性。如有必要，VM 在池主机之间进行实时迁移以避免停机。

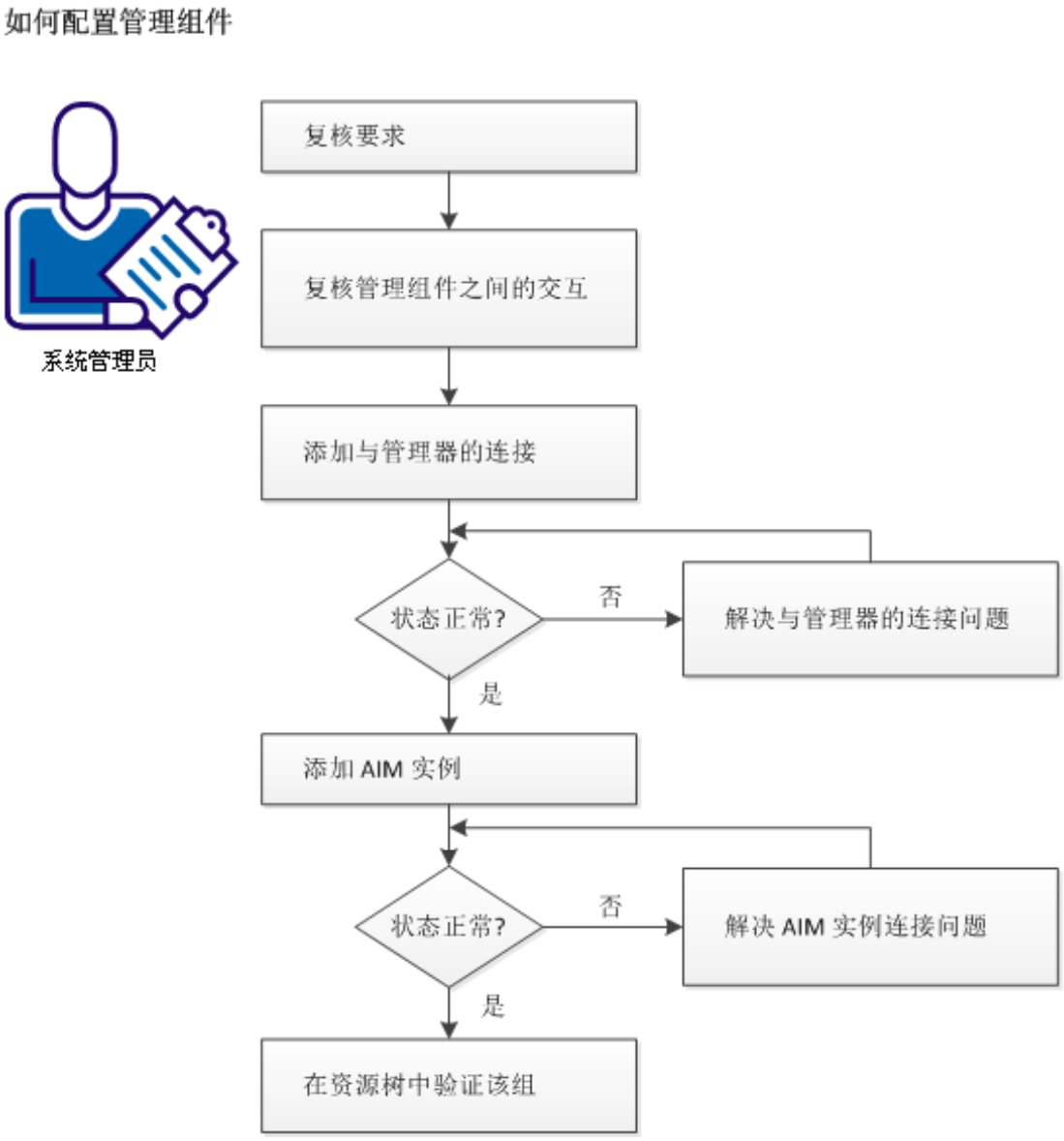
虚拟机管理

在 VM 管理级别上，可以执行以下任务：

- 控制 VM（发现、启动、挂起、关闭、从磁盘删除）
- 管理 VM（克隆）

如何配置 XenServer 管理组件

下图提供了有关配置管理组件所需操作的概述。该图包括针对连接问题的相应故障排除策略。



请执行以下步骤：

查看要求

在配置 CA Virtual Assurance 的管理组件之前，请查看以下要求：

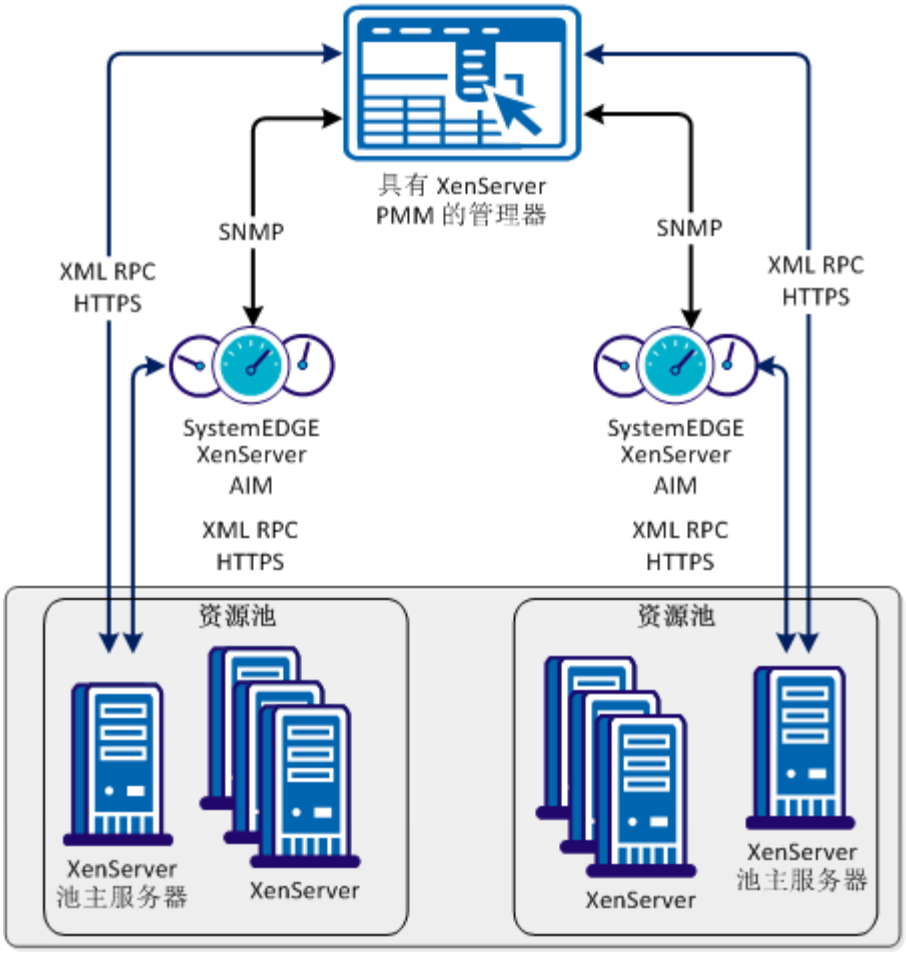
- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您熟悉 CA Virtual Assurance 和 SystemEDGE。
- 您可以访问包括以下内容的 CA Virtual Assurance 管理器安装：
  - 平台管理模块 (PMM)
  - Application Insight Module (AIM)
  - 监控代理 (SystemEDGE)
- 您可以访问 CA Virtual Assurance 用户界面。
- 您具有有效的凭据（用户名和密码），可访问要管理的环境中的服务器。
- 您知道使用哪个协议（HTTP 或 HTTPS）和端口，以通过 Web 服务访问环境中的服务器。默认：HTTPS，端口：443。
- 您已验证环境中的服务器运行正常。
- 如果将 PMM 和 AIM 安装在不同系统上，请确认 PMM 和 AIM 系统上的 SNMP 设置一致。读和写团体字符串以及 SNMP 端口号必须是相同的。
- 您已验证 CA Virtual Assurance 管理器已发现您要使用的远程 AIM 服务器。

Citrix XenServer 管理组件之间的交互

将 Citrix XenServer AIM 作为多实例、远程 AIM 实施。CA Citrix XenServer AIM 可远程监控多个独立 Citrix XenServer 和 Citrix XenServer 资源池。将 Citrix XenServer AIM 作为 x86 和 x64 模块实施。

Citrix XenServer 的管理 API 基于 XML RPC。对于 Citrix XenServer 资源池，所有的 XML RPC 通信仅在 AIM、PMM 和池主服务器之间发生。

XenServer 管理组件之间的交互



将 Citrix XenServer 连接添加到管理器中

您可以使用 CA Virtual Assurance 用户界面的“管理”选项卡来添加 Citrix XenServer 连接。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“Citrix XenServer”。
3. 在“注册的 Citrix XenServer”窗格工具栏上单击  （添加）。

   此时将显示“添加 Citrix XenServer”对话框。

4. 输入所需的连接数据（服务器名称、用户名、密码、资源池 UUID），指定首选 AIM，并启用“受管状态”（复选框）。

   重要信息!验证是否已将池主服务器添加到已注册的 Citrix XenServer 中。

5. 单击“确定”。

   如果网络连接已成功建立，服务器会添加到右上角的窗格并带有绿色状态图标。CA Virtual Assurance 自动发现 Citrix XenServer 系统。

   如果连接失败，将显示“验证失败”对话框。如果您单击“是”，CA Virtual Assurance 会将服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。

服务器连接到管理器失败 (Citrix XenServer)

症状：

在“管理”、“配置”下添加服务器连接后，对服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的服务器连接数据是否仍然有效。如有必要，请更新连接数据。
- 验证服务器系统是否正在运行并且可以访问。
- 验证服务器系统中的管理服务是否正常运行。

更新服务器连接数据：

1. 单击与失败的连接关联的  （添加）或  （编辑）。
2. 添加连接详细信息，启用“受管状态”，然后单击“确定”。

   将更新连接数据。
3. 单击右上角的  （验证）以验证新设置。

   如果无法建立与服务器的连接，请继续执行下一步骤。

验证服务器系统是否正在运行并且可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```
2. 验证命令的输出，以确定服务器是否具有有效的 DNS 条目和 IP 地址。

   如果服务器不在 DNS 中，请将服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。
3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress <Server Name>
   ```

   输入正确的 IP 地址和服务器名称。例如：

   ```
   192.168.50.50 myServer
   ```
4. 单击右上角的  （验证）。

   即使服务器凭据和连接数据正确并且您可以 ping 服务器，连接仍然可能失败。在这种情况下，可能是服务器引起该问题。如果无法建立与服务器的连接，请继续执行下一步骤。

验证服务器系统中的管理服务是否正常运行：

1. 联系管理员来访问服务器系统。
2. 登录到服务器系统并执行 xsconsole 命令。

   此时将启动服务控制控制台。
3. 验证服务的状态并解决所有报告的问题。
4. 切换到管理器系统上的 CA Virtual Assurance 用户界面、服务器窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证服务器连接。

   如果与服务器的连接失败，请验证根据该方案的要求收集的数据是否仍然有效。

   与管理员或技术支持合作，解决服务器连接问题。

添加发现的 Citrix XenServer AIM 实例

将 Citrix XenServer 连接添加到 CA Virtual Assurance 管理器后，添加 AIM 实例以管理 Citrix XenServer。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。
2. 从左侧窗格的“开通”部分中选择“Citrix XenServer”。
3. 在“发现的 Citrix XenServer AIM 实例”窗格工具栏上单击 （添加）。

   此时将显示“添加 Citrix XenServer AIM”对话框。
4. 从下拉列表中选择“Citrix XenServer AIM 服务器”。

   将显示发现的 XenServer AIM 服务器的列表。如果您已在本地系统上安装了 XenServer AIM，本地系统的名称也会显示在列表中。
5. 从下拉列表中选择 Citrix XenServer。

   CA Virtual Assurance 将向 XenServer 下拉列表中填充“注册的 Citrix XenServer”窗格中列出的 XenServer。您只能管理您的 CA Virtual Assurance 管理器与之建立了有效连接的那些 XenServer。

   注意：如果 AIM 位于远程系统中，则 CA Virtual Assurance 一定会首先发现该系统。在发现之后，AIM 服务器将在下拉列表中显示。
6. 单击“确定”。

   将添加选定的服务器的新 AIM 实例。如果实例未处于错误或已停止状态，CA Virtual Assurance 将开始发现关联的环境。当发现过程完成时，您可以开始管理您的 Citrix XenServer 环境。

排除 AIM 实例连接的故障

如果 AIM 连接处于未就绪状态，将出现以下状态图标之一：

- 发现正在进行
- 无轮询
- 错误
- 警告
- 已禁用
- 未知

有关 AIM 实例状态的详细信息，请参阅工具提示。以下故障排除部分提供了用于解决该问题的详细信息和步骤。

AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为服务器添加 AIM 实例后，状态图标显示（发现正在进行）。

解决方案：

等到环境的发现过程完成。发现持续时间取决于与环境中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示指示未完成发现请求数量的工具提示。发现作业完成时，CA Virtual Assurance 会向资源树中添加一个服务器文件夹。然后，您可以开始管理您的环境。

AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示（无轮询）。

解决方案：

关联实例不需要特定的操作。此图标表示 CA Virtual Assurance 管理器不轮询此 AIM。AIM 不是首选。

如果多个 AIM 已配置为管理特定服务器，PMM 将选择其中一个 AIM 作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决可能导致与 AIM 连接失败的最常见问题：

- 验证是否可以访问 AIM 服务器。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 确认命令的输出对于 AIM 服务器有有效的 DNS 条目和 IP 地址。

   如果 AIM 服务器不在 DNS 中，则将 AIM 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress servername
   ```

   输入正确的 IP 地址和 AIM 服务器名称。例如：

   ```
   192.168.50.51 myAIM
   ```

4. 在“AIM 服务器”窗格的右上角，单击  （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“AIM 服务器”窗格，并单击右上角的  （验证）。

   CA Virtual Assurance 将验证 AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否有效。

AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 AIM 实例之后，几个实例的状态图标显示  （已禁用）。该 AIM 实例未受管理。

如果 CA Virtual Assurance 发现具有以下关系的 AIM，则显示该状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的服务器配置了 AIM。
- AIM 连接到未配置的服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的服务器连接并将其受管状态更改为已启用。

验证资源树中的 Citrix XenServer 组

在成功配置和发现之后，新发现的资源将在“资源”、“浏览”窗格中的相应组下列出。

遵循这些步骤:

1. 单击“资源”，然后打开“浏览”窗格。
2. 展开 Citrix XenServer 组。

   将显示受管的 Citrix 资源池。
3. 展开“资源池”条目。

   将显示受管的 Citrix XenServer。

CA Virtual Assurance 现在已准备好管理配置的 Citrix XenServer 环境。

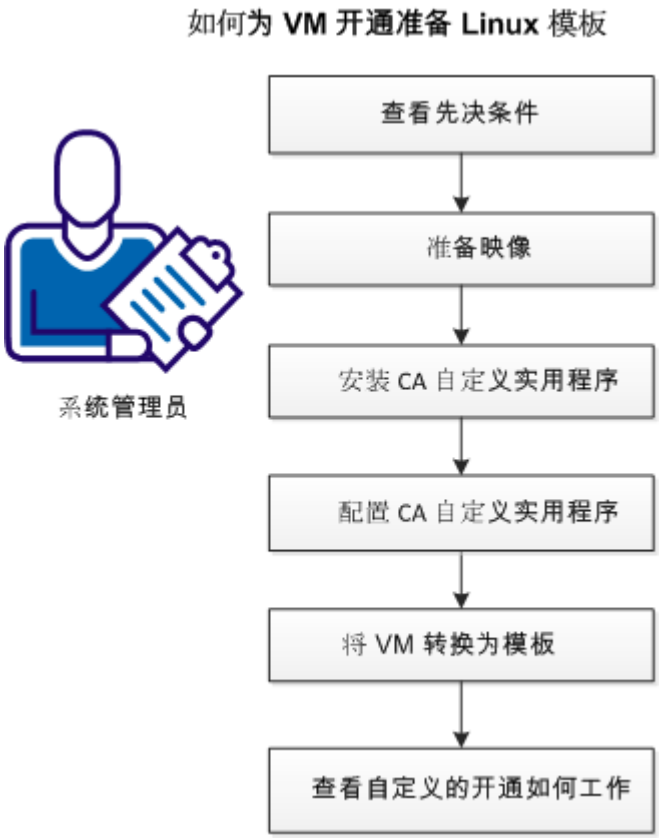
如何为 XenServer 开通准备 Linux 模板

CA Virtual Assurance 支持运行以下操作系统的新虚拟机 (VM) 的自定义开通：

- Red Hat Enterprise Server 6.0
- SUSE Linux Enterprise Server 11

自定义选项包括主机名、密码、域或网络配置。

下图说明了系统管理员如何为 VM 开通准备 Linux 模板。



请执行以下步骤：

自定义 VM 开通的先决条件 (p. 315)
准备 Linux 映像 (XenServer) (p. 316)
安装 CA 自定义实用工具 (p. 316)
配置 CA 自定义实用工具 (p. 317)
将虚拟机转换为模板 (p. 317)
自定义的开通如何工作 (p. 318)

自定义 VM 开通的先决条件

要自定义 Linux 来宾，需要具有对文件系统或控制台的直接访问权限。

对于 XenServer 环境，确保满足下列先决条件：

- 资源池中的每个 XenServer 必须已启用 SSH 或 SFTP 访问。

准备 Linux 映像 (XenServer)

在创建包含 Linux 操作系统的模板之前，可通过遵循此步骤来准备映像。根据 Linux 分发包，具体步骤可能会有所不同。

遵循这些步骤:

1. 在新虚拟机上从头开始安装 Linux 操作系统。
2. 在虚拟计算机上安装适用于 Citrix XenServer 的 XenTools。
3. 应用您想在新虚拟机上应用的任何自定义项，如用户帐户、策略、应用程序、即时修正。

可以使用 CA 自定义实用工具对此 Linux 映像进行进一步自定义。

安装 CA 自定义实用工具

CA 自定义实用工具允许 CA Virtual Assurance 从外部更改虚拟机设置。来宾实用工具可在 OS 启动时监视 CD 驱动器。如果连接了特殊 ISO，则会执行下列操作：

1. 一组用于自定义来宾的命令。
2. 将来宾系统标记为已自定义。
   无法再次修改系统，除非有人重置此状态。
3. 暂停系统以表示自定义已成功。

安装正确的 CA 自定义来宾实用工具：

1. 该实用工具位于以下位置：
   - 适用于 Red Hat Enterprise Server 6.0

     ```
     <InstallationRoot>\Utilities\linuxCustomization\rh6
     ```
   - 适用于 SUSE Linux Enterprise Server 11

     ```
     <InstallationRoot>\Utilities\linuxCustomization\sles11
     ```
2. 将此可执行文件传输到正在准备的 VM 的硬盘驱动器上的下列位置：

   ```
   /usr/bin/ca-customize
   ```
3. （可选）提供您自己的 CA 自定义脚本版本，以支持我们不支持的其他来宾系统。
4. 启用 CA 自定义实用工具的可执行位：

   ```
   chmod 755 /usr/bin/ca-customize
   ```

配置 CA 自定义实用工具

您可以为 Linux 开通设置模板。要自定义来宾，请使用可用的脚本。您也可以使用自己的脚本以进行进一步设置。

遵循这些步骤:

1. 禁用网络接口，这样网络便不会影响自定义过程。

   注意：在自定义期间会自动启用网络。

2. 必要时使用 */etc/ca-customize.conf* 文件覆盖默认的 CDROM 设备名。

   CD_DEVICE=/dev/cdrom

   定义用于 CD 驱动器的设备名。

   默认值：/dev/cdrom

3. 设置在引导过程结束时自动启动。

   - （适用于 SUSE Linux）创建或修改 */etc/init.d/after.local* 文件：

     ```
     #!/bin/bash
     [ -e /etc/ca-customized ] || /usr/bin/ca-customize
     ```

   - （适用于 Red Hat Linux）将以下行添加到 */etc/rc.local* 文件中：

     ```
     [ -e /etc/ca-customized ] || /usr/bin/ca-customize
     ```

4. 关闭系统。

将虚拟机转换为模板

该模板允许您创建任意数量的自定义虚拟机。

遵循这些步骤:

1. 关闭 VM。
2. 要将准备好的映像转换成 XenServer 模板，请使用 XenCenter。

模板显示在 CA Virtual Assurance 中，并且可用于自定义开通。

执行了这些步骤之后，即可使用新模板来新建任意数量的自定义虚拟机。

自定义的开通如何工作

下列步骤描述了自定义 VM 开通的工作流程。

1. 平台管理服务开通新的 Linux VM。
2. 平台管理服务使用自定义参数准备新的 ISO，并将其附加到新 VM。
3. 平台管理服务启动 VM。
4. VM 检测到已连接了自定义 ISO。VM 应用自定义更改。
5. 如果自定义成功，VM 会关闭。PMM 检测到 VM 已停止。平台管理服务再次启动 VM 并完成开通。
6. 如果自定义失败，VM 不会暂停。平台管理服务将采取以下操作：
   a. 返回开通失败
   b. 将开通作业设置为异常状态

自定义日志

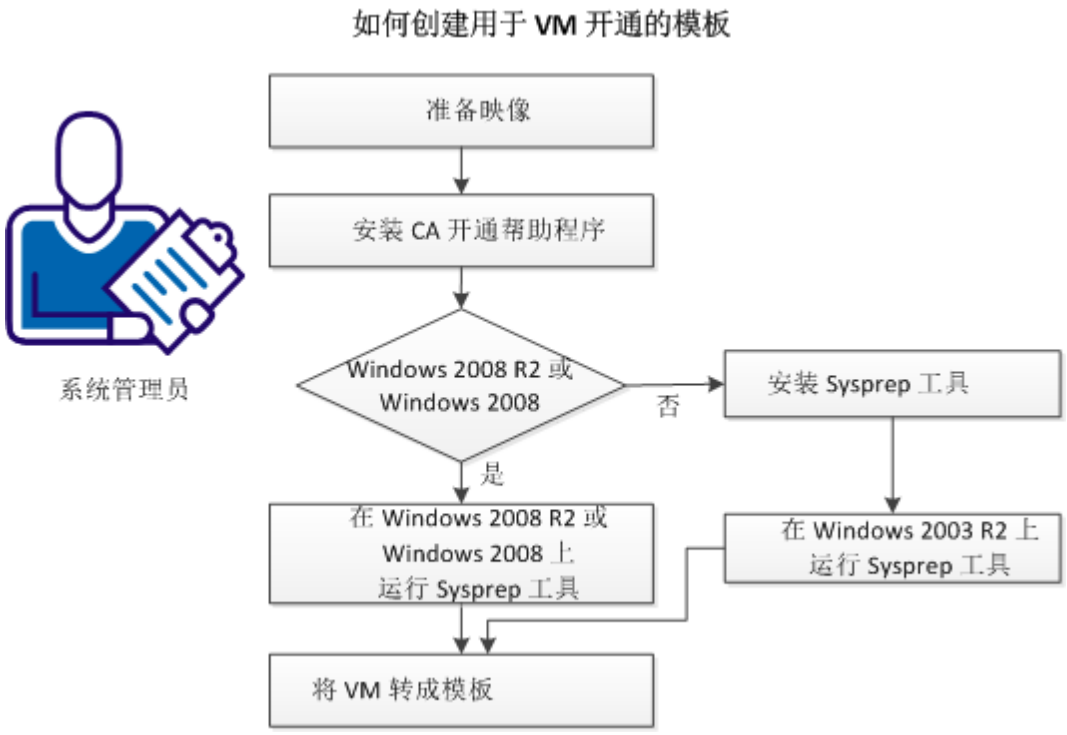
成功的自定义将存储在 */etc/ca-customized* 文件中。此文件包括自定义更改列表。

如果自定义失败，日志将存储在 */etc/ca-customized.tmp* 文件中。

如何为 XenServer 开通准备 Windows 模板

CA Virtual Assurance 支持自定义开通运行 Windows 2003 R2 Server（32 位和 64 位）、Windows 2008（32 位和 64 位）或 Windows 2008 R2 Server（64 位）的新虚拟机 (VM)。自定义选项包括大量设置。例如，更改内置的管理员帐户密码、计算机名和网络配置。

下图说明了系统管理员如何为 XenServer 开通准备 Windows 模板。



遵循这些步骤:

1. 准备 Windows 映像 (p. 320)。
2. 安装 CA 开通帮助程序。 (p. 320)
3. （对于 Windows 2003 R2 有效）安装 Sysprep 工具。 (p. 321)
4. 根据您的操作系统选择以下操作之一:
   - 在 Windows 2003 R2 上运行 Sysprep 工具。 (p. 321)
   - 在 Windows 2008 上或在 Windows 2008 R2 上运行 Sysprep 工具。 (p. 321)
5. 在 XenCenter 中将 VM 转换为模板 (p. 321)。

准备 Windows 映像

在创建包含 Windows 操作系统的模板时，通过遵循此程序来准备映像。按照下述步骤操作以启用 CA Virtual Assurance 开通操作从而自定义模板。特定步骤会根据 Windows 的版本而有所不同。

遵循这些步骤:

1. 在新的虚拟机上从头开始安装 Windows 操作系统。
2. 在虚拟计算机上安装适用于 Citrix XenServer 的 XenTools。
3. 应用您想在新的虚拟机上应用的任何自定义，如用户帐户、策略、应用程序、修补程序等。
4. （在 Windows 2003 上有效）删除内置的管理员帐户密码。

   注意：如果管理员密码不为空，SysPrep 将无法在开通期间设置新的密码，现有密码仍会保留。

XenServer 环境的先决条件

对于 XenServer 环境，确保满足下列先决条件：

- 资源池中的每个 XenServer 必须已启用 SSH 或 SFTP 访问。

安装 CA 开通帮助程序

CA 开通帮助程序使 CA Virtual Assurance 可以在外部更改虚拟机设置。

遵循这些步骤:

1. 在 <InstallationRoot>\Utilities\Sysprep\CAProvisioningHelper.exe 处查找该实用工具
2. 将此可执行文件传输到正在准备 VM 的硬盘驱动器的任何位置。
3. 从命令行执行一次 CA 开通帮助程序。

Sysprep 工具

Microsoft 提供了 Sysprep 工具，以概括、冻结并关闭已配置的 Windows 安装。以下部分详细描述了如何使用 Windows 2003 R2 和 Windows 2008 R2 的 Sysprep 工具。

在 Windows 2003 R2 上安装并运行 Sysprep 工具

在 Windows 2003 上，默认情况下不安装 Sysprep 工具，但是其可以在 Windows 安装 CD-ROM 中找到。

安装 Sysprep 工具

从 Windows 安装 CD-ROM 安装 Sysprep 工具。

在 Windows 2003 R2 上运行 Sysprep 工具

在配置 Sysprep 工具安装之后，运行 Sysprep 工具。

遵循这些步骤:

1. 查找并打开以下 CAB 文件：

   ```
   \SUPPORT\TOOLS\DEPLOY.CAB
   ```

2. 选择包含在 CAB 文件中的所有文件，并将其复制到以下位置：%SystemDrive%\Sysprep（通常为 C：\Sysprep）。

   注意：不要更改目录名称。

3. 转到 Sysprep 目录并运行以下命令：

   ```
   sysprep -quiet -reseal -mini -forceshutdown
   ```

在 Windows 2008 R2 上运行 Sysprep 工具

常规的 Windows 安装过程安装所有文件以执行 SysPrep 过程。在您配置 Windows 安装之后，请执行以下步骤：

1. 使用 Windows Server 2008 R2 的 Windows 自动安装工具包 (WAIK) 来生成有效的 XML 响应文件。可从 Microsoft 网站获取 WAIK。

   注意：开通的方式需要模拟的无人值守响应文件，否则它将无法关闭。由于开通进程将替换响应文件的内容，因此响应文件的内容将无关紧要，但文件必须遵循特定于 SysPrep 的 XML 架构。

2. 将生成的 XML 文件命名为“sysprep.xml”，并将其放置在 Sysprep 目录中：

   %SystemRoot%\system32\sysprep

3. 运行下列命令：

   ```
   sysprep /generalize /oobe /shutdown /unattend:sysprep.xml
   ```

在 XenCenter 中将 VM 转换为模板

该模板允许您创建任意数量的自定义虚拟机。

遵循这些步骤:

1. 关闭虚拟机。
2. 要将准备好的映像转换成 XenServer 模板，请使用 XenCenter。

   模板显示在 CA Virtual Assurance 中，并且可用于自定义开通。

管理 VM 状态 (XenServer)

可以通过执行以下操作之一来控制虚拟机的状态：

- 发现
  - 服务器
  - 网络
- 启动
- 挂起
- 关闭
- 从磁盘删除

控制 VM 状态：

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 右键单击 VM 并选择“管理”，然后选择下列选项之一：

   发现

   发现服务器或网络。

   启动

   在指定的 XenServer 主机上启动 VM。

   挂起

   在指定的 XenServer 主机上挂起正在运行的 VM，并保存其当前状态。在您恢复 VM 之前，所有活动都会被挂起。

   关闭

   在指定的 XenServer 主机上关闭正在运行的 VM。

   从磁盘删除

   从磁盘删除 VM。

   此时将显示相应的向导。

3. 填充必要信息，然后继续下一步。
4. 提交。

   状态操作发生后，将出现一条确认信息。刷新界面以查看新的 VM 状态。会出现一个确认操作结果的事件。

开通 Citrix XenServer 虚拟机

可以通过执行以下过程开通虚拟机。确保您为 VM 开通准备了 Windows 模板。

遵循这些步骤:

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 右键单击 Citrix XenServer 组，并依次选择“开通”、“开通 Citrix XenServer 虚拟机”。

   此时将显示开通向导。

3. 填充所需信息：

   VM 名称

   定义新的 VM 名称。

   模板

   指定 Windows 开通模板。

   管理员密码

   定义新 VM 的管理员密码。

   产品激活密钥

   定义 Windows 2003 激活密钥。

   全名

   定义完整的 VM 名称。

4. （可选）填写其他信息（工作组、内存、CPU、VM 主机、组织）。如果您要使用静态 IP 地址，请禁用 DHCP，并提供 IP 地址、掩码和默认网关。

   注意：内存和 CPU 设置取决于使用的 Windows 开通模板。

5. 提交。

   将显示确认消息。

6. 刷新“作业”面板以查看进度。

   会出现一个确认操作结果的事件。

Huawei GalaX

Huawei GalaX 包含以下平台：

虚拟化基础架构平台

将物理资源（如计算、存储和网络）虚拟化为可以集中管理、灵活排定和动态分配的虚拟资源。虚拟化基础架构是用于构建基于云计算的数据中心的主要平台。

云计算基础架构平台

封装并且管理由虚拟化基础设施平台提供的虚拟资源。帮助运送者和企业使用 OMM 功能来建造他们的数据中心。管理功能包括资源管理、映像管理、计费管理、排定管理以及用户管理。

操作和维护管理 (OMM) 平台

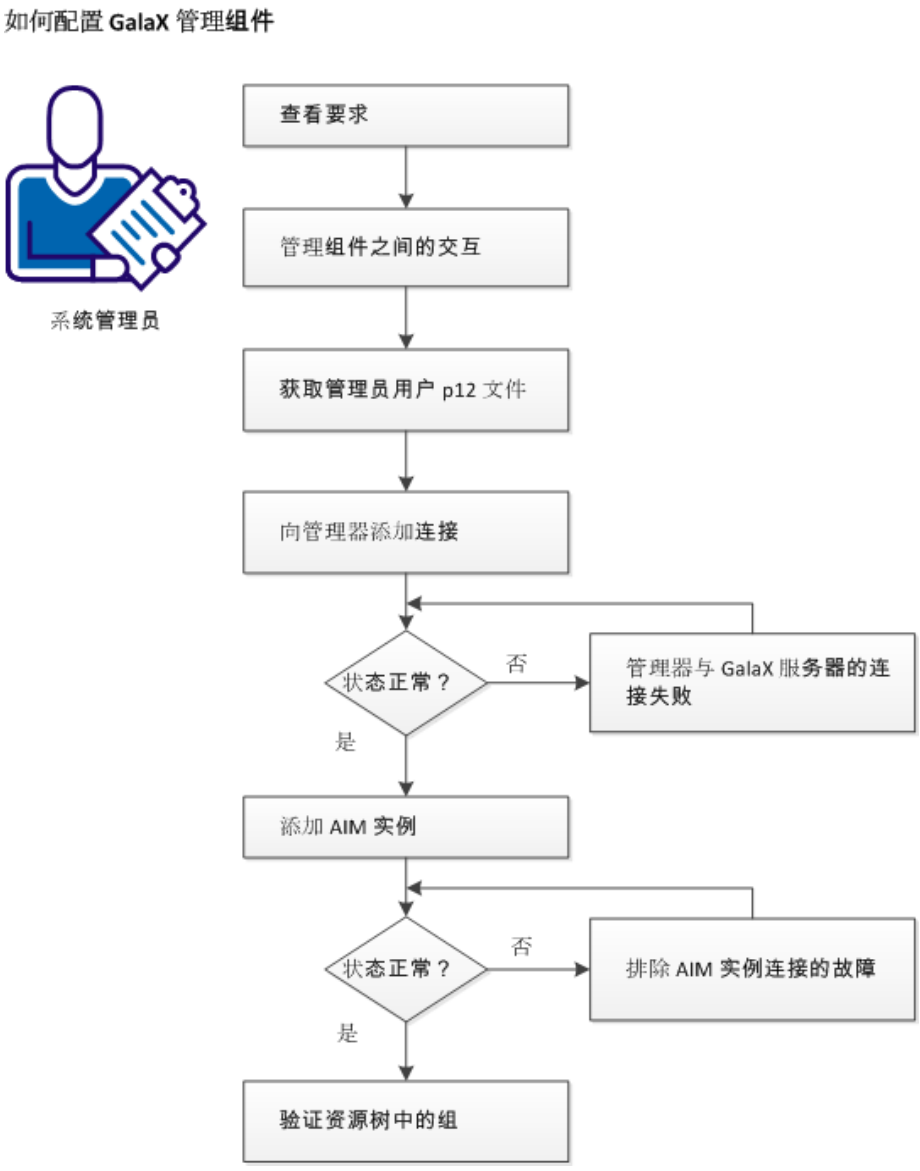
为 OMM 用户提供统一的 OMM 界面。OMM 用户可以通过 Web 界面远程访问 SingleCLOUD OMM 系统。用户可以执行资源管理、资源监控和资源统计信息报告等操作。

详细信息：

如何配置 Huawei GalaX 管理组件 (p. 325)
如何创建虚拟私有云 VLAN (p. 336)
如何管理 Huawei SingleCLOUD 环境 (p. 345)
如何为 GalaX 开通准备 Windows 模板 (p. 353)

如何配置 Huawei GalaX 管理组件

作为系统管理员，您可以配置 CA Virtual Assurance 以连接到您的 Huawei GalaX 环境并监控其性能。



请执行以下步骤：

查看要求

在配置 CA Virtual Assurance 的管理组件之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您熟悉 CA Virtual Assurance 和 SystemEDGE。
- 您可以访问包括以下内容的 CA Virtual Assurance 管理器安装：
  - 平台管理模块 (PMM)
  - Application Insight Module (AIM)
  - 监控代理 (SystemEDGE)
- 您可以访问 CA Virtual Assurance 用户界面。
- 您具有有效的凭据（用户名和密码），可访问要管理的环境中的服务器。
- 了解使用哪个端口来通过 Web 服务访问您环境中的服务器。
  默认 HTTP 端口：8773。
- 您已验证环境中的服务器运行正常。
- 如果将 PMM 和 AIM 安装在不同系统上，请确认 PMM 和 AIM 系统上的 SNMP 设置一致。读和写团体字符串以及 SNMP 端口号必须是相同的。
- 您已验证 CA Virtual Assurance 管理器已发现您要使用的远程 AIM 服务器。

查看 HUAWEI GalaX 管理组件之间的交互

作为系统管理员，您希望使用 CA Virtual Assurance 管理新的 Huawei GalaX 环境。通过 CA Virtual Assurance，可以动态管理一个或多个 GalaX 环境的物理资源和虚拟资源。Huawei GalaX 包括与一个或多个计算资源管理器 (CRM) 通信的弹性服务控制器 (ESC)。CRM 可与多个计算节点代理 (CNA) 通信。

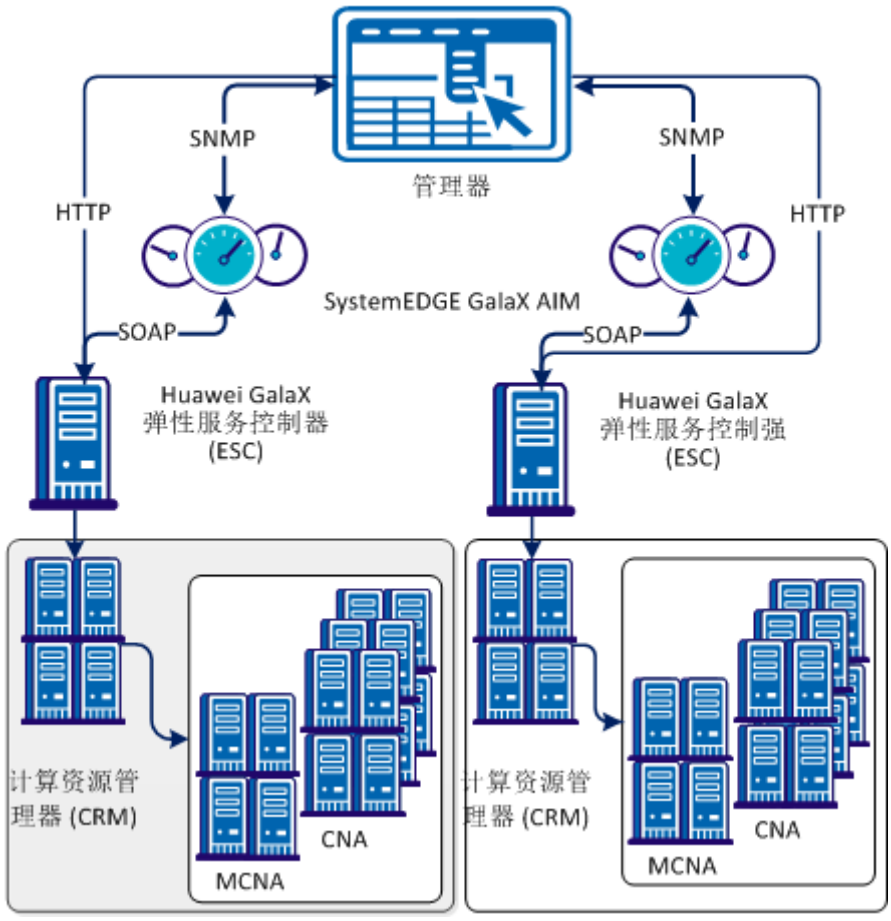
要管理 GalaX，CA Virtual Assurance 需要其 GalaX 平台管理模块 (PMM)、GalaX Application Insight Module (AIM) 和弹性服务控制器 (ESC) 之间具备网络连接。要建立这些网络连接，需配置 CA Virtual Assurance GalaX 管理组件（即 GalaX PMM 和 GalaX AIM）。

GalaX AIM 是可扩展 SystemEDGE 功能范围的 SystemEDGE 代理插件。GalaX AIM 使 SystemEDGE 能够监控多个 GalaX 环境的性能，以及评估受监控的 GalaX 资源的状态。SystemEDGE 和 AIM 根据阈值确定受监控资源的状态，并应用 SNMP 将此信息传播到 CA Virtual Assurance 管理器。

GalaX PMM 是 CA Virtual Assurance 管理器的一个组件。PMM 负责使用 SOAP 为所有的 Huawei GalaX 操作提供连接和支持。PMM 管理与计算资源管理器的连接、执行与 GalaX 相关的操作、从 AIM 检索数据，以及填充 CA Virtual Assurance 管理数据库。

下图显示了在具有两个 GalaX ESC 的示例环境中受影响组件之间的交互。通常，GalaX PMM 和每个具有多实例支持的 GalaX AIM 可以连接到多个弹性服务控制器。图中所示的连接没有指定任何限制。所需的网络连接基于 TCP/IP、SNMP 和 SOAP。

Huawei GalaX 管理组件之间的交互



获取管理员用户 p12 文件

要在 CA Virtual Assurance UI 中执行操作，请从 GalaX 环境中获取管理员用户 p12 文件。p12 文件为您提供配置、监控和管理 GalaX 环境的管理员权限。

p12 认证文件在 GalaX 安装过程中生成。认证文件具有全局唯一性，仅适用于特定弹性服务控制器 (ESC) API。您不能使用该文件访问其他 GalaX ESC 服务器。

在执行以下步骤之前，请确认 GalaX ESC 服务器的 IP 地址和用户 root 的密码。

遵循这些步骤:

1. 指定用于生成 p12 文件的密码。

   配置 CA Virtual Assurance 管理器和 GalaX ESC 服务器之间的连接时也需要该密码。

2. 使用 root 登录 GalaX ESC 服务器。
3. 打开终端窗口并运行以下命令：

   ```
   cd /opt/eucalyptus/.euca
   ```

   该目录包含认证文件。

4. 要获取数字签名认证文件和私钥认证文件的名称，请运行 ls 命令。

   文件名称具有以下格式：

   - 数字签名认证文件：euca2-admin-*-cert.pem
   - 私钥认证文件：euca2-admin-*-pk.pem

5. 运行下列命令：

   ```
   Openssl pcks12 -export -in <数字签名认证文件> -out admin.p12 -inkey <私钥认证文件>
   ```

   示例：

   ```
   openssl pkcs12 -export -in euca2-admin-109f9d47-cert.pem -out admin.p12 -inkey euca2-admin-109f9d47-pk.pem
   ```

6. 系统提示您："输入导出密码"
7. 输入步骤 1 中指定的密码。

   系统在 /opt/eucalyptus/.euca 目录中生成所需的 admin.p12 认证文件。

8. 将 admin.p12 文件复制到 CA Virtual Assurance 管理器所在的服务器。在服务器上，该目录可为任意目录。您可以使用如 WinSCP 一样的工具将 admin.p12 文件复制到该 Windows 系统。
9. admin.p12 文件和您的密码现在便可以用于建立 CA Virtual Assurance 管理器和 GalaX ESC 服务器之间的连接。

将新的 GalaX 连接添加到管理器中

您可以使用 CA Virtual Assurance 用户界面的“管理”选项卡添加 GalaX 连接。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分选择“Huawei SingleCLOUD”。

   右侧窗格将刷新并显示受管的 GalaX 服务器和关联的 GalaX AIM 服务器。

3. 在“GalaX 服务器”窗格工具栏上单击  （添加）。

   此时将显示“新建 GalaX 服务器”对话框。

4. 输入所需连接数据（用户名、服务器、端口、P12 文件路径以及密码），然后单击“确定”。

   如果网络连接已成功建立，GalaX 服务器会添加到右上角的“GalaX 服务器”窗格并带有绿色状态图标。CA Virtual Assurance 自动发现 GalaX 服务器。

   如果连接失败，将显示“验证失败”对话框。如果您单击“是”，CA Virtual Assurance 会将 GalaX 服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。

管理器到 GalaX 服务器的连接失败

症状：

在“管理”、“配置”下添加服务器连接后，对服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的服务器连接数据是否仍然有效。如有必要，请更新连接数据。
- 验证服务器系统是否正在运行并且可以访问。
- 验证 CA Virtual Assurance 服务器和 GalaX 服务器之间的时差是否小于 5 分钟。
- 确认连接所需的服务正在服务器上正常运行。

更新服务器连接数据：

1. 单击与失败的连接关联的  （添加）或  （编辑）。
2. 添加连接详细信息，启用“受管状态”，然后单击“确定”。

   将更新连接数据。
3. 单击右上角的  （验证）以验证新设置。

   如果无法建立与服务器的连接，请继续执行下一步骤。

验证服务器系统是否正在运行并且可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```
2. 要确定服务器是否具有有效的 DNS 条目和 IP 地址，请检查这些命令的输出。

   如果服务器不在 DNS 中，请将服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ipaddress <Server Name>

   输入正确的 IP 地址和服务器名称并保存文件。例如：

   192.168.50.50 myServer

4. 切换到 CA Virtual Assurance 用户界面、“管理”选项卡、“配置”、“服务器”窗格，并单击右上角的 （验证）。

   即使服务器凭据和连接数据正确并且您可以 ping 服务器，连接仍然可能失败。在这种情况下，可能是服务器引起该问题。如果无法建立与服务器的连接，请继续执行下一步骤。

验证 CA Virtual Assurance 服务器和 GalaX 服务器之间的时差是否小于 5 分钟：

1. 要访问 GalaX 服务器，请联系系统管理员。
2. 检查 GalaX 服务器上的系统时间。
3. 检查 CA Virtual Assurance 管理器系统上的系统时间。
4. 如果系统时差大于 5 分钟，则相应地更新时间设置。

验证连接所需的所有服务是否在服务器系统上运行良好。

1. 登录到 GalaX 服务器。
2. 确认连接所需的服务在正常运行。
3. 如有必要，请启动或重新启动服务。
4. 切换到管理器系统上的 CA Virtual Assurance 用户界面、服务器窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证服务器连接。

   如果与服务器的连接失败，请验证根据该方案的要求收集的数据是否有效。

   与管理员或技术支持合作，解决服务器连接问题。

添加 GalaX 服务器的 AIM 实例

将新的 GalaX 连接添加到 CA Virtual Assurance 管理器后，添加 GalaX AIM 实例来管理新的 GalaX 服务器。CA Virtual Assurance 然后发现整个 Huawei GalaX 环境及其所有物理组件和虚拟组件。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分选择“Huawei SingleCLOUD”。

   右侧窗格将刷新并显示受管的 GalaX 服务器和关联的 GalaX AIM 服务器。

3. 在“GalaX AIM 服务器”窗格工具栏上单击  （添加）。

   此时将显示“新建 GalaX AIM 服务器”对话框。

4. 打开“GalaX AIM 服务器”下拉列表。

   将显示发现的 GalaX AIM 服务器的列表。

5. 从下拉列表中选择一个 GalaX AIM 服务器。

   CA Virtual Assurance 使用“GalaX 服务器”窗格中列出的 GalaX 服务器填充“GalaX 服务器”下拉列表。您只能管理 CA Virtual Assurance 管理器为之建立了有效连接的 GalaX 服务器。

   注意：如果 AIM 位于远程系统上，CA Virtual Assurance 必须首先探测该系统，以便让 AIM 服务器显示在下拉列表中。

6. 选择要管理的 GalaX 服务器，然后单击“确定”。

   即添加选定 GalaX 服务器的新 AIM 实例。如果该实例的状态不是错误或已停止，则 CA Virtual Assurance 便开始发现关联的 Huawei GalaX 环境。发现完成后，您便可以开始管理 Huawei GalaX 的虚拟资源和物理资源。

在资源树中检验 Huawei GalaX

在成功配置和发现之后，新发现的资源将在“资源”、“浏览”窗格中的相应组下列出。

遵循这些步骤:

1. 单击“资源”，然后打开“浏览”窗格。
2. 展开 Huawei SingleCLOUD 组。

   此时将显示 Huawei GalaX 资源。

CA Virtual Assurance 现在便可以管理配置的 Huawei GalaX 环境。您可以监控资源的状态和属性。

排除 AIM 实例连接的故障

如果 AIM 连接处于未就绪状态，将出现以下状态图标之一：

 发现正在进行

 无轮询

 错误

 警告

 已禁用

 未知

有关 AIM 实例状态的详细信息，请参阅工具提示。以下故障排除部分提供了用于解决该问题的详细信息和步骤。

AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为服务器添加 AIM 实例后，状态图标显示  （发现正在进行）。

解决方案：

等到环境的发现过程完成。发现持续时间取决于与环境中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示指示未完成发现请求数量的工具提示。发现作业完成时，CA Virtual Assurance 会向资源树中添加一个服务器文件夹。然后，您可以开始管理您的环境。

AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （无轮询）。

解决方案：

关联实例不需要特定的操作。此图标表示 CA Virtual Assurance 管理器不轮询此 AIM。AIM 不是首选。

如果多个 AIM 已配置为管理特定服务器，PMM 将选择其中一个 AIM 作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决可能导致与 AIM 连接失败的最常见问题：

- 验证是否可以访问 AIM 服务器。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 确认命令的输出对于 AIM 服务器有有效的 DNS 条目和 IP 地址。

   如果 AIM 服务器不在 DNS 中，则将 AIM 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ipaddress servername

   输入正确的 IP 地址和 AIM 服务器名称。例如：

   192.168.50.51 myAIM

4. 在“AIM 服务器”窗格的右上角，单击 （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“AIM 服务器”窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证 AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否有效。

AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 AIM 实例之后，几个实例的状态图标显示 （已禁用）。该 AIM 实例未受管理。

如果 CA Virtual Assurance 发现具有以下关系的 AIM，则显示该状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的服务器配置了 AIM。
- AIM 连接到未配置的服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的服务器连接并将其受管状态更改为已启用。

如何创建虚拟私有云 VLAN

作为系统管理员，您希望在 GalaX 环境中使用关联的虚拟机和虚拟磁盘创建虚拟私有云。*虚拟私有云 (VPC)* 是具有多个虚拟机及相关虚拟磁盘的 Huawei SingleCLOUD 用户的私有本地网络。由于 CA Virtual Assurance 已发现 GalaX 环境（请参阅查看要求 (p. 337)），所以 CA Virtual Assurance 用户界面提供用于创建所需 VPC VLAN 资源的基础架构。

下图说明有关如何创建 VPC VLAN 的所需步骤。

请执行以下步骤：

查看要求

在 CA Virtual Assurance 中设置 Huawei SingleCLOUD 实例之前，请查看以下先决条件：

- 熟悉 Huawei GalaX 环境。
- 熟悉 CA Virtual Assurance 用户界面以及开通资源的方式。
- 熟悉部署和配置监控软件 (SystemEDGE)。
- 已安装 CA Virtual Assurance，且可以访问 CA Virtual Assurance 用户界面。
- Huawei GalaX 环境可用且在运行。
- Huawei GalaX 环境中具有计算群集（对于虚拟机）和存储群集（对于虚拟磁盘）的服务器。
- Huawei GalaX 环境中出现具有要应用于虚拟机的操作系统的映像。
- CA Virtual Assurance 和 Huawei GalaX 服务器之间的连接建立。
- GalaX AIM 即被配置为监测 Huawei GalaX 服务器。
- 用户 VLAN 池和 VPC VLAN 池的服务器可用。
- CA Virtual Assurance 已发现 Huawei GalaX 服务器及其关联的资源（如群集、存储群集和虚拟机）。
- 共享磁盘需要 Microsoft 群集服务 (MSCS)。

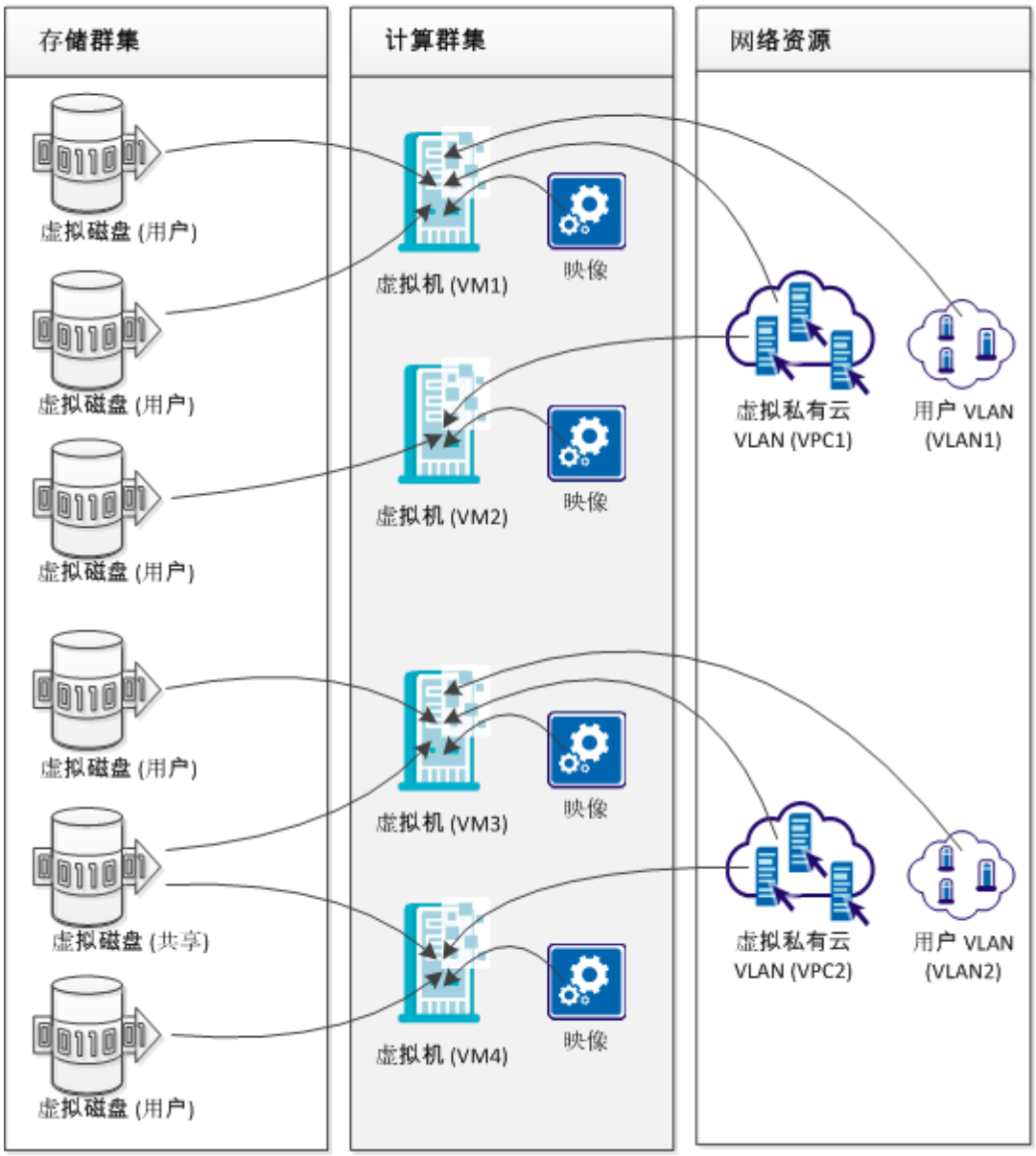
查看 Huawei SingleCLOUD 组件关联关系

Huawei GalaX 环境是 Huawei SingleCLOUD 解决方案的一部分，旨在用于云服务提供商或企业客户的云计算数据中心。

Huawei SingleCLOUD 解决方案包含分层体系结构。物理层和网络层上的设备集成于该解决方案中。基于群集、分布式存储、NAS 存储和虚拟化技术，这些集成设备向上层服务提供存储、计算和网络服务。CA Virtual Assurance 中的 Huawei SingleCLOUD 实例包括必要的基础架构，用于管理和监测您的 Huawei GalaX 环境。Huawei GalaX 环境包括群集和它们的相关资源。

下图说明可通过 CA Virtual Assurance 管理的 SingleCLOUD 解决方案的 GalaX 组件以及这些组件之间的依存关系。

Huawei SingleCLOUD GalaX 组件及其关系



最初，创建向云中的虚拟机及其用户提供 VLAN 访问的 VPC VLAN。或者，您可以将用户 VLAN 添加到虚拟机中。计算群集中的虚拟机需要适当的映像以及虚拟机所属的 VPC VLAN。映像包含此虚拟机的操作系统和应用程序。

然后，可以在存储群集中创建虚拟磁盘，并将这些磁盘附加到相应虚拟机，以便存储用户特定的数据。支持两种类型的虚拟磁盘：用户磁盘和共享磁盘。用户磁盘与虚拟机之间是一对一的关联关系，而共享磁盘与虚拟机之间可以是一对多的关联关系。共享磁盘需要 Microsoft 群集服务 (MSCS) 支持。

（可选）分配 VLAN

由于虚拟私有云对象需要使用 VLAN，因此首先分配 VLAN。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹，然后选择适当的 SingleCLOUD 服务器。

   右侧窗格将刷新并显示“资源管理”和“网络管理”选项卡。

3. 依次单击“网络管理”、“VLAN”。

   此时将显示现有 VLAN 对象的列表。

4. 在 VLAN 窗格工具栏上单击  （添加）。

   此时将显示“分配 VLAN”对话框。

5. 指定 VLAN 名称，从下拉菜单中选择群集，指定方法（自动或手动填充），然后单击“确定”。

   此时将分配 VLAN。

创建 VPC VLAN

VPC 充当云用户的私有本地网络，具有几个虚拟机和关联虚拟磁盘。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹，然后选择适当的 SingleCLOUD 服务器。

   右侧窗格将刷新并显示“资源管理”和“网络管理”选项卡。

3. 依次单击“网络管理”、“VPC”。

   此时将显示现有 VPC 实例的列表。

4. 在 VPC 窗格工具栏上单击 （添加）。

   此时将显示“创建 VPC”对话框。

5. 指定 VPC 名称，从下拉菜单中选择群集，分配 VLAN（自动或手工从列表进行操作），然后单击“确定”。

   此时将创建 VPC 实例。

（可选）创建用户规范

用户规范是可用于创建虚拟机的一组 CPU、内存和系统卷大小配置值。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹，然后选择适当的 SingleCLOUD 服务器。

   右侧窗格将刷新并显示“资源管理”和“网络管理”选项卡。

3. 依次单击“资源管理”、“用户规范”。

   此时将显示现有用户规范的列表。

4. 在“用户规范”窗格工具栏上单击 （添加）。

   此时将显示“创建用户规范”对话框。

5. 指定 CPU、内存和系统卷大小的用户规范名称和值。单击“确定”。

   此时将创建用户规范。

创建虚拟机

虚拟机需要系统卷、CPU、内存和磁盘空间设置、VPC 和 NIC 规范的映像。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹，然后右键单击适当的计算群集。

   此时将打开弹出式菜单。

3. 依次选择“管理”、“从模板创建 VM”。

   此时将打开“创建 VM”对话框。

4. 指定下列参数并单击“确定”。
   - VM 数
   - VM 名称
   - 映像 ID
   - 用户规范或 CPU、内存、磁盘空间
   - VPC VLAN
   - （可选）附加网络接口控制器 (NIC)
   - 服务质量（QoS）设置
     - 保留的内存
     - 已保留 CPU
     - CPU 限制
     - 高可用性
     - NIC 速度限制

   CA Virtual Assurance 将创建指定的虚拟机。虚拟机属于分配的 VPC VLAN。要获得虚拟机的列表，请打开“存储群集”面板中的“详细信息”选项卡。

   以下参数需要进一步说明：

   保留的内存

   指定分配给虚拟机的物理内存最小比例。保留被定义为百分比 (%)，可以分配从 0% 到 100% 的值。

   示例：如果您将内存设置为 2G，将保留设置为 25%，系统确保至少 512 MB 内存用于虚拟机。

   已保留 CPU

   指定为该虚拟机保留的物理 CPU 性能的最小比例。保留以百分比 (%) 定义，可以指定值 0%、50% 或 100%。

   示例：如果您将保留设置为 50%，系统将确保至少 50% 的 CPU 时间用于每个 CPU 内核。

   CPU 限制

   指定该虚拟机可分配的 CPU 性能的最大百分比。

   注意：限制值必须大于或等于为保留指定的值。

（可选）创建虚拟磁盘

虚拟磁盘用于存储用户特定的数据，可以连接到虚拟机。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹，然后右键单击适当的存储群集。

   此时将打开弹出式菜单。

3. 依次选择“管理”、“创建磁盘”。

   此时将打开“创建磁盘”对话框。

4. 指定下列参数并单击“确定”。

   - 磁盘名称
   - 磁盘类型（用户磁盘或共享磁盘）。用户磁盘可以附加到一个虚拟机。共享磁盘可以附加到多个虚拟机。
   - 动态分配（普通或精简开通）

     精简开通需要 IP SAN 设备支持。
   - 磁盘大小 (GB)
   - 虚拟磁盘说明

   CA Virtual Assurance 将创建虚拟磁盘。要获得虚拟磁盘的列表，请打开“存储群集”面板中的“详细信息”选项卡。

（可选）将虚拟磁盘附加到虚拟机

根据指定的虚拟磁盘类型，可以将用户磁盘附加到一个虚拟机，将共享磁盘附加到多个虚拟机。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹，然后选择适当的存储群集。

   “存储群集”面板将打开并列出指定的虚拟磁盘。

3. 选择要附加的虚拟磁盘，然后单击 附加图标。

   此时将显示可用虚拟磁盘的列表。

4. 选择适当的虚拟机并单击“确定”。

   此时将附加虚拟磁盘。

管理 VPC VLAN 和其组件

您指定了具有附加虚拟磁盘且使用 VLAN 进行通信的虚拟机。这些资源属于可通过 CA Virtual Assurance 管理的虚拟私有云。

如何管理 Huawei SingleCLOUD 环境

由于用户界面的大部分都是一目了然的，因此该方案只是用于简单了解 Huawei SingleCLOUD 环境的对象层次结构及浏览其关联管理功能的指导。

请执行以下步骤：

查看要求

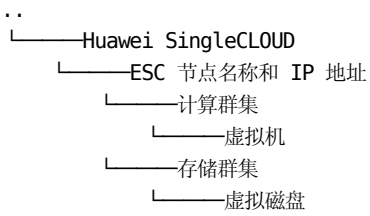
在 CA Virtual Assurance 中管理 Huawei SingleCLOUD 实例之前，请复查以下先决条件：

- 熟悉 Huawei GalaX 环境。
- 熟悉 CA Virtual Assurance 用户界面以及开通资源的方式。
- 熟悉部署和配置监控软件 (SystemEDGE)。
- 已安装 CA Virtual Assurance，且可以访问 CA Virtual Assurance 用户界面。
- Huawei GalaX 环境可用且在运行。
- Huawei GalaX 环境中具有计算群集（对于虚拟机）和存储群集（对于虚拟磁盘）的服务器。
- Huawei GalaX 环境中出现具有要应用于虚拟机的操作系统的映像。
- CA Virtual Assurance 和 Huawei GalaX 服务器之间的连接建立。
- GalaX AIM 即被配置为监测 Huawei GalaX 服务器。
- 用户 VLAN 池和 VPC VLAN 池的服务器可用。
- CA Virtual Assurance 已发现 Huawei GalaX 服务器及其关联的资源（如群集、存储群集和虚拟机）。
- 存在具有虚拟机的虚拟私有云。

浏览树层次结构

服务级别显示在 Huawei SingleCLOUD 文件夹的顶部。SingleCLOUD 服务包括一个或多个弹性服务控制器 (ESC)。每个 ESC 控制多个具有虚拟机和虚拟磁盘的计算群集和存储群集。

下图所示为 Huawei SingleCLOUD 文件夹下的对象层次结构：



遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹。

   - 要打开 Huawei SingleCLOUD 事件的列表，请选择 Huawei SingleCLOUD 对象。
   - 要访问“资源管理”和“网络管理”，请选择 ESC 节点。
   - 要获取可用虚拟机的列表或创建虚拟机，请选择计算群集。
   - 要获取可用虚拟磁盘的列表或创建虚拟磁盘，请选择存储群集。

浏览 GalaX SingleCLOUD 服务器级别

GalaX SingleCLOUD 位于树层次结构中的第二层。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹。

   此时将显示文件夹层次结构。

3. 选择 ESC 节点。

   此时将显示“资源管理”和“网络管理”选项卡。

   - “资源管理”用于快照、映像和用户规范。
   - 将网络管理用于 VPC VLAN 和用户 VLAN。

使用资源管理操作

在用户界面的“资源管理”选项卡中可以进行以下操作：

- 查看快照及其属性
- 将快照还原到虚拟机
- 删除快照
- 查看映像及其属性
- 查看用户规范及其属性
- 创建用户规范
- 编辑用户规范
- 删除用户规范

用法和对话框一目了然。如有必要，可以将光标悬停在图标上获得工具提示。

使用网络管理操作

在用户界面的“资源管理”选项卡中可以进行以下操作：

- 创建 VPC VLAN
- 查看 VPC VLAN 和其属性
- 删除 VPC VLAN
- 分配用户 VLAN
- 删除用户 VLAN

用法和对话框一目了然。如有必要，可以将光标悬停在图标上获得工具提示。

浏览计算群集级别

计算群集位于树层次结构的第三个级别。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹。

   此时将显示文件夹层次结构。

3. 选择或展开计算群集。

   此时将显示可用虚拟机的列表。

4. 右键单击计算群集以创建虚拟机。

   您需要一个包含一个磁盘以及用于系统卷的操作系统（资源管理）的映像、VPC VLAN、用户规范（可选）、用户 VLAN （可选）。

5. 右键单击虚拟机以执行虚拟机管理操作。

   不提供不适用的操作。

使用虚拟机管理操作

用户界面提供通过右键单击虚拟机进行的虚拟机管理操作。用法和对话框一目了然。

- 删除 VM
- 重新启动 VM
- 打开 VM 电源
- 关闭 VM 电源
- 安全重新启动 VM（关闭操作系统）
- 安全关闭 VM 电源（关闭操作系统）
- 使 VM 休眠
- 唤醒 VM
- 修改 VM 名称
- 查看初始密码
- 设置启动顺序
- 回滚快照
- 创建 VM 快照

下列管理操作需要更多的解释：

- 修改 CPU 配置和 QoS
- 修改内存配置和 QoS
- VNC 登录
- 挂接/卸载工具

修改 CPU 配置和 QoS

指定以下值：

CPU 数

指定分配给虚拟机的 CPU 内核数。可分配给虚拟机的最大 CPU 内核数为 8。

示例：如果您将数目设置为 5，那么 5 个 CPU 内核可用于虚拟机。

保留

指定为该虚拟机保留的物理 CPU 性能的最小比例。保留以百分比 (%) 定义，可以指定值 0%、50% 或 100%。

示例：如果您将保留设置为 50%，系统将确保至少 50% 的 CPU 时间用于每个 CPU 内核。

限制

指定该虚拟机可分配的 CPU 性能的最大百分比。

注意：限制值必须大于或等于为保留指定的值。

修改内存配置和 QoS

指定以下值：

内存

指定分配给虚拟机的内存量。内存单位为兆字节 (MB)，范围在 512 MB 到 256 GB 之间。

示例：如果您将内存设置为 512 MB，512 MB 是虚拟机可以分配的最大内存量。

保留

指定分配给虚拟机的物理内存最小比例。保留被定义为百分比 (%)，可以分配从 0% 到 100% 的值。

示例：如果您将内存设置为 2G，将保留设置为 25%，系统确保至少 512 MB 内存用于虚拟机。

VNC 登录

可以使用 VNC 访问 VM 之前，VNC 登录需要初始设置：下载 VncViewer.jar 并将其安装在您的 CA Virtual Assurance 管理器系统上。

遵循这些步骤:

1. 登录 CA Virtual Assurance 管理器服务器，打开用户界面，展开浏览树，右键单击 Huawei SingleCloud VM，然后选择“管理”、“VNC 登录”。

   一条消息会显示，为您提供如何继续的说明。

2. 从 CA Virtual Assurance 管理器服务器，连接到您的 ESC 或 OMM 服务器，并从以下目录下载 VncViewer.jar：

   ```
   /opt/omm/oms/webapps/oms/business/resourcemanage/virtualresources
   ```

3. 再次单击“VNC 登录”。

   此时将打开消息对话框。

4. 单击对话框中的消息。

   “上传文件”对话框打开。

5. 单击“浏览...”，导航到下载的 VncViewer.jar 文件，并单击“打开”。

   文件路径显示在对话框中。

6. 单击“确定”。

   CA Virtual Assurance 将 VncViewer.jar 上传至 *Install_Path**product*\tomcat\webapps\UI 目录。

   VNC 查看器自动打开并连接到 VM。

完成此一次性步骤后，VNC 登录便可用了，您可以远程访问在环境中的任何 Huawei SingleCloud VM。

挂接/卸载工具

要充分利用功能，请在 VM 上安装 SingleCloud Tools。

遵循这些步骤:

1. 登录 CA Virtual Assurance 管理器服务器，打开用户界面，展开浏览树，右键单击 VM，然后选择“管理”、“挂接/卸载工具”。

   CA Virtual Assurance 在对话框中显示当前 VM 状态和 SingleCloud Tools 状态。

2. 要更改 SingleCloud Tools 状态为挂接/卸载，请单击“确定”。
3. 在 VM 上成功挂接 SingleCLOUD 工具后，请安装 PV 驱动程序。如果 VM 运行在 Linux 操作系统上，请重新启动 VM，然后安装 PV 驱动程序。

资源分配最佳实践

指定适用于 Huawei SingleCLOUD 环境中的虚拟机的资源分配设置（保留和限制）。

下列准则可以帮助您的虚拟基础架构获得更好的性能：

- 使用保留来指定可接受的*最小* CPU 或内存量，而非您希望的可用量。主机根据估计的需求和虚拟机的限制，分配额外的资源作为可用资源。在您修改环境（如增加或删除虚拟机）后，您通过保留指定的 CPU 或内存的数量保持不变。
- 为虚拟机指定保留时，请勿分配所有资源。应计划将适当的部分留作未保留，因为在要保留的容量接近所有系统容量时，更改保留会越来越困难。

浏览存储群集级别

存储群集位于树层次结构的第三个级别。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“资源”。

   此时将打开“浏览”树。

2. 展开 Huawei SingleCLOUD 文件夹。

   此时将显示文件夹层次结构。

3. 展开存储群集。

   此时将显示可用虚拟磁盘的列表。

4. 右键单击存储群集以创建虚拟磁盘。

   以下参数需要额外说明：

   磁盘类型：用户磁盘

   可以附加到一个虚拟机。

   磁盘类型：共享磁盘

   可以附加到多个虚拟机。

   动态分配：精简开通

   保留指定磁盘空间，但是只有需要空间来存储数据时，才会将整个保留空间分配给磁盘。精简开通的虚拟磁盘的大小随存储的数据量的增长而增长。

   精简开通允许您通过超量使用数据存储，并通过减少保留但未使用的空间量来增加存储使用率。

5. 右键单击“浏览”树中的虚拟磁盘，以执行虚拟磁盘管理操作。

   可以查看虚拟磁盘的详细信息，也可以删除虚拟磁盘。

使用存储管理操作

用户界面提供通过右键单击虚拟机进行的虚拟机管理操作。用法和对话框一目了然。

- 删除虚拟磁盘
- 查看虚拟磁盘的详细信息
- 选择虚拟磁盘以查看虚拟磁盘的事件

选择存储群集以打开可用虚拟磁盘的列表。可用操作如下：

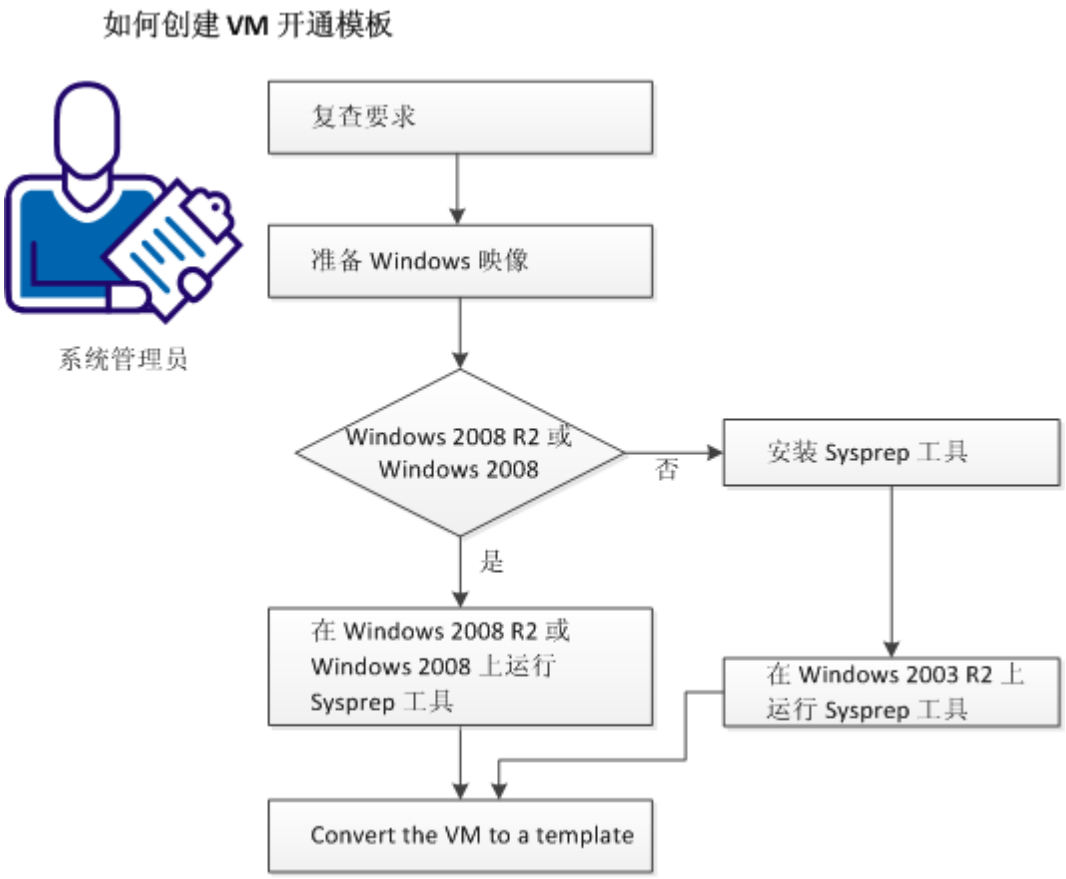
- 附加虚拟磁盘 
- 分离虚拟磁盘 
- 删除虚拟磁盘 

用法一目了然。如有必要，可以将光标悬停在图标上获得工具提示。

如何为 GalaX 开通准备 Windows 模板

CA Virtual Assurance 支持自定义开通运行 Windows 2003 R2 Server（32 位和 64 位）、Windows 2008（32 位和 64 位）或 Windows 2008 R2 Server（64 位）的新虚拟机 (VM)。自定义选项包括大量设置。例如，更改内置的管理员帐户密码、计算机名和网络配置。

下图说明了系统管理员如何为 GalaX 开通准备 Windows 模板。



Microsoft sysprep 工具允许您概括、冻结和关闭已配置好的 Windows 安装。以下部分详细描述了如何使用 Windows 2003 R2 和 Windows 2008 R2 的 Sysprep 工具。

在 Windows 2003 上，默认情况下不安装 Sysprep 工具，但是其可以在 Windows 安装 CD-ROM 中找到。

请执行以下步骤：

查看要求 (p. 355)
准备 Windows 映像 (p. 355)
在 Windows 2003 R2 上运行 Sysprep 工具 (p. 355)
在 Windows 2008 R2 上运行 Sysprep 工具 (p. 356)
在 GalaX 中将 VM 转换为模板 (p. 356)
使用开通的虚拟机 (p. 356)

查看要求

在 CA Virtual Assurance 创建虚拟机开通模板前请复查以下先决条件：

- 熟悉 Huawei GalaX 环境。
- 熟悉 CA Virtual Assurance 用户界面以及开通资源的方式。
- 已安装 CA Virtual Assurance，且可以访问 CA Virtual Assurance 用户界面。
- Huawei GalaX 环境可用且在运行。
- Huawei GalaX 环境中具有计算群集（对于虚拟机）和存储群集（对于虚拟磁盘）的服务器。
- 用户 VLAN 池和 VPC VLAN 池的服务器可用。
- CA Virtual Assurance 已发现 Huawei GalaX 服务器及其关联的资源（如群集、存储群集和虚拟机）。

准备 Windows 映像

在创建包含 Windows 操作系统的模板时，通过遵循此程序来准备映像。按照下述步骤操作以启用 CA Virtual Assurance 开通操作从而自定义模板。特定步骤会根据 Windows 的版本而有所不同。

遵循这些步骤:

1. 在新的虚拟机上从头开始安装 Windows 操作系统。
2. 在虚拟机上安装 SingleCloud Tools。
3. 应用您想在新的虚拟机上应用的任何自定义，如用户帐户、策略、应用程序、修补程序等。

在 Windows 2003 R2 上运行 Sysprep 工具

在配置 Sysprep 工具安装之后，运行 Sysprep 工具。

遵循这些步骤:

1. 查找并打开以下 CAB 文件：

   ```
   \SUPPORT\TOOLS\DEPLOY.CAB
   ```

2. 选择包含在 CAB 文件中的所有文件，并将其复制到以下位置：%SystemDrive%\Sysprep（通常为 C：\Sysprep）。

   注意：不要更改目录名称。

3. 转到 Sysprep 目录并运行以下命令：

   ```
   sysprep -quiet -reseal -mini -forceshutdown
   ```

在 Windows 2008 R2 上运行 Sysprep 工具

常规的 Windows 安装将安装所有文件以执行 Sysprep 过程。在您配置 Windows 安装之后，请执行以下步骤：

1. 转到以下目录：

   C:\Windows\system32\sysprep

2. 运行下列命令：

   ```
   sysprep /generalize /shutdown
   ```

sysprep 命令为安装准备映像，并关闭虚拟机。generalize 参数将删除所有唯一性系统信息，如计算机名称、日志文件、还原点和硬件特定信息。

在 GalaX 中将 VM 转换为模板

sysprep 命令关闭虚拟机后，转到 SingleCloud 用户界面以创建模板。

遵循这些步骤:

1. 登录 SingleCloud 用户界面。
2. 单击“VM”选项卡，并选择使用 sysprep 准备的虚拟机。
3. 右键单击虚拟机，然后选择“导出映像”。

   “导出映像”对话框打开。

4. 指定文件名，将映像类型设置为“Ghost”，然后单击“确定”。

   虚拟机即被存为 Ghost 映像。

5. 在 SingleCloud 用户界面中注册 Ghost 映像。

   现在，您便可以将 Ghost 映像用作开通模板。

使用开通的虚拟机

根据以前方案 (p. 353)创建的模板会导致已开通虚拟机出现以下行为：

初始启动已开通的虚拟机时，启动过程等待您的输入，例如区域设置、产品密钥、EULA，并让您指定该特定计算机的主机名。

要访问虚拟机，请确认 VNC 可用。

IBM PowerVM (LPAR)

IBM PowerVM 系统提供将系统划分为逻辑分区 (LPAR) 的功能。每个逻辑分区作为独立的系统运行，您可以在分区之间分发资源。通常每个系统都有一个称为“虚拟 I/O 服务器 (VIOS)”的专用分区，该分区虚拟化磁盘资源和网络接口。通过将系统分区，您可以考虑在动态共享虚拟化资源时进行单独计算的需要。PowerVM 系统有一个虚拟化管理器组件，该组件可以是硬件管理控制台 (HMC) 或集成虚拟化管理器 (IVM)。HMC 是在单个系统上运行的组件，用于管理多个 PowerVM 系统。IVM 是虚拟 I/O 服务器的扩展，只能管理本地 PowerVM 系统。

PowerVM AIM 允许 SystemEDGE 监控 LPAR 资源。

LPAR 平台管理模块 (PMM) 针对所有 LPAR 操作提供连接和操作支持。PMM 负责管理连接和从硬件管理控制台 (HMC) 或集成虚拟化管理器 (IVM) 检索数据，执行各种与 LPAR 相关的操作，填充数据库，以及为所有 HMC/IVM 交互提供 Web 服务/ssh。

您可以从 HMC/IVM 检索受管系统和 LPAR 数据，并执行以下与 LPAR 相关的操作：

服务器级别

在服务器级别上，可以执行以下任务：

- 开通 LPAR
- 删除 LPAR

电源操作级别

在电源操作级别上，可以执行以下任务：

- 激活 LPAR
- 关闭 LPAR
- 重新启动 LPAR

资源调整级别

在资源调整级别上，可以执行以下任务：

- 增加 LPAR 处理器和内存单元
- 减少 LPAR 处理器和内存单元

IBM PowerVM 服务器管理概述

使用 CA Virtual Assurance 的 CA IBM PowerVM 组件可以监控和管理 IBM PowerVM 资源。受监控资源和受管资源包括以下类型：

- 硬件管理控制台 (HMC)
- 集成虚拟化管理器 (IVM)
- 虚拟 IO 服务器 (VIOS)
- 受管系统（POWER 服务器）
- 逻辑分区 (LPAR)

硬件管理控制台 (HMC) 是一个外部组件，用于在 IBM PowerVM 系统上执行管理任务。HMC 可用于创建或更改逻辑分区，包括为分区动态分配资源。HMC 与 POWER 系统的服务器固件层进行通信，在大型 PowerVM 环境中提供单一控制点。

集成虚拟化管理器 (IVM) 是虚拟 I/O 服务器 (VIOS) 的增强，使用 IVM 可以管理单个 POWER 系统。使用 IVM 可以创建和管理 LPAR。IVM 支持 VIOS 功能的管理并提供基于 Web 的用户界面。

虚拟 I/O 服务器 (VIOS) 是一个配置为拥有所有物理 I/O 资源的特殊逻辑分区，它向其他 LPAR 提供其虚拟化功能。LPAR 作为虚拟设备通过虚拟 I/O 服务器访问磁盘、网络和光学设备。具有虚拟化资源的每个 PowerVM 系统均具有虚拟 I/O 服务器。

逻辑分区 (LPAR) 是硬件资源的子集，虚拟化为单独的系统。一个物理系统可以分区为多个 LPAR，每个 LPAR 都提供单独的操作系统和应用程序。逻辑分区的数目取决于系统的硬件配置。LPAR 作为单独的系统在网络中进行通信。

要管理 IBM PowerVM 资源，请向 HMC/IVM 服务器和虚拟 I/O 服务器提供 SSH 访问凭据。

通过使用 CA Virtual Assurance 管理、配置、开通、IBM PowerVM 组，您可以配置 CA Virtual Assurance 来管理 PowerVM 资源。

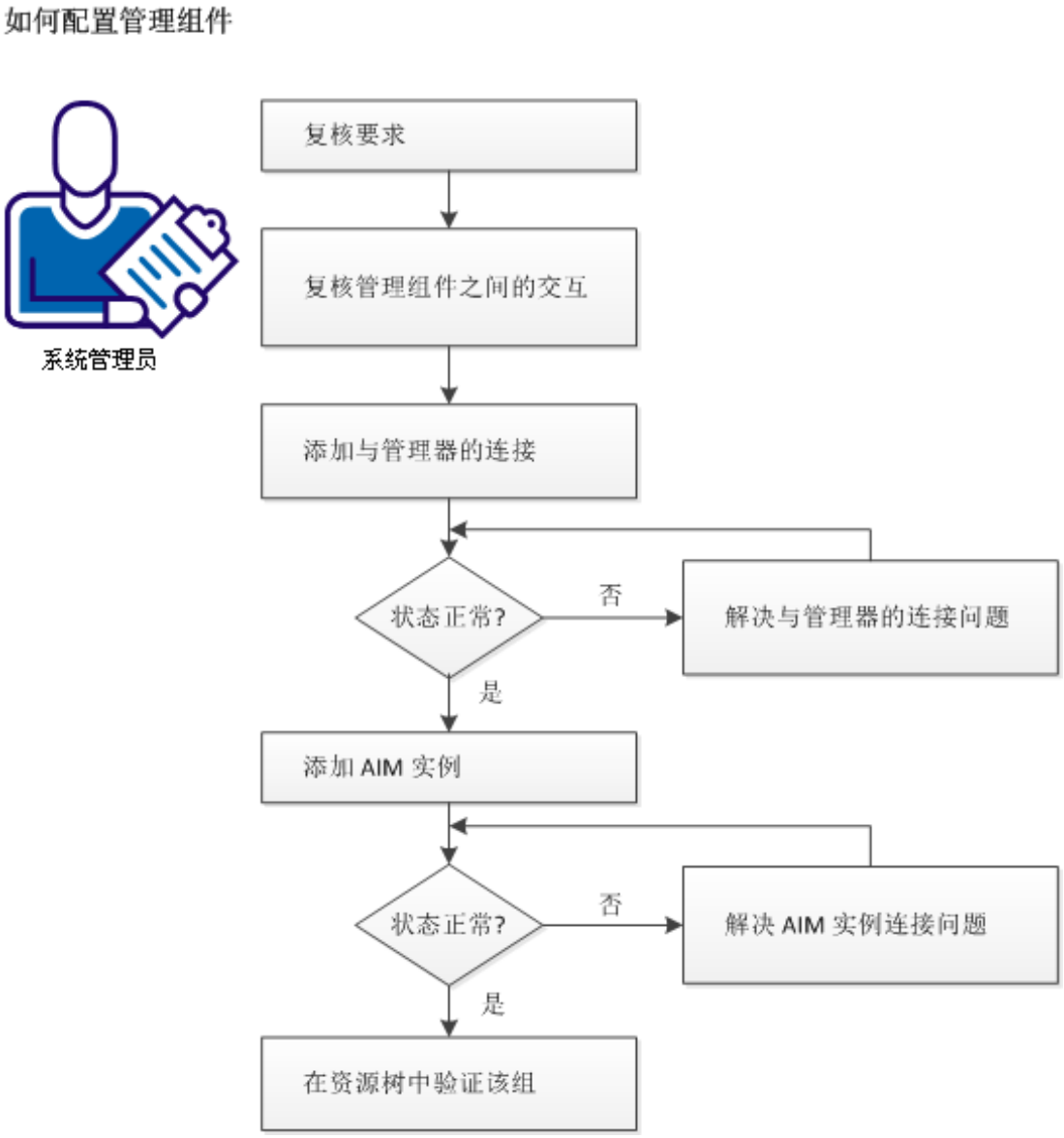
可用面板如下：

- HMC/IVM 服务器
- 虚拟 I/O 服务器
- LPAR AIM 服务器

LPAR AIM 服务器是运行 SystemEDGE 和 LPAR AIM 的系统。LPAR AIM 可以在本地 CA Virtual Assurance 管理器系统或远程 Windows 服务器上运行。LPAR AIM 是一个可以连接到多个 HMC 或 IVM 的多实例 AIM。一旦 AIM 开始管理 HMC 或 IVM 服务器，AIM 就会发现和管理连接到此 HMC 或 IVM 服务器的所有 P 服务器。

如何配置 PowerVM 管理组件

下图提供了有关配置管理组件所需操作的概述。该图包括针对连接问题的相应故障排除策略。



请执行以下步骤：

查看要求

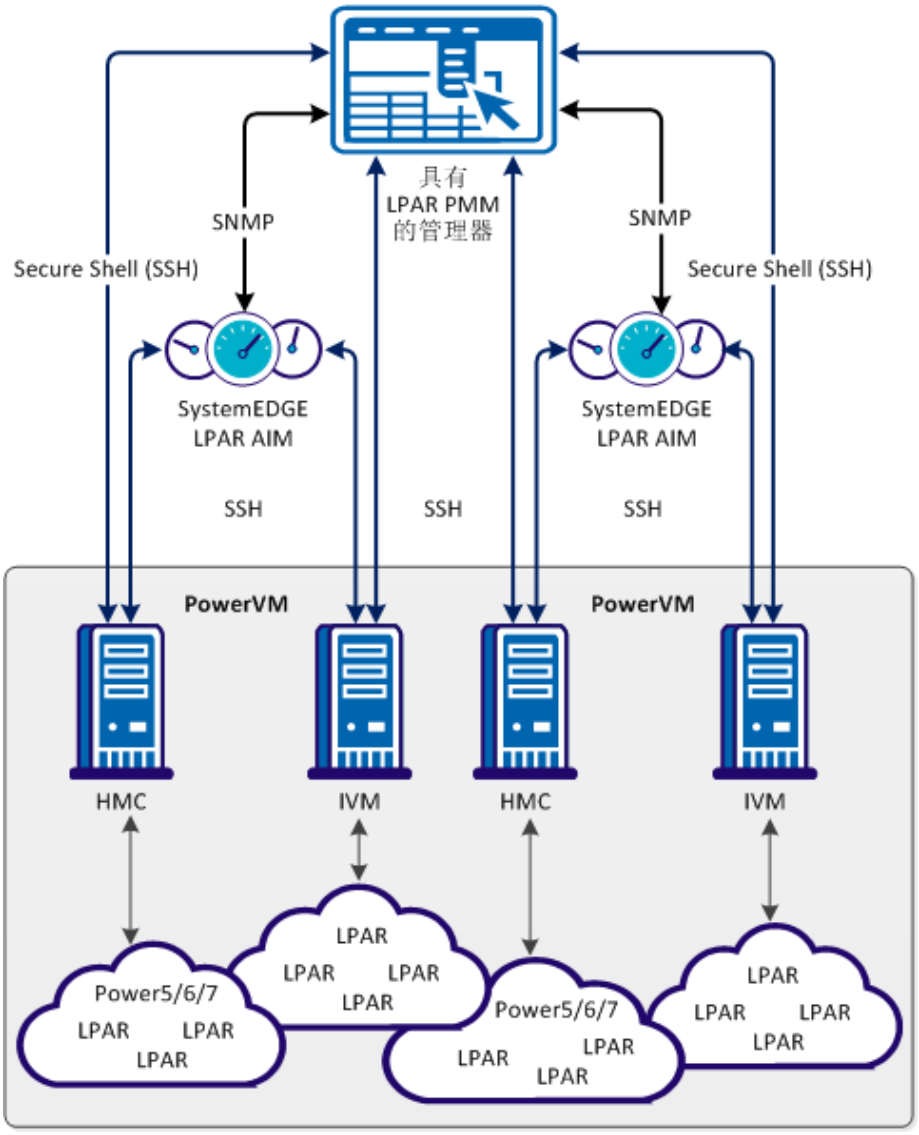
在配置 CA Virtual Assurance 的管理组件之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您熟悉 CA Virtual Assurance 和 SystemEDGE。
- 您可以访问包括以下内容的 CA Virtual Assurance 管理器安装：
  - 平台管理模块 (PMM)
  - Application Insight Module (AIM)
  - 监控代理 (SystemEDGE)
- 您可以访问 CA Virtual Assurance 用户界面。
- 您具有有效的凭据（用户名和密码），可访问要管理的环境中的服务器。
- 您知道使用哪个协议（HTTP 或 HTTPS）和端口，以通过 Web 服务访问环境中的服务器。默认：HTTPS，端口：443。
- 您已验证环境中的服务器运行正常。
- 如果将 PMM 和 AIM 安装在不同系统上，请确认 PMM 和 AIM 系统上的 SNMP 设置一致。读和写团体字符串以及 SNMP 端口号必须是相同的。
- 您已验证 CA Virtual Assurance 管理器已发现您要使用的远程 AIM 服务器。

AIX LPAR 管理组件之间的交互

下图说明 IBM LPAR 管理中的组件是如何交互的。AIM 服务器是运行 SystemEDGE 和 LPAR AIM 的 Windows 服务器。AIM 和 HMC/IVM 服务器根据 SSH（安全外壳）进行通信。因为 CA Virtual Assurance 可以连接到多个 HMC 或 IVM 服务器，所以 CA Virtual Assurance 可以获得 LPAR 环境的概览视图。

PowerVM 管理组件之间的交互



安装之后，通过为每个需要的 HMC/IVM 和虚拟 I/O 服务器添加必需的连接信息来配置您的环境。使用以下方法之一：

- 用户界面的“管理”选项卡
- AIM 服务器上的 NodeCfgUtil.exe 实用工具

连接信息将写入受管节点上的配置文件中。LPAR AIM 调查配置文件并开始通过 HMC/IVM 监控您的 LPAR 环境。

IBM PowerVM 配置用例

以下用例介绍了对“管理”选项卡中受管 PowerVM 环境的 LPAR AIM 实例条目的处理：

- 您添加了一个 HMC 服务器和一个 LPAR AIM 实例。

  AIM 将发现：

  - 与 HMC 关联的 Power 系统。
  - 与 Power 系统关联的虚拟 I/O 服务器。在添加 HMC 时，AIM 将应用指定的默认 VIOS 凭据。

    重要信息！如果您不指定 HMC 服务器的默认 VIOS 凭据，请在“虚拟 I/O 服务器”面板中为*每个* VIOS 提供 VIOS 凭据，以完成发现的 VIOS 的配置。如果默认 VIOS 凭据不适用于特定 VIOS，您可以在“虚拟 I/O 服务器”面板中覆盖这些凭据。

- 首选 AIM

  两个 AIM 可以管理一个 HMC。第二次添加的 AIM 将成为冗余 AIM，而第一次添加的 AIM 将成为首选 AIM。冗余 AIM 下的 HMC 的状态变为“已挂起”。此状态反映 HMC 由首选 AIM 管理。您可以在“HMC/IVM 服务器”面板中更改首选 AIM。

- 双 HMC 功能支持 P 系统与两个 HMC 服务器关联的配置。

  P 服务器和关联的 HMC 服务器是一个原子管理实体，因此，它们必须由一个 AIM 管理。双 HMC 配置仅在一个 AIM 的范围内受支持。例如，一个 Power 系统 (P1) 连接到两个 HMC 服务器（HMC1 和 HMC2）。两个 HMC 服务器将由一个 AIM (AIM1) 管理。

- 双 HMC 故障切换

  如果首选 HMC 失败，冗余 HMC 将自动开始管理您的系统。冗余 HMC 成为当前 HMC。然而，在首选 HMC 可用时，当前 HMC 将不发生更改。要再次通过首选 HMC 管理您的系统，请在“管理”、“配置”选项卡上的“LPAR AIM 服务器”面板中更改当前 HMC。

  注意：如果首选 HMC 失败，冗余 HMC 将管理您的系统。在故障切换之后，您可以为您的系统手动更改当前 HMC。

- 您未指定输入错误的虚拟 I/O 服务器凭据的默认 VIOS 凭据。

  用户界面将显示有关操作失败的消息。尝试应用错误的虚拟 I/O 服务器凭据 () 时，虚拟 I/O 服务器将更改为“身份验证失败”状态。由于连接问题，受管系统实例将从“挂起的 VIOS”状态更改为“过期”。

- 添加没有虚拟 I/O 服务器的受管系统实例。

  受管系统实例将显示在实例表中，状态为“就绪”。

- 将 P 服务器添加到受管系统中。

  将自动发现新的 P 服务器和 VIOS。如果 VIOS 凭据匹配默认 VIOS 凭据，则将不需要配置。如果 VIOS 凭据不匹配默认 VIOS 凭据，请设置 AIM 实例 () 的 VIOS 凭据。

- 将从受管系统中删除处于“无效配置”状态的虚拟 I/O 服务器。

  LPAR AIM 将从实例表中删除相应的记录并将受管系统更改为“就绪”状态。

- 将从受管系统中删除处于“就绪”状态的虚拟 I/O 服务器。

  LPAR AIM 将从实例表中删除相应的记录。

- 删除具有一个或多个虚拟 I/O 服务器的受管系统实例。

  受管系统实例及关联的虚拟 I/O 服务器条目将从实例表中消失。

- IBM PowerVM 管理窗格通过图标和工具提示显示状态信息。

  将光标悬停在警告和错误图标上时，将看到详细工具提示。

  可能会显示以下图标：

   发现正在进行

   无轮询

   错误

   警告

   已禁用

   未知

将 HMC 或 IVM 服务器连接添加到管理器中

您可以使用 CA Virtual Assurance 用户界面的“管理”选项卡来添加 HMC 或 IVM 服务器连接。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“IBM PowerVM”。

   右侧窗格将刷新和显示受管 HMC 和 IVM 服务器、关联的虚拟 I/O 服务器以及 LPAR AIM 服务器。

3. 在“HMC/IVM 服务器”窗格工具栏上单击  （添加）。

   此时将显示“新建 HMC/IVM 服务器”对话框。

4. 输入所需的连接数据（服务器名称、用户、密码），指定首选 AIM，启用“受管状态”（复选框）。
   注意：只有为给定 HMC 或 IVM 服务器指定了多个 AIM 实例，首选 AIM 字段才处于活动状态。

5. （可选）指定虚拟 I/O 服务器默认凭据。

   默认 VIOS 凭据适用于最发现的 VIO 服务器。

   重要信息！如果您不指定 HMC 服务器的默认 VIOS 凭据，请在“虚拟 I/O 服务器”面板中为*每个* VIOS 提供 VIOS 凭据，以完成发现的 VIOS 的配置。如果默认 VIOS 凭据不适用于特定 VIOS，您可以在“虚拟 I/O 服务器”面板中覆盖这些凭据。

6. 单击“确定”。

   如果网络连接已成功建立，该服务器将被添加到右上角的“HMC/IVM 服务器”窗格并带有绿色状态图标。CA Virtual Assurance 自动发现 HMC/IVM 服务器。

   如果连接失败，将显示“验证失败”对话框。如果您单击“是”，CA Virtual Assurance 会将服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。

管理器到服务器的连接失败

症状：

在“管理”、“配置”下添加服务器连接后，对服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的服务器连接数据是否仍然有效。如有必要，请更新连接数据。
- 验证服务器系统是否正在运行并且可以访问。
- 验证连接所需的所有服务是否在服务器系统上运行良好。

更新服务器连接数据：

1. 单击与失败的连接关联的  （添加）或  （编辑）。
2. 添加连接详细信息，启用“受管状态”，然后单击“确定”。

   将更新连接数据。
3. 单击右上角的  （验证）以验证新设置。

   如果无法建立与服务器的连接，请继续执行下一步骤。

验证服务器系统是否正在运行并且可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```
2. 要确定服务器是否具有有效的 DNS 条目和 IP 地址，请检查这些命令的输出。

   如果服务器不在 DNS 中，请将服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ipaddress <Server Name>

   输入正确的 IP 地址和服务器名称并保存文件。例如：

   192.168.50.50 myServer

4. 切换到 CA Virtual Assurance 用户界面、“管理”选项卡、“配置”、“服务器”窗格，并单击右上角的（验证）。

   即使服务器凭据和连接数据正确并且您可以 ping 服务器，连接仍然可能失败。在这种情况下，可能是服务器引起该问题。如果无法建立与服务器的连接，请继续执行下一步骤。

验证连接所需的所有服务是否在服务器系统上运行良好。

1. 要访问服务器，请联系系统管理员。
2. 登录到服务器系统。
3. 验证连接所需的所有服务是否运行良好。
4. 如有必要，请启动或重新启动服务。
5. 切换到管理器系统上的 CA Virtual Assurance 用户界面、服务器窗格，并单击右上角的（验证）。

   CA Virtual Assurance 将验证服务器连接。

   如果与服务器的连接失败，请验证根据该方案的要求收集的数据是否有效。

   与管理员或技术支持合作，解决服务器连接问题。

添加 LPAR AIM 实例

在将 HMC 或 IVM 服务器连接添加到 CA Virtual Assurance 管理器之后，添加 AIM 实例以管理新的服务器。CA Virtual Assurance 随后发现 PowerVM 环境。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“IBM PowerVM”。

   右侧窗格将刷新和显示受管 HMC 和 IVM 服务器、关联的虚拟 I/O 服务器以及 LPAR AIM 服务器。

3. 在“LPAR AIM 服务器”窗格工具栏上单击  （添加）。

   此时将显示“新建 LPAR AIM 服务器”对话框。

4. 从下拉列表中选择“LPAR AIM 服务器”。

   将显示发现的 LPAR AIM 服务器的列表。如果您已在本地系统上安装了 LPAR AIM，本地系统的名称也会显示在列表中。

5. 从下拉列表中选择“HMC 或 IVM 服务器”。

   CA Virtual Assurance 使用“HMC/IVM 服务器”窗格中列出的 HMC 和 IVM 服务器填充“HMC/IVM 服务器”下拉列表。您只能管理您的 CA Virtual Assurance 管理器与之建立了有效连接的那些 HMC 或 IVM 服务器。

   注意：如果 AIM 位于远程系统中，则 CA Virtual Assurance 一定会首先发现该系统。在发现之后，AIM 服务器将在下拉列表中显示。

6. 单击“确定”。

   将添加选定的服务器的新 AIM 实例。如果实例未处于错误或已停止状态，CA Virtual Assurance 将开始发现关联的 PowerVM 环境：

   - 对于每个 HMC 服务器，AIM 可发现所有 Power 系统和虚拟 I/O 服务器。
   - 对于每个 IVM 服务器，AIM 可发现 IVM 管理的 Power 系统。

   在发现过程完成后，您可以开始管理您的 PowerVM 环境。

“管理”选项卡将显示 AIM 发现的所有 P 系统和 VIO 服务器的聚合状态。要查看其各自的配置状态，请按“显示受管系统”  图标。

更改受管 Power 系统的首选 HMC

如果您的 Power 系统使用双 HMC，您可以更改首选 HMC。

重要信息！确认一个 LPAR AIM 可同时管理主 HMC 服务器和冗余 HMC 服务器。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“IBM PowerVM”。

   右侧窗格将刷新和显示受管 HMC 和 IVM 服务器、关联的虚拟 I/O 服务器以及 LPAR AIM 服务器。

3. 单击 （配置受管/VIO 服务器），其与 HMC 服务器关联。

   将显示带有受管/VIO 服务器的“IBM PowerVM”对话框。

4. 在“操作”行下单击 （切换首选 HMC）并确认。

   冗余 HMC 已设置为首选 HMC。

排除 AIM 实例连接的故障

如果 AIM 连接处于未就绪状态，将出现以下状态图标之一：

- 发现正在进行
- 无轮询
- 错误
- 警告
- 已禁用
- 未知

有关 AIM 实例状态的详细信息，请参阅工具提示。以下故障排除部分提供了用于解决该问题的详细信息和步骤。

AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为服务器添加 AIM 实例后，状态图标显示  （发现正在进行）。

解决方案：

等到环境的发现过程完成。发现持续时间取决于与环境中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示指示未完成发现请求数量的工具提示。发现作业完成时，CA Virtual Assurance 会向资源树中添加一个服务器文件夹。然后，您可以开始管理您的环境。

AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （无轮询）。

解决方案：

关联实例不需要特定的操作。此图标表示 CA Virtual Assurance 管理器不轮询此 AIM。AIM 不是首选。

如果多个 AIM 已配置为管理特定服务器，PMM 将选择其中一个 AIM 作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决可能导致与 AIM 连接失败的最常见问题：

- 验证是否可以访问 AIM 服务器。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 确认命令的输出对于 AIM 服务器有有效的 DNS 条目和 IP 地址。

   如果 AIM 服务器不在 DNS 中，则将 AIM 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress servername
   ```

   输入正确的 IP 地址和 AIM 服务器名称。例如：

   ```
   192.168.50.51 myAIM
   ```

4. 在“AIM 服务器”窗格的右上角，单击 （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“AIM 服务器”窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证 AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否有效。

AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 AIM 实例之后，几个实例的状态图标显示 （已禁用）。该 AIM 实例未受管理。

如果 CA Virtual Assurance 发现具有以下关系的 AIM，则显示该状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的服务器配置了 AIM。
- AIM 连接到未配置的服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的服务器连接并将其受管状态更改为已启用。

验证资源树中的组

在成功配置和发现之后，新发现的资源将在“资源”、“浏览”窗格中的相应组下列出。

遵循这些步骤:

1. 单击“资源”，然后打开“浏览”窗格。
2. 展开 IBM PowerVM 组。

   将显示受管 HMC 和 IVM 服务器。
3. 展开 HMC 或 IVM 服务器条目。

   将显示受管系统。

CA Virtual Assurance 现在可以用于管理添加的 PowerVM 环境及其虚拟基础架构。

calpara.xml 文件

calpara.xml 文件的主要的目的是存储 LPAR AIM 配置数据，如：持久数据和默认值。可调整监控设置，以适应特定环境。

本文档适用于熟悉 XML 格式的系统管理员。我们建议谨慎更改此文件。要更改 calpara.xml 文件，请先停止 SystemEDGE，然后在更改文件之后再次启动 SystemEDGE。

重要信息！如果需要调整监控阈值、延迟或严重度，仅可更改默认值。修改轮询组和 DisableOutOfDate 设置的操作仅可应 CA 支持部门要求进行。

calpara.xml 文件位于以下位置：

```
<SystemEDGE_InstallDir>\plugins\calpara\calpara.xml
```

持久数据

持久数据在 AIM 下次启动时可用。根据 SNMP 设置要求，此数据在 AIM 生命周期内可以更改并可供用户设置。

以下列表提供了持久数据的示例：

- 实例
- 系统
- 分区
- 插槽
- 轮询组

实例

对于实例表 (lparAimInstanceTable) 中每个配置的实例，存储类似于以下示例的部分：

```
<ManagedInstance>
    <InstIndex>7</InstIndex>
    <SerialNr>1010101</SerialNr>
    <ServerName>vios1.company.com</ServerName>
    <ServerType>vios</ServerType>
    <RowStatus>1</RowStatus>
</ManagedInstance>
```

ServerType

指定下列其中一种服务器类型：hmc、vios 或 ivm。

RowStatus

指定其状态为 active (1) 或 notInService (2)。

系统

对于系统表 (lparAimStatSysTable) 中的每个受管 Power 系统，类似于以下示例的部分将存储在相关的“ManagedInstance”部分中：

```
<System>
    <MonitorIndices>530091,530092,530093,530094,530095</MonitorIndices>
</System>
```

MonitorIndices

存储 SystemEDGE 监视器的索引，该监视器由 AIM 创建以监控 Power 系统的操作状态、CPU 和内存使用情况。

注意：如果 AIM 不再管理电源系统，相应的监视器将被删除。

分区

对于分区表 (lparAimStatLPTable) 中的每个受管逻辑分区，类似于下列的示例的四个相应的条目将存储在相关“ManagedInstance”部分的“分区”部分中：

```
<Partitions>
    ...
    <LparIndex>7</LparIndex>
    <LparId>7</LparId>
    <LparName>LPAR12345</LparName>
    <MonitorIndices>530141,530142,530143,530144,530145</MonitorIndices>
    ...
</Partitions>
```

注意：如果 AIM 不再管理电源系统，相应的监视器将被删除。

插槽

对于插槽表 (lparAimStatSlotTable) 中的每个物理插槽，类似于下列的示例的四个相应的条目将存储在相关“ManagedInstance”部分的“插槽”部分中：

```
<Slots>
    ...
    <SlotIndex>3</SlotIndex>
    <DRCName>U787B.001.DNWFF77-P1-C3</DRCName>
    <DRCIndex>553713666</DRCIndex>
    <SlotName>C3</SlotName>
    ...
</Slots>
```

LPAR AIM 在启动之后立即使用此数据来检测任何与插槽相关的变更，此操作可能导致发送相应的 SNMP 陷阱。

轮询组

轮询组是一组相关命令，所有命令都以相同的轮询时间间隔执行。对于轮询表 (lparAimPollTable) 中的每个轮询组，将存储各自“轮询组”部分中的三个相应条目。以下示例显示了基本轮询组：

```
<Basic>
    <PollDefault>5</PollDefault>
    <PollSpecific>30,30</PollSpecific>
    <PollInstances>4,6</PollInstances>
</Basic>
```

PollDefault

存储默认的轮询时间间隔（以分钟为单位）以适用除 PollInstances（其中列出了实例的索引）中所列实例之外的所有实例。

PollSpecific

存储轮询时间间隔（以分钟为单位）的列表，以便一对一应用到存储在 PollInstances 中的相应实例列表。

注意：初始状态下，PollSpecific 和 PollInstances 为空。

默认值

以下部分介绍了 calpara.xml 文件（其中指定了延迟、阈值和严重度）中存储的默认值，当创建新的 SystemEDGE 监视器时，AIM 将使用这些值。

重要信息！默认值在 AIM 生命周期内无法更改，且用户不可对其进行设置。

```
<LowestPollInterval>5</LowestPollInterval>
<DisableOutOfDate>0</DisableOutOfDate>
<MonitorIndexStart>530001</MonitorIndexStart>
<SysAliveSev>fatal</SysAliveSev>
<CpuLagValue>3</CpuLagValue>
<CpuThresh1Val>95</CpuThresh1Val>
<CpuThresh1Sev>warning</CpuThresh1Sev>
<CpuThresh2Val>98</CpuThresh2Val>
<CpuThresh2Sev>critical</CpuThresh2Sev>
<MemLagValue>2</MemLagValue>
<MemThresh1Val>95</MemThresh1Val>
<MemThresh1Sev>warning</MemThresh1Sev>
<MemThresh2Val>98</MemThresh2Val>
<MemThresh2Sev>critical</MemThresh2Sev>
```

LowestPollInterval

存储允许的最短轮询时间间隔（以分钟为单位）。

DisableOutOfDate

指定数据状态 (lparAimInstDataStatus) outOfDate 是否已排除。

注意：将此变量设置为 1 可在任何命令执行失败的情况下禁用数据状态变为 outOfDate(7)。

默认：0

MonitorIndexStart

指定 AIM 在启动后创建的第一个 SystemEDGE 监视器的索引。

注意：当创建新监视器时，AIM 将始终搜索等于或大于该值的下一个自由索引。

SysAliveSev

指定 AIM 创建的 SystemEDGE 监视器的重要级别，相应监视器可用于监控电源系统或逻辑分区的操作状态。

有效值：正常、警告、轻微、重大、严重、致命。

注意：更改此值不会对现有监视器产生影响。

CpuThresh1Val 和 CpuThresh2Val

指定 AIM 创建的两个 SystemEDGE 监视器的阈值，相应监视器可用于监控电源系统或逻辑分区的 CPU 使用情况。

限制：0 到 100。

注意：更改此值不会对现有监视器产生影响。

CpuThresh1Sev 和 CpuThresh2Sev

指定 AIM 创建的两个 SystemEDGE 监视器的重要级别，相应监视器可用于监控电源系统或逻辑分区的 CPU 使用情况。

有效值：正常、警告、轻微、重大、严重、致命。

注意：更改此值不会对现有监视器产生影响。

MemThresh1Val 和 MemThresh2Val

指定 AIM 创建的两个 SystemEDGE 监视器的阈值，相应监视器可用于监控电源系统或逻辑分区的内存使用情况。

限制：0 到 100。

注意：更改此值不会对现有监视器产生影响。

MemThresh1Sev 和 MemThresh2Sev

指定 AIM 创建的两个 SystemEDGE 监视器的重要级别，相应监视器可用于监控电源系统或逻辑分区的内存使用情况。

有效值：正常、警告、轻微、重大、严重、致命。

注意：更改此值不会对现有监视器产生影响。

CpuLagValue 和 MemLagValue

指定 AIM 创建的 SystemEDGE 监视器的延迟值，相应监视器可用于监控电源系统或逻辑分区的 CPU 和内存使用情况。延迟值指定监视器在更改其状态之前达到阈值的连续轮询时间间隔（基本轮询组）数。

注意：更改此值不会对现有监视器产生影响。

LPAR 监控

要监控 LPAR 资源，请基于 sysedge.cf 文件中的 LPAR AIM MIB 和 SystemEDGE 组件对象模型创建 SystemEDGE 监视器，而无需使用 UI 功能。使用适当对象类并根据 LPAR 资源指定对象实例。创建的受监控 LPAR 对象将其状态传递到安装 LPAR AIM 的计算机系统。建议您在 monObjInstance 属性中提供 HMC、POWER5/POWER6/POWER7 和 LPAR 系统信息，类似如下示例。

示例

sysedge.cf 文件的以下监控定义设置为监视名为 *powersys* 的 POWER5 或 POWER6 系统的活动状态。将名为 *lpar01* 的 LPAR 设置为大于 2，也就是说，3 为警告、4 为轻微等。

```
monitor oid monCurrState.53001 98 0x0 60 absolute > 2 'Lpar System status'   ''
'System' 'hmc/powersys/Total'        Alive critical
monitor oid monCurrState.53006 99 0x0 60 absolute > 2 'Lpar01 System status' ''
'System' 'hmc/powersys/lpar01/Total' Alive critical
```

注意：监视器的实例名不能以 lpar:// 开头

下表显示了与 sysedge.cf 文件的监控定义示例相对应的自主监视器表的示例。

mon Index	monOID	mon ObjClass	monObjInstance	mon ObjAttribute	mon Severity	mon CurrState
530001	lparAimStatSys Status.1	系统	lpar://System:Serial Number/Total	活动	严重	确定
530002	lparAimStatSys CPUUsage PerMil.1	CPU	lpar://System:Serial Number/Total	PercentUsed	警告	确定
530003	lparAimStatSys CPUUsage PerMil.1	CPU	lpar://System:Serial Number/Total	PercentUsed	轻微	确定
530004	lparAimStatSys MemoryUsage PerMil.1	内存	lpar://System:Serial Number/Total	PercentUsed	警告	警告
530005	lparAimStatSys MemoryUsage PerMil.1	内存	lpar://System:Serial Number/Total	PercentUsed	轻微	轻微
530006	lparAimStatLP Status.1.1	系统	lpar://System:Serial Number/lpar01/Total	活动	严重	严重

mon Index	monOID	mon ObjClass	monObjInstance	mon ObjAttribute	mon Severity	mon CurrState
530007	lparAimStatLPCPU Usage.1.1	CPU	lpar://System:Serial Number/lpar01/Total	PercentUsed	警告	确定
530008	lparAimStatLPCPU Usage.1.1	CPU	lpar://System:Serial Number/lpar01/Total	PercentUsed	轻微	确定
530009	lparAimStatLP MemoryUsage.1.1	内存	lpar://System:Serial Number/lpar01/Total	PercentUsed	警告	确定
530010	lparAimStatLP MemoryUsage.1.1	内存	lpar://System:Serial Number/lpar01/Total	PercentUsed	轻微	确定
530011	lparAimStatLP Status.1.2	系统	lpar://System:Serial Number/lpar02/Total	活动	严重	严重
530012	lparAimStatLPCPU Usage.1.2	CPU	lpar://System:Serial Number/lpar02/Total	PercentUsed	警告	确定
530013	lparAimStatLPCPU Usage.1.2	CPU	lpar://System:Serial Number/lpar02/Total	PercentUsed	轻微	确定
530014	lparAimStatLP 内存 Usage.1.2	内存	lpar://System:Serial Number/lpar02/Total	PercentUsed	警告	确定

IBM PowerVM 管理

本节介绍可通过“资源”页面执行的 IBM PowerVM 管理操作。

通过“资源”页面，您可以查看事件并对 LPAR 执行管理操作。在“浏览”窗格中展开 IBM PowerVM 组可列出以下对象：

- HMC/IVM 服务器
- PowerVM 系统
- 逻辑分区 (LPAR)

查看资源摘要和事件

CA Virtual Assurance 在右侧窗格中显示“摘要”。“摘要”页面在对象层次结构中的以下级别提供资源属性：

- PowerVM Server
- LPAR

“性能图表”窗格以可用度量标准和选项显示使用率。使用相应的筛选设置来显示所需的性能图表：

- CPU
- 内存
- 其他度量标准

“常规信息”窗格包括以下属性：

- Name, Item Type, Type (pSeries)
- CPU 和内存的数量特征
- LPAR 的数量和可用的处理单元
- 序列号

“概述”窗格显示有关以下内容的信息：

- CPU 状态
- 内存状态
- 操作状态
- 运行状况
- 传播的运行状况
- 收集引擎状态

通过“摘要”选项卡，您可以查看与该对象相关的信息，例如，总内存、操作系统、CPU 数目、IP 地址、CPU 和内存总体使用率以及与资源相关的事件。在“用法”面板上单击“配置”选项卡可配置阈值限制。

控制逻辑分区的电源状态

可以通过执行以下操作之一来控制逻辑分区的状态：

- 激活
- 重新启动
- 关闭
- 删除

您可以同时对一个或多个逻辑分区执行上述任意操作。

遵循这些步骤:

1. 在“浏览”窗格中选择要在其上执行状态操作的受管计算机。
2. 右键单击该分区，选择“管理”。还可以单击“快速启动”，然后单击相关的电源控制链接。选择以下选项之一：

   激活

   激活当前已关闭或挂起的选定逻辑分区。

   重新启动

   关闭来宾操作系统并重新启动。

   关闭

   关闭选定逻辑分区。您只能关闭当前已打开的逻辑分区。

   删除

   永久删除选定逻辑分区。您只能删除当前已关闭的逻辑分区。

   这时将会出现确认对话框。
3. 单击“确定”。

   状态操作发生后，将出现一条确认信息。刷新界面以查看新的逻辑分区状态。会出现一个确认操作结果的事件。

激活逻辑分区

激活逻辑分区，以便确认分区的资源并启动安装的操作系统。仅当分区未运行时才能将其激活。

激活逻辑分区

1. 在“浏览”窗格上右键单击某个分区，然后选择“管理”、“激活”。

   此时将显示“激活逻辑分区”对话框。

2. 填写下列字段，然后单击“确定”。

   配置文件

   指定用于激活分区的分区配置文件。

   键盘锁定

   指定键盘锁定位置。键盘锁定将建立系统所允许的打开电源和关闭电源模式。CA Virtual Assurance 支持以下有效的键盘锁定模式：

   不要覆盖

   LPAR 使用在选择的配置文件中指定的键盘锁定模式。

   正常

   LPAR 正常启动。使用该选项可执行大多数日常任务。

   手动

   将键盘锁定位置设置为“手动”时，请考虑安全影响。

   启动模式

   指定引导模式。仅当要使用不同于在选择的配置文件中指定的引导模式时，才选择引导模式并选中“激活”复选框。除非您在激活分区配置文件时指定其他模式，否则系统将使用该启动模式启动逻辑分区上的操作系统。CA Virtual Assurance 支持以下有效的引导模式：

   不要覆盖

   LPAR 使用在选择的配置文件中指定的引导模式。

   正常

   LPAR 正常启动。使用该选项可执行大多数日常任务。

   开放固件

   LPAR 引导至开放固件提示。该选项供服务人员获得其他调试信息使用。

3. 单击分区对应的“事件”选项卡。

   会出现一个确认操作结果的事件。

为 IBM AIX 计算机添加逻辑分区

可以使用“开通”向导为 IBM AIX 系统创建逻辑分区。

为 IBM AIX 计算机添加逻辑分区

1. 单击“资源”。
2. 右键单击“浏览”窗格中的 IBM PowerVM 组，并依次选择“开通”、“开通 LPAR”。

   此时将显示“开通”向导，以及“分区和内存”页面。
3. 选择 HMC/IVM 服务器和受管系统的名称。指定分区名称，以及配置文件名称（如果使用 HMC 服务器）。指定分区的最小内存、所需内存和最大内存。单击“下一步”。

   此时将显示“处理器”页面。
4. 指定要分配部分处理器单元还是专用处理器，以及最小、期望和最大处理器单元。高级设置适用于共享模式和虚拟处理器。单击“下一步”。

   此时将显示“I/O 组件”页面。
5. 选择要与分区关联的 I/O 设备，然后单击“下一步”。

   注意：对于每个 I/O 设备，您可以指定该 I/O 设备对于逻辑分区激活是必需的还是可选的。如果 I/O 设备是必需的，且 I/O 设备不可用或正被其他逻辑分区使用，则无法该激活分区。如果 I/O 设备是可选的，且激活分区时期望的 I/O 设备可用，则受管系统会将 I/O 设备提交到分区。如果可选的 I/O 设备不可用，则受管系统将跳过该 I/O 设备。

   此时将显示“I/O 池”页面。
6. （可选）要创建新的 I/O 池，请单击“I/O 池”表上的 +（添加），输入数值，然后单击“保存”。

   注意：当您将 I/O 设备添加到分区，且 I/O 设备属于 I/O 池时。激活该分区后，受管系统会自动将为该分区定义的 I/O 池添加到逻辑分区中。
7. 单击“下一步”。

   如果选择了 HMC 服务器，将显示“虚拟序列”页面。
8. （可选）为分区指定最大数目的虚拟适配器。要创建新的虚拟串行适配器，请单击 +（添加）并指定适配器 ID、远程分区和远程插槽号。您可以要求必须分配虚拟适配器，受管系统必须有足够内存来运行分区配置文件所需的虚拟适配器，否则不激活逻辑分区。

9. 单击“下一步”。

   此时将显示“虚拟以太网”页面。

10. 为分区指定最大数目的虚拟以太网适配器。（可选）您可以添加新的虚拟以太网适配器，具体步骤为：单击 +（添加）并选择适配器 ID、虚拟 LAN ID、访问外部网络、链接汇聚优先级、IEEE 802.1 Q 兼容性、其他虚拟 LAN ID 以及是否需要以太网适配器。

11. 单击“下一步”。

    此时将显示“虚拟磁盘”页面。

12. 指定分区的虚拟 SCSI 设备。（可选）要添加新的虚拟 SCSI 适配器，请单击“虚拟 SCSI 适配器”表上的 +（添加）。

    选择适配器 ID，指定是否需要 SCSI 适配器，并从“SCSI 设备”表中选取某一设备名称。如果期望的设备在“SCSI 设备”列表上，单击“确定”，在“虚拟 SCSI”面板中单击“下一步”，并跳到最后一步。要添加新的 SCSI 支持设备，请单击“SCSI 设备”表上的 +（新建后备设备）。

    注意：如果选定的设备具有插槽号，则该插槽号是定义到虚拟 I/O 服务器分区的虚拟 SCSI 服务器适配器的插槽号。如果选定的设备没有插槽号，则意味着该设备尚未与虚拟 SCSI 服务器适配器关联。执行要创建分区的作业时，将创建虚拟 SCSI 服务器适配器并将其分配给设备。

    注意：如果选择了支持 NPIV 的物理光纤通道端口，则将为分区创建虚拟光纤通道服务器适配器和虚拟光纤通道客户端适配器。

13. 单击“下一步”。

    此时将显示“摘要”页面。

14. 验证“摘要”，然后单击“添加计算机”。

    逻辑分区现已创建完成。

删除逻辑分区

您可以将不再需要的分区从受管系统中删除。删除逻辑分区时，所有硬件资源会恢复到主分区。只能删除已关闭电源的分区。

删除逻辑分区

1. 在“浏览”窗格中右键单击某个分区，然后选择“管理”、“删除”。

   这时将会出现确认对话框。

2. 单击“确定”。

   此时将显示一条消息，确认已提交请求。

3. 单击分区对应的“摘要”选项卡。

   会出现一个确认操作结果的事件。如果分区没有关闭电源，删除将不成功。如果删除成功，在您刷新界面之后分区会从“浏览”窗格中消失。

重新启动逻辑分区

您可以重新启动已在运行的分区。重新启动分区会将其关闭并重新启动操作系统。

注意：逻辑分区必须处于“正在运行”或“开放固件”状态才能重新启动。

重新启动逻辑分区

1. 在“浏览”窗格上右键单击某个分区，然后选择“管理”、“重新启动”。

   此时将显示“重新启动逻辑分区”对话框。

2. 使用“类型”下拉列表选择以下重新启动类型之一并单击“确定”：

   立即

   立即关闭逻辑分区。HMC/IVM 立即结束所有活动作业。不允许这些作业中运行的程序执行任何作业清理。如果已更新部分数据，该选项可能导致不适当的结果。仅在尝试受控关闭失败后使用该选项。

   操作系统关闭

   以通常方式通过向逻辑分区发出关闭命令来关闭逻辑分区。在该操作期间，逻辑分区将执行任何必要的关闭活动。该选项仅适用于 AIX 逻辑分区。

   操作系统立即关闭

   通过向逻辑分区发出带 -F 参数的关闭命令来立即关闭逻辑分区。在该操作期间，逻辑分区将跳过发送到其他用户的消息和其他关闭活动。该选项仅适用于 AIX 逻辑分区。

3. 单击分区对应的“摘要”选项卡。

   会出现一个确认操作结果的事件。

关闭逻辑分区

关闭分区时将会关闭操作系统。分区必须处于“正在运行”或“开放固件”状态才能关闭。

关闭逻辑分区

1. 在“浏览”窗格上右键单击某个分区，然后选择“管理”、“关闭”。

   此时将显示“关闭逻辑分区”页面。

2. 使用“类型”下拉列表选择以下关闭类型之一并单击“确定”：

   立即

   立即关闭逻辑分区。HMC/IVM 立即结束所有活动作业。不允许这些作业中运行的程序执行任何作业清理。如果已更新部分数据，该选项可能导致不适当的结果。仅在尝试受控关闭失败后使用该选项。

   操作系统关闭

   以通常方式通过向逻辑分区发出关闭命令来关闭逻辑分区。在该操作期间，逻辑分区将执行任何必要的关闭活动。该选项仅适用于 AIX 逻辑分区。

   操作系统立即关闭

   通过向逻辑分区发出带 -F 参数的关闭命令来立即关闭逻辑分区。在该操作期间，逻辑分区将跳过发送到其他用户的消息和其他关闭活动。该选项仅适用于 AIX 逻辑分区。

3. 单击分区对应的“摘要”选项卡。

   会出现一个确认操作结果的事件。

配置 CPU 和内存

您可以配置分配给虚拟机的内存份额，以调整其分配的资源。添加资源时，适当数量的未分配内存或 CPU 份额必须可用，以使操作成功。如果允许的内存或 CPU 份额存在最大值和最小值，则任何资源分配变更都必须在此限制范围内。您可以使用“资源”选项卡上的“快速启动”链接编辑 VM CPU 和内存分配。您还可以将创建和排定策略用于特定 VM 资源分配操作。

重要信息！对于动态 LPAR 操作（如添加或删除 CPU 和内存），请在每个 LPAR 系统上安装 AIX 版本 5.2、5.3、6.0 或更高版本。或者，在 LPAR 系统上运行 AIX 资源控制后台进程 IBM.DRM。

配置 CPU

配置 VM CPU 分配

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到虚拟机并右键单击，然后选择“配置”、“配置处理器...”

   此时将显示“配置处理器资源分配”对话框。

3. 请选择下列调整类型之一：

   动态调整

   更新运行的 VM。

   配置文件更新

   更新活动的配置文件。VM 必须重新启动，才能从配置文件中选取更改。

   动态调整和更新配置文件

   更新运行的 VM 和活动的配置文件。

4. 编辑相应字段，然后单击“确定”。

   即会出现一条确认消息。

配置内存

配置 VM 内存分配

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到虚拟机并右键单击，然后选择“配置”、“配置内存...”

   此时将显示“配置内存资源分配”对话框。

3. 请选择下列调整类型之一：

   动态调整

   更新运行的 VM。

   配置文件更新

   更新活动的配置文件。VM 必须重新启动，才能从配置文件中选取更改。

   动态调整和更新配置文件

   更新运行的 VM 和活动的配置文件。

4. 编辑相应字段，然后单击“确定”。

   即会出现一条确认消息。

Microsoft Hyper-V Server

Windows Server 2008 R2 Hyper-V 是基于管理程序的服务器虚拟化技术，作为 Windows Server 2008 R2 不可或缺的一项功能，支持您执行服务器虚拟化。SystemEDGE AIM for Hyper-V 服务器在 Hyper-V 服务器计算机上运行。

Hyper-V 服务器 PMM 向所有 Hyper-V 服务器操作提供连接和操作支持。PMM 负责管理连接、执行 VM 相关操作，以及用从 Hyper-V 服务器检索的数据填充数据库。

AIM Hyper-V 服务器监控以下资源类型：

Hyper-V 服务器

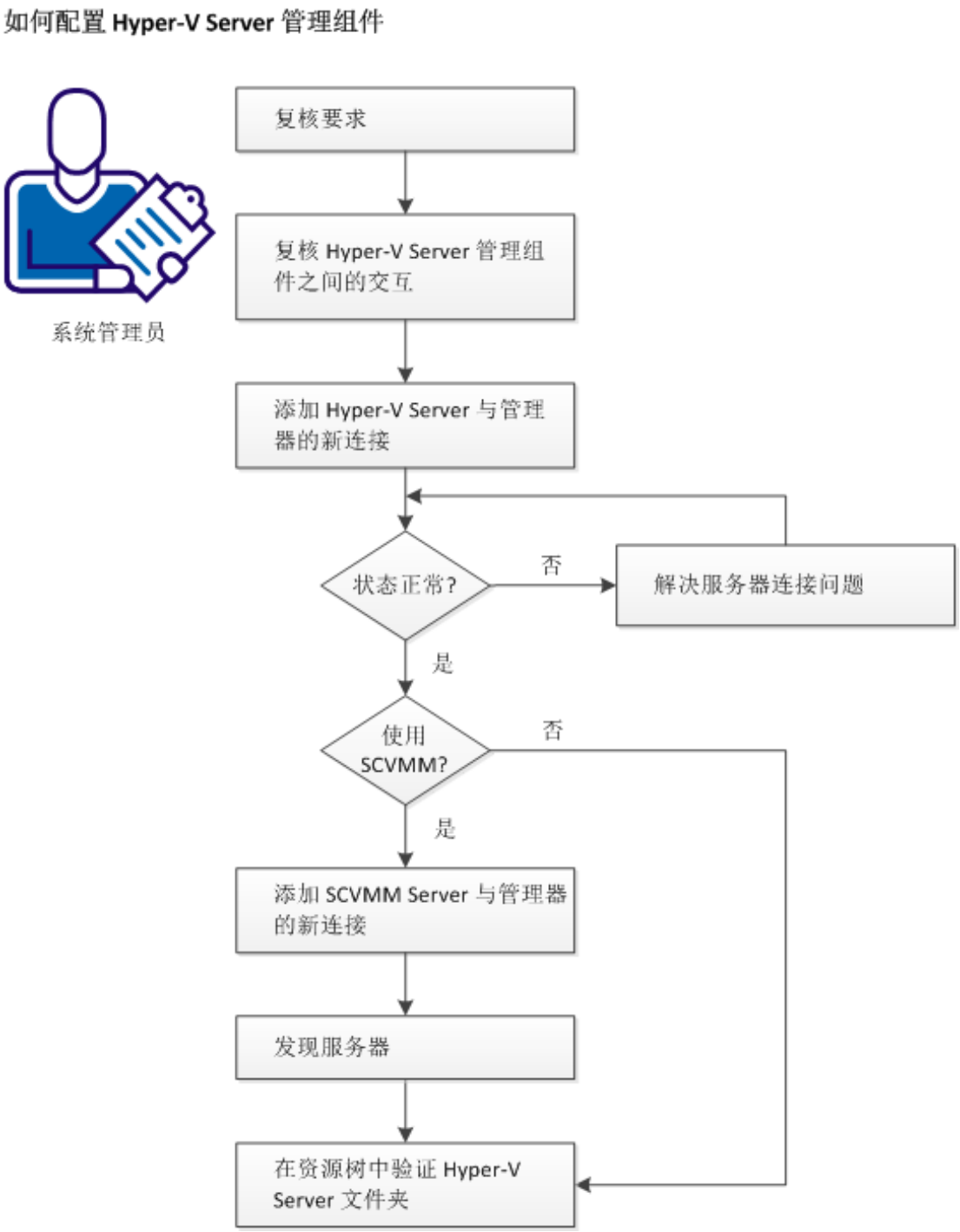
代表运行 Hyper-V 的物理服务器上的所有计算和内存资源。Hyper-V AIM 提供 Hyper-V 服务器计算机的运行状态方面的信息。例如，关于 CPU 和内存使用情况的状态和数据。

虚拟机

指定可运行来宾操作系统和应用程序的虚拟化 x86 环境。在创建虚拟机时，虚拟机将分配给特定的主机、群集或资源池及数据存储。虚拟机在其物理主机上动态地消耗资源，与物理设备根据其工作负荷动态消耗能源的方式相同。

如何配置 Hyper-V 管理

下图提供了有关所需操作的概述。该图包括针对连接问题的故障排除策略。



请执行以下步骤：

查看 Hyper-V 要求 (p. 390)
应用必要的设置以使用 Microsoft Hyper-V (p. 391)
将新的 Hyper-V 服务器连接添加到管理器中 (p. 393)
（可选）将 SCVMM 管理实例添加到 CA Virtual Assurance 管理器中 (p. 395)
发现服务器 (p. 399)
验证资源树中的 Hyper-V 服务器文件夹 (p. 400)

查看 Hyper-V 要求

在您开始配置 CA Virtual Assurance 的 Hyper-V 管理组件之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您对 CA Virtual Assurance、CA SystemEDGE 和 Hyper-V 服务器有基本了解。
- 您可以访问 CA Virtual Assurance 管理器安装，该安装包括 Hyper-V 平台管理模块 (PMM)、Hyper-V Application Insight Module (AIM) 和监控代理 (CA SystemEDGE)。
- 您可以访问 CA Virtual Assurance 用户界面。
- 验证 Hyper-V AIM 是否已安装在 Hyper-V 服务器中。
- 您具有有效的凭据（用户名和密码），可用于访问要管理的 Hyper-V 服务器。
- 您已验证 Hyper-V 服务器运行正常。
- 验证 CA Virtual Assurance 管理器上的 SNMP 设置是否与 Hyper-V 服务器上的 SNMP 设置一致。读和写团体字符串以及 SNMP 端口号必须是相同的。
- 您已验证 CA Virtual Assurance 管理器已发现要使用的 Hyper-V 服务器。

详细信息：

应用必要的设置以使用 Microsoft Hyper-V (p. 391)
Hyper-V 服务器管理组件之间的交互 (p. 392)
将新的 Hyper-V 服务器连接添加到管理器中 (p. 393)
（可选）将 SCVMM 管理实例添加到 CA Virtual Assurance 管理器中 (p. 395)
发现服务器 (p. 399)
验证资源树中的 Hyper-V 服务器文件夹 (p. 400)

应用必要的设置以使用 Microsoft Hyper-V

验证先决条件并对 Microsoft Hyper-V 管理应用以下设置：

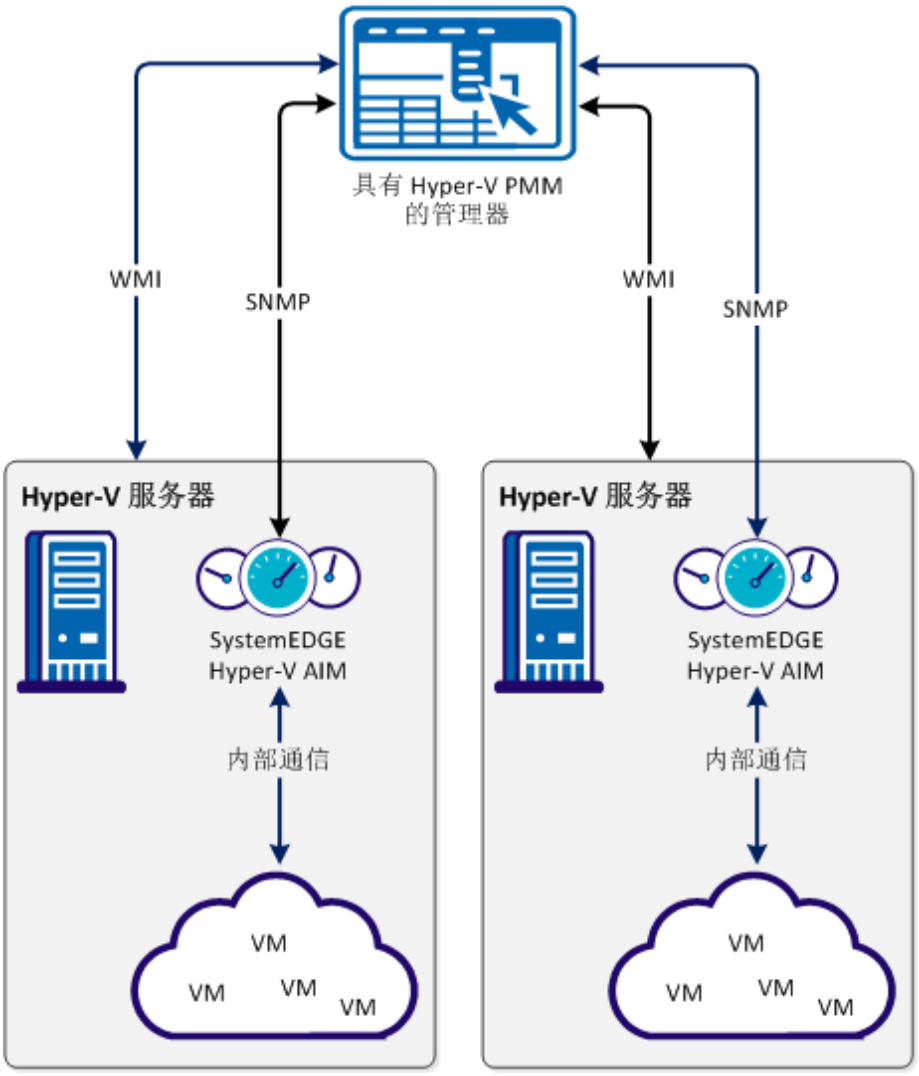
应用必要的设置以使用 Microsoft Hyper-V

1. 确定已在 Hyper-V 服务器上安装 SystemEDGE Advanced Encryption 和 Hyper-V AIM。每台受管 Hyper-V 服务器只能分配一个 AIM。
2. 在 Hyper-V 服务器上禁用本地用户访问控制 (UAC)。
3. 通过设置以下注册表值禁用网络 UAC：
   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy,1 (REG_DWORD)
   ```
4. 通过从命令提示符中运行以下命令来启用远程 WMI 防火墙例外：
   ```
   netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes
   ```
5. 确定在服务器访问的管理组件中配置的用户是“分布式 COM 用户”组的成员。

Hyper-V 服务器管理组件之间的交互

下图说明了 Hyper-V 管理中涉及的组件是如何交互的。在 Windows 2008 (Hyper-V) 服务器上运行以管理虚拟环境的 SystemEDGE 和 Hyper-V AIM。Hyper-V AIM 为与 Hyper-V 服务器相关联的物理和虚拟资源的整个视图收集数据。

Hyper-V Server 管理组件之间的交互



可以通过添加连接信息来配置 Hyper-V 管理。使用以下方法之一：

- 用户界面的“管理”选项卡
- AIM 服务器上的 NodeCfgUtil.exe 实用工具

详细信息：

将新的 Hyper-V 服务器连接添加到管理器中 (p. 393)
（可选）将 SCVMM 管理实例添加到 CA Virtual Assurance 管理器中 (p. 395)
发现服务器 (p. 399)
验证资源树中的 Hyper-V 服务器文件夹 (p. 400)

将新的 Hyper-V 服务器连接添加到管理器中

您可以使用 CA Virtual Assurance 用户界面的“管理”选项卡添加 Hyper-V 连接。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“Hyper-V 服务器”。

   右侧窗格可刷新并显示受管 Hyper-V 服务器。

3. 在“Hyper-V 服务器”窗格工具栏上单击  （添加）。

   此时将显示“新建 Hyper-V 服务器”对话框。

4. 输入所需的连接数据（服务器名称、用户、密码），然后单击“确定”。

   如果网络连接已成功建立，Hyper-V 服务器会被添加到右上角的“Hyper-V 服务器”窗格并带有绿色状态图标。CA Virtual Assurance 自动发现 Hyper-V 服务器。

   如果连接失败，将显示“验证失败”对话框。如果您单击“是”，CA Virtual Assurance 会将 Hyper-V 服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。有关排除连接故障的信息，请参阅排除 Hyper-V 服务器连接的故障 (p. 394)。

详细信息：

（可选）将 SCVMM 管理实例添加到 CA Virtual Assurance 管理器中 (p. 395)
发现服务器 (p. 399)
验证资源树中的 Hyper-V 服务器文件夹 (p. 400)
Hyper-V 服务器连接失败 (p. 394)

Hyper-V 服务器连接失败

症状：

在“管理”、“配置”下添加新的 Hyper-V 服务器连接后，对 Hyper-V 服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的 Hyper-V 服务器连接数据（服务器名称、用户、密码）是否仍然有效。如有必要，请更新连接数据。
- 验证 Hyper-V 服务器系统是否正在运行并且可以访问。

更新 Hyper-V 服务器连接数据

1. 单击与失败的连接关联的  （添加）或  （编辑）。

   此时将显示“新建 Hyper-V 服务器”或“编辑 Hyper-V 服务器”对话框。

2. 添加有效的服务器名称、用户和密码。启用“受管状态”，然后单击“确定”。

   将更新连接数据。

3. 单击右上角的  （验证）以验证新设置。

   如果无法建立与 Hyper-V 服务器的连接，请继续执行下一个步骤。

验证 Hyper-V 服务器系统是否正在运行并且可以访问

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <Hyper-V Server Name>
   ping <IP Address of Hyper-V Server>
   ```

2. 验证命令的输出，以确定 Hyper-V 服务器是否具有有效的 DNS 条目和 IP 地址。

   如果 Hyper-V 服务器不在 DNS 中，请将 Hyper-V 服务器添加到 CA Virtual Assurance 管理器系统上的 Windows 主机文件中。继续执行步骤 3。

   如果 Hyper-V 服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ipaddress <Hyper-V Server Name>

   输入正确的 IP 地址和 Hyper-V 服务器名称。例如：

   `192.168.50.50 myHyper-V`

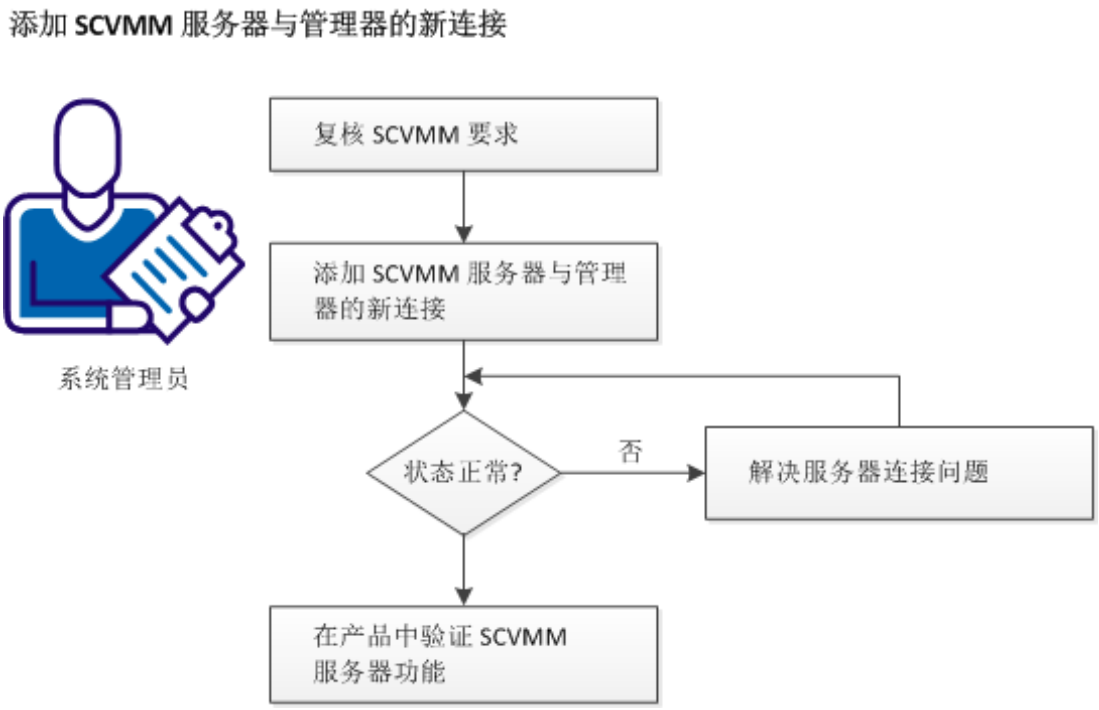
4. 单击右上角的（验证）。

   如果与 Hyper-V 服务器的连接失败，请验证根据该方案的要求收集的数据是否仍然有效。

   与 Hyper-V 管理员或 VMware 技术支持合作，解决 Hyper-V 服务器连接问题。

（可选）将 SCVMM 管理实例添加到 CA Virtual Assurance 管理器中

下图提供有关所需操作的概述。该图包括针对连接问题的相应故障排除策略。



请执行以下步骤：

应用必要的设置以使用 Microsoft SCVMM (p. 396)
将新的 SCVMM 服务器连接添加到管理器中 (p. 397)
SCVMM 服务器连接失败 (p. 398)

应用必要的设置以使用 Microsoft SCVMM

CA Virtual Assurance 可选择与 Microsoft System Center Virtual Machine Manager (SCVMM) 集成以用于 Hyper-V 开通。SCVMM 不是 Hyper-V 监控和管理所必需的。也可以使用本地模板（与 Hyper-V 服务器绑定）来取代 SCVMM 进行虚拟机开通。

在使用可选的 SCVMM 集成时，请验证以下先决条件并应用必要的设置：

应用必要的设置以使用 Microsoft SCVMM

1. 确定 SCVMM 服务器、用于虚拟机开通的所有潜在 Hyper-V 目标主机及运行 Hyper-V PMM 的 CA Virtual Assurance 管理器是同一 Active Directory 域的成员。
2. 确定在 CA Virtual Assurance 和 SCVMM 中配置了用于虚拟机开通的 Hyper-V 目标主机。CA Virtual Assurance 不执行 SCVMM 发现。
3. 确定 SCVMM 已配置 Windows 远程管理 (WinRM)。
4. 在 SCVMM 服务器的命令行上运行以下命令以配置 WinRM：

   ```
   winrm quickconfig
   ```

5. 在 SCVMM 服务器上，除了基本的 WinRM 配置之外，还允许未加密的 HTTP 或启用 HTTPS。

   运行以下命令可允许未加密的 HTTP 通信：

   ```
   winrm set winrm/config/service @{AllowUnencrypted="true"}
   ```

   要启用 HTTPS，请获取 SCVMM 服务器的 SSL 证书，安装证书，并运行以下命令：

   ```
   winrm quickconfig -transport:https
   ```

根据您的环境中 SCVMM 服务器的预期使用率，SCVMM 服务器上远程外壳的配额管理的参数设置可能不足，从而导致虚拟机开通失败。受影响的参数包括：

MaxShellsPerUser

指定每个用户的最大外壳数。

默认值： 5

MaxConcurrentUsers

指定可以打开外壳的最大并发用户数。

默认值： 5

如果预计一次执行多个开通作业，可以按照以下方式在 SCVMM 服务器上增加参数设置：

```
winrm set winrm/config/winrs @{MaxShellsPerUser="number"}
winrm set winrm/config/winrs @{MaxConcurrentUsers="number"}
```

示例

```
winrm set winrm/config/winrs @{MaxShellsPerUser="30"}
winrm set winrm/config/winrs @{MaxConcurrentUsers="10"}
```

另请参阅 Microsoft 的《远程外壳的配额管理》一文。

将新的 SCVMM 服务器连接添加到管理器中

您可以使用 CA Virtual Assurance 用户界面的“管理”选项卡添加 SCVMM 连接。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“SCVMM 服务器”。

   右侧窗格可刷新并显示受管 SCVMM 服务器。

3. 在“SCVMM 服务器”窗格工具栏上单击  （添加）。

   此时将显示“新建 SCVMM 服务器”对话框。

4. 输入所需的连接数据(服务器名称、用户、密码),然后单击“确定”。

   如果网络连接已成功建立，SCVMM 服务器会添加到右上角的“SCVMM 服务器”窗格并带有绿色状态图标。CA Virtual Assurance 自动发现 SCVMM 服务器。

   如果连接失败，将显示“验证失败”对话框。如果您单击“是”，CA Virtual Assurance 会将 SCVMM 服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。有关排除连接故障的信息，请参阅排除 SCVMM 服务器连接的故障 (p. 398)。

SCVMM 服务器连接失败

症状：

在“管理”、“配置”下添加新 SCVMM 服务器连接后，对 SCVMM 服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的 SCVMM 服务器连接数据（服务器名称、用户、密码）是否仍然有效。如有必要，请更新连接数据。
- 验证 SCVMM 服务器系统是否正在运行并且可以访问。

更新 SCVMM 服务器连接数据

1. 单击与失败的连接关联的  （添加）或  （编辑）。

   此时将显示“新建 SCVMM 服务器”或“编辑 SCVMM 服务器”对话框。

2. 添加有效的服务器名称、用户和密码。启用“受管状态”，然后单击“确定”。

   将更新连接数据。

3. 单击右上角的  （验证）以验证新设置。

   如果无法建立与 SCVMM 服务器的连接，请继续执行下一个步骤。

验证 SCVMM 服务器系统是否正在运行并且可以访问

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <SCVMM Server Name>
   ping <IP Address of SCVMM Server>
   ```

2. 验证命令的输出，以确定 SCVMM 服务器是否具有有效的 DNS 条目和 IP 地址。

   如果 SCVMM 服务器不在 DNS 中，请将 SCVMM 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果 SCVMM 服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ipaddress <SCVMM Server Name>

   输入正确的 IP 地址和 SCVMM 服务器名称。例如：

   192.168.50.50 mySCVMM

4. 单击右上角的  （验证）。

   如果与 SCVMM 服务器的连接失败，请验证根据该方案的要求收集的数据是否仍然有效。

   与 SCVMM 管理员或 Microsoft 技术支持合作，解决 SCVMM 服务器连接问题。

发现服务器

在将新的 Hyper-V 服务器连接和可选的 SCVMM 连接添加到 CA Virtual Assurance 管理器后，可发现 Hyper-V 服务器和 SCVMM 服务器。CA Virtual Assurance 随后发现整个 Hyper-V 环境及其所有虚拟组件。

验证 CA Virtual Assurance 管理器上的 SNMP 凭据是否与 Hyper-V 和 SCVMM 服务器上的 SNMP 凭据一致。在必要时，相应地更新 SNMP 配置。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“资源”、“数据中心”。

   此时将显示“数据中心”页面。

2. 从右侧窗格的“快速启动”单击“发现系统”。

   右侧窗格将刷新并显示“发现系统”向导。

3. 输入所需的数据，然后单击“完成”。

   CA Virtual Assurance 发现系统。

详细信息：

验证资源树中的 Hyper-V 服务器文件夹 (p. 400)

验证资源树中的 Hyper-V 服务器文件夹

在成功配置和发现之后，新的 Hyper-V 服务器将在“资源浏览”窗格的 Hyper-V 服务器文件夹之下列出。

遵循这些步骤:

1. 单击“资源”、“浏览”。

   此时将显示“资源”树。

2. 展开 Hyper-V 服务器。

   将显示受管的 Hyper-V 服务器。

3. 展开新的 Hyper-V 服务器条目。

   将显示受管的 Hyper-V 基础架构。

CA Virtual Assurance 现在可以用于管理添加的 Hyper-V 环境及其虚拟基础架构。

Hyper-V 奢燴

使用 Hyper-V 服务器可以管理 Hyper-V 服务器和虚拟机。Hyper-V 服务器位于中央位置，可以从中查看所有虚拟资源并执行启动、停止、删除等管理操作。

本节描述了可以从“资源”页面的 Hyper-V 服务器资源上执行的管理操作。通过“资源”页面，您可以查看以下对象的基本信息和详细信息：

- Hyper-V 服务器
- 虚拟机

单击“资源”，打开“浏览”窗格，选择一项 Hyper-V 资源，然后单击该资源的“摘要”。

通过“摘要”页面，您可以查看与对象相关的信息（例如，Hyper-V 服务器或 Hyper-V 服务器上的虚拟机）和与资源相关的事件。

通过“详细信息”页面，您可以查看其他详细资源信息，如系统属性、软件、硬件、性能等。

可以使用“浏览”窗格的右键单击菜单来执行管理和策略任务。

详细信息

添加虚拟机（Hyper-V 服务器）

您可以创建数据中心的 VM。您必须使用预定义的模板来创建 VM。

注意：Hyper-V“总存储”的值包括基于模板创建 VM 所需要的总空间。该值是几个因素的组合，包括所有虚拟磁盘、VM、快照和缓冲区的 RAM 大小。使用此信息作为指导，可确定基于选定模板创建 VM 所需的最大存储量。

创建 VM

1. 依次选择“资源”、“浏览”。

   此时将显示“浏览”窗格。
2. 右键单击 Hyper-V 资源，并依次选择“开通”、“开通 Hyper-V VM”。
3. 指定以下详细信息，然后单击“下一步”。
   - SCVMM 服务器和 Hyper-V 服务器。
   - 要用于创建 VM 的模板名称。
   - 要在其中创建 VM 的目标路径。
   - 要创建的 VM 的名称。
   - 指定在创建 VM 之后是否启动它。

   此时将显示“虚拟机内存”页面。
4. 指定 VM 内存详细信息，然后单击“下一步”。

   此时将显示“来宾操作系统自定义”页面。
5. 指定来宾操作系统详细信息，然后单击“下一步”。

   此时将显示“网络管理”页面。

6. 指定 VM 的网络详细信息，然后单击“下一步”。

   注意：如果自定义规格指定使用 DHCP，您将只能编辑表中的网络连接单元格。如果您的自定义规格指定使用静态 IP 地址，您将能够编辑除 NIC 单元格以外的所有单元格。CA Virtual Assurance 不支持自定义规格网络设置“提示用户”。使用此设置的自定义规格将被筛选掉并且不可用。

7. 单击“添加计算机”。

   窗格顶部将显示一条确认消息。

   注意：映像创建需要花费时间，因此您应预测到在操作系统安装期间会有延迟。为实现更高效的发现，您可以在位于以下路径的 caimgconf.cfg 文件中调整发现重试时间或间隔：*install_path*\CA*productname*\conf。。

详细信息

开通计算机：Microsoft Hyper-V (p. 659)

管理 VM 状态 (Hyper-V)

可以通过执行以下 VM 操作之一来控制 Hyper-V 服务器虚拟机的状态：

- 启动
- 停止
- 暂停
- 重新启动
- 关闭
- 保存

可以在多个 VM 上同时执行上述任意操作。

控制 VM 状态

1. 在“浏览”窗格中选择要在其上执行状态操作的虚拟机。
2. 右键单击该 VM，选择“管理”。还可以单击“快速启动”，然后单击相关的电源控制链接。选择以下选项之一：

   启动

   启动虚拟机并引导来宾操作系统。您只能打开当前已关闭或挂起的虚拟机。

   停止

   关闭虚拟机电源。您只能关闭当前已打开或挂起的虚拟机。

   暂停

   暂停虚拟机并保存其当前状态。在您恢复该虚拟机之前所有活动都会被挂起。

   重新启动

   关闭来宾操作系统并重新启动。

   关闭

   关闭来宾操作系统。您仅可关闭当前已打开的虚拟机。

   保存

   保存虚拟机的当前状态。在其他平台中，此选项与“挂起”类似。

   这时将会出现确认对话框。
3. 单击“确定”。

   状态操作发生后，将出现一条确认信息。刷新界面以查看新的 VM 状态。会出现一个确认操作结果的事件。

删除虚拟机

当您从 Hyper-V 服务器中删除虚拟机时，该虚拟机会从虚拟磁盘中删除。

删除虚拟机

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、“删除”。

   将出现“删除 Hyper-V VM”对话框，其中提供了删除其他组件的选项。

3. 单击“确定”。

   将显示一条消息，确认请求提交。

4. 单击该虚拟机的“摘要”选项卡。

   此时应出现一个确认操作结果的事件。如果成功，该虚拟机会从虚拟磁盘中删除，且界面更新后会从“浏览”窗格中消失。

注意：仅可删除处于关机状态的 VM，否则删除链接将被禁用。

重命名虚拟机

可以重命名 Hyper-V 服务器的现有虚拟机。

重命名虚拟机

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、“重命名”。

   将显示“重命名 VM”对话框。

3. 输入新 VM 名称，然后单击“确定”。

   将显示一条消息，确认请求提交。

4. 单击该虚拟机的“摘要”选项卡。

创建操作和规则

可以根据不同类型资源（如虚拟机）的预定策略来创建操作和规则。

为虚拟机创建操作和规则

1. 依次选择“资源”、“浏览”、“数据中心”。
2. 打开“策略”选项卡和“操作”子选项卡。
3. 单击 +（添加）以创建新操作。
4. 从下拉菜单中选择相应的项，并按照用户界面中的说明完成操作。
5. 选择“规则”子选项卡，然后单击 +（添加）以创建新规则。

   将出现“规则/模板标识和计算”对话框。

   向导将指导您完成创建过程。将可用操作列表中的操作分配到该规则。

   有关操作和规则的详细信息，请参阅创建操作 (p. 598)和创建规则。

编辑启动和关闭操作

可以编辑操作来启动和关闭虚拟机。

编辑启动和关闭操作

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“配置”、“启动和关闭操作”。

   将出现“启动和关闭操作”对话框。

3. “启动和关闭操作”对话框包含以下字段：

   启动操作

   指定 Hyper-V 服务器启动时执行的操作。从下拉列表中选择下列项之一：

   - 始终

     在 Hyper-V 服务器启动时始终启动 VM。

   - 趁雄

     如果 VM 在运行模式下处于关机状态，则在 Hyper-V 服务器启动时自动启动 VM。

   - 无
     在 Hyper-V 服务器启动时不启动 VM。

   启动延迟

   调整 Hyper-V 服务器启动后启动 VM 的延迟（秒）。

   关闭操作

   指定虚拟机关闭时执行的操作。从下拉列表中选择下列项之一：

   - 关

     在 Hyper-V 服务器关闭前关闭 VM。

   - 保存

     在 Hyper-V 服务器关闭前保存（挂起）VM。

   - 关闭

     在 Hyper-V 服务器关闭前关闭 VM。

   恢复操作

   指定 Hyper-V 服务器出现故障时重新获取虚拟机之前的详细信息的操作。从下拉列表中选择下列项之一：

- 无

  服务器出现故障后启动 Hyper-V 服务器时不采取具体操作。

- 重新启动

  在 VM 服务器发生故障后启动 Hyper-V 服务器时，重新启动 VM。

- 还原

  服务器出现故障后启动 Hyper-V 服务器时，使用最新的快照还原 VM。

4. 在编辑所有详细信息后单击“确定”。即会出现一条确认消息。

编辑 VM CPU 和内存分配

您可以编辑分配给虚拟机的 CPU 数目和内存份额，以调节其分得的资源。添加资源时，适当数量的未分配内存或 CPU 份额必须可用，以使操作成功。如果允许的内存或 CPU 份额存在最大值和最小值，则任何资源分配变更都必须在此限制范围内。

您还可以为特定 VM 资源分配操作创建并排定策略。

编辑 VM CPU 和内存分配

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“配置”、“资源分配”、“CPU 和内存”。

   将出现“CPU 和内存资源分配”对话框。

3. 调整 CPU 数量、保留的 CPU 百分比和 CPU 限制百分比。

4. 调整分配给虚拟机的内存份额，在编辑所有详细信息后单击“确定”。

   即会出现一条确认消息。

Hyper-V 管理操作

以下操作类型可与 Hyper-V 服务器一起使用：

- 删除计算机 (p. 634)
- 更改计算机状态 (p. 608)
- 配置电源 (p. 620)
- 配置 CPU/Memory (p. 612)

在满足分配的规则条件后，可以使用这些操作类型来创建自动化 Hyper-V 服务器的启动和关闭选项的配置及其他操作的新操作。还可以排定这些操作在特定时间发生。

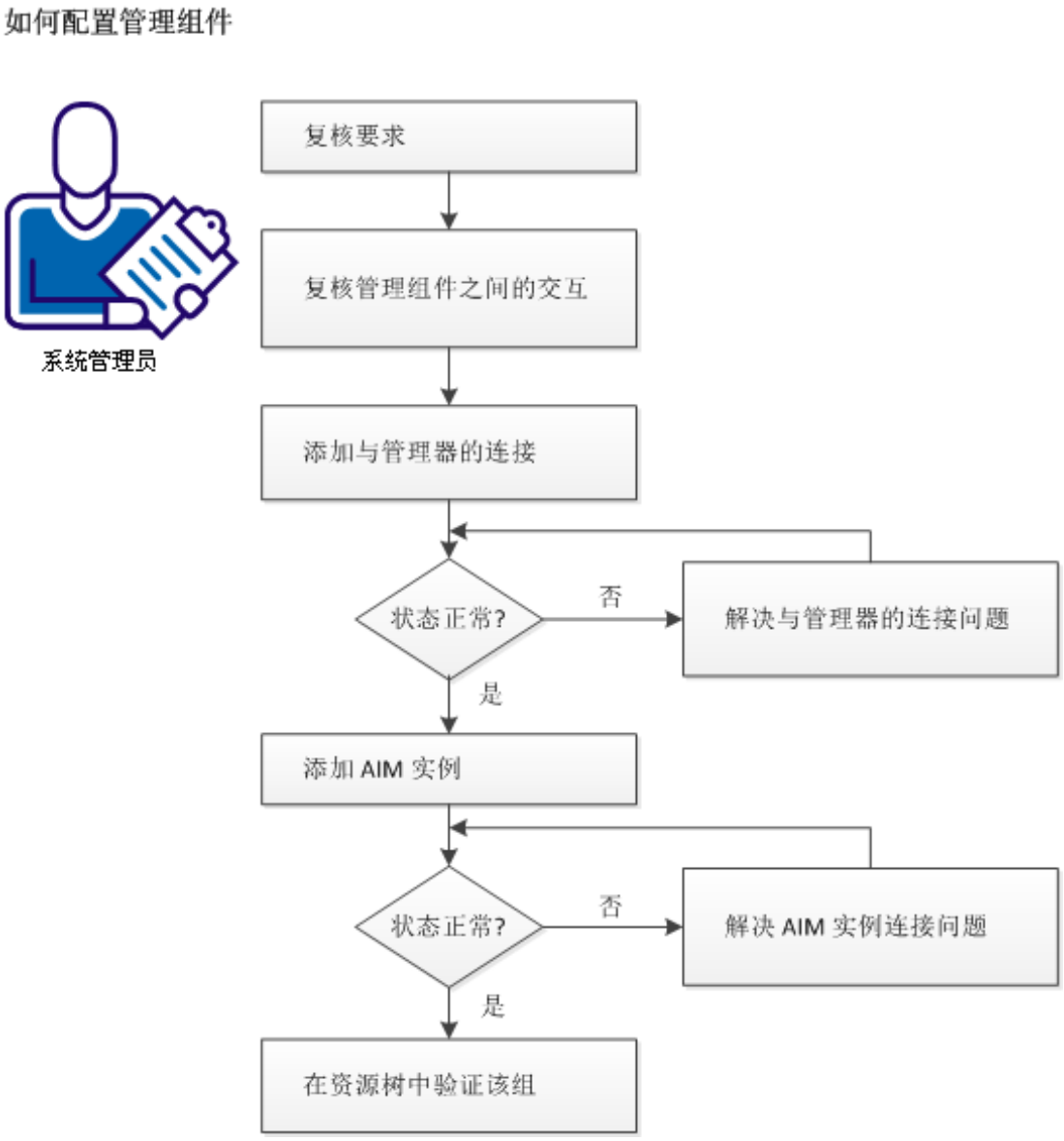
有关使用操作和规则来创建自动化策略的详细信息，请参阅“策略”一节。

Red Hat Enterprise Virtualization

CA Virtual Assurance 引入了基于内核的虚拟计算机支持。*基于内核的虚拟机 (KVM)* 是 Linux 内核的硬件辅助虚拟化基础架构。CA KVM AIM 将作为多实例的远程 AIM 实施。CA KVM AIM 启用了 RHEV 监控。*Red Hat Enterprise Red Hat Enterprise Virtualization (RHEV)* 是基于 KVM 管理程序的企业虚拟化产品。

如何配置 Red Hat Enterprise Virtualization 管理组件

下图提供了有关配置管理组件所需操作的概述。该图包括针对连接问题的相应故障排除策略。



请执行以下步骤：

查看要求

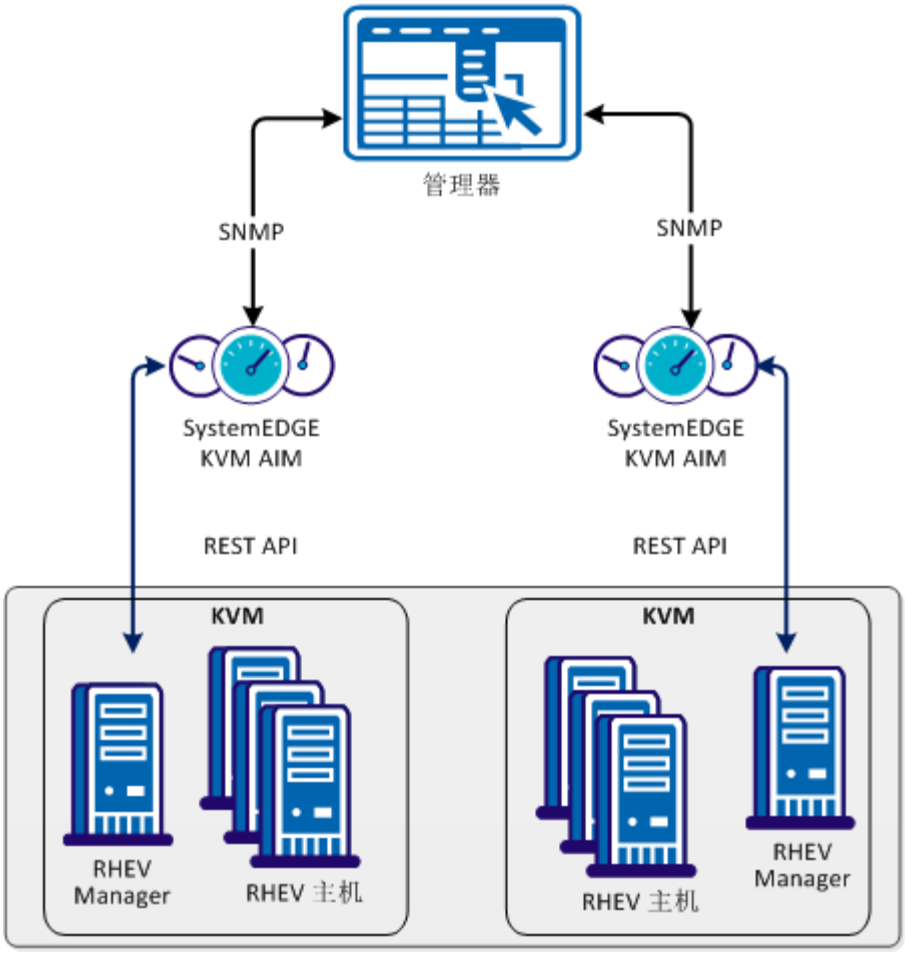
在配置 CA Virtual Assurance 的管理组件之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您熟悉 CA Virtual Assurance 和 SystemEDGE。
- 您可以访问包括以下内容的 CA Virtual Assurance 管理器安装：
  - 平台管理模块 (PMM)
  - Application Insight Module (AIM)
  - 监控代理 (SystemEDGE)
- 您可以访问 CA Virtual Assurance 用户界面。
- 您具有有效的凭据（用户名和密码），可访问要管理的环境中的服务器。
- 您知道使用哪个协议（HTTP 或 HTTPS）和端口，以通过 Web 服务访问环境中的服务器。默认：HTTPS，端口：443。
- 您已验证环境中的服务器运行正常。
- 如果将 PMM 和 AIM 安装在不同系统上，请确认 PMM 和 AIM 系统上的 SNMP 设置一致。读和写团体字符串以及 SNMP 端口号必须是相同的。
- 您已验证 CA Virtual Assurance 管理器已发现您要使用的远程 AIM 服务器。

RHEV 管理组件之间的交互

下图说明了 RHEV 监控中涉及的组件是如何交互的。SystemEDGE 和 KVM AIM 在 Windows 服务器上运行。AIM 使用 REST API 与一个或多个 RHEV 管理器进行通信。

KVM 管理组件之间的交互



将 Red Hat Enterprise Virtualization 连接添加到管理器

您可以使用 CA Virtual Assurance 用户界面的“管理”选项卡添加 Red Hat Enterprise Virtualization 连接。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择 Red Hat Enterprise Virtualization。
3. 在“注册的 Red Hat Enterprise Virtualization 服务器”窗格工具栏上单击 （添加）。

   此时将显示“添加 Red Hat Enterprise Virtualization 服务器”对话框。

4. 输入所需的连接数据（服务器名称、用户、密码、ISO 库凭据、端口），指定首选的 AIM，启用“受管状态”（复选框）。

   注意：ISO 库包含用于开通的 ISO 映像。没有 ISO 映像，开通不起作用。

5. 单击“确定”。

   如果网络连接已成功建立，服务器会添加到右上角的窗格并带有绿色状态图标。

   如果连接失败，将显示“验证失败”对话框。如果您单击“是”，CA Virtual Assurance 会将服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。

管理器到服务器的连接失败

症状：

在“管理”、“配置”下添加服务器连接后，对服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的服务器连接数据是否仍然有效。如有必要，请更新连接数据。
- 验证服务器系统是否正在运行并且可以访问。
- 验证连接所需的所有服务是否在服务器系统上运行良好。

更新服务器连接数据：

1. 单击与失败的连接关联的  （添加）或  （编辑）。
2. 添加连接详细信息，启用“受管状态”，然后单击“确定”。

   将更新连接数据。
3. 单击右上角的  （验证）以验证新设置。

   如果无法建立与服务器的连接，请继续执行下一步骤。

验证服务器系统是否正在运行并且可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```
2. 要确定服务器是否具有有效的 DNS 条目和 IP 地址，请检查这些命令的输出。

   如果服务器不在 DNS 中，请将服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。
3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress <Server Name>
   ```

   输入正确的 IP 地址和服务器名称并保存文件。例如：

   ```
   192.168.50.50 myServer
   ```
4. 切换到 CA Virtual Assurance 用户界面、“管理”选项卡、“配置”、“服务器”窗格，并单击右上角的  （验证）。

   即使服务器凭据和连接数据正确并且您可以 ping 服务器，连接仍然可能失败。在这种情况下，可能是服务器引起该问题。如果无法建立与服务器的连接，请继续执行下一步骤。

验证连接所需的所有服务是否在服务器系统上运行良好。

1. 要访问服务器，请联系系统管理员。
2. 登录到服务器系统。
3. 验证连接所需的所有服务是否运行良好。
4. 如有必要，请启动或重新启动服务。
5. 切换到管理器系统上的 CA Virtual Assurance 用户界面、服务器窗格，并单击右上角的  （验证）。

   CA Virtual Assurance 将验证服务器连接。

   如果与服务器的连接失败，请验证根据该方案的要求收集的数据是否有效。

   与管理员或技术支持合作，解决服务器连接问题。

添加发现的 Red Hat Enterprise Virtualization AIM 实例

将 Red Hat Enterprise Virtualization 连接添加到 CA Virtual Assurance 管理器之后，添加 AIM 实例以管理 Red Hat Enterprise Virtualization 环境。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择 Red Hat Enterprise Virtualization。

3. 在“发现的 Red Hat Enterprise Virtualization AIM 实例”窗格工具栏上单击 （添加）。

   此时将显示“添加 Red Hat Enterprise Virtualization AIM 实例”。

4. 从下拉列表中选择“RHEV AIM 服务器”。

   将显示发现的 RHEV AIM 服务器的列表。

5. 从下拉列表中选择“RHEV 服务器”。

   CA Virtual Assurance 使用“注册的 Red Hat Enterprise Virtualization”窗格中列出的 RHEV 服务器填充“RHEV 服务器”下拉列表。您只能管理 CA Virtual Assurance 管理器为之建立了有效连接的 RHEV 服务器。

   注意：如果 AIM 位于远程系统中，则 CA Virtual Assurance 一定会首先发现该系统。在发现之后，AIM 服务器将在下拉列表中显示。

6. 单击“确定”。

   将添加选定的服务器的新 AIM 实例。如果实例未处于错误或已停止状态，CA Virtual Assurance 将开始发现关联的环境。发现过程完成之后，您可以开始管理您的 Red Hat Enterprise Virtualization 环境。

排除 AIM 实例连接的故障

如果 AIM 连接处于未就绪状态，将出现以下状态图标之一：

- 发现正在进行
- 无轮询
- 错误
- 警告
- 已禁用
- 未知

有关 AIM 实例状态的详细信息，请参阅工具提示。以下故障排除部分提供了用于解决该问题的详细信息和步骤。

AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为服务器添加 AIM 实例后，状态图标显示  （发现正在进行）。

解决方案：

等到环境的发现过程完成。发现持续时间取决于与环境中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示指示未完成发现请求数量的工具提示。发现作业完成时，CA Virtual Assurance 会向资源树中添加一个服务器文件夹。然后，您可以开始管理您的环境。

AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （无轮询）。

解决方案：

关联实例不需要特定的操作。此图标表示 CA Virtual Assurance 管理器不轮询此 AIM。AIM 不是首选。

如果多个 AIM 已配置为管理特定服务器，PMM 将选择其中一个 AIM 作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决可能导致与 AIM 连接失败的最常见问题：

- 验证是否可以访问 AIM 服务器。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 确认命令的输出对于 AIM 服务器有有效的 DNS 条目和 IP 地址。

   如果 AIM 服务器不在 DNS 中，则将 AIM 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress servername
   ```

   输入正确的 IP 地址和 AIM 服务器名称。例如：

   ```
   192.168.50.51 myAIM
   ```

4. 在“AIM 服务器”窗格的右上角，单击 （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“AIM 服务器”窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证 AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否有效。

AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 AIM 实例之后，几个实例的状态图标显示  （已禁用）。该 AIM 实例未受管理。

如果 CA Virtual Assurance 发现具有以下关系的 AIM，则显示该状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的服务器配置了 AIM。
- AIM 连接到未配置的服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的服务器连接并将其受管状态更改为已启用。

验证“资源”树中的 Red Hat Enterprise Virtualization 组

在成功配置和发现之后，新发现的资源将在“资源”、“浏览”窗格中的相应组下列出。

遵循这些步骤:

1. 单击“资源”，然后打开“浏览”窗格。
2. 展开 Red Hat Enterprise Virtualization 组。

   将显示受管的 Red Hat Enterprise Virtualization 资源。

CA Virtual Assurance 现在已准备好管理配置的 Red Hat Enterprise Virtualization 环境。

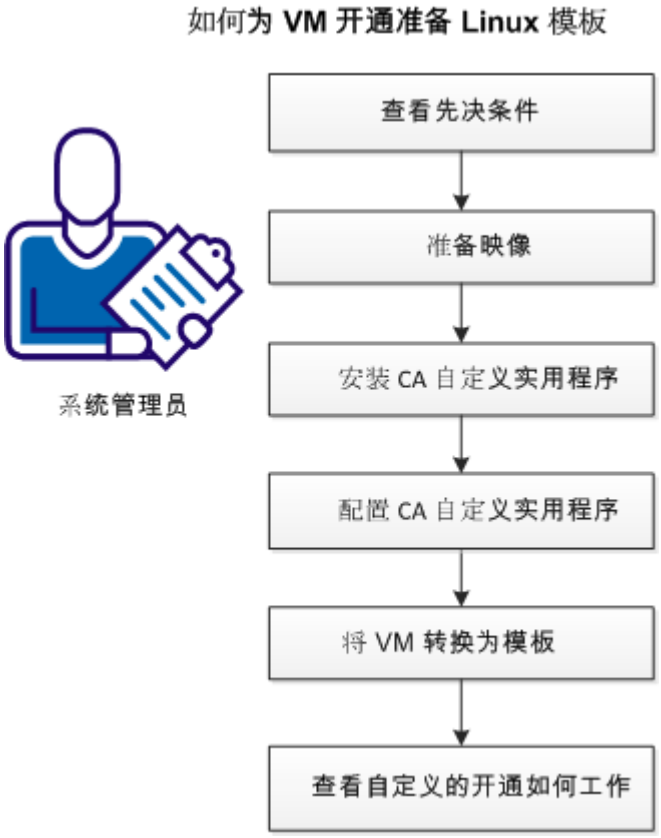
如何为 KVM 开通准备 Linux 模板

CA Virtual Assurance 支持运行以下操作系统的新虚拟机 (VM) 的自定义开通：

- Red Hat Enterprise Server 6.0
- SUSE Linux Enterprise Server 11

自定义选项包括主机名、密码、域或网络配置。

下图说明了系统管理员如何为 VM 开通准备 Linux 模板。



请执行以下步骤：

自定义 VM 开通的先决条件 (p. 419)
准备 Linux 映像 (KVM) (p. 420)
安装 CA 自定义实用工具 (p. 420)
配置 CA 自定义实用工具 (p. 421)
将虚拟机转换为模板 (p. 421)
自定义的开通如何工作 (p. 422)

自定义 VM 开通的先决条件

要自定义 Linux 来宾，需要具有对文件系统或控制台的直接访问权限。

对于 RHEV 环境，确保满足下列先决条件：

- 每个 RHEV 数据中心在 RHEV 管理器系统上均使用本地 ISO 库。
- 每个计算机均启用了 SFTP 访问。
- RHEV 管理器已启用了 SSH 访问。

准备 Linux 映像 (KVM)

在创建包含 Linux 操作系统的模板之前，可通过遵循此步骤来准备映像。根据 Linux 分发包，具体步骤可能会有所不同。

遵循这些步骤:

1. 在新虚拟机上从头开始安装 Linux 操作系统。
2. 在虚拟机内安装 RHEV Guest Tools。
3. 应用您想在新虚拟机上应用的任何自定义项，如用户帐户、策略、应用程序、即时修正。

可以使用 CA 自定义实用工具对此 Linux 映像进行进一步自定义。

安装 CA 自定义实用工具

CA 自定义实用工具允许 CA Virtual Assurance 从外部更改虚拟机设置。来宾实用工具可在 OS 启动时监视 CD 驱动器。如果连接了特殊 ISO，则会执行下列操作：

1. 一组用于自定义来宾的命令。
2. 将来宾系统标记为已自定义。
   无法再次修改系统，除非有人重置此状态。
3. 暂停系统以表示自定义已成功。

安装正确的 CA 自定义来宾实用工具：

1. 该实用工具位于以下位置：
   - 适用于 Red Hat Enterprise Server 6.0

     ```
     <InstallationRoot>\Utilities\linuxCustomization\rh6
     ```
   - 适用于 SUSE Linux Enterprise Server 11

     ```
     <InstallationRoot>\Utilities\linuxCustomization\sles11
     ```
2. 将此可执行文件传输到正在准备的 VM 的硬盘驱动器上的下列位置：

   ```
   /usr/bin/ca-customize
   ```
3. （可选）提供您自己的 CA 自定义脚本版本，以支持我们不支持的其他来宾系统。
4. 启用 CA 自定义实用工具的可执行位：

   ```
   chmod 755 /usr/bin/ca-customize
   ```

配置 CA 自定义实用工具

您可以为 Linux 开通设置模板。要自定义来宾，请使用可用的脚本。您也可以使用自己的脚本以进行进一步设置。

遵循这些步骤:

1. 禁用网络接口，这样网络便不会影响自定义过程。

   注意：在自定义期间会自动启用网络。

2. 必要时使用 */etc/ca-customize.conf* 文件覆盖默认的 CDROM 设备名。

   CD_DEVICE=/dev/cdrom

   定义用于 CD 驱动器的设备名。

   默认值：/dev/cdrom

3. 设置在引导过程结束时自动启动。

   - （适用于 SUSE Linux）创建或修改 */etc/init.d/after.local* 文件：

     ```
     #!/bin/bash
     [ -e /etc/ca-customized ] || /usr/bin/ca-customize
     ```

   - （适用于 Red Hat Linux）将以下行添加到 */etc/rc.local* 文件中：

     ```
     [ -e /etc/ca-customized ] || /usr/bin/ca-customize
     ```

4. 关闭系统。

将虚拟机转换为模板

该模板允许您创建任意数量的自定义虚拟机。

遵循这些步骤:

1. 关闭 VM。
2. 要将关闭虚拟机转换成 RHEV 模板，请使用 RHEV 管理门户。

模板显示在 CA Virtual Assurance 中，并且可用于自定义开通。

执行了这些步骤之后，即可使用新模板来新建任意数量的自定义虚拟机。

自定义的开通如何工作

下列步骤描述了自定义 VM 开通的工作流程。

1. 平台管理服务开通新的 Linux VM。
2. 平台管理服务使用自定义参数准备新的 ISO，并将其附加到新 VM。
3. 平台管理服务启动 VM。
4. VM 检测到已连接了自定义 ISO。VM 应用自定义更改。
5. 如果自定义成功，VM 会关闭。PMM 检测到 VM 已停止。平台管理服务再次启动 VM 并完成开通。
6. 如果自定义失败，VM 不会暂停。平台管理服务将采取以下操作：
   a. 返回开通失败
   b. 将开通作业设置为异常状态

自定义日志

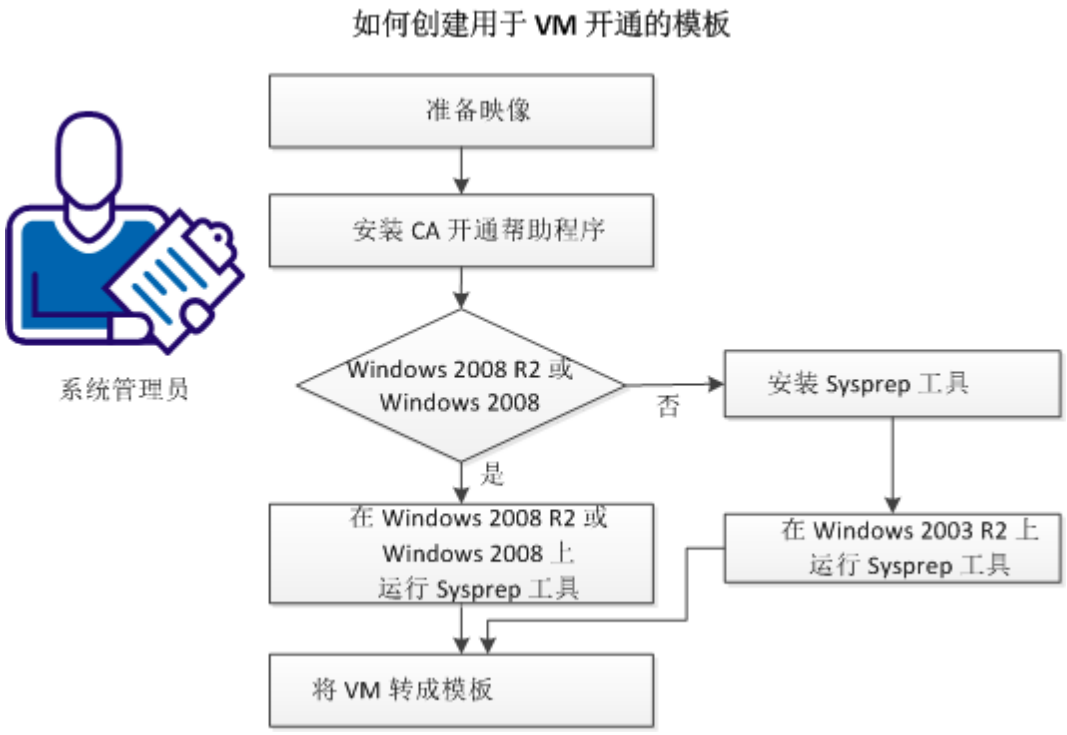
成功的自定义将存储在 */etc/ca-customized* 文件中。此文件包括自定义更改列表。

如果自定义失败，日志将存储在 */etc/ca-customized.tmp* 文件中。

如何为 KVM 开通准备 Windows 模板

CA Virtual Assurance 支持自定义开通运行 Windows 2003 R2 Server（32 位和 64 位）、Windows 2008（32 位和 64 位）或 Windows 2008 R2 Server（64 位）的新虚拟机 (VM)。自定义选项包括大量设置。例如，更改内置的管理员帐户密码、计算机名和网络配置。

下图说明了系统管理员如何为 KVM 开通准备 Windows 模板。



遵循这些步骤:

1. 准备映像。 (p. 424)
2. 安装 CA 开通帮助程序。 (p. 320)
3. （对于 Windows 2003 R2 有效）安装 Sysprep 工具。 (p. 321)
4. 根据您的操作系统选择以下操作之一：
   - 在 Windows 2003 R2 上运行 Sysprep 工具。 (p. 321)
   - 在 Windows 2008 R2 上运行 Sysprep 工具。 (p. 321)
5. 将虚拟机转换为模板。 (p. 425)

RHEV 环境的先决条件

对于 RHEV 环境，确保满足下列先决条件：

- 每个 RHEV 数据中心在 RHEV 管理器系统上均使用本地 ISO 库。
- 每个计算机均启用了 SFTP 访问。
- RHEV 管理器已启用了 SSH 访问。

准备 Windows 映像

在创建包含 Windows 操作系统的模板时，通过遵循此程序来准备映像。按照下述步骤操作以启用 CA Virtual Assurance 开通操作从而自定义模板。特定步骤会根据 Windows 的版本而有所不同。

遵循这些步骤:

1. 在新的虚拟机上从头开始安装 Windows 操作系统。
2. 在虚拟机内安装 RHEV Guest Tools。
3. 应用您想在新的虚拟机上应用的任何自定义，如用户帐户、策略、应用程序、修补程序等。
4. （在 Windows 2003 上有效）删除内置的管理员帐户密码。

   注意：如果管理员密码不为空，SysPrep 将无法在开通期间设置新的密码，现有密码仍会保留。

安装 CA 开通帮助程序

CA 开通帮助程序使 CA Virtual Assurance 可以在外部更改虚拟机设置。

遵循这些步骤:

1. 在 <InstallationRoot>\Utilities\Sysprep\CAProvisioningHelper.exe 处查找该实用工具
2. 将此可执行文件传输到正在准备 VM 的硬盘驱动器的任何位置。
3. 从命令行执行一次 CA 开通帮助程序。

安装 Sysprep 工具

从 Windows 安装 CD-ROM 安装 Sysprep 工具。

Sysprep 工具

Microsoft 提供了 Sysprep 工具，以概括、冻结并关闭已配置的 Windows 安装。以下部分详细描述了如何使用 Windows 2003 R2 和 Windows 2008 R2 的 Sysprep 工具。

在 Windows 2003 R2 上运行 Sysprep 工具

在配置 Sysprep 工具安装之后，运行 Sysprep 工具。

遵循这些步骤:

1. 查找并打开以下 CAB 文件：

   ```
   \SUPPORT\TOOLS\DEPLOY.CAB
   ```

2. 选择包含在 CAB 文件中的所有文件，并将其复制到以下位置：%SystemDrive%\Sysprep（通常为 C：\Sysprep）。

   注意：不要更改目录名称。

3. 转到 Sysprep 目录并运行以下命令：

   ```
   sysprep -quiet -reseal -mini -forceshutdown
   ```

在 Windows 2008 R2 上运行 Sysprep 工具

常规的 Windows 安装过程安装所有文件以执行 SysPrep 过程。在您配置 Windows 安装之后，请执行以下步骤：

1. 使用 Windows Server 2008 R2 的 Windows 自动安装工具包 (WAIK) 来生成有效的 XML 响应文件。可从 Microsoft 网站获取 WAIK。

   注意:开通的方式需要模拟的无人值守响应文件，否则它将无法关闭。由于开通进程将替换响应文件的内容，因此响应文件的内容将无关紧要，但文件必须遵循特定于 SysPrep 的 XML 架构。

2. 将生成的 XML 文件命名为“sysprep.xml”，并将其放置在 Sysprep 目录中：

   %SystemRoot%\system32\sysprep

3. 运行下列命令：

   ```
   sysprep /generalize /oobe /shutdown /unattend:sysprep.xml
   ```

在 RHEV 中将 VM 转换为模板

要将关闭虚拟机转换成 RHEV 模板，请使用 RHEV 管理门户。

模板显示在 CA Virtual Assurance 中，并且可用于自定义开通。

执行了这些步骤之后，即可使用新模板来新建任意数量的自定义虚拟机。

管理 VM 状态 (KVM)

可以通过执行以下操作之一来控制虚拟机的状态：

- 发现
  - 服务器
  - 网络
- 启动
- 挂起
- 关闭
- 销毁

控制 VM 状态：

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 右键单击 VM 并选择“管理”，然后选择下列选项之一：

   发现

   发现服务器或网络。

   启动

   在指定的 RHEV 主机上启动 VM。

   挂起

   在指定的 RHEV 主机上挂起正在运行的 VM，并保存其当前状态。在您恢复 VM 之前，所有活动都会被挂起。

   关闭

   在指定的 RHEV 主机上关闭正在运行的 VM。

   销毁

   删除 VM。

   此时将显示相应的向导。

3. 填充必要信息，然后继续下一步。

4. 提交。

   状态操作发生后，将出现一条确认信息。刷新界面以查看新的 VM 状态。会出现一个确认操作结果的事件。

开通 RHEV 虚拟机

可以通过执行以下过程开通虚拟机。确保您为 VM 开通准备了 Windows 模板。

遵循这些步骤:

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 右键单击 Red Hat Enterprise Virtualization 组，选择“开通”、“开通 RHEV 虚拟机”。

   此时将显示开通向导。

3. 填充所需信息：

   VM 名称

   定义新的 VM 名称。

   模板

   指定 Windows 开通模板。

   管理员密码

   定义新 VM 的管理员密码。

   产品激活密钥

   定义 Windows 2003 激活密钥。

   全名

   定义完整的 VM 名称。

4. （可选）填写其他信息（工作组、内存、CPU、VM 主机、组织）。如果您要使用静态 IP 地址，请禁用 DHCP，并提供 IP 地址、掩码和默认网关。

   注意：内存和 CPU 设置取决于使用的 Windows 开通模板。

5. 提交。

   将显示确认消息。

6. 刷新“作业”面板以查看进度。

   会出现一个确认操作结果的事件。

Solaris Zones

Solaris Zones 定义虚拟化操作系统，为运行应用程序提供隔离且安全的环境。该环境允许在应用程序和服务中分配资源，并确保此过程不会影响其他区域。Solaris 将各个区域作为一个实体进行管理。*容器*也是使用操作系统资源管理的区域。Solaris Zones PMM 提供 Solaris Zones 环境的运行状况监控、管理和开通。

Solaris Zones 容器资源可分为以下三个级别进行管理：

Solaris Zones 区域管理

Solaris 服务器使用 *zones* 在隔离的环境中运行应用程序，使其看似在物理上独立的计算机上运行。服务器上的每个区域从资源池获取其资源，并且包括虚拟网络接口、文件系统、内存和其他专用单元。

Solaris Zones 项目管理

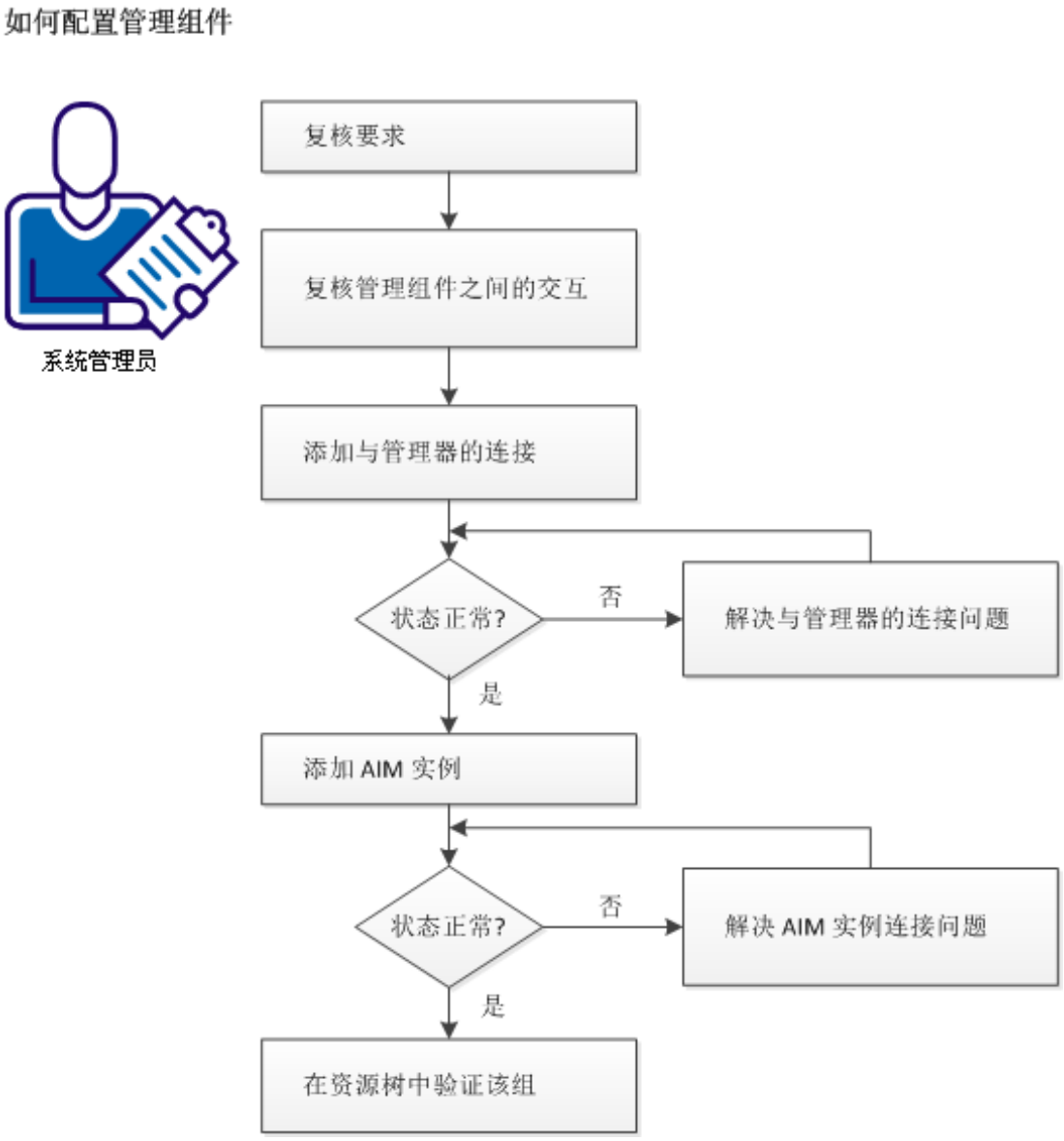
*项目*是您想要分割为单独的工作负荷实体的一个应用程序或一组应用程序。根据工作负荷和配置设置，区域将资源分别分配给来自其他资源或项目的项目。

Solaris Zones 资源池管理

*资源池*为处理器集配置和调度类分配提供永久配置机制。根据其配置方式，资源池可以将资源动态地分配给区域中的项目和任务。

如何配置 Solaris Zones 管理组件

下图提供了有关配置管理组件所需操作的概述。该图包括针对连接问题的相应故障排除策略。



Solaris Zone PMM 提供了 Solaris Zone 环境的运行状况监控、管理和开通。

请执行以下步骤：

查看要求

在配置 CA Virtual Assurance 的管理组件之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您熟悉 CA Virtual Assurance 和 SystemEDGE。
- 您可以访问包括以下内容的 CA Virtual Assurance 管理器安装：
  - 平台管理模块 (PMM)
  - Application Insight Module (AIM)
  - 监控代理 (SystemEDGE)
- 您可以访问 CA Virtual Assurance 用户界面。
- 您具有有效的凭据（用户名和密码），可访问要管理的环境中的服务器。
- 您知道使用哪个协议（HTTP 或 HTTPS）和端口，以通过 Web 服务访问环境中的服务器。默认：HTTPS，端口：443。
- 您已验证环境中的服务器运行正常。
- 如果将 PMM 和 AIM 安装在不同系统上，请确认 PMM 和 AIM 系统上的 SNMP 设置一致。读和写团体字符串以及 SNMP 端口号必须是相同的。
- 您已验证 CA Virtual Assurance 管理器已发现您要使用的远程 AIM 服务器。

详细信息：

Solaris Zones 管理的要求 (p. 431)

Solaris Zones 管理的要求

验证 CA Virtual Assurance 对于 Solaris Zones 管理所需的用户帐户是否满足 Solaris 服务器上的以下设置和权限：

- Solaris 服务器上的用户提示必须是“#”（默认）。
- Solaris 用户需要执行以下命令的权限：
  - zlogin
  - zoneadm
  - zonecfg
- 在全局区域中，用户必须拥有通过 zlogin 登录到单独 Solaris Zones 并运行以下命令的权限：
  - uname -a
  - sar
  - prstat
  - netstat

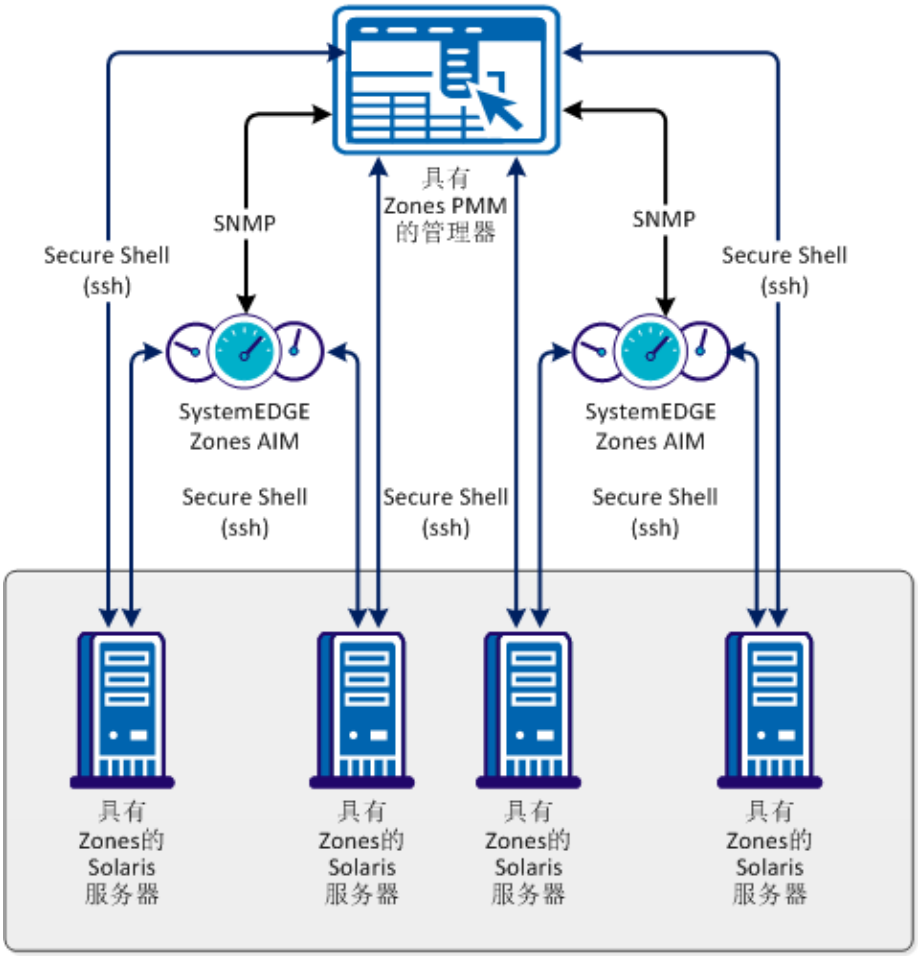
使用用户界面或 Solaris Zones AIM 所在的受管节点上的 NodeCfgUtil.exe 实用工具，在配置期间将该用户名及相应密码添加到 CA Virtual Assurance。

从“浏览”、“管理”、“创建资源池”中创建资源池，以便在 Solaris Zones 服务器上为区域、项目和应用程序分配资源。在区域创建过程中将其分配给区域。

Solaris Zones 管理组件之间的交互

下图说明 Solaris Zones 管理中的组件是如何交互的。受管节点是运行 SystemEDGE 和 Solaris Zones AIM 的 Windows 服务器。AIM 和 Solaris Zones 服务器根据 SSH（安全外壳）进行通信。

Solaris Zones 管理组件之间的交互



要为每个 Solaris Zones 服务器添加所需连接信息，请在受管节点上使用用户界面的“管理”选项卡或 NodeCfgUtil.exe 实用工具。连接信息将写入受管节点上的配置文件中。AIM 调查配置文件并开始监控 Solaris Zones 环境。

将 Solaris Zones 连接添加到管理器中

您可以使用 CA Virtual Assurance 用户界面的“管理”选项卡添加 Solaris Zones 连接。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“Solaris Zone”。

3. 在“Solaris Zone 服务器”窗格工具栏上单击  （添加）。

   此时将显示“添加 Solaris Zone 服务器”对话框。

4. 输入所需的连接数据（服务器名称、用户、密码、端口），指定首选 AIM，并启用“受管状态”（复选框）。

5. 单击“确定”。

   如果网络连接已成功建立，服务器会添加到右上角的窗格并带有绿色状态图标。

   注意：如果连接失败，将显示“验证失败”对话框。单击“是”，CA Virtual Assurance 将服务器添加到列表中并带有红色状态图标。如果您单击“否”，将不添加任何内容。

管理器到服务器的连接失败

症状：

在“管理”、“配置”下添加服务器连接后，对服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的服务器连接数据是否仍然有效。如有必要，请更新连接数据。
- 验证服务器系统是否正在运行并且可以访问。
- 验证连接所需的所有服务是否在服务器系统上运行良好。

更新服务器连接数据：

1. 单击与失败的连接关联的 （添加）或 （编辑）。
2. 添加连接详细信息，启用“受管状态”，然后单击“确定”。

   将更新连接数据。
3. 单击右上角的 （验证）以验证新设置。

   如果无法建立与服务器的连接，请继续执行下一步骤。

验证服务器系统是否正在运行并且可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```
2. 要确定服务器是否具有有效的 DNS 条目和 IP 地址，请检查这些命令的输出。

   如果服务器不在 DNS 中，请将服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。
3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress <Server Name>
   ```

   输入正确的 IP 地址和服务器名称并保存文件。例如：

   ```
   192.168.50.50 myServer
   ```
4. 切换到 CA Virtual Assurance 用户界面、“管理”选项卡、“配置”、“服务器”窗格，并单击右上角的 （验证）。

   即使服务器凭据和连接数据正确并且您可以 ping 服务器，连接仍然可能失败。在这种情况下，可能是服务器引起该问题。如果无法建立与服务器的连接，请继续执行下一步骤。

验证连接所需的所有服务是否在服务器系统上运行良好。

1. 要访问服务器，请联系系统管理员。
2. 登录到服务器系统。
3. 验证连接所需的所有服务是否运行良好。
4. 如有必要，请启动或重新启动服务。
5. 切换到管理器系统上的 CA Virtual Assurance 用户界面、服务器窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证服务器连接。

   如果与服务器的连接失败，请验证根据该方案的要求收集的数据是否有效。

   与管理员或技术支持合作，解决服务器连接问题。

添加 Zones AIM 服务器

将 Solaris Zone 连接添加到 CA Virtual Assurance 管理器后，添加 AIM 实例以管理 Solaris Zone 环境。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。
2. 从左侧窗格的“开通”部分中选择“Solaris Zone”。
3. 在“区域 AIM 服务器”窗格工具栏上单击 （添加）。

   此时将显示“新建区域 AIM 服务器”对话框。
4. 从下拉列表中选择“AIM 服务器”。

   CA Virtual Assurance 将向“实例”下拉列表中填充“注册的 Solaris Zones”窗格中列出的 Zone 服务器。您只能管理您的 CA Virtual Assurance 管理器与之建立了有效连接的那些 Zone 服务器。

   注意：如果 AIM 位于远程系统中，则 CA Virtual Assurance 一定会首先发现该系统。在发现之后，AIM 服务器将在下拉列表中显示。
5. 从下拉列表中选择“实例”，然后单击“确定”。

   将添加选定的服务器的新 AIM 实例。

   AIM 服务器上的 AIM 现已配置为从指定的 Zone 服务器收集数据。如果实例未处于错误或已停止状态，CA Virtual Assurance 将开始发现关联的环境。当发现过程完成时，您可以开始管理 Solaris Zone 环境。

排除 AIM 实例连接的故障

如果 AIM 连接处于未就绪状态，将出现以下状态图标之一：

- 发现正在进行
- 无轮询
- 错误
- 警告
- 已禁用
- 未知

有关 AIM 实例状态的详细信息，请参阅工具提示。以下故障排除部分提供了用于解决该问题的详细信息和步骤。

AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为服务器添加 AIM 实例后，状态图标显示 （发现正在进行）。

解决方案：

等到环境的发现过程完成。发现持续时间取决于与环境中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示指示未完成发现请求数量的工具提示。发现作业完成时，CA Virtual Assurance 会向资源树中添加一个服务器文件夹。然后，您可以开始管理您的环境。

AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示 （无轮询）。

解决方案：

关联实例不需要特定的操作。此图标表示 CA Virtual Assurance 管理器不轮询此 AIM。AIM 不是首选。

如果多个 AIM 已配置为管理特定服务器，PMM 将选择其中一个 AIM 作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决可能导致与 AIM 连接失败的最常见问题：

- 验证是否可以访问 AIM 服务器。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 确认命令的输出对于 AIM 服务器有有效的 DNS 条目和 IP 地址。

   如果 AIM 服务器不在 DNS 中，则将 AIM 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress servername
   ```

   输入正确的 IP 地址和 AIM 服务器名称。例如：

   ```
   192.168.50.51 myAIM
   ```

4. 在“AIM 服务器”窗格的右上角，单击  （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“AIM 服务器”窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证 AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否有效。

AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 AIM 实例之后，几个实例的状态图标显示 （已禁用）。该 AIM 实例未受管理。

如果 CA Virtual Assurance 发现具有以下关系的 AIM，则显示该状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的服务器配置了 AIM。
- AIM 连接到未配置的服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的服务器连接并将其受管状态更改为已启用。

验证资源树中的 Solaris Zones 组

在成功配置和发现之后，新发现的资源将在“资源”、“浏览”窗格中的相应组下列出。

遵循这些步骤：

1. 单击“资源”，然后打开“浏览”窗格。
2. 展开 Solaris Zone 组。

   此时将出现受管 Solaris Zone 资源。

CA Virtual Assurance 已准备好管理已配置的 Solaris Zone 环境。

Solaris Zones 管理

Solaris Zones 服务器使用区域在隔离的环境中运行应用程序，使其看似在物理上独立的计算机上运行。服务器上的每个区域从资源池获取其资源，并且包括虚拟网络接口、文件系统、内存和其他专用单元。

本节说明可通过“资源”页面对 Solaris Zones 资源执行的管理操作。通过“资源”页面，您可以查看以下对象的基本信息和详细信息：

- Solaris Zones 服务器
- Solaris Zones

单击“资源”，打开“浏览”窗格，并选择其中一个资源；然后单击该资源的“摘要”。通过“摘要”页面，您可以查看与资源相关的信息（例如，Solaris Zones 服务器上的区域、资源池和磁盘或区域上的网络接口和项目）以及与资源相关的事件。

注意：如果使用“使用率”面板中的“配置”按钮选择报警为正常，则即使 CPU 或内存处于严重或警告状态，区域仍会以正常状态（绿色）显示。同样地，如果选择报警为警告，则区域将始终以警告状态显示。

组件树仅显示区域使用的资源池。该面板中不会列出非活动资源池。

通过“详细信息”页面，您可以查看其他详细的资源信息，如系统属性、软件、硬件、性能等。

其他页面可用来执行资源管理任务。也可以使用“浏览”窗格的右键单击菜单来执行管理和策略任务。

详细信息

创建资源池 (p. 442)
控制区域状态 (p. 443)
克隆区域 (p. 444)
删除区域 (p. 445)
可用的 Solaris Zones 操作 (p. 445)

添加 Solaris Zone

Solaris Zones 服务器使用区域在隔离的环境中运行应用程序，使其看似在物理上独立的系统上运行。服务器上的每个区域从资源池获取其资源，并且包括虚拟网络接口、文件系统、内存和其他专用单元。在创建区域时，您必须提供所有这些信息。区域会在创建后自动安装。

添加 Solaris Zone

1. 选择“资源”选项卡，右键单击“浏览”窗格中的“区域主机”，并依次选择“开通”、“开通区域”。

   此时将显示“Solaris Zone 开通”向导。

2. 完成“区域身份和类型”页上的以下字段，然后单击“下一步”：

   主机

   定义要在其中创建区域的主机。

   名称

   定义区域的名称。

   说明

   （可选）定义区域的说明。

   类型

   定义区域是“本地”、“整个根”还是“已标记”。“标记”区域基于现有的区域模板。

   模板名称

   （可选）在将“类型”设置为“标记”时，定义创建区域所基于的模板。

   安装存档路径

   定义区域中的安装存档的目录路径。仅当将“类型”设置为“标记”时，才需要该字段。

   此时将显示“CPU”、“内存”和“其他”页面。

3. 填写下列字段，然后单击“完成”：

   类型

   定义排定程序类型。选择 FSS，以使用“公正份额排定”类来基于分配给任务的 CPU 份额来控制 CPU 分配。

   容量

   定义分配到区域的物理内存容量的数量 (MB)。

交换内存

定义分配到区域的交换内存的数量 (MB)。交换内存至少为 50 MB。

锁定内存

定义分配到区域的锁定内存的数量 (MB)。锁定内存必须小于物理内存。

区域路径

定义区域的根目录路径。

NIC 类型

（可选）定义 NIC 类型。从下拉列表中选择类型。如果不选择 NIC，则不为该区域分配 NIC 卡或 IP 地址。

IP 地址

（可选）定义区域的 IP 地址。

资源池

定义要用于区域的资源池。从下拉列表中选择一个池。如果要将新资源池用于区域，请首先创建池。如果不选择池，则使用默认池。

自动重新启动

定义在重新启动全局区域时是否自动重新启动该区域。

创建资源池

您可以创建资源池，用于在 Solaris Zones 服务器上为区域、项目和应用程序分配资源。创建资源池后，您可以在创建区域过程中将其分配给区域。

创建资源池

1. 在“浏览”窗格上右键单击 Solaris Zones 服务器，然后依次选择“管理”、“创建资源池”。

   此时将显示“创建资源池”对话框。

2. 填写下列字段，然后单击“确定”：

   名称

   标识资源池名称。

   最小 CPU 份额

   标识池在任何时候都必须具有的最小 CPU 份额。

   最大 CPU 份额

   标识池可具有的 CPU 份额的最大数目。

   处理器集名称

   标识池的处理器集名称。

   排定程序类型

   标识在分配资源时使用的排定类型。选择 FSS，以使用“公正份额排定”来基于工作负荷重要性（为项目或任务指定的 CPU 份额数目）分配资源。

   池已创建，并显示一条确认消息。

3. 单击在其上创建池的区域服务器的“摘要”选项卡，并在“显示”下拉列表中选择“资源池”以验证是否已创建池。

控制区域状态

您可以执行停止、重新引导、启动和卸载操作来控制区域的状态。您不能对全局区域或处于已安装状态的区域执行这些操作。

控制区域状态

1. 在“浏览”窗格上右键单击一个区域，然后选择“管理”和以下选项之一：

   启动

   启动区域，使其处于正在运行状态。您只能启动处于已安装状态的区域。

   停止

   通过将区域重置为已安装状态来将其暂停。暂停区域会停止所有进程、删除网络接口，并执行其他操作以删除区域的现有应用程序环境和虚拟平台。暂停区域后，必须启动区域才能重新启动环境。您只能暂停当前正在运行的区域。

   重新启动

   暂停区域并重新引导它。您只能重新引导当前正在运行的区域。重新引导区域时，服务器会为其提供一个新的区域 ID。

   删除

   删除区域。有关详细信息，请参阅“删除区域”部分。

   安装

   安装在安装完成后进入已配置状态的本地或已标记区域。安装区域将打开一个对话框，询问您已标记区域的存档路径。如果安装本地区域，请将该字段留空。如果安装已标记区域，请提供存档路径。

   注意：如果您在尝试安装已标记区域时没有输入存档路径参数，或在安装本地区域时输入了存档路径参数，则会收到错误消息。

   卸载

   卸载区域的根文件系统下的所有文件。您只能卸载当前未运行（已安装状态）的区域。您应当先卸载区域，然后再将其删除。

   克隆

   克隆区域。有关详细信息，请参阅“克隆区域”部分

   这时将会出现确认对话框。

2. 单击“确定”。

   此时将显示一条消息，确认已提交请求。

3. 单击区域主机的“摘要”选项卡。

此时应出现一个确认操作结果的事件。

注意：如果当前操作正在进行并且尚未完成，则区域状态将显示不完整。

详细信息

删除区域 (p. 445)
克隆区域 (p. 444)

克隆区域

通过克隆区域，您可以通过从现有区域复制数据来配置和安装新的区域。必须暂停您正在克隆的区域才能执行克隆操作。您不能对全局区域或处于已配置状态或正在运行状态的区域执行此操作。

克隆区域

1. 在“浏览”窗格上右键单击区域，然后依次选择“管理”、“克隆”。

   此时将显示“克隆”窗格。
2. 在“目标”窗格中填写以下字段，然后单击“克隆”。

   名称

   指定要将克隆的信息复制到的区域的名称。

   路径

   指定要将克隆的信息复制到的区域的文件路径。

   即会出现一条确认消息。
3. 单击区域主机的“摘要”选项卡。

   会在显示板中出现一个确认操作结果的事件。操作完成后，克隆的区域将显示在“浏览”窗格中其包含的主机下。

删除区域

可以从 Solaris Zones 服务器中删除非全局区域。删除区域前必须先将其关闭。

如果区域处于已安装状态，该操作将先卸载然后删除该区域。如果区域处于任何其它状态（如运行），将显示一条错误消息。

要删除区域，请执行以下操作：

1. 右键单击“浏览”窗格上的区域并选择“管理”、“删除”。

   这时将会出现确认对话框。

2. 单击“确定”。

   将出现确认删除的消息。

3. 单击区域主机的“摘要”选项卡。

   此时应出现一个确认操作结果的事件。操作完成后，删除的区域应从“浏览”窗格消失。

可用的 Solaris Zones 操作

以下操作类型可与 Solaris Zones 一起使用：

- 克隆区域计算机 (p. 609)
- 删除区域计算机 (p. 635)
- 开通区域计算机 (p. 662)

在满足分配的规则条件后，可以使用这些操作类型来创建自动化区域操作的新操作。还可以排定这些操作在特定时间发生。

有关使用操作和规则来创建自动化策略的详细信息，请参阅“策略”一章。

VMware vCloud

利用 *VMware vCloud Director*，您可通过将虚拟基础架构资源集中到虚拟数据中心中并将其公开给用户来构建安全且具有多承租人的云。CA Virtual Assurance 支持 VMware vCloud Director 管理。
vCloud Director 资源根据基础 vSphere 资源（例如，CPU、内存、存储或 vNetwork 分布式交换机）来运行虚拟机。您可以使用这些基础 vSphere 资源，以在 vCloud 中创建虚拟机和 vApp。

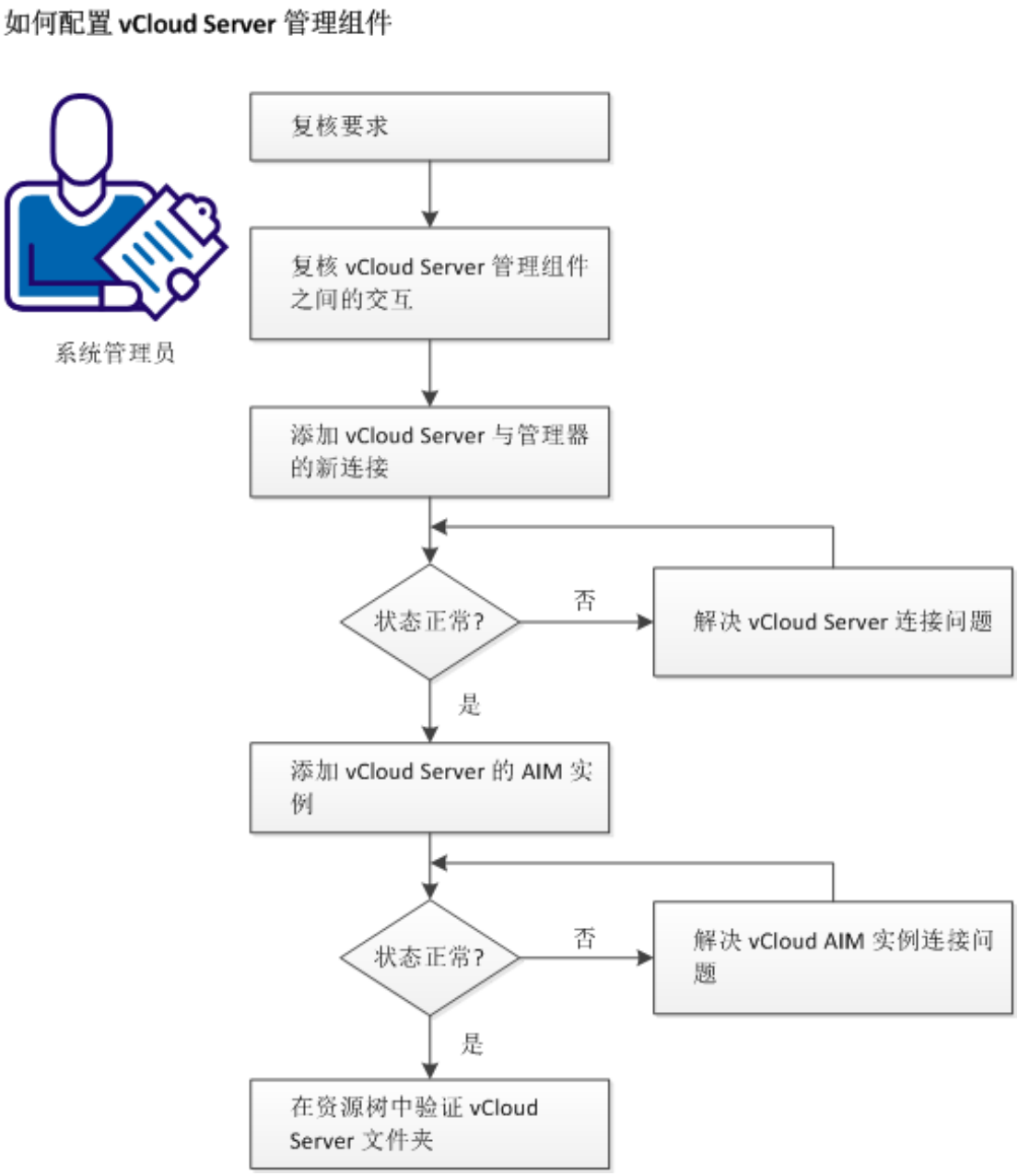
*vCloud 组织*是一个管理单位，表示用户、组和计算资源的集合。关联的虚拟数据中心可提供所需的计算资源。用户在组织级别进行身份验证后，可以创建、使用和管理虚拟机或 vApp。

虚拟数据中心 (vDC) 向 vCloud 组织提供虚拟计算资源。您可以在虚拟数据中心中开通、运行和存储虚拟系统。一个 vCloud 组织可以具有多个虚拟数据中心。

组织提供*目录*来存储 vApp 模板和媒体文件。组织成员可以使用目录中的 vApp 模板和媒体文件来创建自己的 vApp。

如何配置 vCloud Director 管理组件

下图提供有关所需操作的概述。该图包括针对连接问题的相应故障排除策略。



请执行以下步骤：

查看 vCloud 要求

开始配置 CA Virtual Assurance 的 vCloud Director 管理组件之前，请查看以下要求：

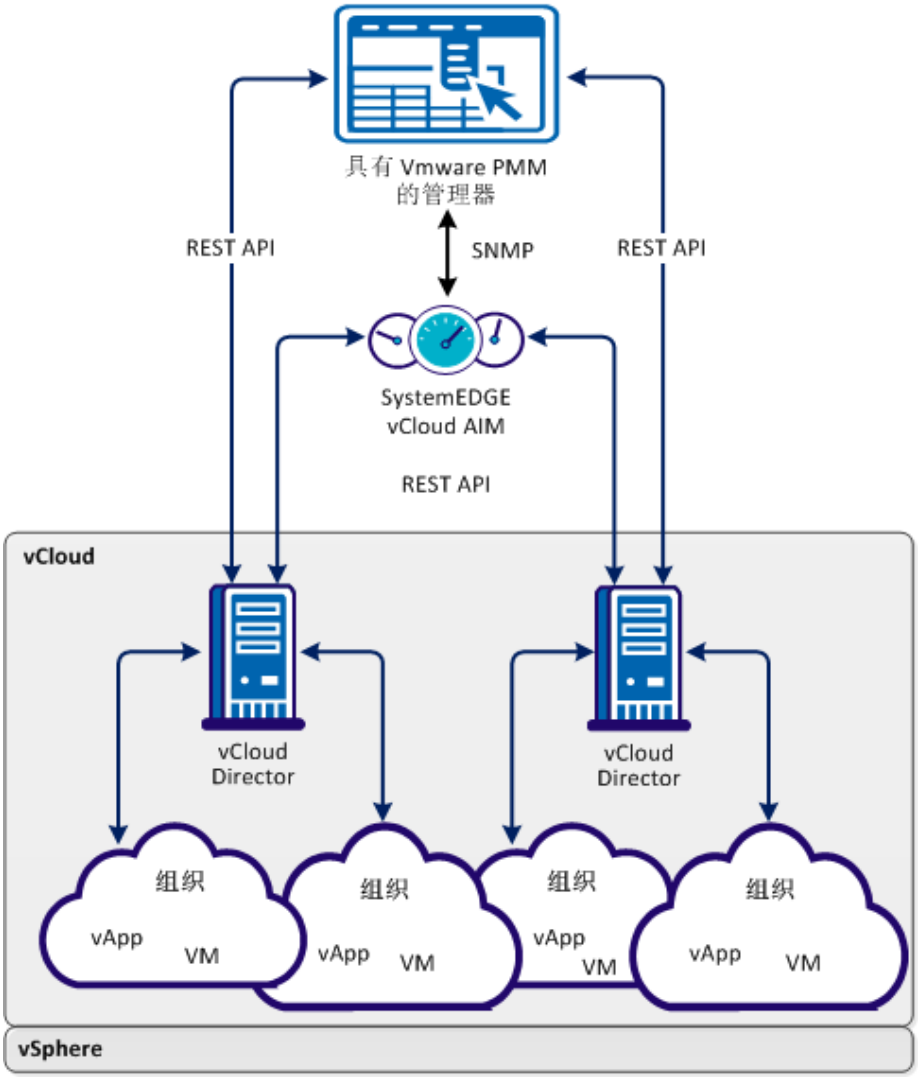
- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您对 CA Virtual Assurance、CA SystemEDGE、VMware vSphere 和 VMware vCloud 有基本的了解。
- 您可以访问 CA Virtual Assurance 管理器安装，该安装包括 vCenter 平台管理模块 (PMM)、vCenter Application Insight Module (AIM) 和监控代理 (CA SystemEDGE)。
- 您可以访问 CA Virtual Assurance 用户界面。
- 您拥有有效的凭据（用户名和密码），可用于访问要管理的 vCloud Director 服务器。
- 您已确定通过 Web 服务访问 vCloud Director 所要使用的协议（HTTP 或 HTTPS）和端口。默认值：HTTPS，端口 443
- 您已经确认 vSphere 环境和 vCloud Director 运行良好。
- 如果 VMware PMM 和 vCloud AIM 安装在不同的系统上，您已验证这些系统上的 SNMP 设置一致。读和写团体字符串以及 SNMP 端口号必须是相同的。
- 您已确认 CA Virtual Assurance 管理器已发现您要使用的任何远程 vCloud AIM 服务器。

详细信息：

vCloud 管理组件之间的交互

下图说明了 vCloud Director 管理中涉及组件的交互方式。SystemEDGE 和 vCloud AIM 在 Windows 服务器上运行。AIM 与一个或多个远程 vCloud Director 服务器进行通信，以管理虚拟环境。vCloud AIM 收集数据，以获得与 vCloud Director 相关联的虚拟资源的完整视图。基础 vSphere 环境提供运行虚拟机和 vApp 的必要资源。

vCloud Director 管理组件之间的交互



您可以通过用户界面上的“管理”选项卡配置 vCloud 管理。

注意：VMware 工具可优化 VM 的虚拟化，建议在 VMware 环境中的每个 VM 上安装这些工具。对于没有安装 VMware 工具的 VM，该产品的一些功能将不可用或无法正常运行。因此，不支持没有安装 VMware 工具的 VM。

将 vCloud Director 连接添加到管理器中

您可以使用 CA Virtual Assurance 用户界面上的“管理”选项卡添加 vCloud Director 连接。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“vCloud 服务器”。

   右侧窗格将刷新和显示受管的 vCloud 服务器、关联的 vCloud AIM 服务器以及 vCloud 服务器的 AIM 实例。

3. 在“vCloud 服务器”窗格工具栏上单击  （添加）。

   此时将显示“添加 vCloud 服务器”对话框。

4. 输入所需的连接数据（服务器名称、用户名、密码、协议、端口），指定首选 AIM，启用“受管状态”（复选框），然后单击“确定”。

   指定用户名时，您可以使用以下语法来考虑用户角色和访问级别：

   - 系统管理员（完全访问）：administrator@System
   - 限制组织级别的操作和角色分配（组织访问）
     username@organization_name

   如果网络连接已成功建立，vCloud 服务器会添加到右上角的“vCloud 服务器”窗格并带有绿色状态图标。CA Virtual Assurance 自动发现 vCloud 服务器。

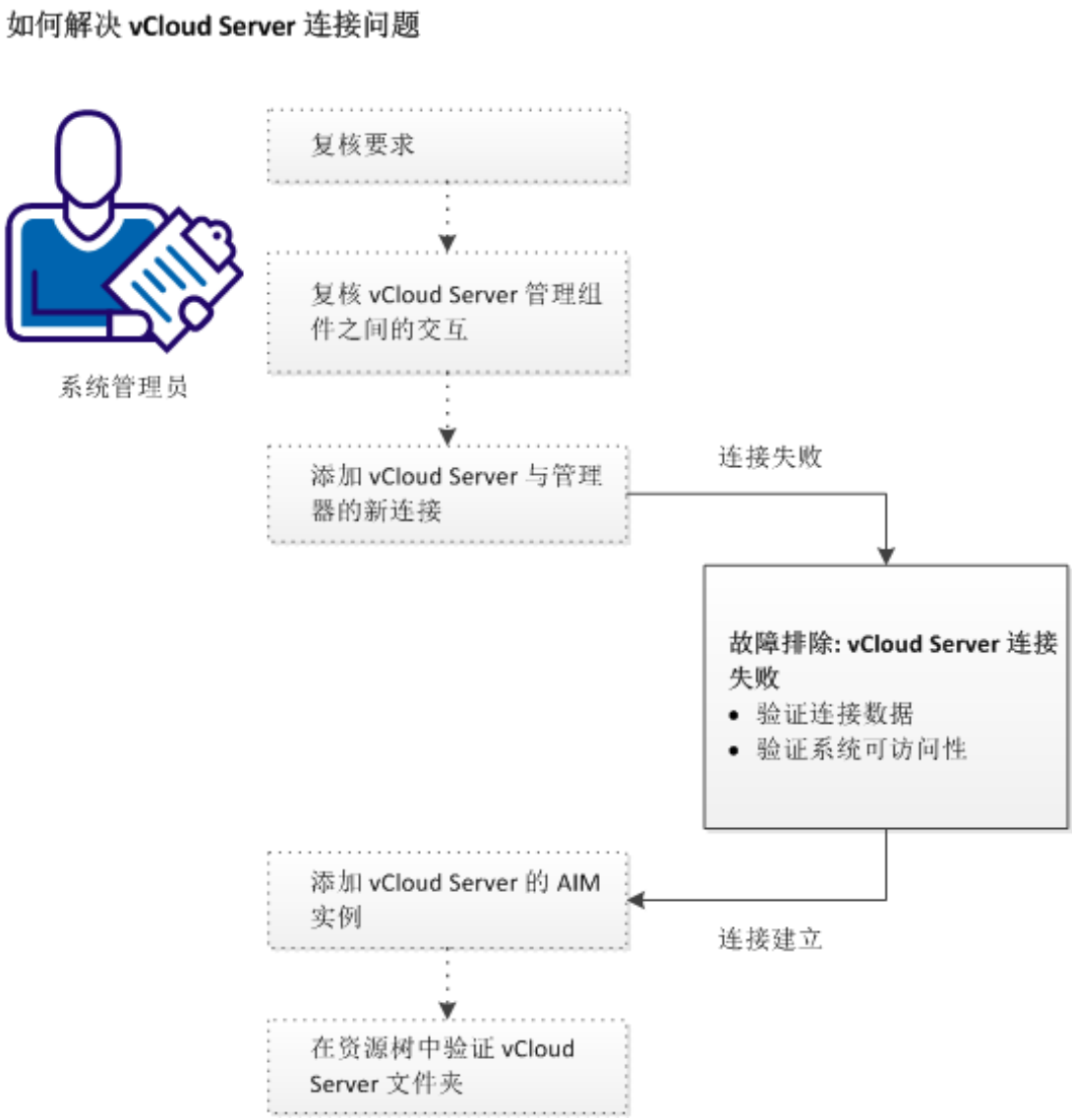
   如果连接失败，将显示“验证失败”对话框。如果单击“是”，则 CA Virtual Assurance 会将 vCloud 服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。有关排除连接故障的信息，请参见排除 vCloud 服务器连接的故障 (p. 451)。

详细信息：

为 vCloud 服务器添加 AIM 实例 (p. 453)
验证资源树中的 VMware vCloud 文件夹 (p. 459)
排除 vCloud 服务器连接的故障 (p. 451)

排除 vCloud 服务器连接的故障

vCloud 服务器连接已失败。遵循下图所示的故障排除信息：



请执行以下步骤：

vCloud 服务器连接失败 (p. 452)
为 vCloud 服务器添加 AIM 实例 (p. 453)
验证资源树中的 VMware vCloud 文件夹 (p. 459)

vCloud 服务器连接失败

症状：

在“管理”、“配置”下添加新 vCloud 服务器连接后，对 vCloud 服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的 vCloud 服务器连接数据（服务器名称、用户、密码、协议、端口）是否仍然有效。如有必要，请更新连接数据。
- 验证 vCloud 服务器系统是否正在运行并且可以访问。

更新 vCloud 服务器连接数据

1. 单击与失败的连接关联的  （添加）或  （编辑）。

   此时将显示“新建 vCloud 服务器”或“编辑 vCloud 服务器”对话框。

2. 添加有效的服务器名称、用户、密码、协议和端口。指定首选 AIM。启用“受管状态”，然后单击“确定”。

   将更新连接数据。

3. 单击右上角的  （验证）以验证新设置。

   如果无法建立与 vCloud 服务器的连接，请继续执行下一个步骤。

验证 vCloud 服务器系统是否正在运行并且可以访问

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <vCloud Server Name>
   ping <IP Address of vCloud Server>
   ```

2. 验证命令的输出，以确定 vCloud 服务器是否具有有效的 DNS 条目和 IP 地址。

   如果 vCloud 服务器不在 DNS 中，则将 vCloud 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果 vCloud 服务器位于 DNS 中，请继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ipaddress <vCloud Server Name>

   输入正确的 IP 地址和 vCloud 服务器名称。例如：

   192.168.50.50 myvCloud

4. 单击右上角的（验证）。

   如果与 vCloud 服务器的连接失败，请验证根据该方案的要求收集的数据是否仍然有效。

   与 vCloud 管理员或 VMware 支持部门合作，解决 vCloud 服务器连接问题。

为 vCloud 服务器添加 AIM 实例

在将新的 vCloud 服务器连接添加到 CA Virtual Assurance 管理器中之后，添加 vCloud AIM 实例来管理新的 vCloud 服务器。然后，CA Virtual Assurance 发现整个 vCloud 环境及其所有的虚拟组件（如组织、vApp、VM 等）。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“vCloud 服务器”。

   右侧窗格将刷新和显示受管的 vCloud 服务器、关联的 vCloud AIM 服务器以及受管 vCloud 服务器的 AIM 实例。

3. 在“vCloud AIM 服务器”窗格工具栏上单击（添加）。

   此时将显示“添加 vCloud AIM 服务器”对话框。

4. 打开“vCloud AIM 服务器”下拉列表。

   此时将显示发现的 vCloud AIM 服务器的列表。如果您已在本地系统上安装了 vCloud AIM，则本地系统的名称也会显示在列表中。

5. 从下拉列表中选择一个 vCloud AIM 服务器。

   CA Virtual Assurance 使用“vCloud 服务器”窗格中列出的 vCloud 服务器填充“vCloud 服务器”下拉列表。换言之，您只能管理您的 CA Virtual Assurance 管理器为之建立了有效连接的 vCloud 服务器。

6. 选择要管理的 vCloud 服务器，然后单击“确定”。

   此时将为选定的 vCloud 服务器添加一个新的 AIM 实例。如果实例未处于错误或已停止状态，则 CA Virtual Assurance 将开始发现关联的 vCloud 环境。发现过程完成后，您可以开始管理 vCloud 的虚拟资源。

详细信息：

验证资源树中的 VMware vCloud 文件夹 (p. 459)
排除 vCloud AIM 实例连接的故障 (p. 455)

排除 vCloud AIM 实例连接的故障

vCloud AIM 连接处于未就绪状态。将显示下列状态图标之一：

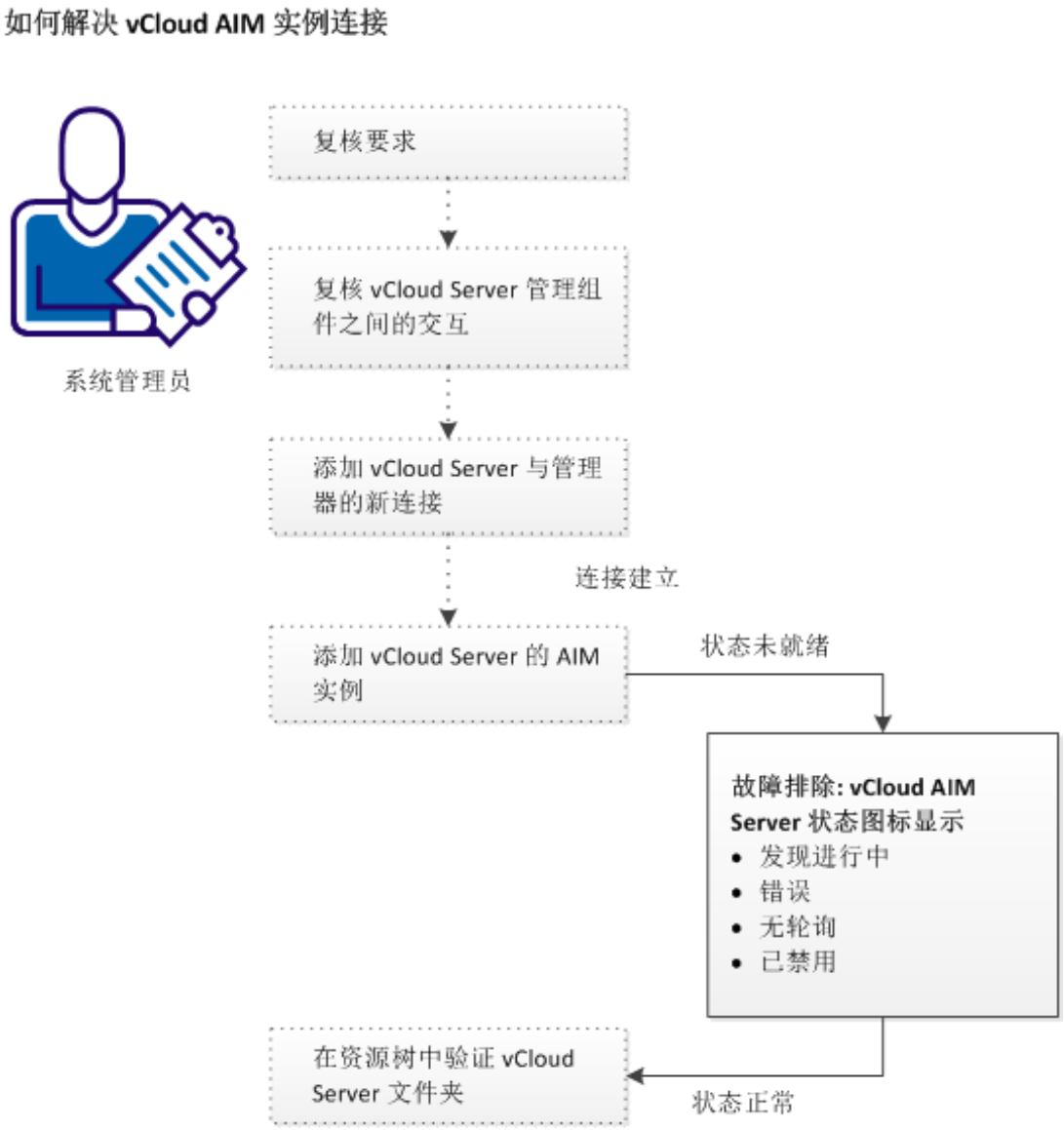
发现正在进行－等到平台管理器使所有数据同步。

错误－无法连接到 AIM。请检查网络配置。

无轮询－CA Virtual Assurance 管理器未轮询此 AIM 实例。

已禁用－该实例未受管理。

遵循下图所示的故障排除信息：



详细信息：

vCloud AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为 vCloud 服务器添加 vCloud AIM 实例后，状态图标显示  （发现正在进行）。

解决方案：

等到 vCloud 环境的发现过程完成。发现持续时间取决于与 vCloud 中的虚拟资源相关的受管对象数量。可将光标悬停于图标上方，以显示用于指示未完成的发现请求数的工具提示。发现作业完成后，CA Virtual Assurance 会向资源树中添加一个 vCloud 服务器文件夹。然后，您可以开始管理 vCloud 及其整个虚拟基础架构。

vCloud AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下为 vCloud 服务器添加 vCloud AIM 实例后，状态图标显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决导致与 vCloud AIM 连接失败的最常见问题：

- 验证是否可以访问 vCloud AIM 服务器。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证是否可以访问 vCloud AIM 服务器系统

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 验证命令的输出，以确定 vCloud AIM 服务器是否具有有效的 DNS 条目和 IP 地址。

   如果 vCloud AIM 服务器不在 DNS 中，则将 vCloud AIM 服务器添加到 CA Virtual Assurance 管理器系统上的 Windows 主机文件中。继续执行步骤 3。

   如果 vCloud 服务器位于 DNS 中，请继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress servername
   ```

   输入正确的 IP 地址和 vCloud AIM 服务器名称。例如：

   ```
   192.168.50.51 myvCloudAIM
   ```

4. 在“vCloud AIM 服务器”窗格的右上角，单击 （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行

1. 登录到 vCloud AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“vCloud AIM 服务器”窗格，然后单击右上角的 （验证）。

   CA Virtual Assurance 将验证 vCloud AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否仍然有效。

vCloud AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下为 vCloud Director 添加 vCloud AIM 实例后，状态图标显示 （无轮询）。

解决方案：

关联实例不需要特定的操作。此图标通知您 CA Virtual Assurance 管理器未轮询此 AIM。AIM 不是首选。

如果配置多个 AIM 来管理特定的 vCloud Director，则 PMM 将选择其中一个 AIM 作为当前的 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

vCloud AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 vCloud AIM 实例之后，几个实例的状态图标显示 （已禁用）。该 vCloud AIM 实例未受管理。

如果 CA Virtual Assurance 已发现具有以下关系的 vCloud AIM，则显示该状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的 vCloud 服务器配置了 vCloud AIM。
- AIM 已连接到未在“vCloud 服务器”窗格中配置的 vCloud 服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺失的 vCloud 服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的 vCloud 服务器连接并将其受管状态更改为已启用。

验证资源树中的 VMware vCloud 文件夹

在成功配置和发现之后，新的 vCloud 服务器将在“资源浏览”窗格的 VMware vCloud 文件夹下列出。

遵循这些步骤:

1. 单击“资源”、“浏览”。

   此时将显示“资源”树。

2. 展开 VMware vCloud。

   将显示受管的 vCloud Director 服务器。

3. 展开新的 vCloud Director 服务器条目。

   将显示受管的 vCloud 基础架构：组织、vApp、VM 等

CA Virtual Assurance 现在可以用于管理添加的 vCloud 环境及其虚拟基础架构。

远程多实例 vCloud Director 支持

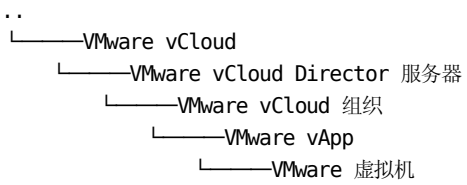
vCloud AIM 与一个或多个远程 vCloud Director 实例进行通信。但是，当您同时使用 CA Virtual Assurance 管理器和多个远程 vCloud AIM 管理多个 vCloud Director 环境时，需考虑以下关系：

每个 vCloud Director 都唯一地与一个您在配置期间指定的首选 vCloud AIM 关联。设置首选 AIM 以指明如果多个 AIM 管理一个 vCloud Director，应将哪个 AIM 用于轮询。

vCloud 文件夹结构

在成功配置到 vCloud Director 服务器的连接之后，CA Virtual Assurance 将发现包括组织、vApp 和虚拟机的 vCloud Director 环境。当发现完成时，VMware vCloud 文件夹将显示在“资源”选项卡的“浏览”窗格中。您可以展开文件夹并管理 vCloud 环境。

下图显示了 VMware vCloud 文件夹下的对象层次结构。



服务级别展示在 VMware vCloud 文件夹的顶部。vCloud 服务可包括多个 VMware vCloud Director 服务器。每个 vCloud Director 通常具有多个配备 vApp 和虚拟机的组织。

在组织级别上，可以基于目录中存储的模板开通 vApp。

vCloud 中的 vApp 支持

在 vCloud 和 vSphere 环境中 vApps 概念是类似的。它们都表示可在其上作为单个实体运行的应用程序对象。通常，vApp 包含多个 VM，每个 VM 均旨在向最终用户提供完整的 vApp 应用程序或服务。对 vApp 执行的操作也会对 vApp 中的所有 VM 执行。例如，两种类型均为 vApp 中的所有 VM 定义了启动和停止顺序，并定义了 vApp 中所有 VM 可使用的 CPU 和内存资源限制。

vCloud 中的 vApp 旨在能够将应用程序或服务定义为模板，使多个组织可以通过组织目录访问该模板。vCloud 将其数据存储在 vCloud 数据库中，该数据库与 vCenter 服务器数据库不同。

重要信息！请勿直接在 vCenter 服务器中对 vCloud 中定义的 VM 执行操作。这些操作可能会导致 vCloud 数据库与实际定义的 VM 不同步。CA Virtual Assurance 为显示在 vCloud 和 vCenter 服务器下的 VM 提供一组受限的操作，以便数据库可以进行同步。

vCloud vApp 与 vSphere vApp 之间的差异

- vCloud vApp 提供的功能不适用于嵌套层次结构。vSphere vApp 可以包含其他 vApp 和资源池。
- 在 vCloud 中，CPU 和内存资源限制是通过虚拟数据中心 (vDC) 定义的，并且 vApp 将映射到其中一个虚拟数据中心。

  在 vSphere 中，vApp 资源限制是针对 vApp 本身定义的。
- vCloud vApp 可以包含在多个不同 vCenter 服务器和 ESX 主机上定义的 VM。

  vSphere vApp 中的 VM 限制为特定数据中心和群集中的 VM。
- vCloud vApp 具有租赁限制。您可以定义对 vApp 的运行时和存储限制。在达到运行时限制时，vCloud vApp 不能再用。在达到存储限制时，vApp 将从 vCloud 中删除，或移至“过期项目”文件夹，具体取决于组织的租赁策略。

  vSphere vApp 将一直存在，直到用户将其手工删除。
- vCloud vApp 是根据模板创建的。vApp 模板是通过从 vCenter 服务器导入 VM 或导入 OVF 软件包创建的。vApp 是通过将模板部署到创建模板所在组织的云创建的。部署之后，可以将其他 VM 移至 vApp 中。

  vSphere vApp 是通过定义 vApp 以及所需 CPU 和内存资源限制创建的。然后，可以将定义 vApp 所在数据中心的 VM 移至 vApp 中。

vCenter 服务器作为 vCloud 的资源池提供者

您可以配置 vCenter 服务器的角色以作为 vCloud 的资源池提供者。在这种情况下，vCenter 服务器为 vCloud 提供计算和内存资源，以创建 VM。资源池以提供商 vDC 形式显示在 vCloud 中。

由于此配置，该资源池的 VM 显示在 vCenter 对象层次结构和 vCloud 对象层次结构中的“CA Virtual Assurance 浏览”窗格中。这类 VM 的“摘要”面板将在 vCloud 下显示与 vCenter 服务器下相同的信息：

- 性能图表
- 常规信息
- 概述（受监控资源的状态信息）
- CPU 和内存使用情况（仅在 vCenter 服务器中支持阈值配置）
- 磁盘使用量

可以应用于这些 VM 的操作集合在 vCloud 和 vCenter 服务器环境中都受到限制。受限制的操作集合会阻止 vCenter 和 vCloud 处于不同步状态。例如，当 vCenter 服务器下的 VM 的父 vApp 正在 vCloud 中运行时，您无法关闭该 VM 的电源。只能通过先在 vCloud 中关闭 vApp 的电源来关闭此类 VM 的电源。

有效的 VM 操作如下所示：

- 部署监控软件
- 管理自动化规则
- 配置服务器度量标准集合
- 配置阈值设置

如果在没有与 vCenter 服务器连接的情况下，在 vCloud 中创建 VM，则“摘要”窗格仅显示以下信息：

- 项目类型
- 名称
- 操作状态

vCloud 组织

vCloud 组织是一个用户、组和计算资源集合的管理单位。组织提供目录来存储 vApp 模板和媒体文件。组织成员可以使用目录中的 vApp 模板和媒体文件来创建自己的 vApp。

虚拟数据中心 (vDC) 向 vCloud 组织提供虚拟计算资源。您可以在虚拟数据中心中开通、运行和存储虚拟系统。一个 vCloud 组织可以具有多个虚拟数据中心。

从模板开通 vApp

在 vCloud 组织级别上，可以从存储在目录中的模板开通 vApp。

遵循这些步骤:

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 展开 VMware vCloud 文件夹。

   此时将显示 vCloud 文件夹结构。

4. 右键单击组织对象。

   此时将显示“开通”弹出式菜单。

5. 单击“从模板开通 vApp”。

   此时将显示“从模板开通新的 vApp”对话框。

6. 指定名称、vApp 模板、部署租赁以及存储租赁。单击“确定”。

   CA Virtual Assurance 将在组织中创建 vApp。

在 vCloud 中对 vApp 执行的操作

在 vCloud 组织级别上，可以从存储在目录中的模板开通 vApp。

遵循这些步骤:

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 展开 VMware vCloud 文件夹。

   此时将显示 vCloud 文件夹结构。

4. 右键单击 vApp 对象。

   此时将显示“管理”弹出式菜单。

5. 选择下列可用操作之一。

   打开 vApp

   打开 vCloud vApp。

   关闭 vApp

   关闭 vCloud vApp。

   重置 VApp

   重置 vCloud vApp。

   挂起 vApp

   挂起 vCloud vApp。

   恢复 vApp

   恢复 vCloud vApp。

克隆 vApp

从现有的 vApp 创建 vCloud vApp。

移动 vApp

将 vCloud vApp 移至另一个虚拟数据中心。

删除 vApp

删除 vCloud vApp。

修改 vApp 租赁

修改部署和存储租赁。

指定所需参数值，然后单击“确定”。

6. 单击“事件”以验证 vApp 的新状态。

此时将显示事件列表。

VMware vSphere 和 vCenter 服务器

CA Virtual Assurance 管理 VMware vSphere 和 vCenter 服务器虚拟环境。vCenter 服务器是 CA Virtual Assurance 和 vCenter AIM 用于访问 vSphere 环境的中心组件。SystemEDGE 和 vCenter AIM 在 CA Virtual Assurance 管理器服务器或任意 Windows 服务器上运行。

CA Virtual Assurance 为所有 VMware vCenter 服务器操作提供连接和操作支持。管理器负责管理连接、执行 VM 相关操作以及使用从 VMware vCenter 服务器检索到的数据填充数据库。开通服务执行 VMware vCenter 服务器操作，包括克隆、电源操作、资源和共享调整以及快照管理。

vCenter AIM 通过 Web 服务与一个或多个远程 vCenter 服务器实例进行通信。AIM 通过 SNMP 与管理器进行通信。如果提供多个 vCenter AIM 来管理 vCenter 服务器，您可以在配置期间指定首选的 vCenter AIM，或者可以让管理器自己选择。

注意：当您在 eHealth、Spectrum Infrastructure Manager 环境中，在没有 CA Virtual Assurance 管理器的情况下运行 vCenter AIM 时，AIM 将仅支持单实例模式。

受监控的 vSphere 和 vCenter 服务器资源

vCenter AIM 在 vSphere 环境中检测组件之间的逻辑和物理关系。AIM 提供整个虚拟化环境的视图，并管理以下资源类型和属性：

数据中心

*数据中心*用作主机、虚拟机、资源池或群集的容器。如果它们的虚拟配置符合特定部门的要求，则数据中心可以表示组织结构（如地理区域或单独的业务功能）。您也可以使用数据中心创建隔离的虚拟环境用于测试，或用于组织环境。

数据存储

*数据存储*指定数据中心中基础物理存储资源组合的虚拟表示。这些物理存储资源可由服务器上的本地磁盘、SAN 磁盘阵列等提供。

ESX 主机

代表运行 ESX 服务器的物理服务器上的所有计算和内存资源。

硬件传感器

提供 CPU、内存、风扇、电压、存储、温度以及电源方面的物理信息。可以通过 vCenter 服务器在 ESX 服务器中访问硬件传感器。

物理 NIC

指定 ESX 服务器上的物理以太网适配器。

资源池

*资源池*定义物理计算的分区和单个主机或群集的内存资源。您可以将任何资源池分割成更小的资源池，从而将资源分开并分配给具体的组或用于特殊目的。您也可以分层组织和嵌套资源池。

vApp

vApp 是一个特殊资源池，它将 VM 集合视为单个单元。vApp 使用开放虚拟化格式。*开放虚拟化格式 (OVF)* 是一种标准，用于指定和封装多层应用程序的所有组件以及与该应用程序关联的操作策略和服务级别。CA Virtual Assurance 可对 vApp 执行操作。针对 vApp 执行的操作将传播给 vApp 上的所有 VM。

vCenter 服务器

提供 vCenter 服务器计算机运行状况方面的信息。例如，关于 CPU、数据存储和内存使用情况的状态和数据。

虚拟磁盘

*虚拟磁盘*在虚拟来宾操作系统中定义磁盘驱动器。虚拟磁盘是位于本地主机或远程文件系统上的一个特定文件或一组文件。它在操作系统中的运行方式类似于物理磁盘驱动器。

虚拟机

指定可运行来宾操作系统和应用程序的虚拟化 x86 环境。在您创建虚拟机时，它将分配给特定主机、群集、资源池或数据存储。虚拟机在其物理主机上动态地消耗资源，和物理设备根据其工作负荷动态消耗能源的方式相同。

VMware 群集/高可用性/容错

通过 VMware vSphere，可以在 VM 上启用*容错 (FT)*，该虚拟机定义到配置用于高可用性 (HA) 的群集。容错会在群集中的其他 ESX 服务器上创建辅助 VM。辅助 VM 以锁步模式与正在执行工作负荷的主 VM 协同运行。如果发生故障，辅助 VM 将立即从故障点接管工作负荷执行。CA Virtual Assurance 发现和管理群集中的主 VM 和辅助 VM。

vNetwork 分布式交换机

将虚拟交换机的配置从主机提取到数据中心级别。vNetwork 分布式交换机作为单个虚拟交换机运行，该交换机跨数据中心中与其关联的所有主机。vNetwork 分布式交换机包含同样配置到标准交换机上的端口组的分布式端口组，但跨多个主机。这些属性可使虚拟机在多个主机之中迁移时维持一致的网络配置。

vNetwork 标准交换机

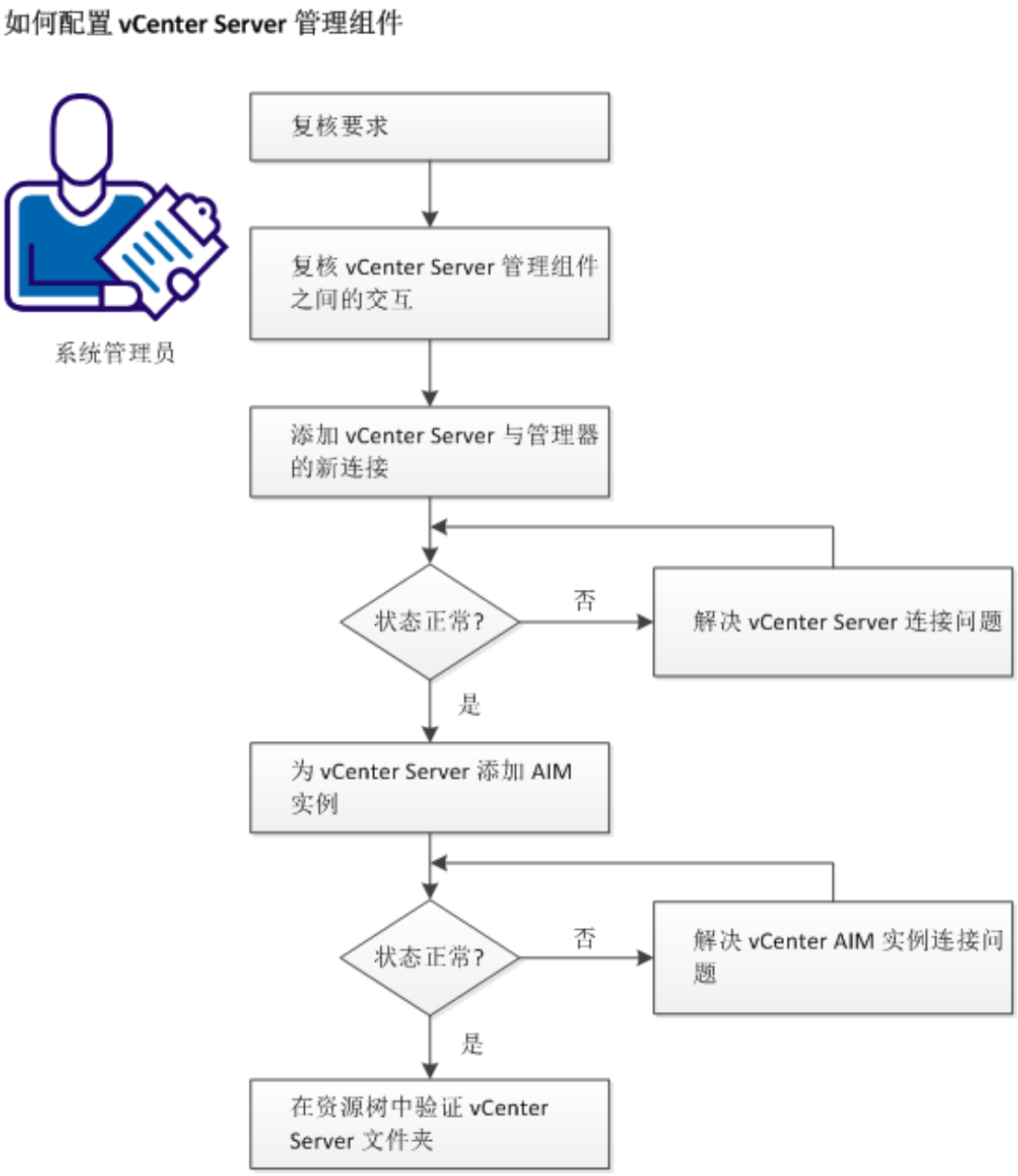
功能类似于物理交换机。每个 ESX 服务器均有自己的虚拟交换机，它们通过端口组连接到虚拟机。这些虚拟交换机还有指向 ESX 服务器上物理以太网适配器的上行链路连接。虚拟机通过连接到虚拟交换机上行链路的物理以太网适配器与外界进行通信。

虚拟 NIC

指定虚拟机上的虚拟以太网适配器。来宾操作系统通过设备驱动程序与虚拟以太网适配器（将虚拟以太网适配器看作物理以太网适配器）进行通信。虚拟以太网适配器有其自己的 MAC 地址、一个或多个 IP 地址，并响应标准以太网协议。

如何配置 vCenter 服务器管理组件

下图提供了有关所需操作的概述。该图包括针对连接问题的相应故障排除策略。



请执行以下步骤：

查看要求 (p. 468)
查看 vCenter 服务器管理组件之间的交互 (p. 469)
将新的 vCenter 服务器连接添加到管理器中 (p. 471)
排除 vCenter 服务器连接的故障 (p. 472)
添加 vCenter 服务器的 AIM 实例 (p. 475)
排除 vCenter AIM 实例连接的故障 (p. 476)
验证资源树中的 vCenter 服务器文件夹外观 (p. 480)

查看要求

在开始配置 CA Virtual Assurance 的 vCenter 服务器管理组件之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您对 CA Virtual Assurance、CA SystemEDGE 和 VMware vSphere 有基本了解。
- 您可以访问 CA Virtual Assurance 管理器安装，该安装包括 vCenter 平台管理模块 (PMM)、vCenter Application Insight Module (AIM) 和监控代理 (CA SystemEDGE)。
- 您可以访问 CA Virtual Assurance 用户界面。
- 您具有有效的凭据（用户名和密码），可用于访问要管理的新 vSphere 环境的 vCenter 服务器。
- 您已了解要使用哪个协议（HTTP 或 HTTPS）和端口来通过 Web 服务访问 vSphere 环境的 vCenter 服务器。默认值：HTTPS，端口 443
- 您已验证新的 vSphere 环境及其 vCenter 服务器是否在正常运行。
- 如果 VMware PMM 和 vCenter AIM 安装在不同的系统上，则已验证这些系统上的 SNMP 设置是否一致。读写团体字符串和 SNMP 端口号必须相同。
- 您已验证 CA Virtual Assurance 管理器是否已发现要使用的远程 vCenter AIM 服务器。

详细信息：

查看 vCenter 服务器管理组件之间的交互 (p. 469)
将新的 vCenter 服务器连接添加到管理器中 (p. 471)
添加 vCenter 服务器的 AIM 实例 (p. 475)
验证资源树中的 vCenter 服务器文件夹外观 (p. 480)

查看 vCenter 服务器管理组件之间的交互

作为系统管理员，您希望使用 CA Virtual Assurance 管理新的 VMware vSphere 环境。通过 CA Virtual Assurance，可以动态管理一个或多个 vSphere 环境的物理资源和虚拟资源。

vSphere 包括一个 vCenter 服务器、多个物理 ESXi 主机以及一个在 ESXi 主机上运行的虚拟基础架构。vCenter 服务器是带有整个虚拟基础架构的 vSphere 环境的中央控制点。该基础架构可以包括数据中心、群集、资源池、vApp、VM、虚拟设备和虚拟交换机。为了管理 vSphere，CA Virtual Assurance 需要其 vCenter 平台管理模块 (PMM)、vCenter Application Insight Module (AIM) 和 VMware vCenter 服务器之间的网络连接。要建立这些网络连接，请配置 CA Virtual Assurance vCenter 服务器管理组件（即 vCenter PMM 和 vCenter AIM）。

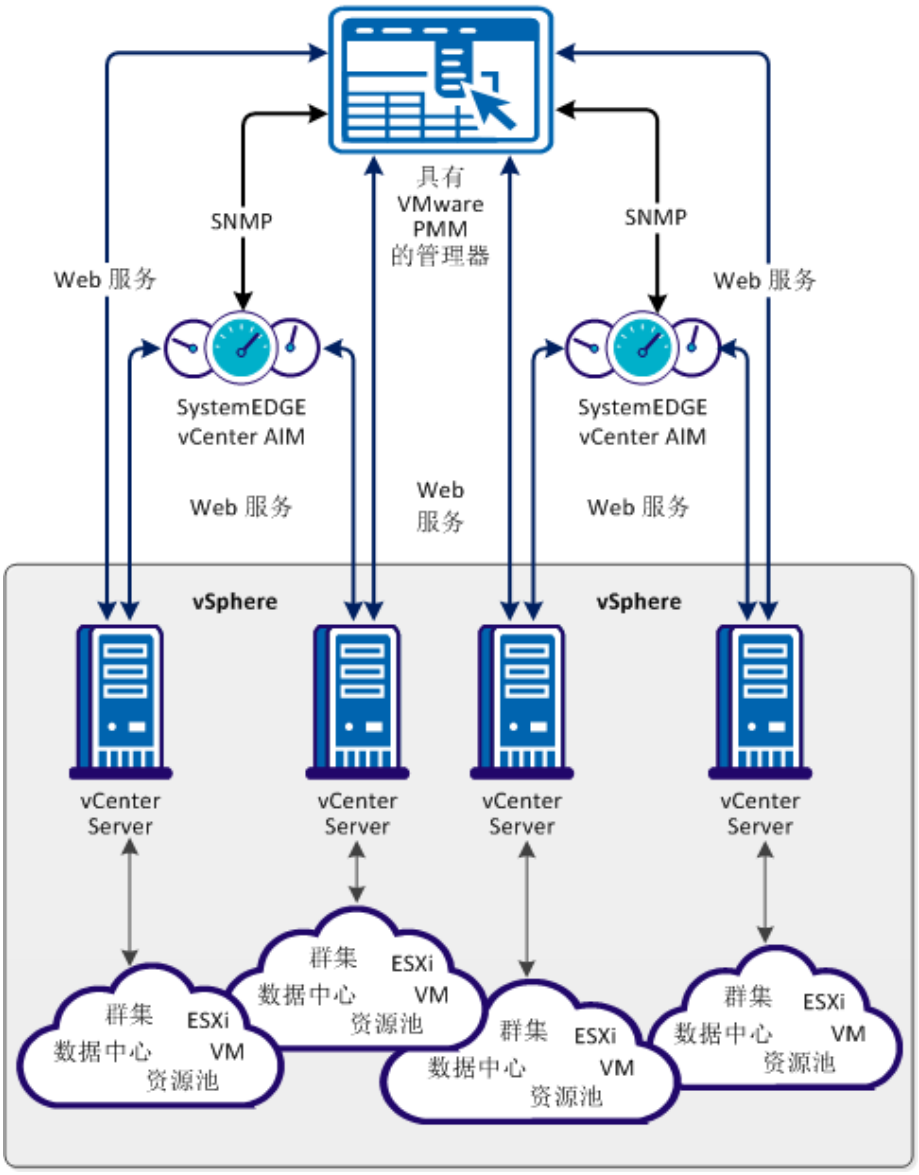
vCenter AIM 是扩展 SystemEDGE 的功能范围的 SystemEDGE 代理插件。vCenter AIM 使 SystemEDGE 能够监控多个 vSphere 环境的性能，并评估受监控的 vSphere 资源的状态。典型的受监控资源是虚拟 CPU、虚拟内存、虚拟交换机、虚拟磁盘、资源池、vApp 和其他虚拟资源。基于阈值，SystemEDGE 和 vCenter AIM 可确定受监控资源的状态，并使用 SNMP 将此信息传播到 CA Virtual Assurance 管理器。

vCenter PMM 是 CA Virtual Assurance 管理器的一个组件。PMM 负责使用 Web 服务为所有的 VMware vCenter 操作提供连接和支持。PMM 管理与 vCenter 服务器的连接，执行与 vSphere 相关的操作，从 vCenter AIM 检索数据，以及填充 CA Virtual Assurance 管理数据库。典型操作包括但不限于：创建、启动、停止或克隆 VM，添加或删除 CPU 份额，在 VM 正在运行时将内存添加到 VM。

由于 vCenter PMM 与 AIM 彼此进行交互，因此 CA Virtual Assurance 可以动态管理多个 vSphere 环境。CA Virtual Assurance 可以运行由阈值、状态和 AIM 收集的值自动控制的操作。例如，CA Virtual Assurance 可以根据 VM 的工作负荷动态添加或删除 CPU 份额。

下图显示了在由四个 vCenter 服务器表示的四个 vSphere 环境的示例环境中受影响组件的交互。通常，vCenter PMM 和具有多实例支持的每个 vCenter AIM 可以连接到多个 vCenter 服务器。图中所示的连接数量没有指定任何限制。所需的网络连接基于 TCP/IP、SNMP 和 Web 服务。

vCenter Server 管理组件之间的交互



在您成功配置 CA Virtual Assurance 组件后，CA Virtual Assurance 会发现新的 vSphere 环境。在成功发现之后，vSphere 环境的 vCenter 服务器及其虚拟基础架构将显示在 CA Virtual Assurance“浏览”窗格的“资源”树中。然后，您可以管理新的 vSphere 环境。

注意：VMware 工具可优化 VM 的虚拟化，建议在 VMware 环境中的每个 VM 上安装这些工具。对于没有安装 VMware 工具的 VM，该产品的一些功能将不可用或无法正常运行。因此，不支持没有安装 VMware 工具的 VM。

详细信息：

将新的 vCenter 服务器连接添加到管理器中 (p. 471)
添加 vCenter 服务器的 AIM 实例 (p. 475)
验证资源树中的 vCenter 服务器文件夹外观 (p. 480)

将新的 vCenter 服务器连接添加到管理器中

您可以使用 CA Virtual Assurance 用户界面的“管理”选项卡添加 vCenter 服务器连接。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“vCenter 服务器”。

   右侧窗格将刷新和显示受管的 vCenter 服务器、关联的 vCenter AIM 服务器以及 vCenter 服务器的 AIM 实例。

3. 在“vCenter 服务器”窗格工具栏上单击  （添加）。

   此时将显示“新建 vCenter 服务器”对话框。

4. 输入所需连接数据（服务器名称、用户、密码、协议、端口），指定首选 AIM，启用“受管状态”（复选框），然后单击“确定”。

   如果网络连接已成功建立，vCenter 服务器会添加到右上角的“vCenter 服务器”窗格并带有绿色状态图标。CA Virtual Assurance 自动发现 vCenter 服务器。

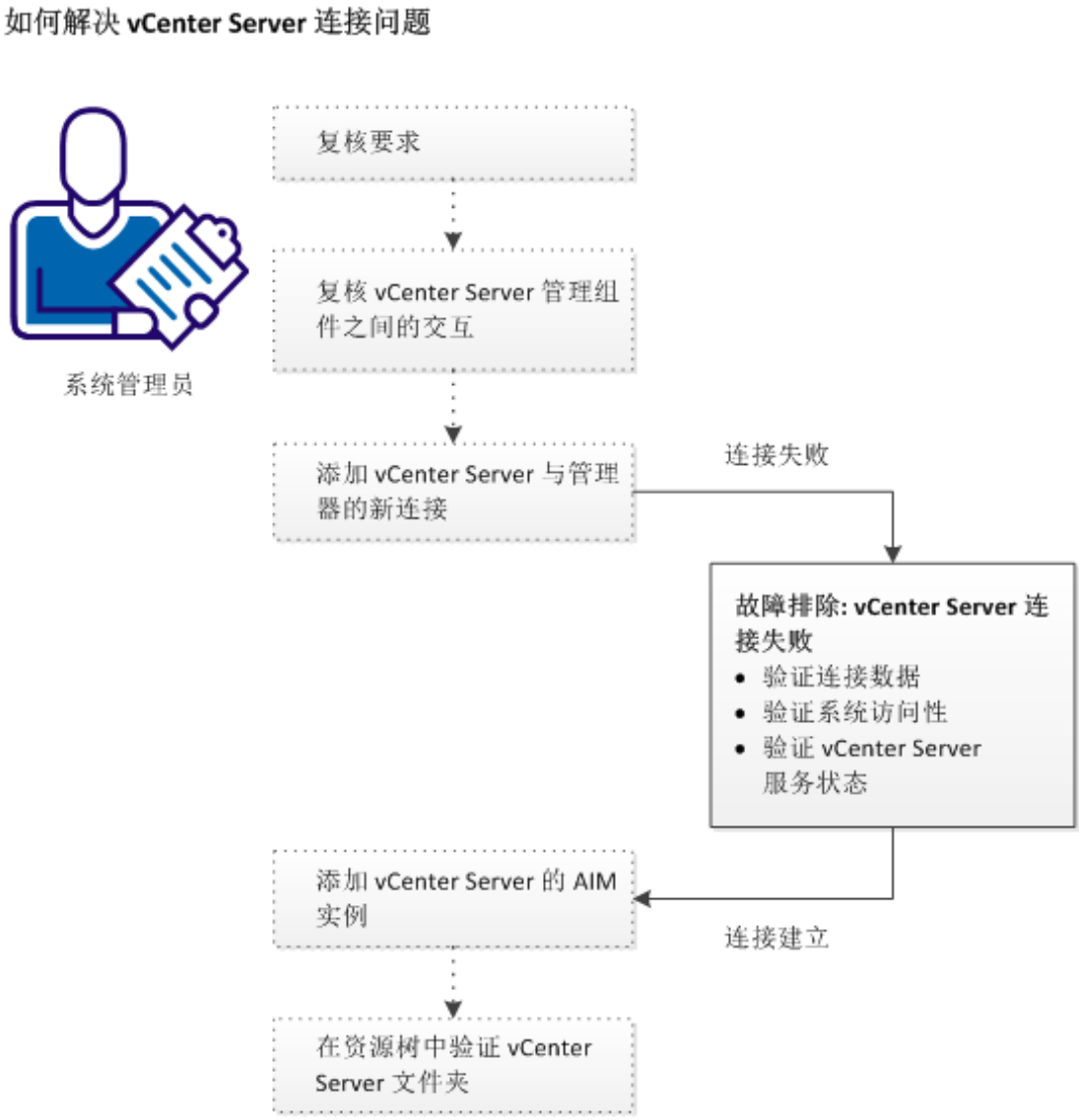
   如果连接失败，将显示“验证失败”对话框。如果您单击“是”，CA Virtual Assurance 会将 vCenter 服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。有关排除连接故障的信息，请参阅排除 vCenter 服务器连接的故障 (p. 472)。

详细信息：

添加 vCenter 服务器的 AIM 实例 (p. 475)
验证资源树中的 vCenter 服务器文件夹外观 (p. 480)
排除 vCenter 服务器连接的故障 (p. 472)

排除 vCenter 服务器连接的故障

vCenter 服务器连接已失败。遵循下图所示的故障排除信息：



请执行以下步骤：

vCenter 服务器连接失败 (p. 473)
添加 vCenter 服务器的 AIM 实例 (p. 475)
验证资源树中的 vCenter 服务器文件夹外观 (p. 480)

vCenter 服务器连接失败

症状：

在“管理”、“配置”下添加 vCenter 服务器连接之后，对 vCenter 服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的 vCenter 服务器连接数据（服务器名称、用户、密码、协议、端口）是否仍然有效。如有必要，请更新连接数据。
- 验证 vCenter 服务器系统是否正在运行并且可以访问。
- 验证 vCenter 服务器系统中的 VMware 管理服务是否正常运行。

更新 vCenter 服务器连接数据：

1. 单击与失败的连接关联的 （添加）或 （编辑）。

   此时将显示“新建 vCenter 服务器”或“编辑 vCenter 服务器”对话框。

2. 添加有效的服务器名称、用户、密码、协议和端口。启用“受管状态”，然后单击“确定”。

   将更新连接数据。

3. 单击右上角的 （验证）以验证新设置。

   如果无法建立与 vCenter 服务器的连接，请继续执行下一个步骤。

验证 vCenter 服务器系统是否正在运行并可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <vCenter Server Name>
   ping <IP Address of vCenter Server>
   ```

2. 验证命令的输出，以确定 vCenter 服务器是否具有有效的 DNS 条目和 IP 地址。

   如果 vCenter 服务器不在 DNS 中，将 vCenter 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果 vCenter 服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress <vCenter Server Name>
   ```

   输入正确的 IP 地址和 vCenter 服务器名称。例如：

   ```
   192.168.50.50 myvCenter
   ```

4. 单击右上角的（验证）。

   即使 vCenter 服务器凭据和连接数据正确并且您可以 ping vCenter 服务器，连接仍然可能失败。在这种情况下，可能是 vCenter 服务器引起该问题。如果无法建立与 vCenter 服务器的连接，请继续执行下一个步骤。

验证 vCenter 服务器系统中的 VMware 管理服务是否正常运行

1. 联系 vSphere 管理员来访问 vCenter 服务器系统。
2. 登录到 vCenter 服务器系统，从“开始”菜单中打开“管理工具”、“服务”。

   将打开“服务”窗口。

3. 选择服务 *VMware VirtualCenter Server*。启动或重新启动该服务。
4. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“vCenter 服务器”窗格，并单击右上角的（验证）。

   CA Virtual Assurance 将验证 vCenter 服务器连接。

   如果与 vCenter 服务器的连接失败，请验证根据该方案的要求收集的数据是否仍然有效。

   与 vSphere 管理员或 VMware 技术支持合作，解决 vCenter 服务器连接问题。

添加 vCenter 服务器的 AIM 实例

在将新的 vCenter 服务器连接添加到 CA Virtual Assurance 管理器中之后，添加 vCenter AIM 实例来管理新的 vCenter 服务器。然后，CA Virtual Assurance 发现整个 vSphere 环境及其所有物理组件和虚拟组件（如 vCenter 服务器、ESX 服务器、VM 和其他虚拟组件）。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“vCenter 服务器”。

   右侧窗格将刷新和显示受管的 vCenter 服务器、关联的 vCenter AIM 服务器以及受管 vCenter 服务器的 AIM 实例。

3. 在“vCenter AIM 服务器”窗格工具栏上单击 （添加）。

   此时将显示“新建 vCenter AIM 服务器”对话框。

4. 打开“vCenter AIM 服务器”下拉列表。

   此时将显示发现的 vCenter AIM 服务器的列表。如果您已在本地系统上安装了 vCenter AIM，本地系统的名称也会显示在列表中。

5. 从下拉列表中选择一个 vCenter AIM 服务器。

   CA Virtual Assurance 使用“vCenter 服务器”窗格中列出的 vCenter 服务器填充“vCenter 服务器”下拉列表。也就是说，您只能管理您的 CA Virtual Assurance 管理器为之建立了有效连接的那些 vCenter 服务器。

6. 选择要管理的 vCenter 服务器，然后单击“确定”。

   将添加选定的 vCenter 服务器的新 AIM 实例。如果实例未处于错误或已停止状态，CA Virtual Assurance 将开始发现关联的 vSphere 环境。发现过程完成后，您可以开始管理 vSphere 的虚拟资源和物理资源。

详细信息：

验证资源树中的 vCenter 服务器文件夹外观 (p. 480)
排除 vCenter AIM 实例连接的故障 (p. 476)

排除 vCenter AIM 实例连接的故障

vCenter AIM 连接处于未就绪状态。将显示下列状态图标之一：

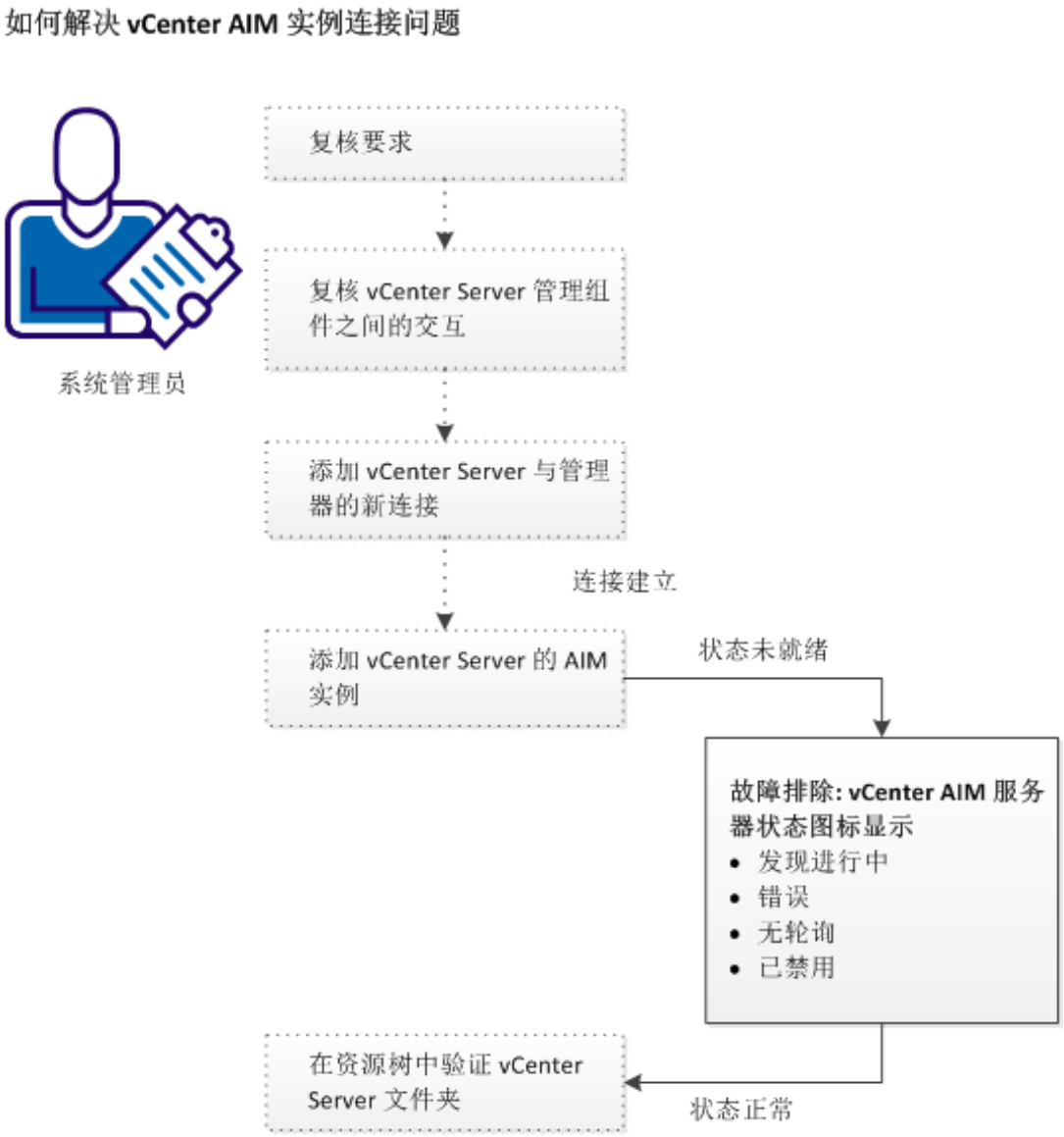
发现正在进行－等到平台管理器使所有数据同步。

错误－无法连接到 AIM。请检查网络配置。

无轮询－CA Virtual Assurance 管理器未轮询此 AIM 实例。

已禁用－该实例未受管理。

遵循下图所示的故障排除信息：



详细信息：

vCenter AIM 实例状态图标显示发现正在进行 (p. 477)
vCenter AIM 实例状态图标显示错误 (p. 477)
vCenter AIM 实例状态图标显示无轮询 (p. 479)
vCenter AIM 实例状态图标显示已禁用 (p. 479)

vCenter AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为 vCenter 服务器添加 vCenter AIM 实例之后，状态图标将显示  （发现正在进行）。

解决方案：

等到 vSphere 环境的发现过程完成。发现持续时间取决于与 vSphere 中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示用于指示未完成的发现请求数的工具提示。当发现作业完成时，CA Virtual Assurance 会将 vCenter 服务器文件夹添加到“资源”树。然后，您可以开始管理 vSphere 及其整个虚拟基础架构。

vCenter AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下为 vCenter 服务器添加 vCenter AIM 实例之后，状态图标将显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决导致与 vCenter AIM 的连接失败的最常见问题：

- 验证 vCenter AIM 服务器是否可以访问。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 vCenter AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 验证命令的输出，以确定 vCenter AIM 服务器是否具有有效的 DNS 条目和 IP 地址。

   如果 vCenter AIM 服务器未在 DNS 中，请将 vCenter AIM 服务器添加到 CA Virtual Assurance 管理器系统上的 Windows 主机文件中。继续执行步骤 3。

   如果 vCenter 服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress servername
   ```

   输入正确的 IP 地址和 vCenter AIM 服务器名称。例如：

   ```
   192.168.50.51 myvCenterAIM
   ```

4. 在“vCenter AIM 服务器”窗格的右上角，单击 （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 vCenter AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“vCenter AIM 服务器”窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证 vCenter AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否仍然有效。

vCenter AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下为 vCenter 服务器添加 vCenter AIM 实例之后，状态图标将显示  （无轮询）。

解决方案：

关联实例不需要特定的操作。此图标通知您 CA Virtual Assurance 管理器未轮询此 AIM。AIM 不是首选。

如果将多个 AIM 配置为管理特定 vCenter 服务器，则 PMM 会选择 AIM 之一作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

vCenter AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 vCenter AIM 实例之后，几个实例的状态图标将显示  （已禁用）。该 vCenter AIM 实例未受管理。

如果 CA Virtual Assurance 已发现具有以下关系的 vCenter AIM，则会显示此状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的 vCenter 服务器配置了 vCenter AIM。
- AIM 已连接到未在“vCenter 服务器”窗格中配置的 vCenter 服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的 vCenter 服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的 vCenter 服务器连接并将其受管状态更改为已启用。

vCenter AIM 实例状态图标显示多个实例

症状：

在“管理”、“配置”下为 vCenter 服务器添加 vCenter AIM 实例后，状态图标显示 （多个 AIM 管理该实例）。

解决方案：

验证 CA Virtual Assurance 管理器是否仅用一个 vCenter AIM 实例来管理每个 vCenter 服务器。如果 CA Virtual Assurance 管理器通过多个 AIM 实例来管理 vCenter 服务器，则会发生管理问题。CA Virtual Assurance 将停止监控关联的 vCenter 服务器。

决定您要使用哪个 AIM 实例来管理 vCenter 服务器，并从“vCenter AIM 服务器”窗格中删除其他实例。

遵循这些步骤:

1. 选择要删除的 AIM 实例，然后单击 （删除）。

   此时将显示“删除项目”对话框。

2. 单击“是”。

   对其他多个实例重复这些步骤，直到在管理器与 AIM 实例之间建立唯一关系。

验证资源树中的 vCenter 服务器文件夹外观

在成功配置和发现之后，新的 vCenter 服务器将在“资源浏览”窗格的 VMware vCenter 服务器文件夹之下列出。

遵循这些步骤:

1. 单击“资源”、“浏览”。

   此时将显示“资源”树。

2. 展开 VMware vCenter 服务器。

   将显示受管的 vCenter 服务器。

3. 展开新的 vCenter 服务器条目。

   将显示受管的 vSphere 基础架构：VMware 数据中心、ESX 服务器、资源池、VM...

CA Virtual Assurance 现在可以用于管理添加的 vSphere 环境及其虚拟基础架构。

vCenter 服务器的用户范围身份验证

通过向位于 *Install_Path**productname*\conf 目录中的 caaipconf.cfg 文件添加配置条目，可为 vCenter 服务器环境启用用户范围的身份验证。因为安装后该条目不存在，所以默认情况下会禁用用户范围的身份验证。在此情况下，CA Virtual Assurance 会使用在 vCenter 服务器配置窗格中的“管理”下指定的用户进行 vCenter 服务器身份验证。

相比之下，启用用户范围的身份验证后，将使用当前登录的用户（用户界面）来验证 vCenter 服务器环境操作。用户范围的身份验证意味着在 vCenter 服务器中指定适当的用户及其权限。还必须在 CA EEM 中指定相同用户，才能登录 CA Virtual Assurance 用户界面。

启用用户范围身份验证

1. 在 vCenter 服务器中指定必需的用户及其权限（管理员或只读）。
2. 在 CA EEM 中指定相同用户。
3. 转到 CA Virtual Assurance 管理器服务器并导航到 *Install_Path**productname*\conf 目录。
4. 使用文本编辑器打开 caaipconf.cfg 文件并将以下条目添加到 AIP product 部分：

```
<property name="USER_SCOPED_AUTHENTICATION">
    <value>VC</value>
    <displayName>vCenter PMM 组件使用当前登录的用户来验证 vCenter 服务器平台操作。
</displayName>
</property>
```

   结果：

```
<properties targetNamespace="http://www.ca.com/cfg/types/2008/05">
    <product name="AIP">
       ...
       <property name="USER_SCOPED_AUTHENTICATION">
          <value>VC</value>
          <displayName>vCenter PMM 组件使用当前登录的用户来验证 vCenter 服务器
平台操作。</displayName>
       </property>
       ...
    </product>
    ...
```

5. 保存文件。

   CA Virtual Assurance 会自动检测更改。

6. 验证当前登录的用户在 CA Virtual Assurance 中是否拥有与 vCenter 服务器中指定的用于管理 VMware 环境的相同权限。

注意：如果要禁用用户范围身份验证，请从 caaipconf.cfg 文件中删除该条目。

示例

初始方案：在 CA Virtual Assurance 安装期间，用户 *CA* 已经配置为在 CA Virtual Assurance 用户界面中登录。在 vCenter 服务器上，*管理员*是具有管理员权限的用户。CA Virtual Assurance 配置为使用*管理员*验证 vCenter 服务器环境操作（请参阅用户界面中“vCenter 服务器配置”页面中的“管理”选项卡）。默认情况下会禁用用户范围身份验证。

该方案符合完全安装和适当的 vCenter 服务器配置。

假设满足以下条件：

- 在 vCenter 服务器上配置了另外两个用户：*超级用户*（管理员）和*读者*（只读权限）
- *超级用户*和*读者*添加到了 CA EEM 中
- 启用了用户范围身份验证

在您作为*超级用户*登录 CA Virtual Assurance 时，您将具有管理 vCenter 服务器的管理员权限。

在您作为*读者*登录 CA Virtual Assurance 时，您将仅具有监控 vCenter 服务器的只读权限。

当您禁用用户范围身份验证时，登录 CA Virtual Assurance 的每个人都具有 vCenter 服务器管理员权限。如果禁用了用户范围身份验证，CA Virtual Assurance 将使用*管理员*在用户界面的“vCenter 服务器配置”窗格中的“管理”选项卡下指定的用户（另请参阅本示例的初始方案）。

针对 VM 的设备管理

设备管理包括以下内容：

- 添加和删除 vDisk
- 添加和删除 vNIC

添加或删除虚拟磁盘

可以从 VM 动态添加或删除虚拟磁盘。可以添加以下磁盘：

- 来自相同或其它数据存储的新磁盘
- 数据存储的现有磁盘
- 从其它数据存储添加现有磁盘

添加虚拟磁盘

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 在“浏览”窗格中找到并右键单击虚拟机，或单击“快速启动”选项卡，然后选择“添加新磁盘”。

   此时将显示“添加新磁盘”对话框。

4. 根据需要输入新磁盘详细信息

   将出现一条消息提示您确认。

5. 单击“确定”。

   将出现一条信息，确认新磁盘已添加。

删除虚拟磁盘

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 在“浏览”窗格中找到并右键单击虚拟机，或单击“快速启动”选项卡，然后选择“删除磁盘”。

   此时将显示“删除磁盘”对话框。

4. 选择硬盘及是否删除数据。

   将出现一条消息提示您确认。

5. 单击“确定”。

   将出现一条信息，确认新磁盘已删除。

添加或删除虚拟网络接口

可以动态地从现有 VM 添加或删除虚拟网络接口。

添加虚拟网络接口

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 在“浏览”窗格中找到并右键单击虚拟机，或单击“快速启动”选项卡，然后选择“添加新虚拟网络接口”。

   此时将显示“添加新虚拟网络接口”对话框。

4. 输入新网络接口详细信息。

   将出现一条消息提示您确认。

5. 单击“确定”。

   将出现一条信息，确认新卡已添加。

删除虚拟网络接口

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 在“浏览”窗格中找到并右键单击虚拟机，或单击“快速启动”选项卡，然后选择“删除虚拟网络接口”。

   此时将显示“删除新虚拟网络接口”对话框。

4. 选择要删除的 NIC。

   将出现一条消息提示您确认。

5. 单击“确定”。

   将出现一条信息，确认网络接口已删除。

虚拟机的容错

通过 VMware vSphere，可以在 VM 上启用*容错 (FT)*，该虚拟机定义到配置用于高可用性 (HA) 的群集。容错会在群集中的其他 ESX 服务器上创建辅助 VM。辅助 VM 以锁步模式与正在执行工作负荷的主 VM 协同运行。如果发生故障，辅助 VM 将立即从故障点接管工作负荷执行。CA Virtual Assurance 发现和管理群集中的主 VM 和辅助 VM。

对于 VM 管理，CA Virtual Assurance 将主 VM 和辅助 VM 看作单个 VM，且启用容错并显示其容错属性。主 VM 出现在左侧窗格（第一个类对象）上，并在右侧窗格中显示其 FT 属性。辅助 VM 属性（第二个类对象）仅列在右侧窗格。不能在辅助 VM 上执行 VM 操作，如启动、停止或克隆。

“常规信息”面板中呈现的 VM 数取决于正在运行的非 FT VM 和主 FT VM 之和。VM 总体计数中不包括辅助 FT VM。

CA Virtual Assurance 收集环境中各级 FT VM 数据。

容错要求

VM 启用容错时，必须禁用以下操作：

- 克隆 VM
- 从清单中删除（取消注册）
- 快照
- 转换为模板

虚拟机的容错属性

对各个 VM，CA Virtual Assurance 显示如下内容：

容错状态

表示 VM 的容错状态。

未容错

表示 VM 未启用容错。

保护

表示 VM 已启用容错并受保护。

未受保护（正在启动）

表示正在启动容错，但是 VM 不受保护。

未受保护（需要辅助 VM）

表示已启用容错但需要辅助 VM。

未受保护（已禁用）

表示已禁用容错，并且 VM 不受保护。

未受保护（VM 未运行）

表示已启用容错，但 VM 未运行。

辅助 VM 的位置

标识辅助主机的位置。

ESX 主机容错属性

ESX 主机容错属性如下所示：

容错

标识主机是否启用容错。

容错版本

标识主机上运行的容错版本。

注意：仅具有同一容错版本的主机才相互兼容。

主 VM 总数（根据 AIM 进行计算）

表示配置给该主机的主 VM 总数。

辅助 VM 总数（根据 AIM 进行计算）

表示配置给该主机的辅助 VM 总数。

已打开的主 VM（根据 AIM 进行计算）

表示在该主机上运行（已打开）的主 VM 总数。

已打开的辅助 VM（根据 AIM 进行计算）

表示在该主机上运行（已打开）的辅助 VM 总数。

监控容错

通过 VMware vSphere，可以在 VM 上启用*容错 (FT)*，该虚拟机定义到配置用于高可用性 (HA) 的群集。容错会在群集中的其他 ESX 服务器上创建辅助 VM。辅助 VM 以锁步模式与正在执行工作负荷的主 VM 协同运行。如果发生故障，辅助 VM 将立即从故障点接管工作负荷执行。CA Virtual Assurance 发现和管理群集中的主 VM 和辅助 VM。

监控容错属性

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 展开 VMware vCenter 服务器文件夹和 ESX 服务器对象。

   此时将出现 VM 列表。

4. （可选）选择 ESX 主机。

   以下 FT 属性将显示在“摘要”选项卡中：

   容错

   标识主机是否启用容错。

   容错版本

   标识主机上运行的容错版本。

   注意：仅具有同一容错版本的主机才相互兼容。

   主 VM 总数

   表示配置给该主机的主 VM 总数。

   辅助 VM 总数

   表示配置给该主机的辅助 VM 总数。

   已打开的主 VM 数

   表示在该主机上运行（已打开）的主 VM 总数。

   已打开的辅助 VM 数

   表示在该主机上运行（已打开）的辅助 VM 总数。

5. （可选）选择 VM。

以下 FT 属性将显示在“摘要”选项卡中。

容错状态。

表示 VM 的容错状态。

未容错

表示 VM 未启用容错。

保护

表示 VM 已启用容错并受保护。

未受保护（正在启动）

表示正在启动容错，但是 VM 不受保护。

未受保护（需要辅助 VM）

表示已启用容错但需要辅助 VM。

未受保护（已禁用）

表示已禁用容错，并且 VM 不受保护。

未受保护（VM 未运行）

表示已启用容错，但 VM 未运行。

辅助 VM 的位置

标识辅助主机的位置。

管理容错

您可以控制 VM 的容错属性。

管理 VM 的容错属性

1. 在“浏览”窗格中选择 VM。

   “常规信息”窗格将显示在右侧，并显示 VM 的容错状态。

2. 右键单击该 VM，选择“管理”，然后从下拉菜单中选择一个操作。管理容错的可用操作如下：

   - 关闭容错
   - 启用容错
   - 禁用容错
   - 迁移辅助 VM

3. 为选定操作提供信息或确认。

   此时将显示确认消息。

VM 的热插拔支持

CA Virtual Assurance 检测是否为 VM 启用热插拔选项。CA Virtual Assurance 支持启用热插拔的 VM 在开机时做出以下调整。

- 添加 vCPU
- 添加 vRAM

注意：有关如何启用或禁用热插拔选项，请参阅*《VMware vSphere 虚拟机管理指南》*。

动态添加或删除 vCPU

可以动态地向已开通的 VM 添加或删除 CPU。如果 VM 支持热插拔，则可在运行时动态添加 vCPU。

CA Virtual Assurance 将验证以下 VM 属性：

- ESX 许可证（ESX 级别）
- 支持的最大 vCPU 数（ESX 级别）
- 启用热插拔（VM 级别）

示例

- 如果 ESX 许可证允许 8 个 CPU (Enterprise Plus) 且支持的最大 vCPU 数为 8 且热插拔被启用，则可添加的 CPU 数量为：1、2、4、8。
- 如果 ESX 许可证允许 8 个 CPU (Enterprise Plus) 且支持的最大 vCPU 数为 8 且热插拔被启用，则可添加的 CPU 数量为：1、2、3、4、5、6、7、8。

添加 vCPU

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 在“浏览”窗格中找到并右键单击虚拟机，或单击“快速启动”选项卡，然后选择“添加/删除 vCPU”。

   将出现“修改 vCPU”对话框。

4. 根据需要调整 CPU 数量。

   将出现一条消息提示您确认。

5. 单击“确定”。

   将出现一条确认修改的消息。

   注意：要删除 vCPU，虚拟机必须处于关闭状态。

动态添加或删除内存

可以动态地向已开通的 VM 添加或删除内存。如果 VM 支持热插拔，则可在运行时动态添加内存。

添加内存

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 在“浏览”窗格中找到并右键单击虚拟机，或单击“快速启动”选项卡，然后选择“添加/删除内存”。

   将显示“修改虚拟内存”对话框。

4. 根据需求调整内存。

   将出现一条消息提示您确认。

5. 单击“确定”。

   将出现一条确认修改的消息。

   注意：要删除内存，VM 必须处于关闭状态.

虚拟机中的逻辑卷

CA Virtual Assurance 支持管理虚拟磁盘中的逻辑卷。例如，您可以管理 VM 中的 C: 驱动器。

资源分配

如果可用的资源容量不满足资源使用者的需求，则自定义虚拟机、vApp 和资源池的资源数量。

使用份额、保留和限制的设置，以确定向虚拟机、资源池或 vApp 提供的 CPU 和内存资源量。

资源分配份额

份额指定虚拟机、资源池或 vApp 相对于其同级的相对优先级或重要性。如果某台虚拟机具有的份额是另一台竞争虚拟机的两倍，则它可以消耗两倍该资源。

份额通常指定为自然数。您可以使用默认值，或为每台虚拟机分配特定数目的份额（比例权重）。

指定份额仅对同级虚拟机、vApp 或资源池有意义。同级虚拟机或资源池在层次结构中有相同父对象。同级根据它们的相对份额值（受保留和限制约束）共享资源。将份额分配给虚拟机时，始终为该虚拟机指定相对于其他已打开电源的虚拟机的优先级。

例如，发生竞争时，具有 2000 份额的虚拟机接收的 CPU 时间多于具有 1000 份额的虚拟机。份额相对于其他份额进行配置；因此，仅与份额的比例有关，而不是份额的值。份额值为 1000、2000、3000 的三个虚拟机与份额值为 1、2、3 的三个虚拟机作用相同。可以使用您喜欢的任何编号方案。如果在编号之间留下大量空间，您今后可以更容易地将资源添加到资源池中。

如果资源之间没有竞争，则份额不会影响虚拟机的操作。指定份额将帮助您平衡资源池或 vApp。

资源分配保留

保留为虚拟机、资源池或 vApp 指定保证的最小 CPU 或内存分配。仅当有足够的未保留资源可供虚拟机使用时，vSphere 才允许您打开虚拟机的电源。即使物理服务器负载过重时，服务器也能保证保留资源的数量。保留以 MHz 或 MB 定义。

例如，假设您有 2 GHz CPU 可用。然后为 VM1 指定 1000 MHz 的保留，为 VM2 指定 1000 MHz 的保留。现在，如有必要，保证每台虚拟机可获得 1 GHz。但是，如果 VM1 仅使用 500MHz，则 VM2 可以使用 1.5 GHz。

保留的默认值为 0。您可以指定保留，以保证始终有所需的最小 CPU 或内存量可供虚拟机使用。

资源分配限制

限制为虚拟机、资源池或 vApp 指定最大 CPU 或内存分配量。服务器可以向虚拟机分配大于保留的量，但是不能分配大于限制的量。在系统上不会分配超出限制的未使用 CPU 或内存。限制以 MHz 或 MB 定义。

CPU 和内存限制默认值设置为没有限制。如果内存限制设置为没有限制，vSphere 将在创建虚拟机时有效地确定内存量。通常，不需要指定限制。

资源分配最佳实践

指定适合于您的 ESX/ESXi 环境的资源分配设置（份额、保留和限制）。

下列准则可以帮助您的虚拟基础架构实现更佳的性能。

- 如果您希望频繁更改可用资源总量，请使用份额来跨虚拟机分配资源。如果使用份额，之后升级主机，份额数不会变化。例如，即使每个份额表示更大的 CPU 或内存量，每台虚拟机也保持同样的优先级。
- 使用保留来指定可接受的*最小* CPU 或内存量，而非您希望的可用量。主机基于虚拟机的份额数、估计的需求以及限制，分配额外的资源作为可用资源。当您修改环境时（如通过添加或删除虚拟机），由保留指定的资源数量不会更改。
- 为虚拟机指定保留时，请勿分配所有资源。计划将相应部分留作未保留，因为在要保留的容量接近所有系统容量时，更改保留和资源池层次结构会越来越困难。
- 有关其他详细信息，请参阅位于 www.vmware.com 的 vSphere 文档。

编辑 VM CPU 和内存分配

您可以编辑分配给虚拟机的 CPU 数目和内存份额，以调节其分得的资源。添加资源时，适当数量的未分配内存或 CPU 份额必须可用，以使操作成功。如果允许的内存或 CPU 份额存在最大值和最小值，则任何资源分配变更都必须在此限制范围内。

您还可以为特定 VM 资源分配操作创建并排定策略。

编辑 VM CPU 和内存分配

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“配置”、“资源分配”。

   此时出现“资源分配”部分。

3. 调节分配给该虚拟机的 CPU 和内存份额数量，然后为编辑的每个数值单击“保存”。

   即会出现一条确认消息。

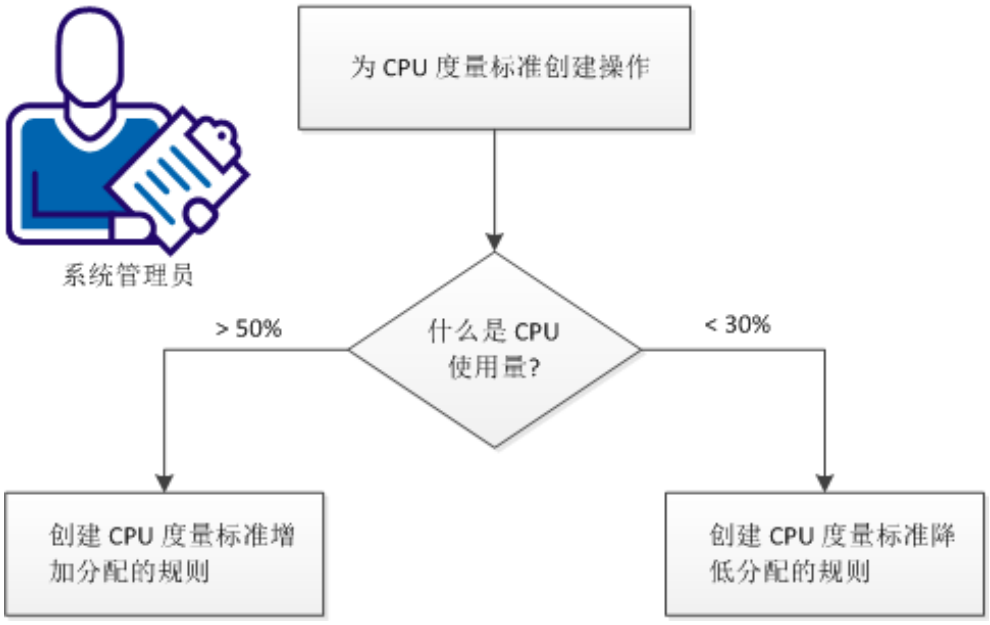
如何使用策略操作来标识性能问题

该方案提供有关系统管理员如何标识和动态解决性能问题的信息。此信息用于帮助系统管理员优化受管 vCenter 环境的资源份额分配。

策略操作标识 VM 资源和动态调整 CPU 份额的分配。*份额*确定了在 VM 竞争资源时，哪个 VM 将获取资源。使用份额可允许动态分配 CPU 资源。每个 VM 都分配有指定的份额数。根据 ESX Server 主机上 CPU 资源的当前使用率动态更改该分配。

如果任何 VM 的 CPU 使用率超过 50%，则 CPU 份额的分配会动态增加。如果 CPU 使用率小于 30%，则 CPU 份额分配会动态减少。策略组件不仅标识有问题的虚拟机，而且确保保持业务连续性的动态操作。使用策略操作可确保在需要虚拟机时对其分配资源，而在不需要虚拟机时取消分配。

如何使用策略操作识别性能问题



要使用策略操作标识和解决性能问题，请执行以下步骤：

1. 创建 CPU 度量标准的操作。 (p. 495)
2. 如果 CPU 使用率大于 50%，请创建用于增加分配的 CPU 度量标准规则 (p. 496)。
3. 如果 CPU 使用率小于 30%，请创建用于减少分配的 CPU 度量标准规则 (p. 496)。

创建 CPU 度量标准的操作

策略提供可用于为系统的自动化管理创建策略的规则和操作的创建。可以为未包括在默认库中的操作创建自定义操作。

遵循这些步骤:

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 依次单击“策略”、“操作”。

   将出现“操作”页面。

4. 单击右上方侧栏中的“+”添加新操作。
5. 输入操作的名称。
6. 从“类别”下拉列表中选择“资源配置”。
7. 从“类型”下拉列表中选择“配置份额”。
8. 在“VC 服务器”字段中，将条目保留为“%VCServer%”，以在跨任何 VC 服务器的任何 VM 上应用该操作。
9. 在“VC 数据中心”字段中，将条目保留为“%DATACENTER%”。
10. 在“目标 VM 计算机”字段中，将条目保留为“%VMNAME%”。
11. 从“操作”下拉列表中选择“设置 CPU”，然后输入值 10000。

    该数目是任意数目，且份额值设置为正常值。

    注意：使用更大或更小数目可相应地增加和减少份额分配。

12. 如果更改需要核准，请启用“帮助台核准”。

    创建该操作之后，事件控制台中将显示一条消息。

    CAAP4521 策略：操作 <action name> 已创建。

创建用于增加分配的 CPU 度量标准规则

创建用于增加分配的 CPU 度量标准规则可以在使用率超过阈值时确保动态资源分配。

遵循这些步骤:

1. 依次单击“资源”选项卡、“策略”、“规则”。
2. 单击右上边栏上的“+”来添加规则。
3. 输入规则的名称，然后单击“下一步”。
4. 从该规则的“操作选择”列表中选择操作，然后单击“下一步”。
5. 输入基于度量标准的规则（其中 CPU 使用率大于 50%）来增加 VM 的 CPU 份额。

创建用于减少分配的 CPU 度量标准规则

创建用于减少分配的 CPU 度量标准规则。在 CPU 使用率低于 30% 时，此规则将减少 CPU 份额。

遵循这些步骤:

1. 依次单击“资源”选项卡、“策略”、“规则”。
2. 单击右上边栏上的“+”来添加规则。
3. 输入规则的名称，然后单击“下一步”。
4. 从该规则的“操作选择”列表中选择操作，然后单击“下一步”。
5. 输入基于规则的度量标准（其中 CPU 使用率小于 30%）来减少 VM 的 CPU 份额。

vApp 支持

vApp 是一个特殊资源池，它将 VM 集合视为单个单元。vApp 使用开放虚拟化格式。*开放虚拟化格式 (OVF)* 是一种标准，用于指定和封装多层应用程序的所有组件以及与该应用程序关联的操作策略和服务级别。CA Virtual Assurance 可对 vApp 执行操作。针对 vApp 执行的操作将传播给 vApp 上的所有 VM。

您可以将任何 vApp 分割成更小的 vApp，从而将资源分开并分配给特定的组或用于特定目的。您可以将资源（如 VM、资源池或 vApp）添加到现有 vApp 中。您也可以分层组织和嵌套 vApp。

vApp 在主机和群集级别上表示。

CA Virtual Assurance 支持在 vApp 级别上执行以下管理操作：

- 发现
  - 服务器
  - 网络
  - vCenter 服务器
- 捕获服务
- 添加资源
- 克隆 vApp
- 打开 vApp
- 关闭 vApp
- 挂起 vApp
- 从 VMware vCenter 删除
- 从 VMware vCenter 取消注册
- 编辑排序

CA Virtual Assurance 支持对 vApp 执行以下开通操作：

- 开通 VMware VM
- 开通 VMware vApp

开通 VMware vApp

可以直接在 ESX 主机或群集级别上创建 vApp，也可以将其创建为现有资源池或 vApp 的一部分。

遵循这些步骤:

1. 从“浏览”窗格的主机或群集级别中，右键单击 ESX 主机或群集。

   此时将打开弹出式菜单。

2. 选择“开通”、“开通 VMware vApp”。

   此时将显示“创建新 vApp”对话框。

3. 指定下列字段，然后单击“确定”。

   名称

   标识 vApp。

   CPU 份额

   指定此 vApp 相对于父主机、资源池或 vApp 的总 CPU 资源分配的 CPU 份额。同级 vApp 根据它们的相对份额值（受保留和限制约束）共享资源。指定表示适当比例权重的份额数。

   例如，假定主机上安装有 vApp1 和 vApp2，并且每个均具有 1000 份 CPU 份额。权重相等，每个 vApp 均可以分配父主机 CPU 时间的 50%。但是，如果 vApp1 有 2000 份 CPU 份额，而 vApp2 有 1000 份，则权重不相等。总份额数为 3000 份，1000 份代表 33.3%，而 2000 份代表 66.6%。因此，vApp2 可以分配 66.6% 的 CPU 时间，而 vApp1 可以分配 33.3% 的 CPU 时间。

   CPU 保留

   为该 vApp 指定保证的 CPU 分配。

   CPU 无限

   禁用 CPU 限制设置。实际限制现已设置为可用的物理资源。

   CPU 限制

   为该 vApp 指定 CPU 分配的上限。通常可以接受默认值。

   内存份额

   指定此 vApp 相对于父资源池或 vApp 的总内存资源分配的内存份额。同级 vApp 根据它们的相对份额值（受保留和限制约束）共享资源。指定表示适当比例权重的份额数。

例如，假定主机上安装有 vApp1 和 vApp2，并且每个均具有 1000 份内存份额。权重相等，每个 vApp 均可以分配父主机内存的 50%。但是，如果 vApp1 有 2000 份内存份额，而 vApp2 有 1000 份，则权重不相等。总份额数为 3000 份，1000 份代表 33.3%，而 2000 份代表 66.6%。因此，vApp2 可以分配 66.6% 的内存，而 vApp1 可以分配 33.3% 的内存。

内存保留

为该 vApp 指定保证的内存分配。

内存无限

禁用内存限制设置。实际限制现已设置为可用的物理资源。

内存限制

为该 vApp 指定内存分配的上限。通常可以接受默认值。

此时新的 vApp 将显示在“浏览”窗格中。

克隆 vApp

可以克隆 vApp，其过程类似于克隆虚拟机。

遵循这些步骤:

1. 从“浏览”窗格的主机或群集级别中，选择要克隆的 vApp。
2. 右键单击 vApp。

   此时将打开弹出式菜单。
3. 依次选择“管理”、“克隆 vApp”。

   此时将显示“克隆 vApp”对话框。
4. 指定下列字段，然后单击“确定”。

   名称

   标识克隆的 vApp。

   位置

   指定适当的位置。展开在弹出式菜单上显示的对象并选择位置。

   数据存储

   从下拉菜单中指定合适的数据存储。

   此时克隆的 vApp 将显示在“浏览”窗格中。

更多 vApp 操作

CA Virtual Assurance 还支持对 vApp 执行以下操作：

- 打开电源
- 关闭电源
- 挂起
- 从 VMware vCenter 删除
- 从 VMware vCenter 取消注册

遵循这些步骤：

1. 从“浏览”窗格的主机或群集级别中，选择相应的 vApp。
2. 右键单击 vApp。

   此时将打开弹出式菜单。
3. 选择“管理”，然后单击所需的操作。

   这时将会出现确认对话框。
4. 单击“确定”。

   CA Virtual Assurance 执行选定的操作。

通过事件监控 vApp

您可以通过下列事件监控 vApp：

- 添加 vApp：

  将 vApp *MyvApp* 添加到父资源池资源。vSphere *vcserver.mycomp.com*
- 删除 vApp：

  从父资源池资源中删除 vApp *MyvApp*。vSphere，vcserver.mycomp.com

可用陷阱如下：

- ResPoolvAppAddedTrap：将 vApp 添加到资源池或 vApp。
- ResPoolvAppRemovedTrap：从资源池或 vApp 中删除 vApp。
- ResPoolvAppVCConfigChangeTrap：vApp 中的 vApp 实体配置数据已更改。
- VMAddedTovAppTrap：VM 已添加到 vApp。
- VMRemovedFromvAppTrap：VM 已从 vApp 删除。
- VMvAppVCConfigChangeTrap：vApp 中的 VM 实体配置数据已更改

通过事件监控 vApp

1. 单击“显示板”选项卡，滚动到“事件”面板，然后单击“显示表筛选器”图标。

   将打开“筛选器”面板。

2. 为要监控的 vApp 事件指定适当的筛选器，然后单击“应用”。

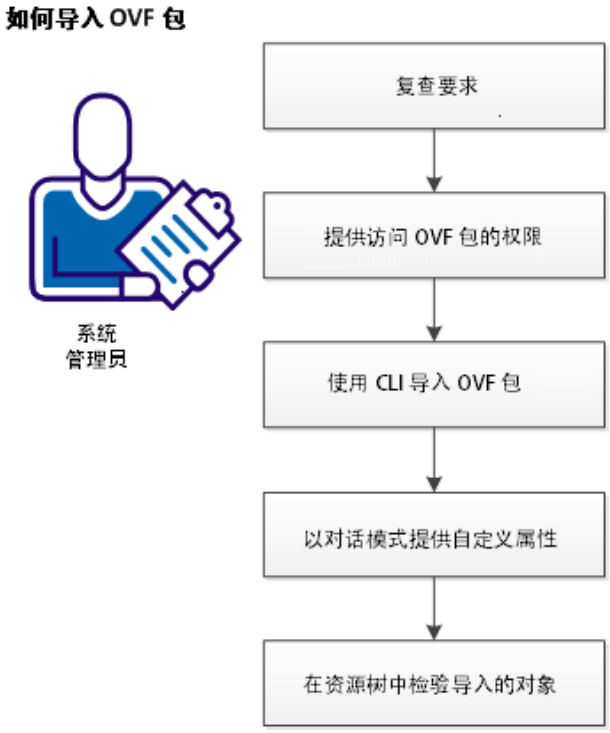
   “事件”面板将列出筛选的事件。

如何使用 CA Virtual Assurance 导入 OVF 包

此方案提供有关使用 CA Virtual Assurance 导入 OVF 包的信息。此信息旨在帮助系统管理员导入 OVF 包以及部署这些 OVF 包中指定的 vApp。

开放虚拟化格式 (OVF) 是一种标准，用于指定和封装多层应用程序的所有组件以及与该应用程序关联的操作策略和服务级别。

下图说明导入 OVF 包的过程。



请执行以下步骤

查看要求 (p. 503)
提供访问 OVF 包的权限 (p. 503)
dpmovf import Command--Import an OVF Package (p. 503)
以对话模式提供自定义属性 (p. 505)
在资源树中检验导入的对象 (p. 505)

查看要求

请查看以下要求：

- 您可以访问 CA Virtual Assurance 用户界面。
- 您确认了目标 vSphere 环境及其 vCenter Server 运行正常。
- 您已确认您可以作为管理员启动 CMD 窗口，并且 dpmovf.exe 文件已安装在计算机上。

详细信息：

查看 vCenter 服务器管理组件之间的交互 (p. 469)
将新的 vCenter 服务器连接添加到管理器中 (p. 471)
添加 vCenter 服务器的 AIM 实例 (p. 475)
验证资源树中的 vCenter 服务器文件夹外观 (p. 480)

提供访问 OVF 包的权限

为了能够从 CA Virtual Assurance 访问 OVF 包，请执行以下任务之一：

- 在管理器上，映射 OVF 包所在的驱动器。
- 在管理器上复制 OVF 包。

dpmovf import Command--Import an OVF Package

dpmovf import 命令将导入 OVF 包并创建 VM 或 vApp。通过使用 -properties 属性，您可以提供自定义属性文件。*自定义属性文件*允许您指定 OVF 包中定义的自定义属性。自定义属性文件包含属性键和相应属性值的列表。

注意：如果您没有自定义属性文件，properties.txt 文件会在工作目录中得以创建。默认目录为 CA*产品名*\bin。

此命令具有以下格式：

```
dpmovf import
-host vCenter_server
-user user_name
-password user_password
-name VM_VApp_name
-path OVF_file_path
-datacenter data_center
-datastore data_store
-resourcepool resource_pool
[-locale iso639value]
[-properties properties_file]
```

-host *vCenter_server*

指定 vCenter 服务器主机的名称。

-user *user_name*

指定要用来登录的用户名。

-password *user_passsword*

指定要用来登录的用户密码。

-name *VM_VApp_name*

指定 VM 或 vApp 的名称。

-path *OVF_file_path*

指定 OVF 文件路径。

-datacenter *data_center*

指定数据中心名称。

-datastore *data_store*

指定数据存储。

-resourcepool *resource_pool*

指定资源池。

-locale *iso639value*

（可选）指定 IS0 639_3166 组合以覆盖默认的英语输出（例如：法语为 fr_FR）。要使用命令提示符的区域设置，请指定“native”。

-properties *properties_file*

（可选）指定自定义属性文件路径。

示例：使用 CA Virtual Assurance 为 CA 平台导入 OVF 文件

此示例导入 CA 平台 OVF 包并创建 vApp 和 VM。CA 平台 OVF 文件是 *CA Platform_v1_0_0_92c.ovf*，文件位置是 *D:\OVF\CA_Platform*。用户名是 *user123* 。指定了 vApp 的以下属性：*my_datastore*、*my_datacenter* 和 *my_resourcepool*。*custom_properties.txt* 文件中提供自定义属性。

```
dpmovf import -path "D:\OVF\CA_Platform\CA Platform_v1_0_0_92c.ovf" -name
"My_CA_Platform" -host my_host.company.com -user user123 -locale en-US -datastore
"my_datastore" -datacenter "my_datacenter" -resourcepool "my_resourcepool"
-properties "custom_properties.txt"
```

以对话模式提供自定义属性

如果 OVF 文件包含自定义属性，您可以通过对话模式编辑自定义属性。如果指定了自定义属性文件，您可以通过对话模式覆盖自定义属性文件。

注意：如果您没有自定义属性文件，properties.txt 文件会在工作目录中得以创建。默认目录为 CA*产品名*\bin。

遵循这些步骤:

1. 键入要编辑的自定义属性的自定义属性数字。
2. 键入自定义属性值。
3. 对要提供或编辑的所有自定义属性，重复步骤 1 到 2。
4. 单击以下*任意*选项：

   r

   读取属性文件

   w

   覆盖属性文件中的所有属性。

   c

   执行导入命令。

   注意：提供的属性某些会被验证，以确认条件是否得到满足，或者提供的值是否有效。

CA Virtual Assurance 将 OVF 部署到 vCenter，您可以看到在 OVF 文件中指定的 vApp 和 VM。

在资源树中检验导入的对象

成功导入 vApp 和 VM 后，添加的实例列于 VMware vCenter Server 文件夹下的“资源浏览”窗格中。

遵循这些步骤:

1. 单击“资源”，然后打开“浏览”窗格。
2. 展开 VMware vCenter 服务器。

   导入的对象显示。

在 OVF 文件中指定的 vApp 即导入到您的 vCenter 环境中。CA Virtual Assurance 现在准备好在您的 vSphere 环境中管理添加的 vApp 和 VM。

群集中的 vCenter 服务器

如果 vCenter 服务器驻留在群集中，则 vCenter 服务器 AIM 必须在该群集外运行。配置 vCenter 服务器 AIM 以指向群集主机。成功启动 vCenter 服务器时，AIM 可以检测到故障切换并重新填充其内部高速缓存。

vNetwork 面板中的虚拟标准交换机和虚拟分布式交换机

VMware 数据中心级别和 ESX 主机级别的用户界面中提供了 vNetwork 面板。在 VMware 数据中心级别，vNetwork 表示该数据中心的虚拟分布式交换机。在 ESX 主机级别，vNetwork 表示关联的虚拟分布式交换机和虚拟标准交换机。

详细信息：

vNetwork 标准交换机 (vSwitch) (p. 506)
分布式虚拟交换机 (p. 507)
属性 (p. 508)
操作 (p. 511)
通过事件监控分布式虚拟交换机 (p. 512)

vNetwork 标准交换机 (vSwitch)

CA Virtual Assurance 监控属于所提取网络设备的标准 vSwitch 的策略以及属性。vSwitch 可以在 VM 内部之间路由流量并且链接到外部网络。vSwitch 结合多个网络适配器的带宽并在它们之间平衡通信流量。vSwitch 可以处理物理 NIC 故障切换。

vSwitch 模拟物理以太网交换机。对于一个 vSwitch，逻辑端口的默认数量是 120。您可以把 VM 的一个网络适配器连接到每个端口。与 vSwitch 相关的每个上行链路适配器使用一个端口。vSwitch 上的每个逻辑端口是单个端口组的成员。每个 vSwitch 还可分配一个或多个端口组。在两个或多个 VM 连接到相同的 vSwitch 时，它们之间的网络通信将在本地路由。如果将上行链路适配器连接到 vSwitch，那么每个 VM 均可以访问适配器所连接的外部网络。

您可以展开虚拟标准交换机对象以查看关联的端口和端口组。

- 端口组包含关联的使用端口组的虚拟机。

分布式虚拟交换机

CA Virtual Assurance 在 vSphere 环境中支持以下分布式虚拟交换机：

- VMware vNetwork 分布式交换机（vDS、vSphere 组件）
- Cisco Nexus 1000V 交换机（与 vSphere 进行集成）

CA Virtual Assurance 在 vSphere 环境中发现分布式虚拟交换机，并且通过事件监控其策略和属性。CA Virtual Assurance VM 开通支持 vNetwork 分布式交换机和 Cisco Nexus 1000V 交换机。

分布式虚拟交换机作为单个虚拟交换机运行，该交换机横跨与其关联的所有主机。分布式虚拟交换机代表适用于这些主机的相同交换机（相同名称、相同网络策略）和端口组。这些属性可使 VM 在多个主机之中迁移时维持一致的网络配置。

与 vNetwork 标准交换机一样，每个分布式虚拟交换机均是可供虚拟机使用的网络集线器。分布式虚拟交换机可以在虚拟机之间内部转发流量，或通过连接到物理 NIC（上行链路适配器）链接到外部网络。

分布式虚拟端口组（dvPort 组）是与分布式虚拟交换机关联的端口组，并且为每个成员端口指定端口配置选项。dvPort 组定义如何通过分布式虚拟交换机连接到网络

分布式虚拟上行链路 (dvUpLinks) 为 ESX 或 ESXi 主机上的物理 NIC (vmnic) 提供一个抽象层。每个物理 NIC 均映射到 dvUplink。dvPort 组到 dvUplink 的映射定义 VM 使用 ESX 或 ESXi 主机上的哪些物理 NIC 来通过分布式虚拟交换机获取对网络的访问权限。

Cisco Nexus 1000V 交换机包括虚拟以太网模块 (VEM) 和虚拟监控模块 (VSM)。在与 Cisco Nexus 1000V 交换机相关的每个 ESX 或 ESXi 主机上，VEM 将替换 VMware vSwitch 并且作为管理程序内核中的模块运行。VSM 控制多个 VEM 作为一个逻辑交换机，并在 ESX 或 ESXi 主机上的 VM 中运行。

有关详细信息，请参阅 http://pubs.vmware.com 上的 VMware vNetwork 分布式交换机文档或 http://www.cisco.com/go/1000vdocs 上的 Cisco Nexus 1000V 交换机文档。

注意：如果使用 Cisco Nexus 1000V 交换机，VSM VM 将不作为特殊 VM 出现在 CA Virtual Assurance 用户界面中。验证您应用于 VSM VM 的规则和操作是否影响 Cisco Nexus 1000V 交换机。

您可以展开虚拟分布式交换机对象以查看关联的端口组和上行链路组。

- 端口组包含关联的使用端口组的 VM。
- “上行链路组”将列出物理上行链路适配器。

属性

“属性”窗格显示虚拟标准交换机或虚拟分布式交换机的属性。

策略

以下列表包含虚拟标准交换机或虚拟分布式交换机的默认策略或已启用的策略。

混杂模式

指示在端口上是否能看到所有流量。

MAC 地址更改

指示是否可以更改介质访问控制 (MAC) 地址。

伪传输

指示 MAC 地址是否与虚拟网络适配器的 MAC 地址不同。

流量调整

指示端口上是否已启用流量调整器。

平均带宽

指示在端口上启用调整的情况下的平均带宽（位/秒）。

带宽峰值

指示在端口上启用流量调整的情况下爆发时的带宽峰值（位/秒）。

脉冲大小

指示在端口上启用调整的情况下允许的最大脉冲大小（字节）。

网络故障检测

指示是否已启用网络故障检测。有效值是：

- false (1)
- true (2)

通知交换机

指定在链接失败的情况下是否通知物理交换机

回退

指示是否已启用回退。

策略入站框架

指示成组策略是否应用于入站帧。

活动适配器

显示用于负载平衡的活动网络适配器的列表。

备用适配器

显示用于故障转移的备用网络适配器的列表。

vSwitch 属性

以下 vSwitch 属性表示端口号特征：

端口数

指示虚拟分布式交换机或虚拟标准交换机当前的端口数。

最大端口数

指示虚拟分布式交换机的最大端口数。

注意：对于虚拟分布式交换机，该信息仅适用于 VMware 数据中心级别。对于 ESX 主机级别，该信息不适用。

端口组属性

以下端口组属性表示 VLAN ID：

VLAN ID

指示端口组的 VLAN ID。

端口属性

以下属性指定端口特征：

VLAN ID

指示端口的 VLAN ID。

类型

指示端口的类型，如 VMkernel 端口或服务端口。

网络属性

以下属性指定虚拟交换机的网络特征：

- IPv4 地址
- IPv6 地址
- MAC 地址

虚拟机计数

以下值提供有关与端口组关联的 VM 的统计信息。

- 已打开电源
- 已关闭电源
- 已挂起
- 未知

操作

使用相应的操作来管理您的虚拟标准交换机和虚拟分布式交换机。可用操作如下：

- 添加 vSwitch
- 更新 vSwitch
- 删除 vSwitch
- 添加端口组
- 更新端口组
- 删除端口组
- 重命名端口组

应用这些操作时，会打开一个对话框提示您输入所需信息。可能的字段有：

交换机名称

指定操作所针对的交换机名称。

NIC

（可选）指定与 ESX 主机成员关联的物理 NIC 的列表。

上行链路端口名称

（可选）指定要使用的上行链路端口名称的列表。

最大端口数

（可选）指定虚拟分布式交换机的最大端口数。

绑定类型

（可选）指定端口组的绑定类型。有效值是：

earlyBinding

在 VM 绑定至端口组时分配端口。这种类型的绑定可确保始终连接，但永久保留端口。此绑定类型为默认值。

lateBinding

如果 VM 电源打开且其 NIC 处于连接状态，则将端口分配给该 VM。当 VM 电源关闭或其 NIC 断开连接时，此绑定类型将重新分配端口。LateBinding 可通过 vCenter 进行配置。

ephemeral

如果 VM 电源打开且其 NIC 处于连接状态，则将端口分配给该 VM。当 VM 电源关闭或其 NIC 断开连接时，此绑定类型将重新分配端口。Ephemeral 绑定可通过 ESX 主机和 vCenter 进行配置。

端口数

（可选）指定端口组的端口数。

端口组名称

指定端口组名称。

新端口组名称

指定新的端口组名称。

LAN ID *vlanid*

（可选）指定用于虚拟端口组操作的整数值 (*vlanid*)。

通过事件监控分布式虚拟交换机

您可以通过下列事件监控分布式虚拟交换机：

- 添加交换机：

  分布式虚拟交换机 VM-dvSwitch 已添加到数据中心 MyDC。vSphere：vcserver.mycomp.com

- 删除交换机：

  分布式虚拟交换机 VM-dvSwitch 已从数据中心 MyDC 中删除。vSphere：vcserver.mycomp.com

- 添加端口组：

  分布式虚拟端口组 VM dvPortGroup 已添加到分布式虚拟交换机 VM-dvSwitch。数据中心：MyDC，vSphere：vcserver.mycomp.com

- 删除端口组：

  分布式虚拟端口组 VM dvPortGroup 已从分布式虚拟交换机 VM-dvSwitch 中删除。数据中心：MyDC，vSphere：vcserver.mycomp.com

- 添加上行链路：

  分布式虚拟上行链路 VM DVUplink 已添加到分布式虚拟交换机 VM-dvSwitch。数据中心：MyDC，vSphere：vcserver.mycomp.com

- 删除上行链路：

  分布式虚拟上行链路 VM DVUplink 已从分布式虚拟交换机 VM-dvSwitch 中删除。数据中心：MyDC，vSphere：vcserver.mycomp.com

通过事件监控分布式虚拟交换机

1. 单击“显示板”选项卡，滚动到“事件”面板，然后单击“显示表筛选器”图标。

   将打开“筛选器”面板。

2. 为想要监控的分布式虚拟交换机事件指定适当的筛选器，然后单击“应用”。

   “事件”面板将列出筛选的事件。

VMware vCenter 开通和常见用例

本节提供了有关如何开通虚拟资源以及执行常见用例的说明。

添加虚拟机（vCenter 服务器）

可以使用两种方法之一添加 VM：

- 克隆预定义的模板
- 克隆现有的 VM 和自定义规格。自定义规格定义来宾操作系统的特征。

虚拟机开通支持标准交换机和分布式虚拟交换机。在开通附加到分布式虚拟交换机的 VM 时，您可以在用户界面中指定已发现的适当 dvPort 组。dvPort 组定义如何通过分布式虚拟交换机连接到网络。

添加 VM

1. 右键单击“浏览”窗格中的 VMware vCenter 服务器，并依次选择“开通”、“开通 VMware VM”。

   此时将显示“VMware vCenter 开通”对话框。

2. 从下拉列表中选择用于指定设置的选项。

   注意：为克隆列出的虚拟机限于 CA Virtual Assurance 监控的虚拟机。访问 VM 限于确保安全。如果要克隆不可用的系统，可像发现其他任何系统那样发现该系统，以使其在下拉列表中可用。

3. 输入您要使用的用户名、密码和主机名。否则，默认情况下将使用规格中指示的名称。

   注意：Windows 和 Linux 的用户名和密码必须与自定义规格文件中定义的用户名和密码匹配。

4. 选择以下选项之一并单击“下一步”：

   - VC 虚拟机，以使用现有 VM
   - VC 模板，以使用模板来创建新 VM
   - VC 规格，以从可用列表中选择自定义规格

   此时将显示“虚拟机内存”页面。

5. （可选）调整 VM 的内存，然后单击“下一步”。

   内存

   用 VM 模板或 VM 中定义的内存值填充该字段。

   默认值：最小值 4 MB，最大值 16 GB

   注意：配置 caimgconf.cfg 文件中的这些值。

   此时将显示“虚拟机 CPU”页面。

6. （可选）调整 VM 的 CPU，然后单击“下一步”。

虚拟处理器数

用 VM 模板或 VM 中定义的虚拟处理器数填充该字段。

默认值：最小值 1 个 CPU，最大值 4 个 CPU

注意：配置 caimgconf.cfg 文件中的这些值。

此时将显示“磁盘”页，并用选定 VM 或选定模板中的默认值填充字段。

7. （可选）设置驱动器大小，并单击“添加驱动器”以添加驱动器，从下拉列表中配置要与硬盘关联的数据存储和要使用的 SCSI 控制器，然后单击“下一步”。

数据存储

标识将在其中创建 VM 的 VMware ESX 主机的数据存储名称。

驱动器大小

允许您指定驱动器大小和向 VM 添加更多硬盘。

限制：最小驱动器大小为 1 MB，但不能超过您选择的数据存储的驱动器大小。

SCSI 控制器

指定要用作虚拟适配器的 SCSI 控制器。

此时将显示“网络”页，并用选定模板中的默认值填充表。

8. （可选）在“网络管理”表的单元格内单击，以激活下拉列表，更改所需的任何设置。

如果自定义规格指定使用 DHCP，您将只能编辑表中的网络连接单元格。现在，网络连接同时支持用于标准和分布式虚拟交换机的网络。您可以根据以下命名约定区分标准交换机和分布式虚拟交换机的名称：

- 对于标准交换机，其名称为网络名称。
- 对于分布式虚拟交换机，其名称为 dvPort 组名称后跟用括号括起来的分布式虚拟交换机名称：dvPortGroupName (dvSwitchName)

如果您的自定义规格指定使用静态 IP 地址，您将能够编辑除 NIC 单元格以外的所有单元格。CA Virtual Assurance 不支持自定义规格网络设置“提示用户”。使用此设置的自定义规格将被筛选掉并且不可用。

单击“下一步”。

9. 单击“添加计算机”。

   窗格顶部将显示一条确认消息。

   注意：映像创建需要花费时间，因此您应预测到在操作系统安装期间会有延迟。为实现更高效的发现，您可以在位于以下路径的 caimgconf.cfg 文件中调整发现重试时间或间隔：*install_path*\CA*productname*\conf。

10. 单击“刷新”，以在左侧窗格中查看新 VM。

    您的数据中心有一个新克隆的 VM。您可以在显示板中查看映像过程的事件，还可以生成映像作业报告。

克隆虚拟机

克隆虚拟机可创建一个虚拟机副本，您可将其置于同一虚拟机场的任意位置。创建克隆时还可自定义来宾操作系统。仅可克隆处于关机状态的虚拟机。

克隆虚拟机

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击要克隆的虚拟机，然后选择“管理”、“克隆”。

   此时将出现“克隆”窗格。

3. 填写下列字段，然后单击“克隆”：

   名称

   指定 VM 克隆名称。

   数据存储

   指定要存储克隆的 VM 的数据存储。该数据存储必须与源 VM 位于同一个场中。

   自定义规格

   指定要使用的来宾操作系统规格。您可以选择默认或自定义。

   目标资源池

   指定克隆的 VM 从中获取资源的资源池。

   将显示一条消息，确认请求提交。

4. 单击该虚拟机的“摘要”选项卡。

   验证是否出现要求确认操作的事件。操作完成后，克隆机将出现在“浏览”窗格中。

管理 VM 状态 (VMware)

您可以通过执行以下 VM 操作来控制 vCenter 服务器虚拟机的状态：

- 打开电源
- 关闭电源
- 挂起
- 重置
- 关闭

可以在多个 VM 上同时执行上述任意操作。

控制 VM 状态

1. 在“浏览”窗格中选择要在其上执行状态操作的虚拟机。
2. 右键单击该 VM，选择“管理”。还可以单击“快速启动”，然后单击相关的电源控制链接。选择以下选项之一：

   打开电源

   启动虚拟机并引导来宾操作系统。您只能打开当前已关闭或挂起的虚拟机。

   关闭电源

   关闭虚拟机电源。您只能关闭当前已打开或挂起的虚拟机。

   挂起

   暂停虚拟机并保存其当前状态。在您恢复该虚拟机之前所有活动都会被挂起。

   重置

   关闭来宾操作系统并重新启动。

   关闭

   关闭来宾操作系统。您仅可关闭当前已打开的虚拟机。

   这时将会出现确认对话框。
3. 单击“确定”。

   状态操作发生后，将出现一条确认信息。刷新界面以查看新的 VM 状态。会出现一个确认操作结果的事件。

以下图标表示不同的 VM 状态：

表示 VM 处于严重状态。

表示 VM 处于警告状态。

表示 VM 处于正常状态。

表示 VM 处于未知状态。

将模板转换为虚拟机

可以将模板转换为虚拟机。将模板转换为 VM 时，该 VM 将使用模板名称和设置。

将模板转换为虚拟机

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、“转换为虚拟机”。

   将出现“转换”页面。

3. 为虚拟机选择 ESX 服务器和资源池，然后单击“转换”。

   将显示一条消息，确认请求提交。

4. 单击该虚拟机模板的“摘要”选项卡。

   验证是否出现要求确认操作的事件。操作完成后刷新界面，该模板将作为虚拟机出现在“浏览”窗格中。

将虚拟机转换为模板

您可以将关闭的虚拟机转换为模板，以将该虚拟机的配置用作其他虚拟机的基础配置。

将虚拟机转换为模板

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、“转换为模板”。

   这时将会出现确认对话框。

3. 单击“确定”。

   将显示一条消息，确认请求提交。

4. 单击该虚拟机的“摘要”选项卡。

   验证是否出现要求确认操作的事件。操作完成后刷新界面，该虚拟机将作为模板出现在“浏览”窗格中。

创建快照

创建快照以保留虚拟机的当前状态，以便您在以后能返回该状态。快照可保留虚拟机的完整状态，包括内存内容、设置和虚拟磁盘状态。可以为打开、关闭或挂起的虚拟机创建快照。

创建快照

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、“快照”。

   将显示“快照”窗格。

3. 从“操作”下拉菜单中选择“新建”。

   将出现“创建新快照”对话框。

4. 输入快照名称和描述，指定是否启用捕获内存，然后单击“确定”。

   即会出现一条确认消息。

5. 单击该虚拟机的“摘要”选项卡。

6. 验证事件是否确认操作。

   操作完成后，快照会出现在“快照”窗格中。

删除快照

可以删除不再需要的快照。

删除快照

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、“快照”。

   将出现“快照”窗格，其中显示该虚拟机的所有现有快照。

3. 选择一个快照，并从“操作”下拉菜单中选择“删除”。

   这时将会出现确认对话框。

4. 单击“确定”。

   将显示一条消息，确认请求提交。

5. 单击该虚拟机的“摘要”选项卡。

   验证是否出现要求确认操作的事件。操作完成后，快照将从“快照”窗格中消失。

删除所有快照

可以通过一个操作删除虚拟机的所有现有快照。

删除所有快照

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、“快照”。

   此时将显示“快照”窗格，其中显示该虚拟机的所有现有快照。

3. 从“操作”下拉菜单中选择“删除全部”。

   这时将会出现确认对话框。

4. 单击“确定”。

   即会出现一条确认消息。

5. 单击该虚拟机的“摘要”选项卡。

   验证是否出现要求确认操作的事件。操作完成后，所有快照将从“快照”窗格中消失。

删除虚拟机

当您从 VMware vCenter Server 中删除虚拟机时，该虚拟机会从虚拟磁盘中删除。

删除虚拟机

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、“从 vCenter Server 中删除”。

   这时将会出现确认对话框。

3. 单击“确定”。

   将显示一条消息，确认请求提交。

4. 单击该虚拟机的“摘要”选项卡。

   此时应出现一个确认操作结果的事件。如果成功，该虚拟机会从虚拟磁盘中删除，且界面更新后会从“浏览”窗格中消失。

从模板部署虚拟机

可以从模板部署虚拟机，以使用该模板的设置来创建并部署新的虚拟机。

从模板部署虚拟机

1. 右键单击“浏览”窗格中的 VMware vCenter 服务器，并依次选择“开通”、“开通 VMware VM”。

   将显示“VMware vCenter 开通”对话框。

2. 指定所有必填字段并选择相应的 VC 模板。

   单击“下一步”

3. 执行剩余的步骤，以便为该虚拟机指定虚拟硬件。单击“完成”。

   将显示一条消息，确认请求提交。

4. 验证事件是否确认操作。

   操作完成后刷新界面，新虚拟机将出现在“浏览”窗格中。

管理群集服务

您可以在 VMware vCenter 群集上控制以下服务的状态：

HA

当主机发生故障时允许自动迁移和重新启动 VM。

DRS

让您将主机作为资源集进行管理。DRS 服务会根据需要将 VM 迁移至主机，将资源迁移至 VM。

管理群集服务

1. 在“浏览”窗格中选择一个 VMware vCenter 群集。

   此时右侧将出现“概述”窗格，显示 HA 和 DRS 服务的状态。

2. 从下拉菜单中选择“启用”或“禁用”。

   服务状态即会改变。

迁移虚拟机

可以将虚拟机迁移至另一个 ESX 主机。可以迁移关闭的虚拟机或打开的带有 VMotion 的虚拟机。不可迁移挂起的虚拟机。

迁移虚拟机

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击要迁移的虚拟机，然后选择“管理”、“迁移”。

   此时将显示“迁移”窗格。

3. 输入虚拟机要迁入的目标 ESX 服务器和资源池，然后单击“迁移”。

   注意：仅当在两个 ESX 主机之间共享 VM 数据存储/磁盘时才支持 ESX 主机之间的 VM 迁移。

   即会出现一条确认消息。

4. 单击该虚拟机的“摘要”选项卡。

   验证是否出现要求确认操作的事件。操作完成后，该虚拟机将在“浏览”窗格中出现在其迁移到的位置。

监控虚拟机

您可以详细监控 VM 的状态和属性。

监控虚拟机

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 展开 VMware vCenter Server 文件夹和 ESX 服务器对象。

   将显示一个 VM 列表。

4. 单击“摘要”选项卡。

   右侧窗格将显示常规信息、FT 属性、概述、CPU 和内存使用情况、磁盘使用情况（逻辑卷）以及事件。

   在“概述” 面板上，磁盘状态是指虚拟磁盘的虚拟硬件状态，由 SystemEDGE 计算得出，并基于 vCenter AIM 中配置的监视器。此信息基于虚拟磁盘的实际性能数据，以每秒的读写操作数为依据。

   在“磁盘使用量”面板中，磁盘状态是指通过来宾操作系统查看的逻辑卷的使用情况。该状态由 SystemEDGE 计算，并基于 vCenter AIM 中配置的监视器。该信息仅在 VM 和来宾操作系统运行时有效。

   “常规信息”面板提供了有关 VM 连接状态的详细信息。有效的连接状态值如下：

   - 未连接
   - 已连接
   - 孤立

   在群集进行故障转移的情况下可能会出现孤立的连接状态。当虚拟机被标记为孤立时，“概述”部分中反映的状态基于在孤立之前收集的数据。

监控 ESX 服务器

您可以详细监控 ESX 服务器的状态和属性。

监控 ESX 服务器

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 展开 VMware vCenter Server 文件夹并选择一个 ESX 服务器。

4. 单击“摘要”选项卡。

   右侧窗格将显示常规信息、FT 属性、概述、CPU 和内存使用情况、使用率以及事件。

5. 单击“vNetwork”选项卡。

   右侧窗格将显示关联的虚拟标准交换机 (vSwitch) 和虚拟分布式交换机 (vDS) 列表。

6. 从列表中选择一个虚拟交换机。

   右侧窗格将显示虚拟交换机的属性。

还原到快照

还原到快照时，您可以使虚拟机精确返回到获取快照时所处的状态。

还原到快照

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、“快照”。

   将出现“快照”窗格，其中显示该虚拟机的所有现有快照。

3. 选择一个快照，并从“操作”下拉菜单中选择“还原”。

   这时将会出现确认对话框。

4. 单击“确定”。

   即会出现一条确认消息。

5. 单击该虚拟机的“摘要”选项卡。

   验证是否出现要求确认操作的事件。

取消注册虚拟机

当您从 vCenter 服务器取消注册虚拟机时，虚拟机仍然存在，但会从 VMware vCenter Server 清单中移除。

取消注册虚拟机

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 在“浏览”窗格中找到并右键单击虚拟机，然后选择“管理”、、“从 vCenter 服务器取消注册”。

   这时将会出现确认对话框。

4. 单击“确定”。

   将显示一条消息，确认请求提交。

5. 单击该虚拟机的“摘要”选项卡。

   此时应出现一个确认操作结果的事件。如果成功，虚拟机已从 vCenter 清单中移除。

vCenter Automation 和策略操作

以下操作类型可与 VMware vCenter Server 一起使用：

- 添加磁盘 (p. 603)
- 添加网络接口 (p. 605)
- 配置共享 (p. 626)
- 配置 CPU/Memory (p. 614)
- 配置电源 (p. 622)
- 将模板转换为虚拟机 (p. 627)
- 将虚拟机转换为模板 (p. 629)
- 删除计算机 (p. 636)
- 管理 VM 快照 (p. 644)
- 修改 CPU (p. 652)
- 修改内存 (p. 653)
- 开通计算机 (p. 665)
- 删除磁盘 (p. 668)
- 删除网络接口 (p. 669)
- 迁移计算机 (p. 651)

在满足分配的规则条件后，可以使用这些操作类型来创建自动化 vCenter 电源、资源分配和其他操作的新操作。还可以排定这些操作在特定时间发生。

有关使用操作和规则来创建自动化策略的详细信息，请参阅“策略”一节。

查看自定义规格

自定义规格是您在虚拟机上使用的来宾操作系统的自定义版本。您可以查看所有当前自定义规格、最后一次更新的日期以及当前的版本号。

查看自定义规格

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 查找并选择 VMware vCenter 服务器。

   将在右侧窗格中显示服务器页面。

3. 单击“配置”选项卡并选择“自定义规格”子菜单。

   此时出现“自定义规格”部分，并显示现有的自定义规格。

查看常规信息

CA Virtual Assurance 在右侧窗格中显示常规信息，并在对象层次结构的以下级别提供资源属性：

- vCenter 服务器
- ESX Server
- 资源池
- VM

资源属性包括有关以下类别的信息：

- 名称、项目类型、版本
- CPU 和内存的定量特征
- VM 和资源池的数量
- 当前的资源模式

此外，CA Virtual Assurance 还显示有关 VM 级别的连接状态、电源状态以及容错信息。

有效容错状态的值为：

- 未容错
- 保护
- 未受保护（正在启动）
- 未受保护（需要辅助 VM）
- 未受保护（已禁用）
- 未受保护（VM 未运行）

辅助位置的值为：

- 不可用
- 辅助 CPU 使用量总计
- 辅助内存总计

“常规”信息面板提供了关于容错是否配置、版本和支持的 FT VM 的各种计数的详细信息。这些计数考虑了以下内容：

- 主 VM 总数
- 辅助 VM 总数
- 已打开的主 VM 数
- 已打开的辅助 VM 数

“常规信息”面板中呈现的 VM 数取决于正在运行的非 FT VM 和主 FT VM 之和。VM 总体计数中不包括辅助 FT VM。

详细信息

监控 ESX 服务器 (p. 525)
监控虚拟机 (p. 524)

第 7 章： 监控群集和虚拟桌面

此部分包含以下主题：

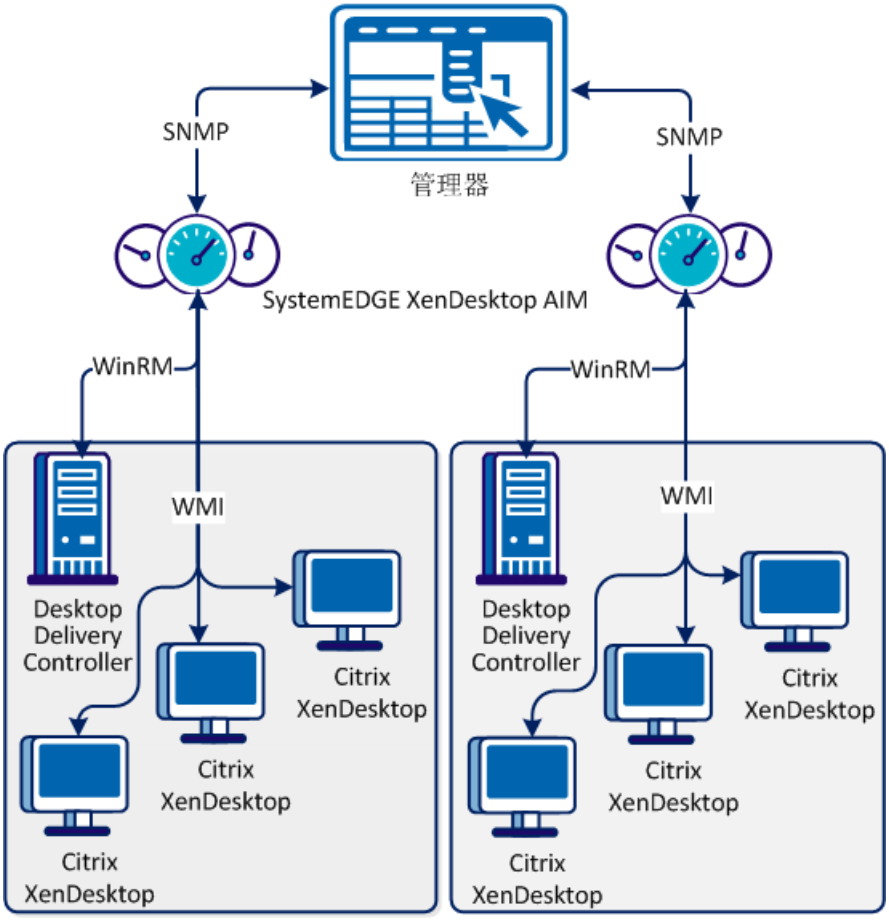
Citrix XenDesktop 环境

CA Virtual Assurance 远程监控 Citrix XenDesktop 环境。Citrix XenDesktop AIM 提供统计数据并帮助检测 Citrix XenDesktop 环境中的问题。监控包括但不仅限于桌面、控制器、计算机、目录、管理程序连接以及服务统计信息。

Citrix XenDesktop 管理组件之间的交互

下图说明了 Citrix XenDesktop 管理中涉及的组件是如何交互的。AIM 服务器是运行 SystemEDGE 和 XenDesktop AIM 的 Windows 服务器。XenDesktop AIM 和 Citrix XenDesktop 控制器之间的通信使用 Windows 远程管理 (WinRM)。环境中的 XenDesktop AIM 和 Citrix XenDesktop 之间的通信使用 WMI。CA Virtual Assurance 可以连接到多个 Citrix XenDesktop 控制器，您可以从整体上了解 Citrix XenDesktop 环境。

Citrix XenDesktop 管理组件相互协作关系



要添加 Citrix XenDesktop 控制器的必要连接信息，请使用以下方法：

- AIM 服务器上的 NodeCfgUtil.exe 实用工具

连接信息将写入受管节点上的配置文件中。XenDesktop AIM 轮询配置文件，并开始通过 Citrix XenDesktop 控制器或直接从 Citrix XenDesktop 监控您的 Citrix XenDesktop 环境。

Citrix XenDesktop 先决条件

列出的先决条件是安装 XenDesktop AIM 所必需的。确认以下组件安装在安装 XenDesktop AIM 的计算机上：

- Microsoft .NET Framework 4.0
- Windows 管理框架核心（Windows PowerShell 2.0、Windows 远程管理 (WinRM) 2.0）

  注意：有关 Windows 管理框架的详细信息，请参阅 Microsoft 968929 知识库文章。

将计算机名称添加到信任的主机列表中

如果 Citrix XenDesktop 位于不同域中，请将计算机名称添加到 AIM 计算机上 WinRM 服务的信任的主机配置设置中。

使用以下命令：

```
set-Item wsman:\localhost\client\trustedhosts machine_dnsname
```

machine_dnsname

指定 XenDesktop AIM 连接到的计算机的完整 dns 名称的列表。

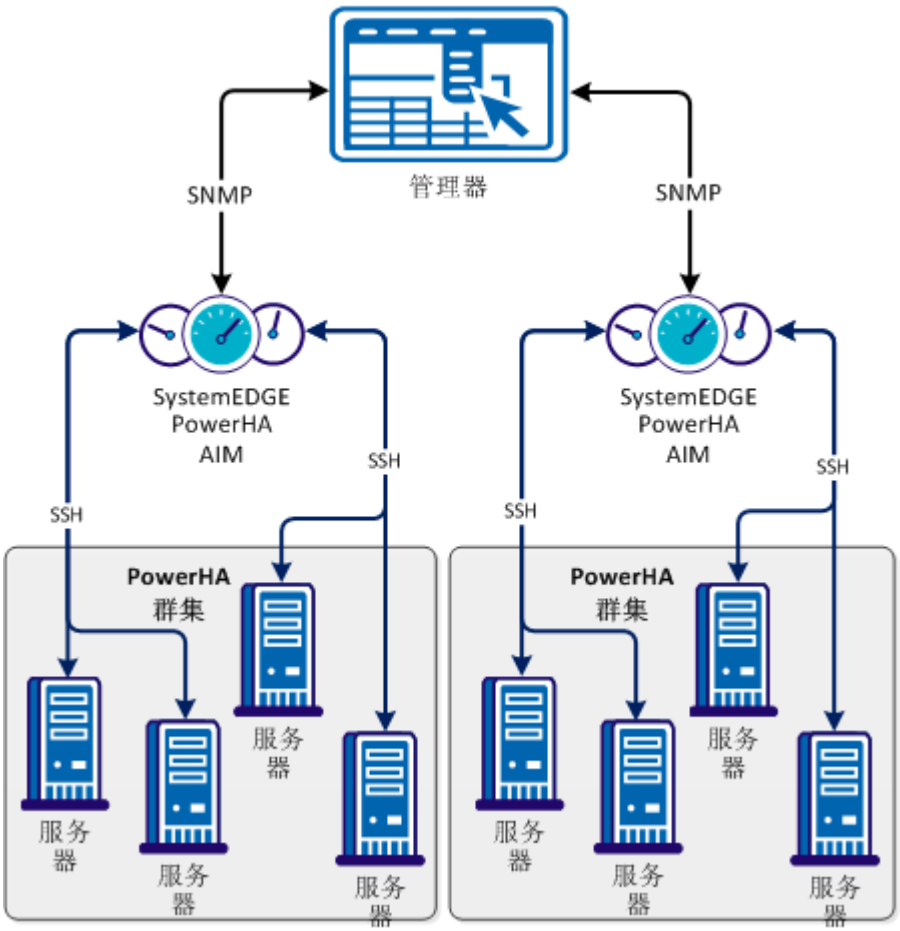
IBM PowerHA

CA Virtual Assurance 监测 IBM PowerHA（以前称为 High Availability Cluster Multiprocessing (HACMP)）。CA Virtual Assurance 远程监测群集，检测任何故障，并提供有关群集中报警和其他任何环境问题的详细信息。

IBM PowerHA 管理组件之间的交互

下图说明 IBM PowerHA 中涉及的管理组件如何交互。AIM 服务器是运行 SystemEDGE 和 PowerHA AIM 的 Windows 服务器。AIM 和 PowerHA 群集之间的通信使用安全外壳 (SSH)。由于 CA Virtual Assurance 可以连接到多个群集，因此 CA Virtual Assurance 可以获得 IBM 环境的总体视图。

PowerHA 管理组件之间的交互



要为每个所需的 IBM PowerHA 群集添加所需的连接信息，请使用以下方法：

- AIM 服务器上的 NodeCfgUtil.exe 实用工具

连接信息将写入受管节点上的配置文件中。PowerHA AIM 轮询配置文件，并开始通过主节点监测您的 IBM PowerHA 环境。

配置 SSH

要监控群集节点，请为远程访问配置 SSH。

遵循这些步骤:

1. 在群集（节点）上安装并运行 SSH 后台进程。
2. 配置本地防火墙以允许 SSH 连接。

在对话框模式下使用 NodeCfgUtil 配置 PowerHA AIM

NodeCfgUtil.exe 是可用于修改 AIM 配置的实用工具。在对话框模式下使用该实用工具可配置相应 AIM 管理的节点。

遵循这些步骤:

1. 以管理员身份登录，并在安装 AIM 的计算机上打开 Windows 资源管理器。
2. 转到 *SystemEDGE_InstallPath*\plugins\AIPCommon 目录，然后启动 NodeCfgUtil.exe。

   NodeCfgUtil 将发现已安装的 AIM，并在随后的对话框中将其列出。
3. 输入 *1* 添加一个新的受管节点。
4. 按照屏幕指示完成配置。每个节点都需要有效的用户名和密码进行身份验证。
5. 在配置之后，输入 0 返回上一菜单或退出实用工具。

NodeCfgUtil 将 PowerHA 的配置文件 (hacmp.cfg) 写入到 *SystemEDGE_InstallPath\plugins\AIPCommon* 目录。还可使用 NodeCfgUtil 实用工具编辑或删除现有条目。

示例

以下示例显示了已成功添加到 PowerHA AIM 配置的 *mycluster* 的“安装受管节点”对话框。PowerHA AIM 是多实例 AIM。您可以重复该程序，添加更多要使用该 AIM 管理的实体。

```
****  选择受管节点  ****
1. Microsoft 群集
2. IBM PowerHA
0. 返回上一个菜单
*******************************
输入选择：2
输入 IBM PowerHA 节点的以下信息...
（要在任一点返回到上一个菜单，请按 CTRL + Q 键）。
```

```
1. 群集名称：mycluster
2. 用户名：administrator
3. 密码：************
4. 端口 [默认=22]：
CAAC1016 正在身份验证，请稍候...
CAAC1019 身份验证成功。
CAAC1023 添加节点成功。
按任意键继续...
```

在命令模式下使用 NodeCfgUtil 配置 PowerHA AIM

NodeCfgUtil.exe 是可用于修改 AIM 配置的实用工具。在命令模式下使用该实用工具时，只能将受管节点添加到 AIM 配置。

注意：以 Windows 管理员身份运行 NodeCfgUtil.exe。

此命令具有以下格式：

```
(1) nodecfgutil -help
(2) nodecfgutil powerha -u user -p password -h cluster_name [-t port]
```

-help

显示有关控制台的用法信息。

powerha

指定虚拟环境或物理环境。

-u *user*/*usercertificate*

相应地指定管理用户或用户证书的名称。

-p *password*

指定该用户的密码。

- h *cluster_name*

指定群集的名称。

-t *port*

（可选）指定端口号。

默认值：22

遵循这些步骤:

1. 在安装 AIM 的系统上打开命令提示符。

   将显示命令提示符。

2. 输入以下命令之一:

   ```
   (1) nodecfgutil -help
   (2) nodecfgutil powerha -u user -p password -h cluster_name [-t port]
   ```

   (1) 显示有关控制台的用法信息。

   (2) 验证并存储为 IBM PowerHA 传递的凭据

   该实用工具将 IBM PowerHA 的配置文件 (hacmp.cfg) 写入到 *SystemEDGE_InstallLpath\plugins\AIPCommon* 目录。

CA IBM SystemEDGE PowerHA AIM 陷阱

CA SystemEDGE PowerHA AIM 陷阱类型

以下列表提供了 CA SystemEDGE PowerHA AIM 的陷阱类型。有关 varbind 的完整说明，请参考 MIB 文件。

hacmpAimInstanceAddedTrap

添加新实例或新服务器时，发送陷阱。

陷阱 ID： 165800

hacmpAimInstanceRemovedTrap

删除实例或服务器时，发送陷阱。

陷阱 ID： 165801

hacmpAimInstanceDataStatusChanged

更改实例或服务器数据状态时，发送陷阱。

陷阱 ID： 165802

hacmpAimNodeAddedTrap

添加节点时，发送陷阱。

陷阱 ID： 165803

hacmpAimNodeRemovedTrap

删除节点时，发送陷阱。

陷阱 ID： 165804

hacmpAimResourceGroupAddedTrap

添加资源组时，发送陷阱。

陷阱 ID：165805

hacmpAimResourceGroupRemovedTrap

删除资源组时，发送陷阱。

陷阱 ID：165806

hacmpAimResourceGroupMigration

迁移资源组时，发送陷阱。

陷阱 ID：165807

hacmpAimResourceAddedTrap

添加资源时，发送陷阱。

陷阱 ID：165808

hacmpAimResourceRemovedTrap

删除资源时，发送陷阱。

陷阱 ID：165809

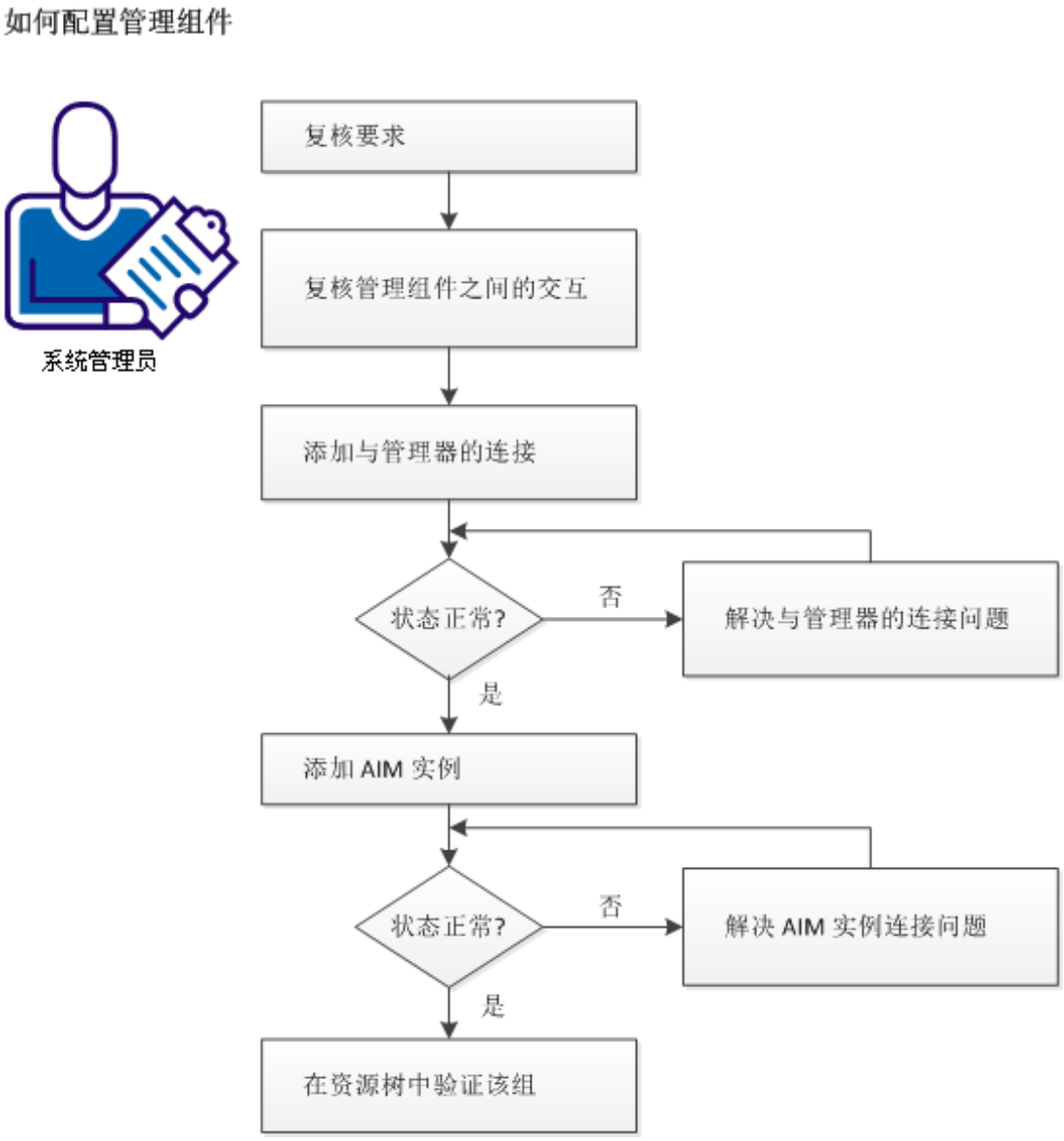
Microsoft 群集服务

Microsoft 群集服务 (MSCS) 将两个或多个服务器连接起来，从而使它们作为单个计算机呈现给客户端。群集化可帮助您获得自动防故障应用程序。类似于 Microsoft SQL Server 的群集感知应用程序一次在一个节点上运行。如果该节点关闭，其他节点将接管此服务。此外，群集化还有助于确保您的应用程序始终处于运行状态。

性能监控需要远程访问群集和单个群集节点以供度量标准集合之用，如 CPU 和内存使用。每个节点上提供了特定群集信息。MSCS AIM 使用 WMI（端口 135）与群集进行通信。

如何配置 Microsoft 群集服务管理组件

下图提供了有关配置管理组件所需操作的概述。该图包括针对连接问题的相应故障排除策略。



Microsoft 群集服务 (MSCS) 将两个或更多服务器连接到一起，并在客户端将它们显示为单个计算机。群集化可帮助您获得自动防故障应用程序。支持群集的应用程序（如 Microsoft SQL Server）每时在一个节点上运行。如果该节点出现故障，则其他节点接管服务。群集可确保应用程序始终可用。

如果使用 CA Virtual Assurance 安装 Microsoft 群集组件，则管理员可以注册群集并使用“管理”选项卡管理群集。

请执行以下步骤：

查看要求

在配置 CA Virtual Assurance 的管理组件之前，请查看以下要求：

- 您熟悉 TCP/IP、SNMP、Web 服务以及 Windows Server 操作系统。
- 您熟悉 CA Virtual Assurance 和 SystemEDGE。
- 您可以访问包括以下内容的 CA Virtual Assurance 管理器安装：
  - 平台管理模块 (PMM)
  - Application Insight Module (AIM)
  - 监控代理 (SystemEDGE)
- 您可以访问 CA Virtual Assurance 用户界面。
- 您具有有效的凭据（用户名和密码），可访问要管理的环境中的服务器。
- 您知道使用哪个协议（HTTP 或 HTTPS）和端口，以通过 Web 服务访问环境中的服务器。默认：HTTPS，端口：443。
- 您已验证环境中的服务器运行正常。
- 如果将 PMM 和 AIM 安装在不同系统上，请确认 PMM 和 AIM 系统上的 SNMP 设置一致。读和写团体字符串以及 SNMP 端口号必须是相同的。
- 您已验证 CA Virtual Assurance 管理器已发现您要使用的远程 AIM 服务器。

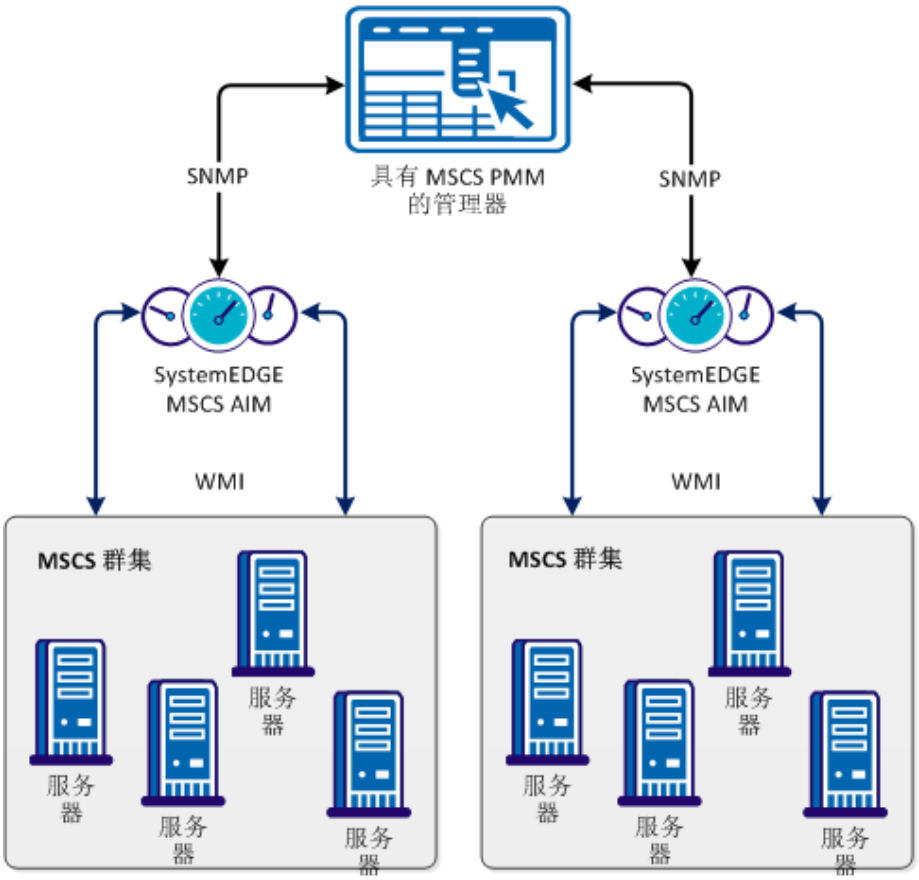
MSCS 管理组件之间的交互

下图说明了 MSCS 监控中涉及的组件是如何交互的。SystemEDGE 和 MSCS AIM 在 Windows 服务器上运行。

Microsoft 群集服务 (MSCS) 将两个或多个服务器连接起来，从而使它们作为单个计算机呈现给客户端。群集化可帮助您获得自动防故障应用程序。类似于 Microsoft SQL Server 的群集感知应用程序一次在一个节点上运行。如果该节点关闭，其他节点将接管此服务。此外，群集化还有助于确保您的应用程序始终处于运行状态。

性能监控需要远程访问群集和单个群集节点以供度量标准集合之用，如 CPU 和内存使用。每个节点上提供了特定群集信息。MSCS AIM 使用 WMI（端口 135）与群集进行通信。

MSCS 管理组件之间的交互



将 Microsoft 群集服务添加到管理器中

您可以使用 CA Virtual Assurance 用户界面的“管理”选项卡添加 Microsoft 群集。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格的“开通”部分中选择“Microsoft 群集服务”。
3. 在“Microsoft 群集服务”窗格工具栏上单击  （添加）。

   此时将显示“注册新群集”对话框。

4. 输入所需的连接数据（服务器名称、用户、密码、端口），指定首选 AIM，并启用“受管状态”。
5. 单击“确定”。

   将注册 Microsoft 群集。

   当网络连接已成功建立后，服务器会添加到右上角的窗格并带有绿色状态图标。

   注意：如果连接失败，将显示“验证失败”对话框。如果您单击“是”，CA Virtual Assurance 会将服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。

管理器到服务器的连接失败

症状：

在“管理”、“配置”下添加服务器连接后，对服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的服务器连接数据是否仍然有效。如有必要，请更新连接数据。
- 验证服务器系统是否正在运行并且可以访问。
- 验证连接所需的所有服务是否在服务器系统上运行良好。

更新服务器连接数据：

1. 单击与失败的连接关联的  （添加）或  （编辑）。
2. 添加连接详细信息，启用“受管状态”，然后单击“确定”。

   将更新连接数据。
3. 单击右上角的  （验证）以验证新设置。

   如果无法建立与服务器的连接，请继续执行下一步骤。

验证服务器系统是否正在运行并且可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```
2. 要确定服务器是否具有有效的 DNS 条目和 IP 地址，请检查这些命令的输出。

   如果服务器不在 DNS 中，请将服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。
3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress <Server Name>
   ```

   输入正确的 IP 地址和服务器名称并保存文件。例如：

   ```
   192.168.50.50 myServer
   ```
4. 切换到 CA Virtual Assurance 用户界面、“管理”选项卡、“配置”、“服务器”窗格，并单击右上角的  （验证）。

   即使服务器凭据和连接数据正确并且您可以 ping 服务器，连接仍然可能失败。在这种情况下，可能是服务器引起该问题。如果无法建立与服务器的连接，请继续执行下一步骤。

验证连接所需的所有服务是否在服务器系统上运行良好。

1. 要访问服务器，请联系系统管理员。
2. 登录到服务器系统。
3. 验证连接所需的所有服务是否运行良好。
4. 如有必要，请启动或重新启动服务。
5. 切换到管理器系统上的 CA Virtual Assurance 用户界面、服务器窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证服务器连接。

   如果与服务器的连接失败，请验证根据该方案的要求收集的数据是否有效。

   与管理员或技术支持合作，解决服务器连接问题。

添加发现的 MSCS AIM 实例

将 Microsoft 群集服务连接添加到 CA Virtual Assurance 管理器后，添加 AIM 实例以管理 Microsoft 群集服务环境。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。
2. 从左侧窗格的“开通”部分中选择“Microsoft 群集服务”。
3. 在“发现的 Microsoft 群集 AIM 实例”窗格工具栏上单击 （添加）。

   此时将显示“添加群集 AIM 实例”。
4. 从下拉列表中选择 AIM 主机。

   将显示发现的 AIM 主机的列表。
5. 从下拉列表中选择注册的群集。

   CA Virtual Assurance 将向“注册的群集”下拉列表中填充“注册的 Microsoft 群集”窗格中列出的“群集名称”。您只能管理您的 CA Virtual Assurance 管理器与之建立了有效连接的那些群集。

   注意：如果 AIM 位于远程系统中，则 CA Virtual Assurance 一定会首先发现该系统。在发现之后，AIM 服务器将在下拉列表中显示。
6. 单击“确定”。

   将添加选定群集的新 AIM 实例。如果实例未处于错误或已停止状态，CA Virtual Assurance 将开始发现关联的环境。在发现过程完成后，您可以开始管理您的 Microsoft 群集服务环境。

排除 AIM 实例连接的故障

如果 AIM 连接处于未就绪状态，将出现以下状态图标之一：

- 发现正在进行
- 无轮询
- 错误
- 警告
- 已禁用
- 未知

有关 AIM 实例状态的详细信息，请参阅工具提示。以下故障排除部分提供了用于解决该问题的详细信息和步骤。

AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为服务器添加 AIM 实例后，状态图标显示（发现正在进行）。

解决方案：

等到环境的发现过程完成。发现持续时间取决于与环境中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示指示未完成发现请求数量的工具提示。发现作业完成时，CA Virtual Assurance 会向资源树中添加一个服务器文件夹。然后，您可以开始管理您的环境。

AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示（无轮询）。

解决方案：

关联实例不需要特定的操作。此图标表示 CA Virtual Assurance 管理器不轮询此 AIM。AIM 不是首选。

如果多个 AIM 已配置为管理特定服务器，PMM 将选择其中一个 AIM 作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决可能导致与 AIM 连接失败的最常见问题：

- 验证是否可以访问 AIM 服务器。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 确认命令的输出对于 AIM 服务器有有效的 DNS 条目和 IP 地址。

   如果 AIM 服务器不在 DNS 中，则将 AIM 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress servername
   ```

   输入正确的 IP 地址和 AIM 服务器名称。例如：

   ```
   192.168.50.51 myAIM
   ```

4. 在“AIM 服务器”窗格的右上角，单击  （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“AIM 服务器”窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证 AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否有效。

AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 AIM 实例之后，几个实例的状态图标显示 （已禁用）。该 AIM 实例未受管理。

如果 CA Virtual Assurance 发现具有以下关系的 AIM，则显示该状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的服务器配置了 AIM。
- AIM 连接到未配置的服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的服务器连接并将其受管状态更改为已启用。

验证资源树中的 Microsoft 群集服务

在成功配置和发现之后，新发现的资源将在“资源”、“浏览”窗格中的相应组下列出。

遵循这些步骤:

1. 单击“资源”，然后打开“浏览”窗格。
2. 展开 MSCS 组。

   此时将显示 MSCS 资源。

CA Virtual Assurance 已准备好管理已配置的 MSCS 环境。您可以监控 MSCS 资源的状态和属性。

注册群集

可以使用用户界面的“管理”页面注册 Microsoft 群集。

从用户界面注册 Microsoft 群集

1. 单击“管理”。
   此时将显示“管理”页面。
2. 在“配置”窗格的“开通”部分中，单击“Microsoft 群集服务”。
   右侧将显示“Microsoft 群集服务”部分。
3. 单击“注册的 Microsoft 群集”工具栏上的 +（添加）。
   此时将显示“注册新群集”对话框。
4. 输入所需的群集名称并访问标识信息，然后单击“确定”。
   将注册 Microsoft 群集。

注意：注册群集时，使用群集主机名。

删除群集

可以使用用户界面的“管理”页面删除 Microsoft 群集。

遵循这些步骤:

1. 单击“管理”。
   此时将显示“管理”页面。
2. 在“配置”窗格的“开通”部分中，单击“Microsoft 群集服务”。
   此时将显示“Microsoft 群集服务”页面。
3. 在“注册的 Microsoft 群集”部分中，选择要删除的群集。
4. 单击“注册的 Microsoft 群集”工具栏上的 -（删除）。
5. 单击“确定”。
   群集已删除。

修改群集属性

可以使用用户界面的“管理”页面修改 Microsoft 群集属性。

修改群集属性

1. 单击“管理”。

   此时将显示“管理”页面。
2. 在“配置”窗格的“开通”部分中，单击“Microsoft 群集服务”。

   右侧将显示“Microsoft 群集服务”部分。
3. 选择要编辑的群集。
4. 单击“注册的 Microsoft 群集”工具栏上的“编辑”图标。

   此时将显示“修改群集属性”对话框。
5. 编辑所需的属性，然后单击“确定”。

   群集属性已修改。

Microsoft 群集服务管理

通过 Microsoft 群集服务管理，可以管理 Microsoft 群集、服务和应用程序及节点。Microsoft 群集服务作为中央位置，可从中查看所有群集并执行管理操作。

本节描述了可以从“资源”页面的 Microsoft 群集资源上执行的管理操作。通过“资源”页面，您可以查看以下对象的基本信息和详细信息：

- Microsoft 群集
- 服务和应用程序
- 节点

单击“资源”，打开“浏览”窗格，并选择群集资源之一；然后单击该资源的“摘要”。

通过“摘要”页面，可以查看与该对象相关的信息及与资源相关的事件。

监控 MS 群集服务

可以详细地监控 MS 群集资源的状态和属性。

要监控群集资源，请执行以下操作：

1. 单击“资源”。

   此时将显示“资源”页面。

2. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

3. 展开 MS 群集服务文件夹，然后单击群集对象。

   将出现群集节点和服务对象的列表。

4. 单击“服务”和“应用程序”对象。

   这时将出现服务列表。

5. 单击服务对象。

   右窗格将显示常规信息、资源和事件。

   “常规信息”面板显示服务名称、状态、及服务所属的群集的名称。

   “资源”面板中的“概述”选项卡显示了资源详细信息，如资源名称、类型和状态。“资源”面板中的“私有属性”选项卡显示了各个资源的私有属性。

   “事件”面板显示当前事件。

第 8 章： 无代理的监控

CA Virtual Assurance 提供了对支持的虚拟环境（除 Hyper-V 之外）和 Windows 系统的无代理监控（远程监控）。

此部分包含以下主题：

远程监控

远程监控 (RM) 使您可以监控无代理系统的运行状况。RM 提供了以下灵活性，即您无需在远程系统上安装监控代理（如 SystemEDGE）便可监控系统。

RM 采用名为 RM AIM 的中间级管理器来监控远程系统。RM AIM 使用远程 Windows 系统上的 WMI 查询来收集度量标准信息。

详细信息：

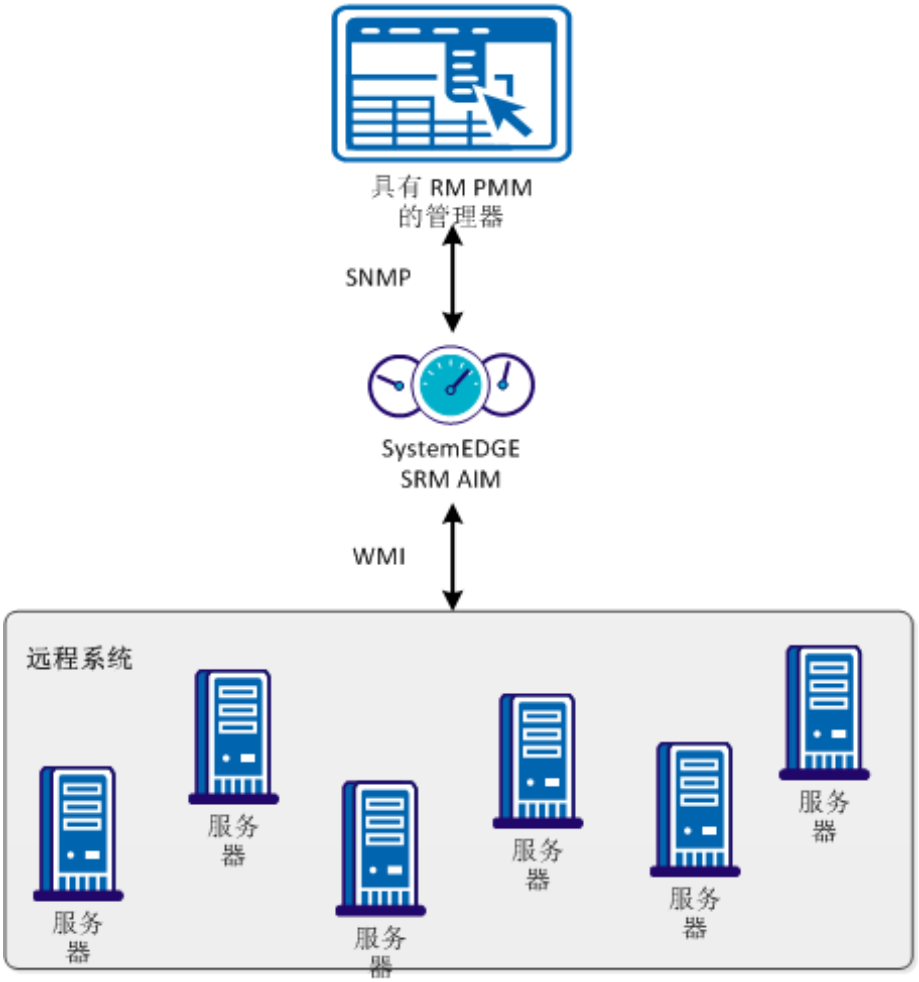
远程监控组件之间的交互

远程监控 AIM 通过利用 DCOM 的 root\CIMV2 命名空间的 WMI 连接来访问 RM 系统。DCOM 需要本地系统管理员用户和密码凭据。如果要监控 Windows 计算机，必须提供 RM AIM 存储在文件中的这些证书。密码已加密。

“远程监控”收集和提供在受监控 RM 系统上执行 WMI 查询（端口 135）的 Windows 系统信息。WMI 使用端口 135（默认）。

下图说明了这些关系。

远程监控组件之间的交互



远程监控的优势

远程监控涉及无代理技术，而非基于代理的技术，这两种策略分别具有各自的优势。在决定使用 RM 还是已部署代理时使用该信息。

RM 具有以下优势：

- 在设置、配置和部署方面花费更少
- 简化软件升级和维护
- 部署快速，并且在受监控环境中不易受到干扰
- 在受管服务器上利用的资源更少

已部署的代理具有以下优势：

- 为受监控的服务器和应用程序提供更详细的数据和更高级别的功能
- 操作需要的网络带宽更少
- 提供更高程度的可扩展性，可扩展到数千台服务器
- 当网络连接不可用时可继续监控服务器运行状况并进行数据收集（就像代理可以自主工作）
- 对受管服务器提供更强大的命令和控制功能

功能和优势

从最终用户的角度，远程监控提供监控的*无缝*集成（即，由代理和 RM 监控的系统的管理接口外观相同）。

RM 包括一些功能，这些功能允许您通过监控运行状况和关键性能指标 (KPI) 度量标准来管理系统。RM 提供有关系统状态和使用率度量标准的报告。RM 包括许多优势，如恢复能力、可扩展性、集成以及自动化。以下部分描述主要功能和优势。

无代理受监控系统

远程监控能够为使用基于代理的技术和无代理技术管理的系统启用无缝运行状况监控。

RM 管理器组件 (RM PMM) 创建代表 RM 系统及其运行状况的 CIM 系统对象。

“显示板”和“资源”面板中会提供该信息。

遵循这些步骤:

1. 依次打开“资源”、“浏览”，然后展开“远程监控”文件夹。

   将在组件树中显示发现的系统。

2. 选择系统。

   将在右侧窗格中显示该系统的页面。

3. 打开“远程监控”选项卡。

   将显示以无代理方式收集的数据。

关键性能指标度量标准

通过在受监控的 RM 系统上执行 WMI 查询，远程监控可收集和提供 Windows 度量标准信息。各种 Win32 CIM 类中有大量的可用信息，这些信息通过 RM AIM 可用。

可视化

通过 RM UI 可以配置以下信息：

- 远程监控哪些系统
- 为这些系统收集哪些度量标准
- 是否监控这些度量标准以及如何监控（包括重要级别和阈值）

配置

在被选中进行监控时，远程监控会监控远程系统上的自带 KPI，而不需要正在执行的监控的配置。您可以调整自带监控阈值来满足需求。

您也可以在配置集中定义和存储配置设置，该配置集随后可以被分配给一个或多个 RM 系统。

访问控制

当用户作为管理员或非管理员用户登录到 UI 时，安全机制会提供身份验证和授权功能。根据用户是管理员用户还是非管理员用户，远程监控允许或禁止特定操作（如配置 RM 系统）。

RM AIM 通过到 root\CIMV2 命名空间的 WMI 连接（使用 DCOM）访问 RM 系统。本地 RM 系统管理员用户和密码凭据是访问所必需的。这些凭据（当 RM 系统受监控时由用户提供）通过密码加密存储在文件中。

恢复能力

RM AIM 是独立于 SystemEDGE 的进程；RM AIM 中的错误不会导致 SystemEDGE 崩溃。如果 RM AIM 崩溃或不再响应 SystemEDGE 请求，则 SystemEDGE 中的 *RM AIM 正在运行*检查将重新启动 RM AIM。

可扩展性

每个 SystemEDGE 有一个 RM AIM，而每个 RM AIM 可以监控大约 200 个 RM 系统。每个管理器有一个 RM PMM，而每个 RM PMM 可以管理大约 20 个 RM AIM。默认配置集包含十个受监控的度量标准，每个度量标准具有两个监视器。

根据 SystemEDGE 可扩展性，这将导致以下结果：

- 10 * 2 * 200 = 4000 monitorTable 条目
- 10 *200 = 2000 aggregateTable 条目

集成

RM 监视器信息在 SNMP MIB 中是公开的，以便轻松访问 eHealth、 和 Spectrum 管理器。

自动化

RM AIM 包括一个命令行实用工具 (rmonwatch)，该实用工具允许使用脚本远程配置 RM 系统及其凭据。

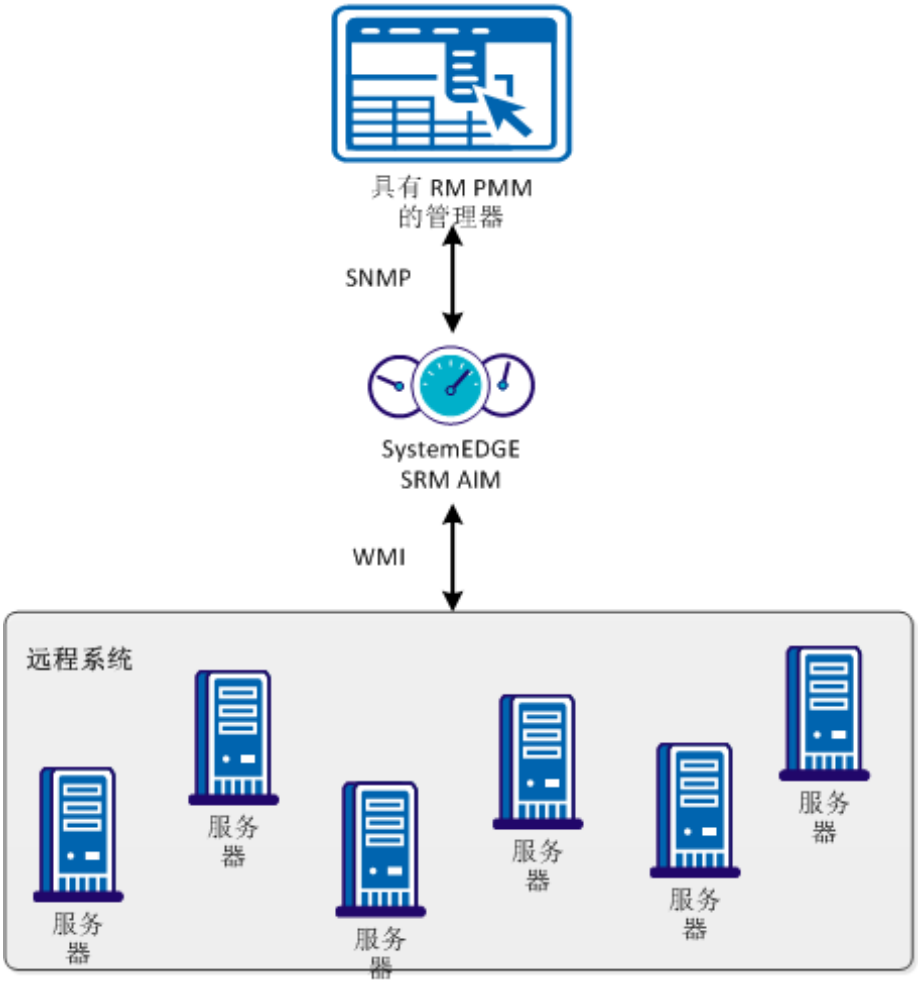
体系结构

下图提供主要的 RM 组件的概述。

一个或多个 RM AIM 通过基于 DCOM/RPC 的 WMI 对 Windows 服务器执行监控。在特定的站点或子网内，需要从 AIM 到受监控 Windows 服务器的直接 TCP 连接。AIM 通过部署组件部署。

平台管理模块 (RM PMM) 向管理器基础架构提供接口，并且在 CIM 对象模型中创建受管对象。PMM 使用 SNMP 与 RM AIM 进行通信。

远程监控组件之间的交互

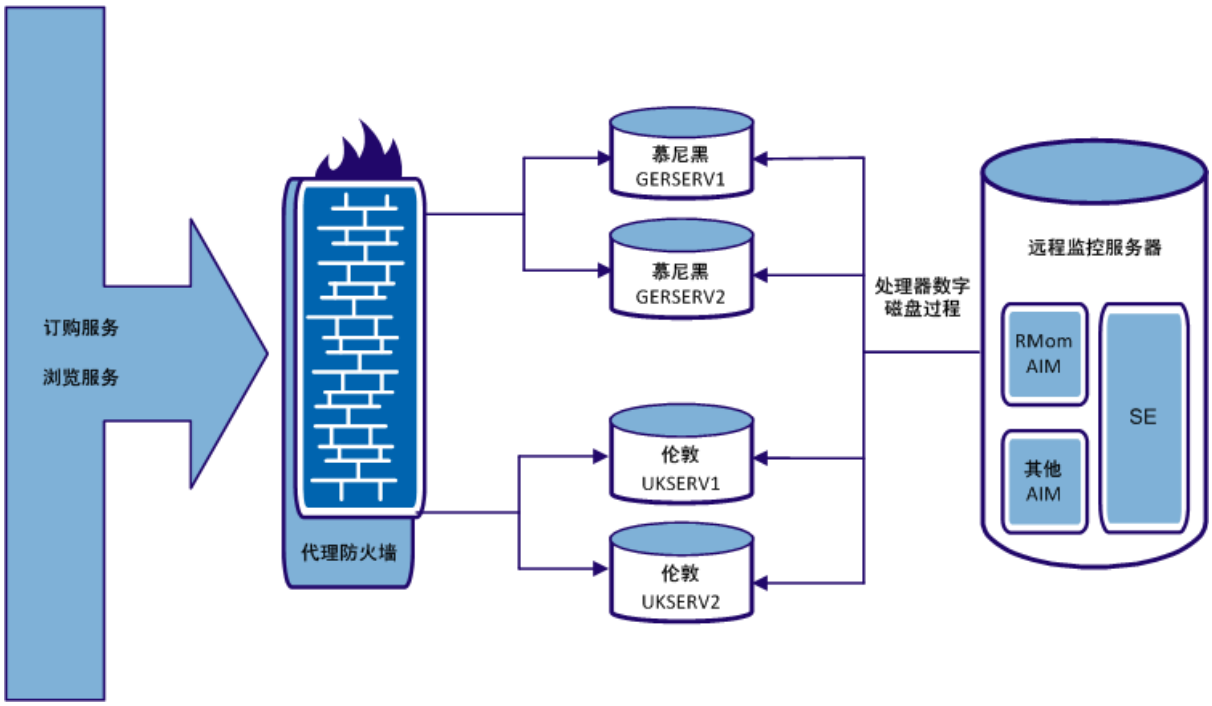


用例方案

考虑以下用于远程监控的用例方案。某企业提供 Web 书店，该书店包含两种服务：订购图书和浏览图书。

- 慕尼黑的两台服务器和伦敦的一台服务器可以提供订购服务
- 伦敦的两台服务器和慕尼黑的一台服务器可以提供浏览服务

慕尼黑的服务器为 GERSERV1 和 GERSERV2，伦敦的服务器为 UKSERV1 和 UKSERV2。它们配置用于负载平衡和故障切换。



对服务的监控取决于该服务是订购服务还是浏览服务。在该示例中，定义了两个配置集（每个服务类型一个）。它们包括以下信息的查询和监视器：

- CPU

  CPU 总空闲时间百分比。

- FSys

  逻辑磁盘的可用空间对于各服务类型很重要（C: 用于订购服务，D: 用于浏览服务）。

- Proc

  订购进程的工作集大小（单个进程 order.exe）或所有浏览进程的工作集大小的总和（进程组浏览）。

对于每个受监控的系统，根据服务角色（订购、浏览，或两者），将分配以下配置集：

SystemName	ConfigSet
GERSERV1	顺序 浏览
GERSERV2	顺序
UKSERV1	顺序 浏览
UKSERV2	浏览

配置先决条件

在配置远程代理之前，验证是否满足以下先决条件。

- RM 系统的防火墙和端口要求

  RM AIM 系统通过 WMI 连接访问 RM 系统。WMI 使用 DCOM 通信，该通信使用 End Point Mapper (EPMAP) Port TCP (135) 和 EPMAP 动态标识的 DCOM TCP 端口。

  要简化配置，RM AIM 必须位于与 RM 系统相同的防火墙边界内。

  注意：有关使用固定端口的详细信息，请在 Microsoft MSDN 网站上搜索文章“为 WMI 设置固定的端口”。

- 管理器系统的防火墙和端口要求

  RM AIM 利用由 SystemEDGE 提供的 SNMP 基础架构；它不需要其他端口。

  RM 配置通过 SNMP 执行。因为配置数据包括密码，所以 RM 使用密码加密。

- SystemEDGE 端口和 SNMP

  管理器系统通过 SNMP 访问 SystemEDGE 系统，这要求在 SystemEDGE 系统上打开 SNMP 端口（UDP 161 传入）。SystemEDGE 系统发送 SNMP 陷阱（UDP 162 传出）。

- SystemEDGE 端口和基于策略的配置

  管理器系统通过 CAM 访问 SystemEDGE 系统，这要求在 SystemEDGE AIM 系统上打开 UDP (4104) 或 TCP (4105) 端口。SystemEDGE AIM 系统使用 CAM 将消息发送到管理器系统。

- WMI 访问最佳实践

  RM AIM 使用 WMI 连接到 RM 系统并需要凭据。作为最佳实践，RM 系统必须是 AD 域的成员（例如，RIVER）。通过该成员身份，您可以使用域帐户，并且不需要在每个 RM 系统上定义本地用户帐户。创建作为 AD 域的 Domain Admins 组成员的 CARMuser 域帐户。

  在 RM 安装期间提示进行用户凭据设置时，向域帐户（例如，RIVER\CARMuser）提供密码。对于该域的任何系统成员，无需其他配置。

  注意：如有需要，可以限制 CARMuser 访问权限，使用户不是 Domain Admins 组的成员。在这种情况下，配置 WMI 命名空间访问和 DCOM 访问。有关定义 WMI 命名空间访问和 DCOM 访问的详细信息，请参阅 Microsoft 网站。

配置远程监控系统

配置集是分配给 RM 系统的实体；它定义收集哪些度量标准（WQL 查询）以及如何监控这些度量标准。

配置集包括若干配置项。配置项包括度量标准定义（WQL 查询）和监控定义（阈值、重要级别等）。

RM 为以下配置集提供自带度量标准和监控定义：

- 默认
- 扩展
- metricDisk
- metricFS
- metricNet

如果必须为具有不同阈值和重要级别设置的 RM 系统监控不同的度量标准，请克隆自带的配置集，并调整已克隆的集以满足系统特定的监控需求。

下表列出了 RM 度量标准和这些度量标准所属的配置集。

量度	配置集
CPU_PercentIdle	默认
Disk_PercentIdle	默认
Event_SystemErrors	默认
FSys_FreeMB	默认
FSys_FreeMBDecrease	默认
Mem_PercentUsed	默认
Net_MACAddress	默认
Net_MACIndex	默认
Net_QueueLength	默认
Proc_PercentCPU	默认
Proc_PercentMemory	默认
Srvc_StoppedAuto	默认
Sys_LastBootTime	默认
Sys_LastLocalTime	默认
Sys_OSInfo	默认
Sys_PhysMemKB	默认
Disk_ReadPerSec	扩展
Disk_WritePerSec	扩展
Disk_QueueLength	扩展

量度	配置集
Mem_FreeMB	扩展
Mem_FreePages	扩展
Mem_NonPagedMB_3GB	扩展
Mem_PagedMB	扩展
Mem_PagedMB_3GB	扩展
Mem_PagingPerSec	扩展
Mem_NonPagedMB	扩展
Net_PercentBusy	扩展
Sys_Is64bit	扩展
Sys_Has3GBSwitch	扩展
Sys_OSType	扩展
BIOS_Version	扩展
BIOS_SerialNumber	扩展
Disk_AvgDiskBytesPerRead	metricDisk
Disk_AvgDiskBytesPerWrite	metricDisk
Disk_AvgDiskReadQueueLength	metricDisk
Disk_AvgDiskWriteQueueLength	metricDisk
Disk_DiskWritesPersec	metricDisk
Disk_PercentDiskReadTime	metricDisk
Disk_PercentDiskWriteTime	metricDisk
Disk_SplitIOPerSec	metricDisk
Net_PacketsOutboundErrors	metricNet
Net_PacketsReceivedErrors	metricNet
Net_PacketsReceivedDiscarded	metricNet
Net_PacketsReceivedNonUnicastPersec	metricNet
Net_PacketsReceivedUnicastPersec	metricNet
Net_PacketsSentNonUnicastPersec	metricNet
Net_PacketsSentUnicastPersec	metricNet
FSys_PercentFreeSpace	metricFS

注意：有关 RM 度量标准的详细信息，请参阅*《性能度量标准参考》*。

创建配置集

远程监控提供了若干即用型配置集，不应对其进行任何更改。使用“配置集”页面创建自定义配置集以满足您的需求。

创建配置集

1. 单击 +（新建）。

   此时将显示“单个配置集的详细信息”窗格。

2. 输入新配置集的名称、输入描述，并突出显示要包括在新集中的配置集（按下 Ctrl 键突出显示多个条目）。

3. 单击“保存”。

   新配置集已添加到“配置集”列表中。

注意：您还可以使用“操作”下拉列表来克隆和删除自定义配置集。

支持远程监控度量标准

CA Virtual Assurance 根据默认配置集中的固定 RM 度量标准集收集度量标准并生成报表。

因此，将默认配置集（或包含这些度量标准的配置集或组集）分配给要为其使用报表的所有系统。

支持的默认配置集度量标准如下：

- CPU_PercentIdle
- Disk_PercentIdle
- Event_SystemErrors
- Mem_PercentUsed
- FSys_FreeMB
- Fsys_FreeMBDecrease
- Net_QueueLength
- Proc_PercentCPU
- Proc_PercentMemory
- Srvc_StoppedAuto

使用远程监控管理系统

通过在“资源”窗格中突出显示受管资源，然后单击“远程监控”，可访问管理系统所必需的 RM 信息和设置。通过“远程监控”页面可以执行以下操作：

- 添加要监控的远程系统
- 管理查询
- 管理凭据设置
- 创建配置集
- 管理配置条目

对于显示板，以下 RM 模块可用：

- CA SystemEDGE 计算机状态
- CA SystemEDGE 对象状态

添加要监控的远程系统

使用“系统”页面来输入要远程监控的系统的系统信息。

添加系统

1. 单击 +（新建）。

   此时将显示“新建”窗格。

2. 在“RM 系统名称”字段中输入您要远程监控的系统的名称并编辑以下设置（如有必要）：

   RM 系统名称

   指定 RM 系统的名称。使用用户界面，您只能以 FQDN 表示法输入 RM 系统名称，例如“vm1234.ca.com”。使用“rmonwatch”实用工具，您还可以按照简称或 IP 地址指定 RM 系统名称。

   状态

   指定系统是活动的还是处于维护中。

   协议

   指定协议是 DCOM 还是 SOAP。

   最大实例数

   指定实例表中由任何系统查询创建的实例的最大数目。

凭据

指定远程系统的用户凭据。

配置集

指定将为远程系统收集的配置集（或度量标准组）。

3. 单击“保存”。

已将系统添加到您正远程监控的系统的列表中。

查看查询结果

您可以使用“查询”页面查看与 RM 系统相关联的查询结果。

通过“查询”页面，您可以执行以下操作：

- 查看详细的查询结果和设置（突出显示“查询”表中的查询并选择“结果”或“设置”）。
- 基于系统、状态、配置集或特定查询筛选查询结果（使用望远镜显示或隐藏查询筛选器）。
- 管理查询表中显示的信息(单击列标头对列进行升序或降序排列及添加或删除列）。

管理凭据设置

您可以使用“凭据”页面来管理与 RM 系统相关联的单个凭据的设置。

通过“凭据”页面，您可以执行以下操作：

- 添加凭据（使用“新建” (+) 图标，在“单个凭据的详细信息”窗格中输入设置，然后单击“保存”）。
- 删除凭据（突出显示现有的凭据，然后单击 (-) 图标）。
- 编辑凭据（突出显示现有的凭据，在“单个凭据的详细信息”窗格中更新设置，然后单击“保存”）。

管理配置条目

使用“配置条目”页来查看和管理与查询相关联的配置设置。

查看或管理配置设置

1. 突出显示“配置条目”表中的查询。使用显示和隐藏筛选器图标（望远镜），您可以针对配置集、重要级别、查询类以及升级重要级别对条目应用筛选器。

   此时将显示“单个配置条目的详细信息”窗格。

2. 查看或更新以下值，然后单击“保存”。

索引

为配置集中的该配置条目指定唯一索引。

查询名称

指定查询的名称（不能包括“.”符号）。

您可以在不同的配置集中使用相同的查询名称；但是，将多个配置集应用于一个系统时，必须确保所有查询名称的唯一性。如果将限定符设置为固定条目，则无法重命名查询。

说明

指定配置条目的描述信息。

间隔

指定连续执行该查询以及评估该监视器的间隔（以秒为单位）（该值必须是 30 秒的倍数）。

查询类

指定配置条目的查询类。

查询范围

指定要应用于查询的范围。

查询属性

指定查询类的属性。

配置集

指定配置集的名称（不要使用“,”）。

查询取决于

指定查询 (Q2) 依赖于另一个查询 (Q1)；因此仅基于 Q1 的结果创建 Q2。

限定符

指定与配置的查询和监视器相关的其他信息。

可能的值如下：

- 条目无法删除，查询名称无法更改（固定条目）
- 查询仅执行一次（至少一次成功）
- 如果不成功，将不再执行查询
- 查询不显示在查询表中

- 结果按实例显示
- 结果显示以前值，而不是当前值
- 结果显示增大的增量值
- 结果显示减少增量值
- 将具有相同对象数据和重要级别的监视器聚合为 AND 关系

查询总计

指定要应用为 Total 引用的查询类的属性。

查询比例

指定适用于属性值的比例，例如 *100/1024 或/1024*100，该比例用作查询表中查询比例的默认值。查询属性的值乘以或除以该比例后，才会存储在结果属性中。

查询实例

指定用于实例表中实例命名的查询类的属性。

条件

指定将结果属性值与阈值和升级阈值进行比较的条件。

阈值

指定结果属性值所比较的阈值。

重要级别

指定如果满足阈值条件，要用于 SysEDGE 对象状态模型的重要级别。

对象 类

指定要用于 SysEDGE 对象状态模型的类名称（不要使用“*”）。

对象 实例

指定要用于 SysEDGE 对象状态模型的实例名称（不要使用“*”）。

对象 属性

指定要用于 SysEDGE 对象状态模型的属性名称（不要使用“*”）。

延迟

指定要使 SysEDGE 对象状态模型中的状态更改，阈值（升级）条件必须满足的次数。

升级 增量

指定与表示升级条件所需的阈值的差。

升级 重要级别

指定如果满足升级条件，要用于 SysEDGE 对象状态模型的重要级别。

结果

指定要使用 SysEDGE 监视器监视的、查询表或实例表中该查询的结果属性。

更新配置设置以反映任何更改。

第 9 章： 安装和配置 Active Directory 和 Exchange Server AIM

此部分包含以下主题：

简介

通过 Active Directory 和 Exchange Server (ADES) AIM，您可以监控 Active Directory 和 Exchange Server 环境的运行状况以及关键性能指标 (KPI) 度量标准。ADES AIM 功能包括：

- 监控邮箱服务器的消息记录管理器、逻辑磁盘使用情况以及逻辑磁盘读取/写入。
- 监控集线器传输服务器的网络延迟、队列、邮件发送度量标准、逻辑磁盘使用情况以及逻辑磁盘读取/写入。
- 监控 Active Directory 性能、复制、逻辑磁盘使用情况以及逻辑磁盘读取/写入。

ADES AIM 收集以下数据用于监控：

- 来自 Active Directory 和 Exchange Server 的配置数据
- 来自 Active Directory 和 Exchange Server 的性能数据

ADES AIM 可扩展性

当计划 ADES AIM 部署时，请考虑以下对基础架构规模和系统性能有影响的关键因素：

- ADES AIM 的可用内存，不包括操作系统和其他应用程序使用的内存：
  - 具有 1-GB 可用内存的主机可以监控 20 个主机（2 个 Active Directory 主机和 18 个 Exchange 主机）。
  - 具有 2-GB 可用内存的主机可以监控 40 个主机（6 个 Active Directory 主机和 34 个 Exchange 主机）。
  - 具有 3-GB 可用内存的主机可以监控 60 个主机（10 个 Active Directory 主机和 50 个 Exchange 主机）。
- 环境的地理分布：
  - 当 ADES AIM 处于邻近地理位置时，它将减少发现和轮询环境的时间。
  - 高延迟或数据包丢失可能导致 AIM 无法获取所有所需的数据。

注意：大小信息是部署需求的大约估计值，并且它不是决定性的。大小信息会根据监控环境而变化。

安装 ADES AIM

完成以下任务以安装 ADES AIM：

1. 安装 CA SystemEDGE r11.6 代理和 CA Advanced Encryption r11.6。
2. 使用以下方法之一安装 ADES AIM：
   - 通过 CA Virtual Assurance 远程部署进行部署。
   - 通过命令模式手工安装。
3. 通过指定要监控的域来配置 ADES AIM：

注意：

- 当使用带有 ADES 管理器的 CA Spectrum 时，不要将 SpectroSERVER 安装到管理 ADES AIM 主机的主机上。此外，ADES AIM 必须是安装在 SystemEDGE 主机上的唯一 AIM。
- 在 Windows 主机上安装 SystemEDGE 和 ADES AIM（该主机是其中一个域中的成员服务器，并与其他域存在信任关系）。
- SystemEDGE 代理和 ADES AIM 主机必须没有任何 Active Directory 或 Exchange Server 角色。

使用远程部署来部署 ADES AIM

创建软件作业，以便使用 CA Virtual Assurance 远程部署在主机上安装 ADES AIM。

遵循这些步骤:

1. 登录到 CA Virtual Assurance 应用程序并转到管理视图。
2. 在“资源”选项卡中查找要部署 ADES AIM 的主机。
3. 创建作业并选择平台类型为 Windows，随后将显示可用的打包程序软件包。

   创建作业时在打包程序软件包中指定以下参数：

   用户

   定义没有完全限定域名 (FQDN) 的域管理员的名称。例如 adminuser。

   密码

   定义用户密码。

   域名

   定义通过 ADES AIM 监控的域的名称。输入 FQDN。

   管理实体

   基于技术指定要管理的主机。

   0

   仅监控 Active Directory 主机。

   1

   仅监控 Exchange Server 主机。

   2

   监控 Active Directory 和 Exchange Server 主机。

管理模式

指定要管理的主机。

0

自动在管理实体定义的域中发现并监控所有主机（基于域的管理）。

注意：不会自动监控子域的主机。

1

发现域中的所有主机，但是只监控通过管理器配置的主机（基于主机的管理）。

4. 选择必需的软件包并将它们部署到主机上。

   从作业面板验证作业状态。如果作业失败，再次重新部署软件包。

注意：有关详细信息，请参阅如何部署 SystemEDGE 和 AIM (p. 113)。

在命令模式下安装 ADES AIM

在命令模式下安装会在不使用远程部署的情况下将 ADES AIM 安装到主机上。

注意：确认在您安装 ADES AIM 之前，CA SystemEDGE r11.6 和 CA Advanced Encryption r11.6 已安装在主机上。

遵循这些步骤:

1. 转到 *DVD1*\Installers\Windows\Data\SysMan，然后将以下 zip 文件复制到您的本地磁盘：
   - CA_SystemEDGE_ESAD-Windows.zip
   - CA_SystemEDGE_ESAD-Windows-metadata.zip
2. 解压缩复制到本地磁盘的 zip 文件。解压缩位置中提供了以下文件：
   - caesadaimx64.msi
   - ca-setup.exe
   - ca-setup.dat
3. 打开命令提示符窗口并转到 *Extracted_Path*\CA_SystemEDGE_ESAD\5.8.0\ENU\Windows_x64。
4. 运行 ca-setup.exe 以安装 ADES AIM。此命令具有以下格式：

```
ca-setup EULA_ACCEPTED="[yes|no]"
CASE_ESAD_DOMAIN_NAME="domain_name"
CASE_ESAD_DOMAIN_USER_NAME="username@fqdn"
CASE_ESAD_DOMAIN_PWD="password"
CASE_ESAD_MANAGEMENT_ENTITY="[0|1|2]"
CASE_ESAD_MANAGEMENT_MODE="[0|1]"
```

EULA_ACCEPTED="[*yes*|*no*]"

指定是否接受该许可。

CASE_ESAD_DOMAIN_NAME="*fully_qualified_domain_name*"

指定通过 ADES AIM 监控的域的完全限定名称。

CASE_ESAD_DOMAIN_USER_NAME="*username@fqdn*"

指定具有域管理员和 Exchange 组织管理员或组织管理权限的用户名。

CASE_ESAD_DOMAIN_PWD="*password*"

指定该用户的密码。

CASE_ESAD_MANAGEMENT_ENTITY="[*0*|*1*|*2*]"

基于技术指定要管理的主机。

0

仅监控 Active Directory 主机。

1

仅监控 Exchange Server 主机。

2

监控 Active Directory 和 Exchange Server 主机。

CASE_ESAD_MANAGEMENT_MODE="[*0*|*1*]"

指定要管理的主机。

0

自动在管理实体定义的域中发现并监控所有主机（基于域的管理）。

注意：不会自动监控子域的主机。

1

发现域中的所有主机，但是只监控通过管理器配置的主机（基于主机的管理）。

5. 重新启动 SystemEDGE 服务以运行 ADES AIM。

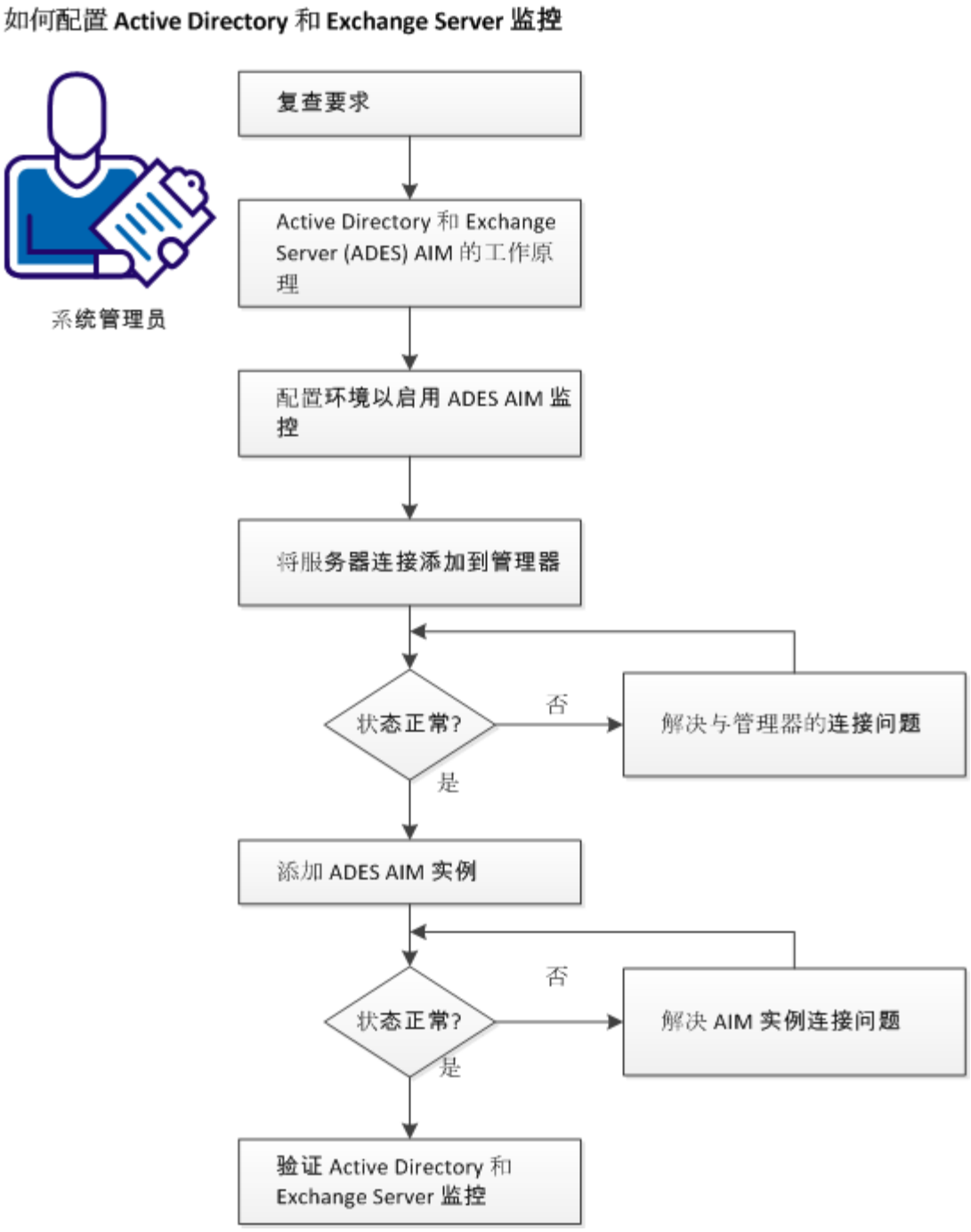
示例

以下示例显示了如何在主机上安装 ADES AIM 以及如何监控域 mydomain.com。

```
ca-setup EULA_ACCEPTED="yes"
CASE_ESAD_DOMAIN_NAME="mydomain.com"
CASE_ESAD_DOMAIN_USER_NAME="adminuser@mydomain.com"
CASE_ESAD_DOMAIN_PWD="domainpass123" CASE_ESAD_MANAGEMENT_ENTITY="2"
CASE_ESAD_MANAGEMENT_MODE="0"
```

如何配置 Active Directory 和 Exchange Server 监控

下图提供了有关配置管理组件所需操作的概述。该图包括针对连接问题的相应故障排除策略。



请执行以下步骤：

要求

安装和配置 ADES AIM 需要以下先决条件：

常规要求

- 具备通过 CA Virtual Assurance 发现服务器和部署软件包的知识。
- 必需的权限：
  - 具有远程部署权限的用户帐户。
  - 具有在主机上手工安装的本地管理员权限的用户帐户。
  - 用于监控域的域管理员和 Exchange 组织管理员或 Exchange 组织管理权限。

    注意：请验证域管理员和 Exchange 组织管理员权限已分配到相同的用户。

软件要求

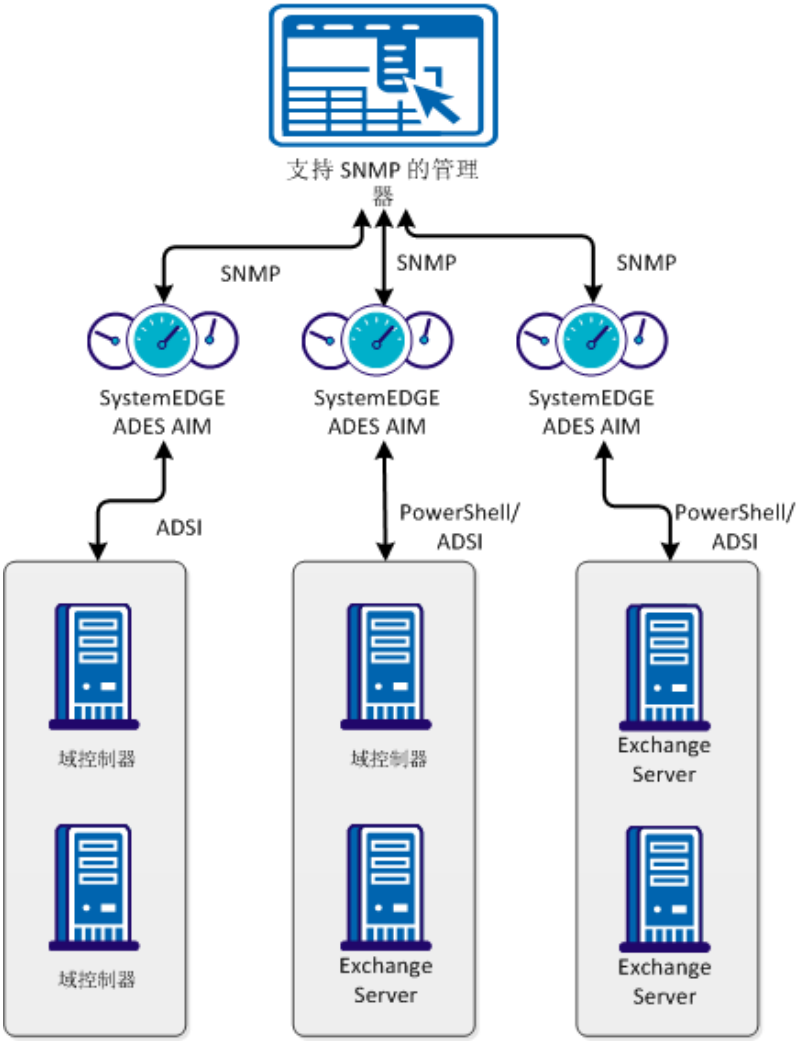
- ADES AIM 主机支持的操作环境：
  - Windows 2008 Server SP2
  - Windows 2008 R2 SP2 x64
- 支持的域控制器操作环境：
  - Windows 2008
  - Windows 2008 R2
- 支持的 Exchange Server 版本：
  - Exchange 2007 SP3
  - Exchange 2010 SP2

  注意：
  - 不支持监控 Exchange 2003 主机。
  - 不支持在整个林中监控 Exchange 2007 主机。
- 必需的应用程序：
  - .Net 3.5 或更高版本
  - Windows PowerShell 2.0
  - 用于监控 Exchange 2007 主机的 Exchange 2007 Management Tools SP3
  - CA SystemEDGE 版本 r11.6 和 CA Advanced Encryption r11.6

Active Directory 和 Exchange Server AIM 的工作原理

下图说明了 ADES AIM 体系结构：

Active Directory 和 Exchange Server 管理组件之间的交互



以下过程说明了 ADES AIM 的工作方式：

1. ADES AIM 通过搜索域控制器发现主机。ADES AIM 收集有关以下内容的信息：
   - Active Directory 服务器角色，如域控制器和全局目录。
   - Exchange Server 角色，如集线器传输、邮箱和客户端访问服务器。

   注意：统一的消息和边传输角色不支持监控。

2. 当发现主机时，AIM 将发送消息，以便从以下项收集数据：
   - 使用 ADSI 调用的域控制器
   - 使用 PowerShell 命令的 Exchange Server
3. AIM 将针对 SystemEDGE 代理接收数据并更新 MIB 表。
4. 管理器（如 CA eHealth 和 CA Spectrum）将轮询 SystemEDGE 主机并收集要显示的数据。
5. AIM 将持续轮询受管主机（为监控设置的 Active Directory 和 Exchange Server 主机）并更新其 MIB 表。

配置环境以启用 ADES AIM 监控

在 Exchange 主机上应用 PowerShell 配置设置，以启用 ADES AIM 来监控域。

注意：在开始监控之前配置每个 Exchange Server。

遵循这些步骤:

1. 依次选择“开始”、“程序”、“附件”、“Windows PowerShell”、“Windows PowerShell (x86)”。

   此时将显示 Windows PowerShell 命令提示符。
2. 运行以下命令以通过 WinRM 服务远程管理主机：

   ```
   Enable-PSRemoting
   ```

   WinRM 设置启动远程管理，并创建 WinRM 侦听程序以接受 WS-Man 请求。
3. 运行以下命令以将主机添加到信任的主机列表中：

   ```
   Set-Item WSMan:Localhost\Client\TrustedHosts -Value * -Force
   ```
4. 运行以下命令以重新启动 WinRM 服务：

   ```
   Restart-Service WinRM
   ```

   TrustedHosts 设置已更新，并且 Exchange Server 可用于监控。

将域服务器或 Exchange Server 添加到管理器中

可以使用用户界面将 Microsoft Active Directory 域控制器或 Exchange Server 连接添加到管理器中。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。

2. 从左侧窗格中的“开通”部分选择 Microsoft Active Directory 和 Exchange Server。

3. 在“服务器”窗格工具栏上单击  （添加）。

   此时将显示“添加服务器”对话框。

4. 输入所需的连接数据（服务器名称、用户、密码、模式、技术），指定首选 AIM，启用“受管状态”。

5. 单击“确定”。

   CA Virtual Assurance 验证提交的连接数据，并且尝试与服务器建立连接。

   如果网络连接成功建立，服务器会添加到右上窗格中并带有绿色状态图标。

   注意：如果连接失败，将显示“验证失败”对话框。如果您单击“是”，CA Virtual Assurance 会将服务器添加到列表中，该服务器带有指示连接失败的红色状态图标。如果您单击“否”，将不添加任何内容。

服务器连接到管理器失败

症状：

在“管理”、“配置”下添加服务器连接后，对服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的服务器连接数据是否仍然有效。如有必要，请更新连接数据。
- 验证服务器系统是否正在运行并且可以访问。
- 验证服务器系统中的管理服务是否正常运行。

更新服务器连接数据：

1. 单击与失败的连接关联的 （添加）或 （编辑）。
2. 添加连接详细信息，启用“受管状态”，然后单击“确定”。

   将更新连接数据。
3. 单击右上角的 （验证）以验证新设置。

   如果无法建立与服务器的连接，请继续执行下一个步骤。

验证服务器系统是否正在运行并且可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```
2. 验证命令的输出，以确定服务器是否具有有效的 DNS 条目和 IP 地址。

   如果服务器不在 DNS 中，请将服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。
3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress <Server Name>
   ```

   输入正确的 IP 地址和服务器名称。例如：

   ```
   192.168.50.50 myServer
   ```
4. 单击右上角的 （验证）。

   即使服务器凭据和连接数据正确并且您可以 ping 服务器，连接仍然可能失败。在这种情况下，可能是服务器引起该问题。如果无法建立与服务器的连接，请继续执行下一个步骤。

验证服务器系统中的管理服务是否正常运行：

1. 联系管理员来访问服务器系统。
2. 登录到服务器系统，从“开始”菜单中打开“管理工具”、“服务”。

   将打开“服务”窗口。
3. 选择服务并启动或重新启动服务。
4. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“服务器”窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证服务器连接。

   如果与服务器的连接失败，请验证根据该方案的要求收集的数据是否有效。

   与管理员或技术支持合作，解决服务器连接问题。

添加 ADES AIM 实例

将 Active Directory 和 Exchange Server 连接添加到 CA Virtual Assurance 管理器后，请添加 AIM 实例以管理环境。

遵循这些步骤:

1. 从“开始”菜单打开 CA Virtual Assurance 用户界面。依次单击“管理”、“配置”。

   此时将显示“配置”页面。
2. 从左侧窗格中的“开通”部分选择 Microsoft Active Directory 和 Exchange Server。

3. 在“AIM 服务器”窗格工具栏上单击  （添加）。

   此时将显示“添加 AIM 服务器”对话框。

4. 从下拉列表中选择 AIM 主机。

   将显示发现的 AIM 主机的列表。

5. 从下拉列表中选择服务器。

   CA Virtual Assurance 使用“服务器”窗格中列出的 GalaX 服务器填充服务器下拉列表。您只能管理 CA Virtual Assurance 管理器与之建立了有效连接的服务器。

   注意：如果 AIM 位于远程系统中，则 CA Virtual Assurance 一定会首先发现该系统。在发现之后，AIM 服务器将在下拉列表中显示。

6. 单击“确定”。

   将添加选定服务器的新 AIM 实例。如果实例未处于错误或已停止状态，CA Virtual Assurance 将开始发现关联的环境。发现过程完成时，您可以开始监控您的 Active Directory 和 Exchange Server 环境。

排除 AIM 实例连接的故障

如果 AIM 连接处于未就绪状态，将出现以下状态图标之一：

 发现正在进行

 无轮询

 错误

 警告

 已禁用

 未知

有关 AIM 实例状态的详细信息，请参阅工具提示。以下故障排除部分提供了用于解决该问题的详细信息和步骤。

AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为服务器添加 AIM 实例后，状态图标显示  （发现正在进行）。

解决方案：

等到环境的发现过程完成。发现持续时间取决于与环境中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示指示未完成发现请求数量的工具提示。发现作业完成时，CA Virtual Assurance 会向资源树中添加一个服务器文件夹。然后，您可以开始管理您的环境。

AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （无轮询）。

解决方案：

关联实例不需要特定的操作。此图标表示 CA Virtual Assurance 管理器不轮询此 AIM。AIM 不是首选。

如果多个 AIM 已配置为管理特定服务器，PMM 将选择其中一个 AIM 作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下添加 AIM 实例后，状态图标显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决可能导致与 AIM 连接失败的最常见问题：

- 验证是否可以访问 AIM 服务器。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   ping servername
   ```

2. 确认命令的输出对于 AIM 服务器有有效的 DNS 条目和 IP 地址。

   如果 AIM 服务器不在 DNS 中，则将 AIM 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress servername
   ```

   输入正确的 IP 地址和 AIM 服务器名称。例如：

   ```
   192.168.50.51 myAIM
   ```

4. 在“AIM 服务器”窗格的右上角，单击 （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“AIM 服务器”窗格，并单击右上角的 （验证）。

   CA Virtual Assurance 将验证 AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否有效。

AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 AIM 实例之后，几个实例的状态图标显示  （已禁用）。该 AIM 实例未受管理。

如果 CA Virtual Assurance 发现具有以下关系的 AIM，则显示该状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的服务器配置了 AIM。
- AIM 连接到未配置的服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的服务器连接并将其受管状态更改为已启用。

验证 Active Directory 和 Exchange Server 监控

成功配置后，CA Virtual Assurance 开始监控 Active Directory 和 Exchange Server。在用户界面中监控 Active Directory 和 Exchange Server 事件。

（可选）使用节点配置实用工具配置 ADES AIM

使用 NodeCfgUtil 而不是用户界面，是 ADES AIM 的备选配置方式。通过配置 ADES AIM，您可以添加、修改或删除 ADES AIM 管理的一个或多个域。NodeCfgUtil 将为 ADES AIM (esad.cfg) 创建配置文件，它位于 *SystemEDGE_InstallPath*\plugins\AIPCommon 目录中。

遵循这些步骤:

1. 打开 Windows 资源管理器并导航到 *SystemEDGE_InstallPath*\plugins\AIPCommon 目录。
2. Start NodeCfgUtil.exe.
3. 根据您的选择输入选项。您可以添加、修改或删除域。例如，输入 1 以添加新的受管节点。
4. 在“选择受管节点”屏幕上输入与 ADES AIM 相对应的编号。例如，输入 1 以选择 ADES AIM。
5. 按照屏幕指示完成配置。每个域均需要用于身份验证的有效用户名和密码，以及适当的管理实体和管理模式。
6. 当配置完成后，输入 0 以保存配置并退出该实用工具。
7. 重新启动 SystemEDGE 服务以应用更改。

示例

以下示例显示了已成功添加到 ADES AIM 配置的 mydomain.net 的“安装受管节点”对话框。“管理实体”设置为“Active Directory”。“管理模式”设置为基于域。

**** 选择受管节点 ****

1. Microsoft Active Directory 和 Exchange Server

0. 返回上一个菜单

****

输入选择：1

输入 Microsoft Active

Directory 和 Exchange Server 节点的以下信息...

（要在任一点回到上一个菜单，请按“CTRL Q”）

1. 域名 (FQDN)：mydomain.com

2. User Name(Example:adminuser@domain.com): administrator@mydomain.com

3. 密码：**********

4. 管理实体（0 - 仅 AD、1 - 仅 Exchange、2 - AD 和 Exchange）：0

5. 管理模式（0 - 基于域/自动、1 - 基于主机/手工）：0

CAAC1016 正在身份验证，请稍候...

CAAC1019 身份验证成功。

CAAC1023 添加节点成功。

按任意键继续。。。

卸载 ADES AIM

卸载代理将从主机中删除代理及其关联的配置数据。

遵循这些步骤:

1. 使用 SystemEDGE 控制面板停止 SystemEDGE 进程。
2. 依次选择“开始”、“控制面板”、“程序”、“程序和功能”。

   此时将打开“卸载或更改程序”窗口。
3. 右键单击 Exchange Server 和 Active Directory 组件的 CA AIM 并选择“卸载”。

   将显示一条确认消息。
4. 单击“是”。

   ADES AIM 组件已删除。验证 ADES AIM 组件不再显示在“添加/删除”控制面板中。

故障排除

详细信息：

AIM 不活动并且不收集数据 (p. 590)
未监控一个或多个域 (p. 590)
未监控某些计数器 (p. 591)
未监控某些主机 (p. 591)

AIM 不活动并且不收集数据

症状

AIM 不活动并且无法收集数据。

解决方案

验证以下各项：

- caesadaim.exe 进程正在运行。
- 为每个配置的域在 AIM 目录中创建了域的日志文件。

如果进程未运行或日志文件未创建，请重新启动 SystemEDGE 服务。

如果重新启动 SystemEDGE 服务后 AIM 未运行，请验证以下要求并采取相应的操作：

- .NET 3.5 SP1 Framework 已安装在 AIM 主机上。
- Exchange Management Tools 2007 SP3 已安装在与 AIM 相同的主机上（如果域包含一个或多个 Exchange 2007 服务器）。

未监控一个或多个域

症状

ADES AIM 未监控一个或多个域。

解决方案

- 验证是否已在 ADES AIM 文件夹中为每个受监控的域创建了日志文件，名为 domain_AIM.log。如果未创建日志文件，请验证是否使用 nodecfgutil.exe 将域配置为监控。
- 如果为域创建了日志文件，请打开日志文件并查找以下错误消息：

  指定的域不存在或无法联系。

  如果日志文件中存在此消息，请验证 ADES AIM 主机和域控制器之间的通信是否被阻止。当可以从 ADES AIM 主机访问域控制器时，通过 CA Spectrum 启动 AIM 的发现。

未监控某些计数器

症状

未监控某些性能计数器。

解决方案

重新启动 ADES AIM 中的发现，以便在不存在计数器的主机上创建计数器。

注意：仅当主机上提供所需的配置或实例时，才会监控特定配置的性能计数器。

未监控某些主机

症状

未监控域中的所有 Active Directory 或 Exchange Server 主机。

解决方案

验证以下配置：

- 在域模式或主机模式中配置了 AIM。

  注意：在主机模式中，使用 CA Spectrum 或 MIB 浏览器更改通用主机表中的每个主机的管理状态。

- AIM 使用管理实体进行配置，以便仅监控 Active Directory 主机或仅监控 Exchange Server 主机。针对 ADES AIM，使用 NodeCfgUtil 将域的“管理实体”选项值更改为 2，以便同时监控这两项技术。

第 10 章： 使用规则和操作

此部分包含以下主题：

规则和操作

要配置规则和操作，您必须首先了解其具体含义以及它们相互之间以及与其他组件之间的交互方式。通过了解这些交互，可以针对如何通过设置规则和操作来高效管理数据中心做出最佳决策。

CA Virtual Assurance 收集和分析度量标准，然后根据有关如何分布资源的分析做出智能决策。例如，如果 CA Virtual Assurance 确定服务器或服务使用过度或使用不足，则可开通新计算机。

在服务器级别和服务级别监控使用情况。服务器级别监控涉及特定服务器的诊断问题，只使用关键性能指示器。服务级别监控诊断服务的整体问题，将总体使用情况用作性能指示器。

可在服务器级别或服务级别创建规则。创建规则以评估性能度量标准和生成的事件。规则由单个条件或条件的组合组成，这些条件必须在总体上计算为 true 状态，才能执行操作。您可以创建自己的规则，也可以选择一组规则模板来使用自动化策略生成规则。

注意：有关性能度量标准和说明的列表，请参阅*《性能度量标准参考》*。

默认情况下，按照数据中心级别的收集设置中定义的记录间隔（默认值 = 300 秒）评估规则，或在由于被监控的度量标准值而发生事件时评估规则。如果要设置与数据中心不同的时间间隔，可以配置特定服务器以覆盖默认的数据中心记录间隔。服务器级别规则按照配置的服务器级别记录间隔进行评估。服务级别规则按照该服务内的所有服务器中最短的记录间隔进行评估。当您更改记录间隔时，请停止并重新启动策略管理器服务，以检索更新的间隔并将其用于规则评估。

度量标准是评估数据的来源。当度量标准规则计算为 true 时，将触发操作。必须超过延迟，规则才会计算为 true。在某些情况下，您可能希望一次违反规则即触发操作，因此您会将延迟设置为一，但在其他情况下，您可能不希望一次事件触发规则。

例如，CA Virtual Assurance 与 CA SDM 集成，后者是一个客户支持应用程序，管理呼叫、跟踪问题解决、共享公司知识库以及管理 IT 资产。如果要在触发操作时自动打开票单，则可将操作设置为与 CA SDM 交互。该分配对于需要第三方核准的操作非常有用。第三方在 CA SDM 中核准您的票单后，操作将自动运行。

还可以使用启动组件将操作排定为在指定时间运行。在创建作业时，会保存操作的当前参数。如果在提交作业后更改操作详细信息，不会影响已排定要运行的作业。如果必须更改已排定作业的操作详细信息，请打开使用该操作的作业并再次保存，以用新的操作详细信息对其进行更新。

配置 CA SDM

对于版本 12.5 之前的 CA SDM 版本，请使用相应的票单状态代码正确配置 CA SDM，以便可以设置操作，从而在必要时自动打开问题。

注意：只要不共享数据库，CA Virtual Assurance 和 CA SDM 两个产品的版本号无需相同。

配置 CA SDM

1. 通过在 Web 浏览器中键入以下信息，登录 CA SDM 服务器：

   http://*servicedesk_servername*:8080

   此时将出现 CA SDM 初始屏幕。

2. 输入您的用户名和密码，然后单击“登录”。

   此时将出现 CA SDM 主页。

3. 单击“管理”并在左侧窗格中展开 Service Desk 树节点。

4. 选择“请求\突发事件\问题”，然后单击“状态”。

   此时将出现“请求/突发事件/状态”列表。

5. 单击“新建”。

   此时将打开“创建新请求状态”窗口。

6. 在“符号”文本框中键入**“已核准”**，从“记录状态”下拉列表中选择“活动”，在“代码”文本框中键入 **APP**，然后单击“保存”。

   新的请求状态将出现在列表中。

7. 在“符号”文本框中键入**“已拒绝”**，从“记录状态”下拉列表中选择“活动”，在“代码”文本框中键入 **REJ**，然后单击“保存”。

   新的请求状态将出现在列表中。

   CA SDM 设置已完成，现在触发操作时，可以自动打开请求。

配置 CA SDM 票单状态设置

12.5 之前的 CA SDM 版本将默认状态代码设置 APP（已核准）和 REJ（已拒绝）用于服务台票单。CA Virtual Assurance 使用和搜索这些核准代码，以运行在服务台票单得到核准时启动的操作。这些操作包括但不限于运行操作、保留系统等。如果您使用的是 CA SDM 版本 12.5，则支持新票单状态代码。PRBAPP（已核准）和 PRBREJ（已拒绝）必须与 CA Virtual Assurance 中现有的核准代码关联。要支持新代码并使产品正常工作，请更新配置文件，如以下步骤中所示。

更改票单状态设置

1. 使用文本编辑器打开位于 CA Virtual Assurance *Install_Path*\conf 目录中的 caaipconf.cfg 文件，并滚动到“服务台”部分。
2. 找到如下所示的特殊状态代码属性：

```
<property name="SPECIAL_STATUS_CODE">
    <!-- APP_CODE=PRBAPP;REJ_CODE=PRBREJ;（每个代码都必须以分号终止）-->
    <value/>
    <displayName>在 SD R12.5 及更高版本中添加的代码类型</displayName>
</property>
```

3. 取消注释并更改代码，如下所示：

```
<property name="SPECIAL_STATUS_CODE">
    <value>APP_CODE=PRBAPP;REJ_CODE=PRBREJ;</value>
    <displayName>在 SD R12.5 及更高版本中添加的代码类型</displayName>
</property>
```

   CA Virtual Assurance 配置为使用 CA SDM 12.5 状态代码。

4. 保存并关闭文件，以启用配置更改。

规则计划

在设置规则和操作时，请注意以下几点：

- 您要分析哪些 VM、服务器和服务？
- 当 CA Virtual Assurance 发现违规时，您希望执行什么操作？
- 哪些规则可以是通用规则，哪些规则应为特定规则？在规划包括脚本或批处理文件的通用规则时，请仔细考虑对环境的影响。
- 您对评估哪些度量标准感兴趣？
- 违反规则多少次后才触发操作？请注意，过度执行操作会对环境的性能造成负面影响。

  注意：指定帮助台核准要求的操作无法用于操作排定。如果需要将相同操作用于排定操作，请创建不包括服务台核准要求的另一个操作。

创建规则

规则条件的计算结果为 true 时，规则充当运行您的操作的触发器。

注意：仅原始创建者或管理员可以编辑或删除规则。

遵循这些步骤:

1. 单击“资源”并在“浏览”树中选择服务器或服务。
2. 单击“策略”选项卡，然后单击“规则”选项卡。

   将显示“规则”页面。
3. 单击 +（添加新规则）。

   此时将显示“规则/模板”向导。
4. 在“标识”部分中为规则键入一个有意义的名称，然后选择“规则”以创建规则。

   注意：选择“模板”可创建可以用于多个规则定义的规则模板。
5. 选择“启用”以使该规则处于活动状态。
6. 选择“无限”或“最大”（重试次数）作为“允许的执行数”。

   注意：设置规则可以运行的次数限制，可防止重试次数过量而降低系统响应速度。
7. 单击“下一步”。

   此时将显示“模板建模和操作选择”部分。
8. 定义是否对模板中的规则建模。选择现有模板或为新模板输入名称，并选择“启用”以继承对模板所做的任何更改。
9. 从列表中为规则选择操作。单击“下一步”。

   此时将显示“定义规则公式”部分。
10. 通过填写“规则计算公式”部分中的以下字段为规则创建条件公式：

    源

    指定规则评估的数据的源，可以是“总使用率”、“事件”或特定服务器度量标准。

运算符

指定如何针对您在“值”字段中输入的值评估源数据。有效运算符取决于源。例如，如果选择“总使用率”，则以下运算符有效：

“=” “!=” “<” “<=” “>” “>=”

如果选择“事件”，则值如下所示：

contains

精确匹配字符串或子字符串。“值”字段中不允许使用通配符。

RegEx（正则表达式）

找到匹配指定正则表达式的字符串时，返回值“true”。没有找到匹配指定正则表达式的字符串时，返回值“false”。

NotRegEx

没有找到匹配指定正则表达式的字符串时，返回值“true”。找到匹配指定正则表达式的字符串时，返回值“false”。

重要信息！确认规则和操作名称不包含要匹配的字符串。在下一个规则计算周期内匹配事件时，此最佳实践帮助避免增量触发操作。

示例：如果“值”字段包含作为匹配字符串的*阈值*，则匹配以下事件：

事件 A：已违反内存*阈值*!

事件 B：阈值

值

指定选定运算符用于评估源数据的数字值或字母数字字符串。

延迟

定义操作触发之前规则必须评估为 true 的频率。您定义的一些操作应该在发出一个信号之后触发。其他操作仅在大量发出永久问题信号之后触发。**注意：**将“源”设置为“事件”时，默认情况下禁用“延迟”。

逻辑 Op

通过使用逻辑运算符 AND 或 OR 定义多个公式。单击“新建”完成每个定义，并将公式添加到已定义公式的列表中。默认情况下，将定义的最后一个公式设置为 NOOP。

当规则的计算结果为 true 时，条件公式将用于触发操作。此时将显示“确认配置”部分。

11. 查看规则的详细信息，然后单击页面顶部的“下一步”。
12. 单击“完成”以提交更新。

    您的规则或模板将添加到“规则”列表中。
13. 单击“返回到规则列表”链接，以确认已添加规则。

示例：设置服务器级别规则

该示例将为超出 CPU 和内存阈值三次以上的服务器设置规则，或发生指示已发现服务器的事件时设置规则。

规则公式：

1. CPU 使用率 % > 80（延迟 3）AND
2. 内存使用率 % > 50（延迟 3）OR
3. 发现事件 RegEx .*
4. 发现事件 NotRegEx .* NOOP

操作：添加 200 个 CPU 份额，最大 8000

使用预定义操作类型

可以为规则选择一个预定义操作类型。如果规则的条件计算为 true，则运行您定义的操作。

遵循这些步骤:

1. 单击“策略”选项卡，然后单击“操作和规则”选项卡。

   将出现“操作和规则”页面。
2. 单击“操作”选项卡。

   将出现“操作”页面。
3. 单击 +（添加新操作）。

   将显示“操作定义: 新操作”页面。

4. 在“名称”文本框中为操作输入有意义的名称，并使用以下菜单选择一种预定义的操作类型：
   - 类别－产品功能区域筛选。要列出所有操作类型，请选择“所有类别”。
   - 类型－可用操作类型
   - 环境－适用的平台（例如，VMware vCenter 或 Microsoft Hyper-V）

   此时将显示“详细信息”部分。此部分中显示的选项取决于您选择的操作类型。
5. 在“操作开始”下拉菜单中选择以下设置之一：

   无延迟

   指定再次触发使用相同操作的规则时可以立即重新运行该操作。

   延迟

   指定再次触发使用相同操作的规则时可以重新运行该操作之前必须等待的时间（以秒为单位）。

   注意：已排定作业运行操作时，“操作开始”设置没有影响。
6. 在“操作完成”下拉列表中选择下列设置之一：

   无等待

   指定在运行操作序列中的后续操作之前不等待该操作完成。

   等待不超过

   指定在运行操作序列中的后续操作之前等待操作完成的时间不超过指定值（以分钟为单位）。

   无限等待

   指定等待操作完成。仅当完成该操作之后，操作序列中的后续操作才会运行。

   注意：仅为长期操作显示“操作完成”下拉列表。
7. 在字段中输入请求的信息。
8. 如果票单需要获得第三方核准，请选中“服务台核准”复选框。

   注意：CA SDM 必须配置为使用该选项。

   “票单类型”和“模板”字段变为启用状态。

   注意：指定帮助台核准要求的操作无法用于操作排定。如果需要将相同操作用于排定操作，请创建不包括服务台核准要求的另一个操作。
9. 如果您要在核准后自动关闭票单，请选择“核准时自动关闭票单”。

10. 从“票单类型”下拉列表中选择票单类型。以下类型是有效选项，但具体取决于您的配置：
    - 默认
    - 突发事件
    - 问题
    - 请求

    “模板”下拉列表将使用与所选票单类型关联的模板进行更新。
11. 从“模板”下拉列表中选择模板。

    使用预先确定的值填充字段，具体取决于您使用的票单模型。
12. 单击“保存”。

    将显示一条确认消息，通知您已成功保存。

    出于测试目的，您可以通过从“操作”页面中选择操作并单击“运行操作”图标来运行该操作。

操作类型

有多种类别的操作类型可供使用。

注意：在任何操作中使用特殊或保留字符时，请考虑操作系统和外壳的行为。行为包括但不限于，调用操作系统外壳运行的自定义脚本。有关外壳行为以及如何转义特殊字符的详细信息，请参阅 Microsoft TechNet 网站：http://technet.microsoft.com/en-us/library/cc723564.aspx。

预定义操作类型

预定义操作类型是在您为规则创建操作时可供使用的常用操作。操作类型将调用命令行实用工具。所有操作类型都会列入用户界面的“策略、操作和规则”页中的下拉列表。

注意：有关操作类型的详细说明，请参阅*联机帮助*。

自定义操作类型

可以使用替代字符串创建自定义操作类型，而不是键入完整命令行。自定义操作类型将添加到预定义操作类型的下拉列表中。通常，可以控制用户对自定义操作的访问，还可以通过用户界面中的“管理”页控制对个别自定义操作的访问。

“运行命令脚本”操作类型提供字符串替代，使您可对服务器执行多个操作。字符串替代可提供更灵活的规则，并可减少对自定义脚本的需求。可用的字符串替代如下：

- %ACTIONNAME%
- %EVENTMESSAGE%
- %EVENTSOURCE%
- %RULENAME%
- %SERVER%
- %SERVICE%

以下字符串替代仅对在操作序列中运行的操作有效：

- %STDOUT%－标准输出
- %STDERR%－标准错误
- %EXITCODE%－操作退出代码

操作序列

操作序列被视为一种操作类型，并且会与其他操作类型一起列入“策略”页的下拉列表中。通过操作序列，您可以按指定的序列为一个规则定义多个操作，并将其作为单个操作来运行。可以使用名称保存您指定的操作序列，该序列将保存到管理数据库中，以供重复使用。使用用户界面中的“策略、操作和规则”页可以将操作序列排定为一项作业。CA SDM 对操作序列的支持的处理方式不同于其他操作类型。可对在序列中运行的各个操作设置服务台核准，但不能为整个操作序列设置服务台核准。

在使用操作序列时，请考虑以下要点：

- 不要配置创建无限循环的序列。操作序列会同步执行，但有些操作会异步执行。因此，如果您期望某些操作在返回时已完成任务，请谨慎。有些通常运行时间较长并且异步执行的操作会有一个 -wait 参数，这会使其在返回之前一直等到任务完成，或等到指定超时之后。
- 如果您尝试删除与操作序列关联的操作，产品将阻止您删除该操作。
- 如果操作序列异常终止，则它会在策略管理器重新启动时在上一个已知序列处重新启动。可以通过用户界面或从 Web 服务中手动取消正在运行的操作序列。
- 当您在操作序列中运行的自定义操作中指定 %STDOUT%（标准输出）、%STDERR%（标准错误）或 %EXITCODE%（操作返回代码）替代字符串操作时，前一个操作的标准输出/标准错误/退出代码可以传输到当前操作中。传输使用第一个操作的输出作为下一个操作的输入。如果在操作中重定向输出，那么它将无法传输到下一个操作。例如，如果将自定义操作 *ipconfig* 重定向到名为 ipconfig_output.txt 的文本文件，那么该输出将无法传输到下一个操作。

预定义操作类型列表

本节介绍了以下预定义的操作类型，这些类型可用于创建策略规则对应的操作。

添加磁盘：VMware vCenter

通过“添加磁盘”操作类型，您可以将磁盘添加到虚拟机中。

操作定义的“详细信息”部分包含以下字段：

虚拟中心

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一个名称。

数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一个名称。

虚拟机

指定要为其添加磁盘的虚拟机的名称。从下拉列表中选择一个名称。

数据存储

指定与选定的 VM 的 ESX 服务器相关联的数据存储的名称。从下拉列表中选择一个名称。

驱动器大小

指定附加磁盘的大小。输入值并从下拉列表中选择 MB 或 GB。

SCSI 控制器

指定要用于创建附加磁盘的 SCSI 控制器。从下拉列表中选择一个。

“精简开通”复选框

指定是否启用精简开通。

磁盘模式

指定磁盘模式。从下拉列表中选择下列项之一：

- 永久
- 独立持久
- 独立非持久

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

添加网络接口：VMware vCenter

通过“添加网络接口”操作类型，您可以将虚拟 NIC 添加到虚拟机中。

操作定义的“详细信息”部分包含以下字段：

虚拟中心

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一项。

数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一项。

虚拟机

指定要为其添加虚拟 NIC 的虚拟机的名称。从下拉列表中选择一项。

设备类型

指定设备类型。从下拉列表中选择一项。

网络

指定与选定的 VM 的 ESX 服务器相关联的网络。从下拉列表中选择一项。

您可以根据以下命名约定区分标准交换机和分布式虚拟交换机的名称：

- 对于标准交换机，其名称为网络名称。
- 对于分布式虚拟交换机，其名称为 dvPort 组名称后跟用括号括起来的分布式虚拟交换机名称：dvPortGroupName (dvSwitchName)

MAC 地址

（可选）指定 MAC 地址。如果要自动生成 MAC 地址，则将该字段保留为空白。

“在 LAN 上唤醒”复选框

指定是否将虚拟 NIC 设置为在 LAN 上唤醒。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

将服务器添加到服务

通过“将服务器添加到服务”操作，您可以将服务器添加到现有服务中。

操作定义的“详细信息”部分包含以下字段：

服务名称

指定服务名称。

服务器列表（逗号分隔）

指定要添加到服务中的服务器列表。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

变更计算机状态：Microsoft Hyper-V

“变更计算机状态”操作类型可控制 Hyper-V 环境中虚拟机的状态变更。

操作定义的“详细信息”部分包含以下字段：

Hyper-V 主机

指定 Hyper-V 服务器所驻留的服务器的名称。从下拉列表中选择一个名称。

Hyper-V VM 名称

指定要更改其状态的虚拟机的名称。从下拉列表中选择一个名称。

状态

指定虚拟机的所需状态。从下拉列表中选择下列项之一：

- 关闭
- 关闭
- 保存
- 暂停
- 启动

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

克隆计算机：Solaris 区域

通过从现有区域复制数据，“克隆 Solaris 区域计算机”操作类型可配置和安装新区域。您无法对全局区域或在某区域处于安装状态时执行该操作。

操作定义的“详细信息”部分包含以下字段：

区域主机

定义包含要克隆的区域的 Solaris 区域主机。

区域

定义要克隆的区域。您可以使用从事件消息中提取的文本。

名称

定义新区域的名称。可以使用自动生成的文本或从事件消息中提取的文本。

路径

定义新区域的安装路径。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

配置 CPU/内存：IBM LPAR

通过“配置 CPU/内存”操作类型，您可以对分配给 IBM LPAR 环境中虚拟机的 CPU 和内存资源设置限制。

操作定义的“详细信息”部分包含以下字段：

HMC/IVM 名称

指定与选定分区所在的受管服务器关联的 HMC/IVM。

系统名称

指定虚拟机所在的 IBM LPAR 中的数据中心的名称。从下拉列表中选择一个名称。

分区名称

显示分区的唯一名称。

鏖离悝璃靡

为选定 LPAR 指定现有配置文件的名称。

操作

指定要执行的操作。从下拉列表中选择下列项之一：

- 加内存单元
- 减内存单元
- 加处理器
- 减处理器

处理器

指定要增加或删除的处理器的数目。

调整类型

指定调整类型。选择一个选项：

- 仅动态调整
- 动态调整和更新配置文件

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

配置 CPU/内存：Microsoft Hyper-V

“配置 CPU/内存”操作类型可以控制分配给 Hyper-V 环境中虚拟机的 CPU 和内存份额的数量。

操作定义的“详细信息”部分包含以下字段：

Hyper-V 主机

指定 Hyper-V 服务器所驻留的服务器的名称。从下拉列表中选择一个名称。

Hyper-V VM 名称

指定要更改其状态的虚拟机的名称。从下拉列表中选择一个名称。

CPU 分配

指定虚拟机的 CPU 配置。从下拉列表中调整以下项之一：

- CPUs 数
- CPU 保留 %
- CPU 权重
- CPU 限制 %
- 目前 CPUID

内存分配

指定分配给虚拟机的内存份额 (MB)。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

配置 CPU/内存：VMware vCenter

通过“配置 CPU/内存”操作类型，您可以对 CUP 和内存资源设置限制。

操作定义的“详细信息”部分包含以下字段：

VC 服务器

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一项。

VC 数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一项。

目标虚拟机

指定要对其调整资源的虚拟机的名称。从下拉列表中选择一项。或者，您也可以使用自动生成的文本或从事件消息中提取的文本。

操作

指定要执行的操作。从下拉列表中选择下列项之一：

- 设置 CPU 限制
- 设置内存限制
- 设置 CPU 保留
- 设置内存保留

MHz，MB

输入一个适用于所选操作的值。

“无限”复选框

允许您选择的操作无限使用资源。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

配置电源：Cisco UCS

该操作类型允许您为 UCS 刀片服务器配置电源管理操作。

操作定义的“详细信息”部分包含以下字段：

UCS 管理器

指定 UCS 管理器的名称

UCS 机箱

指定 UCS 机箱的名称

UCS 刀片服务器

指定 UCS 刀片服务器的名称

电源操作

从下拉列表中选择一个操作：

立即重新启动

立即重新启动刀片服务器

等待重新启动

重新启动通知了所有应用程序有关其关闭情况的刀片服务器

立即硬重置

按照与拔出刀片服务器电源类似的方式重新插入以使刀片服务器通电

硬重置等待

拔出刀片服务器的电源。在拔出之前，刀片服务器会通知所有应用程序有关其关闭的情况

软关闭

关闭刀片服务器。在关闭之前，刀片服务器会通知所有应用程序有关其关闭的情况

关闭

立即关闭刀片服务器

启动

启动刀片服务器

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

配置电源：IBM LPAR

“LPAR 配置电源”操作类型控制 LPAR 上的电源设置。

操作定义的“详细信息”部分包含以下字段：

HMC/IVM 名称

指定与选定分区所在的受管服务器关联的 HMC/IVM。

系统名称

指定虚拟机所在的 IBM LPAR 中的数据中心的名称。从下拉列表中选择一个名称。

分区名称

指定要控制的分区名称。

操作

指定要执行的电源操作。如果您选择“激活”，填写“操作选项”部分的下列字段：

分区配置文件

指定用于激活电源设置的分区配置文件。

键盘锁定

在分区配置文件指定键盘锁定模式。键盘锁定建立系统允许的打开或关闭模式（手工或正常）。出于安全原因，不建议将键盘锁定位置设置为手工。

启动模式

在分区配置文件中指定启动模式。除非您在激活分区配置文件时指定其他模式，否则系统将使用该启动模式启动逻辑分区上的操作系统。CA Virtual Assurance 支持以下有效启动模式：

正常

正常启动逻辑分区。（使用该选项执行大多数日常任务。）

open_firmware

将逻辑分区引导至打开固件提示。服务人员使用该选项获取其他调试信息。

如果您选择“关闭”，填写“操作选项”部分的下列字段：

已延迟

使用延迟关闭序列关闭逻辑分区。该序列给予逻辑分区时间来结束作业并将数据写入磁盘。如果逻辑分区无法在预定的时间长度内关闭，它将异常结束。下次重新启动可能比一般启动时间更长。

立即

立即关闭逻辑分区。HMC 立即结束所有活动作业。不允许这些作业中运行的程序执行任何作业清理。如果已更新部分数据，该选项可能导致不适当的结果。仅在尝试受控关闭失败后使用该选项。

OS 关闭

以通常方式通过向逻辑分区发出关闭命令来关闭逻辑分区。在该操作期间，逻辑分区将执行任何必要的关闭活动。该选项仅适用于 AIX 逻辑分区。

OS 立即关闭

通过向逻辑分区发出带 -F 参数的关闭命令来立即关闭逻辑分区。在该操作期间，逻辑分区将跳过发送到其他用户的消息和其他关闭活动。该选项仅适用于 AIX 逻辑分区。

如果您选择“重新启动”，从“操作选项”部分选择一个选项：

分区配置文件

指定用于重新启动分区的分区配置文件。

立即

立即关闭逻辑分区。HMC 立即结束所有活动作业。不允许这些作业中运行的程序执行任何作业清理。如果已更新部分数据，该选项可能导致不适当的结果。仅在尝试受控关闭失败后使用该选项。

OS 关闭

以通常方式通过向逻辑分区发出关闭命令来关闭逻辑分区。在该操作期间，逻辑分区将执行任何必要的关闭活动。该选项仅适用于 AIX 逻辑分区。

OS 立即关闭

通过向逻辑分区发出带 -F 参数的关闭命令来立即关闭逻辑分区。在该操作期间，逻辑分区将跳过发送到其他用户的消息和其他关闭活动。该选项仅适用于 AIX 逻辑分区。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

配置电源：Microsoft Hyper-V

“配置电源”操作类型控制 Hyper-V 环境中虚拟机的启动和关闭。

操作定义的“详细信息”部分包含以下字段：

Hyper-V 主机

指定 Hyper-V 服务器所驻留的服务器的名称。从下拉列表中选择一个名称。

Hyper-V VM 名称

指定要更改其状态的虚拟机的名称。从下拉列表中选择一个名称。

启动操作

指定 Hyper-V 服务器启动时执行的操作。从下拉列表中选择下列项之一：

- 始终

  在 Hyper-V 服务器启动时始终启动 VM。

- 趁雄

  在 Hyper-V 服务器启动时自动启动 VM。

- 无

  在 Hyper-V 服务器启动时不启动 VM。

启动延迟

调整 Hyper-V 服务器启动后启动 VM 的延迟（秒）。从下拉列表中选择一项。

关闭操作

指定虚拟机关闭时执行的操作。从下拉列表中选择下列项之一：

- 关

  在 Hyper-V 服务器关闭前关闭 VM。

- 保存

  在 Hyper-V 服务器关闭前保存（挂起）VM。

- 关闭

  在 Hyper-V 服务器关闭前关闭 VM。

恢复操作

指定 Hyper-V 服务器出现故障时重新获取虚拟机之前的详细信息的操作。从下拉列表中选择下列项之一：

- 无

服务器出现故障后启动 Hyper-V 服务器时不采取具体操作。

- 重新启动

  服务器出现故障后启动 Hyper-V 服务器时，重新启动 VM。

- 还原

  服务器出现故障后启动 Hyper-V 服务器时，使用最新的快照还原 VM。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

配置电源：VMware vCenter/调整 vApp 电源

“配置电源”操作类型控制您的 VMware vCenter 环境中虚拟机和 vApp 上的电源设置。

操作定义的“详细信息”部分包含以下字段：

VC 服务器

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一项。

VC 数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一项。

VM/vAPP

用于指定目标类型（VM 或 vApp）的单选按钮。

目标

指定要对其调整电源的虚拟机或 vApp 的名称。从下拉列表中选择一项。或者，您也可以使用自动生成的文本或从事件消息中提取的文本。

电源操作

指定要执行的电源操作。从下拉列表中选择下列项之一：

- VC 电源打开
- VC 电源关闭
- VC 电源重置
- VC 电源挂起
- VC 电源关闭
- 打开 vApp
- 关闭 vApp
- 挂起 vApp

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

配置服务配置文件：Cisco UCS

“配置服务配置文件”操作类型允许您将服务配置文件关联到、取消关联到或故障切换到 UCS 刀片服务器。

操作定义的“详细信息”部分包含以下字段：

UCS 管理器

指定 UCS 管理器的名称

UCS 机箱

指定 Cisco UCS 机箱的名称

UCS 刀片服务器

指定 Cisco UCS 刀片服务器的名称

服务配置文件

指定服务配置文件的名称

配置文件操作

从下拉列表中选择一个配置文件：

关联

将服务配置文件关联到刀片服务器

取消关联

从刀片服务器取消服务配置文件的关联

故障切换

使用该选项，将出现一个针对用于将服务配置文件自动故障切换到下一台可用刀片服务器的服务配置文件的复选框。默认情况下，该复选框处于选中状态，并且已禁用机箱和刀片服务器下拉列表。

清除该复选框可选择所需的机箱和刀片服务器来故障切换特定的服务配置文件。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

配置份额：VMware vCenter

“配置份额”操作类型控制您的 VMware vCenter 环境中虚拟机的 CPU 和内存份额。

操作定义的“详细信息”部分包含以下字段：

VC 服务器

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一项。

VC 数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一项。

目标虚拟机

指定要对其调整份额的虚拟机的名称。从下拉列表中选择一项。或者，您也可以使用自动生成的文本或从事件消息中提取的文本。

操作

指定要执行的操作。从下拉列表中选择下列项之一：

- 设置 CPU
- 加 CPU
- 减 CPU
- 设置内存
- 加内存
- 减内存

值

输入一个适用于所选操作的值。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

将模板转换为虚拟机：VMware vCenter

使用“将模板转换为虚拟机”操作类型，您可以将模板转换为虚拟机。

操作定义的“详细信息”部分包含以下字段：

VC Server

指定 VMware vCenter 驻留的服务器的名称。从下拉列表中选择一项。

VC 数据中心

指定虚拟机所在的数据中心。从下拉列表中选择一项。

VC 计算资源

指定在其中创建虚拟机的群集或 VMware ESX 主机。从下拉列表中选择一项。

VC ESX 服务器

指定虚拟机将驻留的 VMware ESX 服务器。从下拉列表中选择一项。

VC 资源池

指定您希望从中选择用于克隆的虚拟机的资源池的名称。从下拉列表中选择一项。

VC 模板

指定要转换的模板的名称。从下拉列表中选择一项。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

将 VM 转换成模板：VMware vCenter

通过“将 VM 转换成模板”操作类型，您可以将已关闭电源的虚拟机转换成模板。

操作定义的“详细信息”部分包含以下字段：

VC 服务器

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一项。

VC 数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一项。

VC 虚拟机

指定要转换的虚拟机的名称。从下拉列表中选择一个，或使用从事件消息中提取的文本。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

创建事件

通过“创建事件”操作类型，您可以创建事件，如系统发现、系统删除、多个系统发现以及系统管理状态更改。

操作定义的“详细信息”部分包含以下字段：

事件状态

指定事件的状态。

事件组件

指定事件涉及的组件名。

事件消息

指定事件生成的消息。

事件源

指定事件的源。

事件目标

指定事件的目标。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

创建报告

“创建报告”操作类型使您可以自动生成报告。可以排定该操作，以便定期创建报告。还可以从“报告”选项卡创建此操作类型。

操作定义的“详细信息”部分包含以下字段：

报告类型

指定创建的报告的类型。有关可用的报告类型以及相关创建选项的说明，请参阅“报告”。

生成的报告可以在“报告”选项卡上的“排定报告”文件夹中进行查看。

创建服务

通过“创建服务”操作类型，您可以将所监控的服务器组织到反映业务需求所需资源的逻辑服务中。

操作定义的“详细信息”部分包含以下字段：

服务名称

指定服务名称。

服务器列表（逗号分隔）

指定可用服务器列表。

下限阈值

从总体上指定服务的下限阈值。

上限阈值

从总体上指定服务的上限阈值。

延迟

定义操作触发之前规则必须评估为 true 的频率。某些操作应该在单个事件后触发，而另一些操作应该仅在表示持久性问题的多个事件之后触发。

优先级

指定在单个轮询周期中执行操作的顺序。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

删除计算机：IBM LPAR

通过“LPAR 删除计算机”操作类型，您可以删除指定的 LPAR。

操作定义的“详细信息”部分包含以下字段：

HMC/IVM 名称

指定与选定分区所在的受管服务器关联的 HMC/IVM。

系统名称

指定虚拟机所在的 IBM LPAR 中的数据中心的名称。从下拉列表中选择一个名称。

分区名称

定义要删除的分区名称。

注意：对于该操作，必须关闭要删除的分区的电源。该操作擦除逻辑分区和存储在分区配置文件中的逻辑分区配置数据。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

删除计算机：Microsoft Hyper-V

通过“删除 Hyper-V VM”操作类型，您可以从 Hyper-V 服务器环境中删除虚拟机。

操作定义的“详细信息”部分包含以下字段：

Hyper-V 主机

指定 Hyper-V 服务器驻留的主机的名称。从下拉列表中选择一个名称。

Hyper-V VM 名称

指定想要删除的虚拟机的名称。从下拉列表中选择一个名称。

附加的资源

指定想要删除的虚拟机上附加的资源。选择您想要删除的资源：

- 硬盘驱动器
- 软盘驱动器
- DVD/ISO 映像

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

删除计算机：Solaris 区域

“删除 Solaris 区域计算机”操作类型可从 Solaris 区域主机删除区域。

操作定义的“详细信息”部分包含以下字段：

区域主机

定义包含要删除区域的 Solaris 区域主机。

区域

定义要删除的区域。可以使用自动生成的文本或从事件消息中提取的文本。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

删除计算机：VMware vCenter

“删除 vCenter VM”操作类型可以从您的 VMware vCenter 服务器环境删除虚拟机。

操作定义的“详细信息”部分包含以下字段：

VC Server

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一个名称。

VC 数据中心

指定虚拟机驻留的数据中心的名称。从下拉列表中选择一个名称。您的选择项通过与数据中心相关联的 VM 名称填充目标 VM 下拉列表。

目标虚拟机

指定想要删除的虚拟机的名称。从下拉列表中选择一个名称。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

发现主机(按名称)

通过“发现主机(按名称)”操作类型，您可以发现使用指定主机名的主机。

操作定义的“详细信息”部分包含以下字段：

主机名

指定主机名。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

发现网络

通过“发现网络”操作类型，您可以发现域中可用的网络。

操作定义的“详细信息”部分包含以下字段：

网络 ID

指定要发现的网络 ID。

网络名称

指定要发现的网络名。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

管理分布式交换机：VMware vCenter

使用该操作类型管理分布式虚拟交换机。

操作定义的“详细信息”部分包含以下字段：

操作

请选择下列操作之一：

- 添加端口组
- 删除端口组
- 更新端口组

虚拟中心

指定 vCenter 服务器。从下拉列表中选择一个。

虚拟交换机

指定想要管理的虚拟交换机。从下拉列表中选择一个。

端口组

指定端口组名称。从下拉列表中选择一个名称。

绑定类型（可选）

请选择下列绑定类型之一：

earlyBinding

在 VM 绑定至端口组时分配端口。这种类型的绑定可确保始终连接，但永久保留端口。此绑定类型为默认值。

lateBinding

如果 VM 电源打开且其 NIC 处于连接状态，则将端口分配给该 VM。当 VM 电源关闭或其 NIC 断开连接时，此绑定类型将重新分配端口。LateBinding 可通过 vCenter 进行配置。

ephemeral

如果 VM 电源打开且其 NIC 处于连接状态，则将端口分配给该 VM。当 VM 电源关闭或其 NIC 断开连接时，此绑定类型将重新分配端口。Ephemeral 绑定可通过 ESX 主机和 vCenter 进行配置。

VLAN ID（可选）

指定用于虚拟端口组操作的整数值。

端口数（可选）

指定端口组的端口数。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

管理容错：VMware vCenter

使用该操作类型管理容错。

操作定义的“详细信息”部分包含以下字段：

操作

为指定 VM 选择下列操作之一：

- 打开
- 关闭
- 启用
- 禁用
- 迁移辅助 VM

虚拟中心

指定 vCenter 服务器主机名。从下拉列表中选择一项。

数据中心

指定 VM 所属的数据中心。从下拉列表中选择一项。

虚拟机

指定容错 VM。从下拉列表中选择一项。

辅助主机

指定辅助 VM 驻留的 ESX 服务器。从下拉列表中选择一项。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

管理 VM 快照：VMware vCenter

通过“管理 VM 快照”操作类型，您可以在指定的目标系统上创建、还原或删除虚拟机快照。

注意：如果由于将 ESXi 主机从 vCenter 删除然后再添加进来而导致“管理 VM 快照”操作失败，请再次选择相应的快照并保存该操作。

操作定义的“详细信息”部分包含以下字段：

操作

指定下列操作之一：

- 创建快照
- 还原快照
- 删除快照

如果您选择“创建快照”，请填写下列字段：

VC 服务器

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一个服务器。

数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一个数据中心。

虚拟机

指定在其上创建快照的虚拟机的名称。从下拉列表中选择一个虚拟机。或者，您也可以使用自动生成的文本或从事件消息中提取的文本。

名称

定义要创建的虚拟机快照的名称。可以使用自动生成的文本或从事件消息中提取的文本。

说明

（可选）描述虚拟机快照。

“捕获内存”复选框

（可选）指定创建快照时是否将正在运行的系统内存作为快照的一部分。

如果您选择“还原快照”，请填写下列字段：

VC 服务器

指定 vCenter 所在服务器的名称。从下拉列表中选择一个服务器。

数据中心

指定虚拟机所在 vCenter 中的数据中心的名称。从下拉列表中选择一个数据中心。

虚拟机

指定在其上还原快照的虚拟机的名称。从下拉列表中选择一个虚拟机。

名称

定义要还原的虚拟机快照的名称。

输入名称，或单击望远镜图标并从对话框中选择您想要还原的快照。

ID

定义要还原的虚拟机快照的 ID。

注意：您可以使用“名称”或“ID”来还原快照，但不需要同时使用这两者。如果一个虚拟机具有多个相同名称的快照，则需要使用 ID。

如果您选择“删除快照”，请填写下列字段：

VC 服务器

指定 vCenter 所在服务器的名称。从下拉列表中选择一个服务器。

数据中心

指定虚拟机所在 vCenter 中的数据中心的名称。从下拉列表中选择一个数据中心。

虚拟机

指定在其上删除快照的虚拟机的名称。从下拉列表中选择一个虚拟机。

名称

定义要删除的虚拟机快照的名称。

键入名称，或单击望远镜图标并从打开的对话框中选择想要删除的快照。

ID

定义要删除的虚拟机快照的 ID。

注意：您可以使用“名称”或“ID”来删除快照，但不需要同时使用这两者。如果一个虚拟机具有多个相同名称的快照，则需要使用 ID。

“删除子项”复选框

（可选）指定是否删除快照的所有子项。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

管理虚拟交换机：VMware vCenter

使用该操作类型管理虚拟交换机。

操作定义的“详细信息”部分包含以下字段：

操作

请选择下列操作之一：

- 添加端口组
- 删除端口组
- 更新端口组

虚拟中心

指定 vCenter 服务器。从下拉列表中选择一个。

数据中心

指定数据中心。从下拉列表中选择一个。

ESX Server

指定虚拟交换机所属的 ESX 服务器。从下拉列表中选择一个。

虚拟交换机

指定想要管理的虚拟交换机。从下拉列表中选择一个。

端口组

指定端口组名称。从下拉列表中选择一个名称。

VLAN ID（可选）

指定用于虚拟端口组操作的整数值。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

管理 Windows 服务

“管理 Windows 服务”操作类型用于通过使用 AutoShell 命令行和脚本环境控制 Windows 服务。

操作定义的“详细信息”部分包含以下字段：

操作选项

指定使用服务执行的操作。

注意：查询服务操作返回的 Windows 服务状态只能从 %STDOUT% 参数获取；事件表中不提供该状态。该参数仅对在操作序列中运行的操作有效。

注意：以下行为不同于直接在 Windows 中执行的服务管理：

- 即使服务处于“已停止”状态，也可以执行“重新启动服务”操作。服务状态将更改为“已启动”。
- 如果服务处于“已启动”状态并且已执行“禁用服务”操作，服务将被禁用且其状态将更改为“已停止”。

主机名

定义正在运行服务的计算机的名称。

用户名

定义用户名。

密码

定义密码。重新输入密码进行确认。

服务名称

定义对其执行操作的服务的名称。键入名称或使用从事件消息中提取的文本。

注意：可以在 Windows 服务的“属性”对话框中检查服务名称。不要将其与在“计算机管理”窗口显示的显示名称相混淆。

如果选择“更改服务启动类型”，请填写以下字段：

启动类型

指定为服务设置的启动类型。选项包括“自动”、“手工”、“已禁用”。“启动”选项意味着由启动加载程序加载设备驱动程序。“系统”选项意味着在内核初始化期间启动设备驱动程序。

如果选择“更改服务依存关系”，请填写以下字段：

依存关系

定义在可以启动服务之前必须正在运行的依存关系（其他服务、系统驱动程序或加载顺序组）。如果定义多个依存关系，请使用正斜杠进行分隔。

如果选择“更改服务帐户”，请填写以下字段：

本地系统帐户/该帐户

指定服务登录所用的帐户。可以使用 LocalSystem 帐户，或在此处定义帐户。

迁移计算机：VMware vCenter

“vCenter VMotion 迁移”操作类型使用 VMware VMotion 迁移虚拟机。必须为该操作正确配置 VMware ESX 服务器，且目标计算机上必须存在 VMotion 许可证。

操作定义的“详细信息”部分包含以下字段：

VC Server

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一个名称。

源数据中心

指定源虚拟机驻留的数据中心的名称。从下拉列表中选择一个名称。

源虚拟机

指定要用作源 VM 的服务器的名称。从下拉列表中选择一个名称。

目标 ESX 服务器

指定作为迁移目标的 ESX 服务器的名称。从下拉列表中选择一个名称。

注意：仅当在两个 ESX 主机之间共享 VM 数据存储/磁盘时才支持 ESX 主机之间的 VM 迁移。

目标资源池

指定要使用的资源池的名称。从下拉列表中选择一个名称。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

修改 CPU：VMware vCenter

通过“修改 CPU”操作类型，您可以修改分配到虚拟机的 CPU 数。

操作定义的“详细信息”部分包含以下字段：

虚拟中心

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一个名称。

数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一个名称。

虚拟机

指定要对其修改内存的虚拟机的名称。从下拉列表中选择一个名称。

CPU

指定要分配到 VM 的 CPU 数。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

修改内存：VMware vCenter

通过“修改内存”操作类型，您可以修改虚拟机的内存分配。

操作定义的“详细信息”部分包含以下字段：

虚拟中心

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一个名称。

数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一个名称。

虚拟机

指定要对其修改内存的虚拟机的名称。从下拉列表中选择一个名称。

内存

指定要分配到 VM 的内存量。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

打开帮助台票单

通过“打开帮助台票单”操作类型，您可以定义用于打开帮助台票单的属性。

操作定义的“详细信息”部分包含以下字段：

摘要

汇总票单的详细信息。

说明

描述票单。

实体

（可选）定义用于将票单与帮助台系统中已知的配置项匹配的服务器或服务的名称。如果配置项主机名与实体名称相同，则该票单与该配置项关联。

类型

指定票单的类型。

模板

指定票单的模板。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

开通计算机：IBM LPAR

该操作类型用于开通 LPAR。

“构建分区”部分包含以下字段：

HMC/IVM 名称

指定与选定分区所在的受管服务器关联的 HMC/IVM。

系统名称

指定虚拟机所在的 IBM LPAR 中的数据中心的名称。从下拉列表中选择一个名称。

分区名称

定义用于创建映像的分区名称。

配置文件名称

为选定 LPAR 定义现有配置文件的名称。

“内存设置”部分包含以下字段：

已安装内存

标识已安装的内存。

可用内存

标识已安装的内存。

最小值

指定最小内存。

期望值

指定所需的内存。

最大值

指定最大内存。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

“处理器”部分包含以下字段：

处理模式

指定处理模式。

从以下选项中进行选择：

- 部分处理器单元(共享)
- 全部处理器数(专用)

可用单元

标识可用处理器单元。

最小值

指定最小处理器单元数。

期望值

指定所需的处理器单元数。

最大值

指定最大处理器单元数。

I/O 组件

指定要与 LPAR 关联的 I/O 组件。

I/O 池

允许您添加、删除和修改 I/O 池。

最大虚拟适配器数

定义虚拟适配器的最大数目。

虚拟适配器数

标识虚拟适配器的数目

虚拟串行适配器

允许您添加、删除和修改虚拟串行适配器。

虚拟以太网适配器

允许您添加、删除和修改虚拟以太网适配器。

虚拟 SCSI 适配器

允许您添加、删除和修改虚拟 SCSI 适配器。

开通过程在客户端计算机上启动，并在作业成功完成时向您发送一条确认消息。

开通计算机：Microsoft Hyper-V

“开通 Hyper-V VM”操作类型可创建和安装 VM。指定下列参数。

操作定义的“详细信息”部分在首页包含下列字段：

SCVMM 服务器

指定 Microsoft System Center Virtual Machine Manager (SCVMM) 库服务器。从下拉列表中选择一项。

Hyper-V 服务器

指定 Hyper-V 服务器。从下拉列表中选择一项。

模板

指定模板。从下拉列表中选择一项。

目标路径

指定想要创建的 VM 的目标路径（存储模板）。从下拉列表中选择一项。

VM 名称

指定 VM 的名称。

启动 VM

在创建 VM 后自动将其启动。默认情况下，新 VM 处于关闭状态。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

在您单击“下一步”之后，第二页上的“详细信息”部分包含下列字段：

硬件配置文件

指定 Microsoft System Center Virtual Machine Manager (SCVMM) 库服务器定义的硬件配置文件的名称。

虚拟处理器数

指定想要分配给 VM 的虚拟处理器数。

默认：1

内存

为想要创建的 VM 指定 RAM 内存 (MB)。

默认：1024

在您单击“下一步”之后，第三页上的“详细信息”部分包含下列字段：

来宾 OS 配置文件

（可选）指定 Microsoft System Center Virtual Machine Manager (SCVMM) 库服务器定义的来宾操作系统配置文件的名称。该参数覆盖存储在 SCVMM 库服务器中的操纵系统配置设置。使用 SCVMM 集成开通 VM 时，该参数有效。

产品密钥

（可选）指定 VM 的 Windows 产品激活密钥。对该参数的支持需要一个使用 Sysprep 工具创建的 Windows 映像。该选项对于异步执行命令无效。

全名

指定安装在新 VM 上的 Windows 映像（使用 Sysprep 工具创建）的用户名。

组织

（可选）指定在新 VM 上安装的 Windows 映像（使用 Sysprep 工具创建）的组织名称。对该参数的支持需要一个使用 Sysprep 工具创建的 Windows 映像。该选项对于异步执行命令无效。

管理员密码

（可选）该选项用于设置 VM 的默认管理员帐户密码。对该参数的支持需要一个使用 Sysprep 工具创建的 Windows 映像。在异步执行中将忽略该参数。

注意：要成功设置该选项，请将使用 Sysprep 工具创建的 Windows Server 管理员密码设置为空。

加入工作组

指定要为 VM 创建的工作组。域和工作组规格互不相容。

加入域

指定 VM 的域名。域和工作组规格互不相容。

域用户

指定要作为默认管理员组的一部分进行创建的域用户名。

域用户密码

指定要作为默认管理员组的一部分进行创建的域用户帐户密码。

在您单击“下一步”之后，第四页上的“详细信息”部分包含下列字段：

使用 DHCP

指定一个选项，为 VM 的网络接口启用 DHCP。如果模板映像有多个网络适配器，则为第一个接口打开 DHCP。如果已启用，则无法访问其他网络参数。

IP 地址

指定想要分配给 VM 的静态 IPv4 地址。

网络掩码

指定想要为 VM 分配的子网掩码。

默认网关

指定 VM 的默认网关。

DNS 服务器

指定要为 VM 设置的 DNS 服务器。

IP 度量标准

（可选）指定要为 VM 设置的接口度量标准。该选项与 -ip4ddr 选项结合使用。如果在 -ip4addr 选项中指定了接口名称，则必须在该选项中使用相同的接口名称。对该参数的支持需要一个使用 Sysprep 工具创建的 Windows 映像。该选项对于异步执行命令无效。

默认：1

开通计算机：Solaris Zones

“开通 Solaris Zones 计算机”操作类型可创建和安装区域。指定 Solaris Zones 主机、区域名称、区域类型以及其他区域属性。区域会在创建后自动安装。

操作定义的“详细信息”部分在首页包含下列字段：

主机

定义要在其上创建区域的 Solaris Zones 主机。

名称

定义区域名称。可以使用自动生成的文本或从事件消息中提取的文本。

说明

（可选）定义区域的说明。

类型

定义区域是“本地”、“整个根”还是“已标记”。“标记”区域基于现有的区域模板。

模板

（可选）在将“类型”设置为“标记”时，定义创建区域所基于的模板。

安装存档路径

定义区域中的安装存档的目录路径。仅当将“类型”设置为“标记”时，才需要该字段。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

在您单击“下一步”之后，第二页上的“详细信息”部分包含下列字段：

类型

定义排定程序类型。选择 FSS，以使用“公正份额排定”类来基于分配给任务的 CPU 份额来控制 CPU 分配。

容量

定义分配到区域的物理内存容量的数量 (MB)。

交换内存

定义分配到区域的交换内存的数量 (MB)。交换内存至少为 50 MB。

锁定内存

定义分配到区域的锁定内存的数量 (MB)。锁定内存必须小于物理内存。

区域路径

定义区域的根目录路径。

NIC 类型

定义 NIC 类型。从下拉列表中选择类型。如果不选择 NIC，则不为该区域分配 NIC 卡或 IP 地址。

IP 地址

定义区域的 IP 地址。

资源池

定义要用于区域的资源池。从下拉列表中选择一个池。如果要将新资源池用于区域，请首先创建池。如果不选择池，则使用默认池。

自动重新启动

定义在重新启动全局区域时是否自动重新启动该区域。

开通计算机：VMware vCenter

“开通 vCenter 计算机”操作类型可开通虚拟机 (VM)。模板以及和模板配套的目标 vCenter 规格是必需的。如果已存在用于开通 VM 的服务规则，则该新 VM 将放置在为其创建规则的服务中。

操作定义的“详细信息”部分包含以下字段：

VC 服务器

指定 vCenter 驻留的服务器的名称。从下拉列表中选择一项。

VC 数据中心

指定在其上开通计算机的数据中心的名称。从下拉列表中选择一项。

VC 计算资源

指定计算资源驻留的服务器的名称。从下拉列表中选择一项。

VC ESX Server

指定作为开通 VM 目标的 VMware ESX 服务器的名称。从下拉列表中选择一项。

VC 数据存储

指定要使用的数据存储的名称。从下拉列表中选择一项。

VC 目标位置

指定 VC 目标位置。从下拉列表中选择一项。

主机名/VM 名称

从规格中指定要使用的名称或 VC 名称。从下拉列表中选择一项。或者，您也可以使用自动生成的文本或从事件消息中提取的文本。

用户名

指定用于访问规格的用户名凭据。

密码

指定用于访问规格的密码。

VC 虚拟机

指定要使用的可用 VC 虚拟机。如果已选定，请单击下拉列表中的一项。

VC 模板

指定要使用的可用 VC 模板。如果已单击，从下拉列表中选择以前已创建的一个软件包组。

NIC（VC 模板）

指定 VC 模板使用的网络接口卡的数目。

VC 规格

指定要使用的 VC 规格的名称。从下拉列表中选择一项。

NIC（VC 规格）

指定 VC 规格使用的网络接口卡的数目。

OS 系统类型

显示开通的 VM 的操作系统类型。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

内存

指定分配给 VM 的内存量 (MB)。

虚拟处理器数

指定分配给 VM 的虚拟处理器数。

数据存储

（可选）指定要在其下创建其他硬盘的存储数据存储。

驱动器大小

（可选）指定其他硬盘驱动器的大小。

SCSI 控制器

（可选）指定用于创建其他硬盘驱动器的 SCSI 控制器。

网络管理

允许您更改网络连接设置。

全局 NIC 设置

允许您添加 DNS 搜索后缀。

删除磁盘：VMware vCenter

通过“删除磁盘”操作类型，您可以从虚拟机中删除磁盘。

操作定义的“详细信息”部分包含以下字段：

虚拟中心

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一个名称。

数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一个名称。

虚拟机

指定要为其添加磁盘的虚拟机的名称。从下拉列表中选择一个名称。

硬盘驱动器

指定要删除的磁盘。从下拉列表中选择一个。

“删除磁盘文件”复选框

指定是否要删除磁盘数据。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

删除网络接口：VMware vCenter

通过“删除网络接口”操作类型，您可以从虚拟机中删除虚拟 NIC。

操作定义的“详细信息”部分包含以下字段：

虚拟中心

指定 VMware vCenter 所在服务器的名称。从下拉列表中选择一个名称。

数据中心

指定虚拟机所在 VMware vCenter 中数据中心的名称。从下拉列表中选择一个名称。

虚拟机

指定要删除其虚拟 NIC 的虚拟机的名称。从下拉列表中选择一个名称。

网络接口

指定要删除的虚拟 NIC。从下拉列表中选择一个。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

从服务中删除服务器

通过“从服务中删除服务器”操作类型，您可以从现有服务中删除服务器。

操作定义的“详细信息”部分包含以下字段：

服务

指定服务名称。

服务器列表（逗号分隔）

指定要从服务中删除的服务器的列表。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

运行操作

通过“运行操作”操作类型，您可以运行操作。

操作定义的“详细信息”部分包含以下字段：

操作名称

指定操作。

事件源

指定操作源。

事件消息

指定事件消息。

规则名称

指定操作的规则。

服务器名称

指定操作的服务器。

服务名称

指定操作的服务。

传播

指定针对 -service_name 选项中指定的服务的所有服务器运行操作。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

运行操作序列

通过“运行操作序列”操作类型，您可以针对某个规则选择多个操作，并以定义的序列运行这些操作。

操作定义的“详细信息”部分包含以下字段：

若中断则重新启动

如果操作序列中断，则重新启动它。操作不会从中断点恢复，而是从头重新启动序列。

操作序列

提供操作和条件的单行选项或多行选项。选择“操作序列”后，会启用下拉列表。如果未选择，则文本将显示在表单元中。

顺序

指定操作的序列。

注意：如果操作序列退出时不符合条件，则默认的返回代码为 -1。

操作

指定操作名称。可以从下拉列表的可用操作中选择操作。

条件名称

指定用于确定下一个要运行的操作的条件。可以创建自己的自定义条件，也可以使用下列预定义条件之一：

- 故障中
- 成功时

注意：按照创建顺序对条件进行评估。

下一步

根据条件的结果，指定下一个要运行的操作。

继续

在条件评估为 true 时，继续下一个操作。

退出 (RC=0)

在条件评估为 true 时，退出序列并将代码 0 返回到日志。

退出并显示 RC（RC=操作 RC）

在条件评估为 true 时，退出操作序列并显示操作的返回代码。

中止 (RC=-1)

在条件评估为 true 时，停止操作序列并将代码 -1 返回到日志。

转到 #

在条件评估为 true 时，继续指定的操作序列号。

添加操作

将新操作添加到表中，并自动生成新的序列号。

添加条件

将新条件添加到操作中。

删除

删除选定的行并更新序列号。行可以包含操作或条件。该功能允许您在不删除整个操作的情况下删除操作的条件。

保存

保存操作序列。

注意：如果序列中最后一个操作的“下一步”设置为*继续*，则设置会自动更改为“退出并显示 RC（RC=操作 RC）”，并有提示性消息通知您，序列中最后一个操作的“下一步”已更改。

运行命令脚本

通过“运行命令脚本”操作类型，您可以使用脚本从处理命令的服务器运行外部命令。例如，如果从“开始”页面运行命令，则目标命令必须与运行该命令的 Windows 排定程序位于同一服务器上。由于进行规则评估而运行命令时，操作会由于运行作业而在托管 Windows 排定程序服务器的计算机上运行。

操作定义的“详细信息”部分包含以下字段：

命令行

指定要运行的命令或替代字符串。或者，您也可以使用自动生成的文本或从事件消息中提取的文本。

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

设置运行状况

通过“设置规则运行状况”操作类型，可将系统的运行状况设置为下列任一状况：“警告”、“轻微”、“重大”或“严重”。

操作定义的“详细信息”部分包含以下字段：

运行状况

指定下列操作之一：

- 警告
- 轻微
- 重大
- 严重

要求核准

选择该字段以指定票单需要第三方核准。

注意：CA SDM 必须配置为使用该选项。

核准或拒绝时自动关闭票单

选择该字段以在核准或拒绝票单后关闭。

注意：CA SDM 必须配置为使用该选项。

票单类型

从下拉列表中选择有效票单类型。根据您的配置，有效类型包括：

- 默认
- 突发事件
- 问题
- 请求

注意：CA SDM 必须配置为使用该选项。

模板

指定要用于创建票单的模板。从下拉列表中选择模板。根据选择的票单类型，使用相应的值填充表单。

注意：CA SDM 必须配置为使用该选项。

创建自定义操作

可以通过定义替代参数来创建自定义操作类型。自定义操作类型将添加到包含预定义操作类型的“操作类型”下拉列表中。

遵循这些步骤:

1. 在“浏览”窗格中，选择“数据中心”节点。
2. 依次单击“资源”、“策略”和“自定义操作类型”选项卡。

   此时将显示“自定义操作类型”页面。
3. 单击 +（添加）。

   此时将显示“自定义操作类型: 新增”部分。

4. 填写下列字段，以定义新的操作类型和替代参数，然后单击“保存”：

   操作类型名称

   指定新操作类型的名称。

   命令

   定义操作类型的命令行结构。您可以作为命令的一部分定义用于替换的替代参数（如 %SERVER%、$MYKEY$ 等等）。每个命令只能使用一次替代密钥。例如，在一个命令中只能使用一次 %SERVER% 替代密钥。

   替代密钥

   为替代密钥定义唯一字符串。替代密钥名称必须与命令中定义的名称匹配。定义多个替代密钥时，请分别定义每个替代密钥。

   提示

   定义与要在创建操作时输入的替代参数关联的参数名称。

   默认值

   定义默认的替代密钥值。

   新参数将出现在替代参数列表中。

5. 从“操作”下拉列表中选择“保存”。

   将保存自定义操作类型。

定义操作序列

可以为规则定义操作序列。如果规则的条件计算为 true，则运行您定义的操作序列。还可以创建自定义条件并将其构建到序列中。

注意：还可以将操作序列排定为作业或使用 dpmpolicy runaction CLI 命令运行。

遵循这些步骤:

1. 在“浏览”窗格中，选择“数据中心”节点。
2. 依次单击“资源”、“策略”和“操作”选项卡。

   此时将显示“操作”页面。

3. 单击 +（添加新操作）。

   此时将显示“操作定义: 新建”部分。

4. 为操作序列键入有意义的“名称”，然后从“类型”下拉菜单中选择“运行操作序列”。

   此时将显示“条件逻辑”部分。

5. 将“若中断重新启动”复选框保留为选中状态，以便在异常终止后重新启动序列。序列将重新启动之前执行的最后一个操作并继续。清除该复选框可阻止序列在异常终止后继续。
6. 在“操作序列”窗格中单击 +（“添加”操作），以向操作序列中添加操作。“添加操作”将在操作序列结尾添加新操作。如果要在序列中间插入操作，请删除所需位置之后的所有操作。插入新操作，然后重新定义删除的操作。
7. 选择条件以为操作序列构建条件逻辑。新条件逻辑只能添加到条件逻辑序列的末尾。如果要在序列中间插入新条件逻辑，请删除所需插入点之后的所有条件逻辑。插入新条件逻辑，然后重新定义删除的条件逻辑。
8. 为每个附加的条件逻辑序列选择条件逻辑评估的类型。输出类型包括：

   返回代码

   评估操作返回代码。

   注意：用于返回代码评估的有效比较运算符包括：==、!=、>、<、>=、<=

   STDOUT

   在标准输出中搜索特定字符串。

   STDERR

   在标准错误中搜索特定字符串。

   注意：用于 STDOUT 和 STDERR 的有效比较运算符包括“包含”和“不包含”。

   注意：可以使用“逻辑 OP”字段 (AND/OR) 来链接条件。对于最后的条件，“逻辑 OP”会自动设置为 NOOP。

   新条件逻辑将添加到序列中。
9. 完成条件时，单击“保存条件”。

   将保存条件。
10. 在“操作序列”窗格中单击“保存”。

    将保存操作。

    出于测试目的，您可以通过从“操作”页面中选择操作并单击“运行操作”图标来运行该操作。

定义排定

您可以排定操作以在预定义的时间运行。例如，可以使用默认的 Windows 排定程序来排定每天必须执行的操作或定期执行的操作，如维护任务。

遵循这些步骤:

1. 在“浏览”窗格中，选择“数据中心”节点。
2. 依次单击“资源”、“策略”和“已排定操作”选项卡。

   此时将显示“已排定操作”页面。
3. 填写下列字段：

   名称

   定义已排定操作的名称。

   前通知

   指定是否在运行已排定操作之前生成事件。事件将显示在显示版中。

   后通知

   指定是否在运行已排定操作之后生成事件。事件将显示在显示版中。

   频率

   指定排定操作运行的频率：一次、每日、每周、每月一次（天）或每月一次（周内某日）

   日期

   定义启动已排定操作的日期。

   时间

   定义运行已排定操作的时间。

   注意：您不需要输入秒数，因为它们不用于排定作业。

   类型

   指定用于您正在排定的操作的操作类型。

   注意：排定程序不支持包含替代参数的操作（唯一的例外是 %AutoIncrement(0)% 和 %AutoDecrement(0)%）。只能通过策略规则评估来运行包含替代参数的操作。

   操作

   列出已为每种操作类型创建的操作。

   注意：列表不包括指定服务台核准要求的操作。

4. 从下拉列表中选择“保存”。

   将显示一条消息，确认您的操作已排定。已排定操作将出现在“已排定操作”列表的“已排定作业”列表中。

   注意：指定帮助台核准要求的操作无法用于操作排定。如果需要将相同操作用于排定操作，请创建不包括服务台核准要求的另一个操作。

创建自动化策略

可以使用创建自动化策略向导基于两个预定义策略类型来创建自动化规则：

- 虚拟机动态资源代理－根据定义的使用率阈值动态更改 CPU 和内存分配。
- 总使用率度量标准阈值监控－运行状况是根据总使用率设置的。

遵循这些步骤:

1. 打开“管理”窗格，然后单击“创建自动化策略”。

   此时将显示“创建自动化策略”向导。

2. 选择策略类型，并且单击“下一步”来选择目标资源并为规则设置条件。

   “策略摘要”将显示结果。

3. 单击“完成”。

   策略已确认，且已创建相应的规则。

策略用例

以下方案演示了实施策略的一些用例。

详细信息：

用例：向服务中添加服务器 (p. 681)
用例：向服务中添加新规则 (p. 681)
用例：定义操作 (p. 681)

用例：向服务中添加服务器

该用例演示向以前创建的服务中添加服务器的过程。

1. 验证向服务中添加服务器的先决条件：
   - 服务存在。
   - 服务器存在。
   - 已为服务分配优先级。
   - 用户有权修改服务。
2. 将服务器添加到服务中。
3. 验证向服务中添加服务器的结果：
   - 该服务器现在是服务的成员。
   - 现在服务的使用率中包含该服务器。
   - 包括该服务现在会影响使用率的任何服务规则。

用例：向服务中添加新规则

该用例演示向服务中添加新规则的过程。

1. 验证向服务中添加规则的先决条件：
   - 服务存在。
   - 用户有权创建规则。
   - 服务器在服务中。
2. 为该服务创建规则定义。
3. 验证向服务中添加规则的结果：
   - 已创建新规则。
   - 将为适用于规则条件的所有服务评估新规则。

用例：定义操作

该用例演示用于排定作业或策略规则的操作的定义过程。

1. 验证定义操作的先决条件：
   - 用户有权定义操作。
   - 已发现预期操作定义需要的资源。

2. 在 CA Virtual Assurance 用户界面中定义操作的属性和操作的名称。
3. 验证向服务中添加服务器的结果：
   - 已使用用户提供的说明创建操作。
   - 操作现在可用于规则。
   - 操作现在可用于作业排定。

   注意：指定帮助台核准要求的操作无法用于操作排定。如果需要将相同操作用于排定操作，请创建不包括服务台核准要求的另一个操作。

配置数据收集

可以控制在数据中心中收集数据的方式，包括以下方面：

- 收集度量标准的时间间隔
- 从中收集度量标准的系统（过滤）
- 针对每个服务器收集的度量标准
- 数据时效和数据到期日期（数据的保留时间）。

详细信息：

有关度量标准收集的要点 (p. 682)
为数据中心配置数据收集 (p. 685)
为服务器配置数据收集 (p. 686)
为虚拟资源配置数据收集 (p. 688)
配置性能阈值 (p. 690)
配置度量标准筛选 (p. 690)

有关度量标准收集的要点

要在选择度量标准时做出明智的决策，请查看这些要点，以了解 CA Virtual Assurance 性能和应用程序度量标准收集：

- CA Virtual Assurance 如何收集度量标准数据？CA Virtual Assurance 与 CA Systems Performance LiteAgent 或远程计算机上的 SystemEDGE 代理通信，以收集指定的系统度量标准。

  在您要从中收集基础系统度量标准的任何服务器上安装 CA Systems Performance LiteAgent 或 SystemEDGE 代理。如果 SystemEDGE 代理已存在，则不需要 CA Systems Performance LiteAgent。如有必要，可以使用产品用户界面安装 SystemEDGE 代理。所有性能度量标准都存储在性能数据库中。

- 如何计算总体使用率？总体使用率是当前为 CA Virtual Assurance 管理的服务器收集的所有度量标准的合计计算。计算基于度量标准的值以及为正常操作定义参数的用户定义阈值。

  注意：在用户界面的“策略、度量标准、阈值”部分中选择“为总体计算包括”，以便在总体使用率计算中包括新度量标准。如果您包括该度量标准，则 CA Virtual Assurance 在评估服务器状态时提供最新结果。

- 度量标准评估如何影响总体使用率？表中提供的度量标准详细信息可帮助您了解 CA Virtual Assurance 对不同度量标准的评估方式。每个度量标准都有一个设置为 *exact* 或 *complement* 的方法属性。较高的精确值与较低的精确值相比，表示更糟糕的情况，因为它指示总体使用率上升。较高的补充值表示较积极的情况，因为它指示总体使用率下降。通常，较高的精确值会对总体使用率产生负面影响，较低的精确值会对总体使用率产生正面影响。相比之下，较高的补充值会对总体使用率产生正面影响，较低的补充值会对总体使用率产生负面影响。例如，如果“内存: 使用中的已提交字节数百分比”的值增大，则系统的总体使用率将上升。如果“内存: 可用 MB”的值增大，则总体使用率将下降。

默认度量标准是什么？默认度量标准定义位于所有受支持平台的“筛选”部分的度量标准列表中。可在度量标准列表中找到默认度量标准指示器，即“默认”列中的值为“是”。添加服务器时，CA Virtual Assurance 使用该列表来获取度量标准定义。在“筛选”部分可以配置平台、类型、子类型、实例以及要收集的数据类型。每个服务器的度量标准筛选和定义都存储在性能数据库中。

- 性能数据当前是否可供我的系统使用？默认情况下，如果无法收集数据，CA Virtual Assurance 不会对服务器状态产生负面影响。缺乏数据不反映服务器的紧急程度。通过查看事件列表或选择特定系统，您可以确定是否正在收集度量标准数据。但是，有时需要使用更直接的方法来确定收集的数据是否可用，或者性能数据很关键。配置 CA Virtual Assurance，以便在无法收集性能数据时，自动将系统的状态更改为“警告”或者“严重”。要在性能数据不可用的情况下轻松标识系统，请修改位于 CA Virtual Assurance *install_path*\conf 目录中的 caaipconf.cfg 文件。使用文本编辑器打开该文件，找到如下所示的运行状况属性：

```
<property name="CONFIG_KEY_DEFAULT_HEALTH_STATE">
            <!-- Valid values: 0 (Unknown); 5 (OK); 10 (Warning); 15 (Minor
Failure); 20 (Major Failure); 25 (CriticalFailure) -->
            <!-- Changes the value of HealthState for the CA_CollectionState
object associated to the CA_ComputerSystem -->
            <!-- If set to 30, CE will not set the HealthState. -->
            <value>5</value>
            <displayName>Default node health state when problem encountered in
metric or data collection</displayName>
        </property
```

CA Virtual Assurance 将值 XML 元素所包围的值修改为其他支持的值之一（例如，分别表示正常或警告的 5 或 10）。这些更改可以在无法收集性能数据时反映所需的状态。例如：

```
<property name="CONFIG_KEY_DEFAULT_HEALTH_STATE">
            <!-- Valid values: 0 (Unknown); 5 (OK); 10 (Warning); 15 (Minor
Failure); 20 (Major Failure); 25 (CriticalFailure) -->
            <!-- Changes the value of HealthState for the CA_CollectionState
object associated to the CA_ComputerSystem -->
            <!-- If set to 30, CE will not set the HealthState. -->
            <value>10</value>
            <displayName>Default node health state when problem encountered in
metric or data collection</displayName>
        </property
```

因为 <value> 已更改为“10”，所以在 CA Virtual Assurance 用户界面中那些没有可用性能数据的系统显示为警告状态。

注意：有关性能度量标准和说明的列表，请参阅*《性能度量标准参考》*。

为数据中心配置数据收集

您可以在数据中心级别配置数据收集。数据中心级别策略会立即生效。

遵循这些步骤:

1. 单击“资源”，并在“浏览”窗格中选择“数据中心”文件夹。
2. 右键单击并依次选择“策略”、“配置收集设置”。

   将显示“设置”对话框。
3. 在“收集设置”部分中填写以下字段：

   数据记录间隔(秒)

   定义数据收集并存储在性能数据库中的频率。

   默认值： 300 秒

   注意： CA Technologies 建议，对于所监控环境中的每 1000 台计算机，以 300 秒为增量增加数据记录间隔。

   轮询数据保留(天)

   定义轮询数据存储在性能数据库中的时长。定义该值时，请考虑收集的受管系统、服务以及度量标准的数量。存储的轮询数据对象随着时间的推移不断累积且可以影响性能。如果出现性能问题，请减少保留天数。

   默认值： 10 天

   每日汇总数据保留(天)

   指定每日数据平均值存储在性能数据库中的时长。

   最大值： 365

   默认值： 365
4. 在“阈值”部分中输入阈值限制，然后单击“保存”。

   设置将会保存。

为服务器配置数据收集

可以为各个服务器配置数据收集。使用此程序可配置特定服务器，以便为数据中心收集数据。您还可以选择要监控的度量标准、设置各个度量标准的阈值以及在总使用率中包括度量标准。

遵循这些步骤:

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 打开“数据中心”文件夹，并选择服务器所属的服务。
3. 右键单击并选择“策略”。

   此时将显示“策略”子菜单。

4. 单击“度量标准”。

   将打开“度量标准”向导。

5. 选择要为其配置数据收集的服务器。
6. 在“设置间隔”对话框中填写以下字段：

   使用默认

   选中复选框时，将数据中心级别指定为默认值。如果取消选中复选框，则使用您指定的值。

数据记录间隔(秒)

定义数据收集并存储在性能数据库中的频率。

默认值：300 秒

注意：CA Technologies 建议，对于所监控环境中的每 1000 台计算机，以 300 秒为增量增加数据记录间隔。

每日汇总数据保留(天)

指定每日数据平均值存储在性能数据库中的时长。

最大值：365

默认值：365

轮询数据保留(天)

定义轮询数据存储在性能数据库中的时长。定义该值时，请考虑收集的受管系统、服务以及度量标准的数量。存储的轮询数据对象随着时间的推移不断累积且可以影响性能。如果出现性能问题，请减少保留天数。

默认值：10 天

7. 从“可用度量标准”部分选择要监控的度量标准，然后单击向下箭头。

   选定的度量标准将移至“要收集的选定度量标准”部分。

   注意：如果禁用默认度量标准（CPU 和内存）并启用其他，则直到您修改最新选定的度量标准的阈值，您才会看到总使用率。

8. 可以为每台服务器配置要监控的性能度量标准并为每个度量标准设置阈值界限。选择要设置阈值的度量标准并填写以下字段：

   上限阈值

   定义所选度量标准组的使用率上限。

   默认值：80%

   下限阈值

   定义所选度量标准组的使用率下限。

   默认值：20%

   包括以计算总体

   指定您希望将选定的度量标准包含在总使用率计算中，且由 CA Virtual Assurance 评估。

9. 单击“完成”以保存设置。

为虚拟资源配置数据收集

您可以为虚拟平台以及在这些平台上创建和管理的虚拟资源配置数据收集。如果您要配置特定虚拟机或其他资源，从而以不同于数据中心默认值的间隔来收集数据，请使用此程序。您还可以选择要监控的度量标准、设置各个度量标准的阈值以及在总使用率中包括度量标准。

您可以为以下虚拟平台对象配置数据收集：

- vCenter 服务器
- vCenter 数据中心
- vCenter ESX 服务器
- vCenter 虚拟机
- Hyper-V
- Microsoft 群集
- Microsoft 群集节点
- IBM PowerVM 服务器
- IBM 逻辑分区
- Solaris Zones 服务器
- Solaris Zone

为虚拟资源配置数据收集

1. 单击“资源”，然后打开“浏览”窗格。
2. 展开“数据中心”或“MS 群集服务”文件夹，然后打开任何子文件夹，并选择要配置的对象。

   该对象的子选项卡将出现在右侧窗格中。

   注意：如果选择顶级文件夹（如“VMware vCenter 服务器”）或尚未为其收集数据的对象（如 vCenter 群集），则必须选择该文件夹中包含的特定对象或要为其配置数据收集的对象。

   注意：如果您选择“MS 群集服务”作为顶级文件夹，则可看到群集及其节点。

3. 右键单击并依次选择“策略”、“配置服务器度量标准收集”。

   注意：如果为 Solaris Zones 选择顶级文件夹，则“系统”部分中的“硬件类”列总是显示“其他”值。

4. 从“可用度量标准”部分中选择要监控的度量标准，然后单击向下箭头。

   所选度量标准将移动到“要收集的选定度量”部分。

   注意：如果禁用默认度量标准（CPU 和内存）并启用其他，则直到您修改最新选定的度量标准的阈值，您才会看到总使用率。

5. 单击“保存”以应用选定的度量标准。

6. 右键单击资源，并依次选择“策略”、“配置收集设置”。

7. 在“收集设置”部分中填写以下字段：

   使用默认

   选中复选框时，将数据中心级别指定为默认值。如果取消选中复选框，则使用您指定的值。

   数据记录间隔(秒)

   定义数据收集并存储在性能数据库中的频率。

   默认值：300 秒

   注意：CA Technologies 建议，对于所监控环境中的每 1000 台计算机，以 300 秒为增量增加数据记录间隔。

   每日汇总数据保留(天)

   指定每日数据平均值存储在性能数据库中的时长。

   最大值：365

   默认值：365

   轮询数据保留(天)

   定义轮询数据存储在性能数据库中的时长。定义该值时，请考虑收集的受管系统、服务以及度量标准的数量。存储的轮询数据对象随着时间的推移不断累积且可以影响性能。如果出现性能问题，请减少保留天数。

   默认值：10 天

8. 单击“保存”以保存设置。

注意：将使用默认阈值。如果要修改阈值，必须单独执行此操作。

配置性能阈值

可以为每台服务器配置要监控的性能度量标准并为每个度量标准设置阈值界限。

遵循这些步骤:

1. 打开“浏览”窗格。

   将出现可用的组、服务和系统。

2. 展开“数据中心”文件夹及任何子文件夹，然后选择要配置的服务器。导航到虚拟服务器，以选择特定虚拟资源，如虚拟机或逻辑分区。

3. 右键单击并选择“策略”。

   此时将显示“策略”子菜单。

4. 单击“配置阈值设置”。

   将显示“配置阈值设置”。

5. 选择要设置阈值的度量标准并填写以下字段：

   阈值上限(%)

   定义所选度量标准组的使用率上限。

   默认值：80%

   阈值下限(%)

   定义所选度量标准组的使用率下限。

   默认值：20%

   为总使用率计算包括

   指定您希望选定的度量标准包含在总使用率计算中，且由 CA Virtual Assurance 评估。

6. 单击“修改”以保存设置。

配置度量标准筛选

您可能需要向数据中心的度量标准筛选中添加度量标准或从中删除度量标准，具体取决于您要监控的性能度量标准。

配置度量标准筛选

1. 在“浏览”窗格中选择“数据中心”文件夹。
2. 右键单击并依次选择“策略”、“配置收集条件”。

   此时将显示“收集条件”对话框。

3. 执行以下操作之一：

   - 选中现有度量标准对应的复选框，以修改现有条目。选定度量标准的信息将填充“详细信息”部分的字段。进行任何更改，然后单击“更新”。
   - 选择一个 OS，填写“详细信息”部分中的字段以添加新度量标准，然后单击“添加”。

   将保存度量标准。

   “详细信息”部分包含以下字段：

   操作系统

   定义受监控的度量标准的操作系统。

   类型

   定义受监控的度量标准的类型。

   示例：

   类型：CA 磁盘组

   子类型：每秒写入（平均）

   子类型

   定义哪方面的度量标准正在受监控。

   示例：

   类型：CA 磁盘组

   子类型：每秒读取（平均）

   实例

   定义 MIB 层次结构中受管对象的实例。

   示例：

   类型：vmvcaim.StatClusterEffectiveCPU

   子类型：1.3.6.1.4.1.546.16.52.2.7.2.1.14

   实例：%3 [%2]

   在 %<n> 中，<n> 是在与各自的 AIM MIB 表中的第 n 列中对应的任意值匹配的实例下列出的数值。例如，vmvcAimStatClusterTable 代表所有行条目（同一受管对象的实例）。这在所有实例可用的情况下瞬时收集其受管对象的度量标准时十分有用（无需用户输入）。

   阈值上限(%)

   定义所选度量标准组的使用率上限。

   默认值：80%

阈值下限(%)

定义所选度量标准组的使用率下限。

默认值：20%

延迟

定义生成阈值事件之前连续违反阈值的次数。配置该选项以避免淹没阈值评估的事件。可以定义记录阈值违反事件的操作，并为阈值监控设置规则。

方法

指定收集方法是补充、补充增量、精确还是精确增量。补充方法包括尚未包含在该集的子集中的度量标准。精确方法收集指定的精确度量标准。

类别

指定监控的度量标准是系统、应用程序还是 SNMP 度量标准。

选定默认收集度量标准

指定 CA Virtual Assurance 是否默认收集筛选指定的度量标准。除非度量标准筛选设为默认，否则 CA Virtual Assurance 不会自动地收集指定的度量标准。

为总使用率计算包括

指定您希望选定的度量标准包含在总使用率计算中，且由 CA Virtual Assurance 评估。

为收集激活

在评估可用于收集的度量标准时，指定该度量标准筛选有效可用。

4. 选中要删除的任何度量标准对应的复选框，然后单击“删除”。

选定的条目将被删除。

附录 A： FIPS 140-2 加密

此部分包含以下主题：

FIPS 概述

联邦信息处理标准 (FIPS) 140-2 发布是产品应用于加密的加密库和算法的安全标准。FIPS 140-2 加密会影响 CA 产品的组件之间以及 CA 产品和第三方产品之间所有敏感数据的通信。FIPS 140-2 指定在安全系统内使用加密算法来保护未分类的敏感数据的要求。

CA Virtual Assurance 使用适用于美国政府的高级加密标准 (AES)。CA Virtual Assurance 合并 RSA Crypto-J v3.5 和 Crypto-C ME v2.0 加密库，这些加密库已经过验证，符合加密模块的 FIPS 140-2 安全要求。

附录 B： 工具

此部分包含以下主题：

使用 NodeCfgUtil 配置 AIM

使用节点配置实用工具，您可以配置 SystemEDGE AIM，而不使用 CA Virtual Assurance 用户界面。

本节描述该实用工具的“对话模式”和“命令模式”。

详细信息：

NodeCfgUtil 概述

要配置 AIM 并发现虚拟环境，请执行以下操作之一：

- 从用户界面打开“管理”选项卡，依次转到“配置”、“开通”，选择相应的服务器类型以添加凭据，然后配置 AIM。CA Virtual Assurance 会自动发现物理组件和虚拟组件并填充管理数据库。
- 在 Windows AIM 服务器上使用 NodeCfgUtil.exe 实用工具来为管理虚拟环境添加所需数据。该实用工具位于 *SystemEDGE_install_path*\plugins\AIPCommon 目录中。然后从 CA Virtual Assurance 管理器重新发现 AIM 服务器。使用该选项可以手工执行所需步骤。

请考虑以下准则

- 为访问虚拟环境或群集指定的用户必须具有足够的权限以进行远程访问。
- 要管理 Hyper-V 服务器，请在 Hyper-V 服务器上安装 SystemEDGE 和 Hyper-V AIM。SystemEDGE 和 Hyper-v AIM 必须在同一台 Hyper-V 服务器上运行。然后配置 AIM 并发现 Hyper-V 服务器。

- Citrix XenServer AIM 只能连接到池主服务器或独立的 Citrix XenServer。否则，AIM 无法运行。
- 要管理 VMware vSphere，请为相应的 vCenter 服务器输入凭据。
- 要优化 VM 的虚拟化，请在 VM 上安装相应的系统工具。仅当安装这些工具时，许多功能才可用。根据您的环境请使用下列系统工具：
  - （适用于 VMware）VMware 工具
  - （适用于 XenServer）XenTools
  - （适用于 RHEV）RHEV Guest Tools

  注意：有关相应系统工具的更多信息，请参阅第三方文档。

从 AIM 服务器中发现支持的环境：

1. 确认未在 CA Virtual Assurance 管理器服务器上运行的 SystemEDGE 和 AIM 使用与其关联的 CA Virtual Assurance 管理器相同的 SNMP 设置。
2. 在 Windows AIM Server 上运行 NodeCfgUtil.exe 实用工具，以便更新相应 AIM 的配置数据。

   NodeCfgUtil.exe 实用工具将每个 AIM 的数据存储在文件（例如，zone.cfg、vc.cfg...）中。
3. 打开管理器服务器上的用户界面，然后依次单击导航窗格中的“资源”、“数据中心”。
4. 右键单击并选择“管理”、“发现”。

   将显示发现选项。
5. 请选择以下操作之一：
   - 发现系统
   - 发现网络

   将打开相应的对话框。
6. 输入要管理的服务器的系统名称。或者，可以为发现过程输入网络属性。单击“确定”。

   CA Virtual Assurance 将启动发现过程。

   发现的资源将显示在“浏览”窗格中。

详细信息

如何配置 vCenter 服务器管理组件 (p. 467)

在对话框模式下使用 NodeCfgUtil 配置 AIMs

通过 NodeCfgUtil.exe，可以修改 IBM PowerVM、IBM PowerHA、Solaris Zones、VMware vCenter、VMware vCloud、Microsoft 群集、Cisco UCS、Citrix XenServer、Citrix XenDesktop、RHEV、Active Directory 和 Exchange Server (ADES) 或 Huawei GalaX 的 AIM 配置。该实用工具将相应 AIM 的配置文件写入 *sysedge_InstallLpath\plugins\AIPCommon* 目录。还可使用 NodeCfgUtil 实用工具编辑或删除现有条目。

在对话框模式下使用该实用工具可配置相应 AIM 管理的节点。

注意：以 Windows 管理员身份运行 NodeCfgUtil.exe。

遵循这些步骤:

1. 以管理员身份登录，并在安装 AIM 的计算机上打开 Windows 资源管理器。
2. 转到 *SystemEDGE_InstallPath*\plugins\AIPCommon 目录，然后启动 NodeCfgUtil.exe。

   NodeCfgUtil 将发现已安装的 AIM，并在随后的对话框中将其列出。
3. 输入 *1* 添加一个新的受管节点。
4. 按照屏幕指示完成配置。每个节点都需要有效的用户名和密码进行身份验证。

   在配置之后，输入 0 返回上一菜单或退出实用工具。

通过 NodeCfgUtil 将 Solaris Zones (zone.cfg)、vCenter 服务器 (vc.cfg)、vCloud Director (vcloud.cfg)、Microsoft 群集 (mscs.cfg)、Citrix XenServer (cxen.cfg)、UCS (ucs.cfg)、PowerVM (lpar.cfg)、PowerHA (hacmp.cfg)、RHEV (kvm.cfg)、Huawei GalaX (galaxa.cfg)、Citrix XenDesktop (xendesktop.cfg) 或 ADES (esad.cfg) 的配置文件写入 *SystemEDGE_InstallPath*\plugins\AIPCommon 目录。

注意：还可使用 NodeCfgUtil 实用工具编辑或删除现有条目。相应的对话框意义自明。

示例

以下示例显示了已成功添加到 vCenter AIM 配置的 myvc5 服务器的“安装受管节点”对话框。AIM 现在已准备好管理 vCenter 服务器。vCenter AIM 是多实例 AIM。因此可以重复该步骤，并可以添加更多想要使用该 AIM 管理的 vCenter 服务器。

```
***** 主菜单 *****
1. 安装受管节点
2. 修改受管节点

3. 删除受管节点

0. 退出

************************

输入选择：

****  选择受管节点  ****
1. IBM PowerVM
2. Oracle Solaris Zones
3. Citrix XenServer
4. VMware vCenter
5. Cisco UCS
6. Microsoft 群集服务
7. Microsoft Active Directory 和 Exchange Server
8. IBM PowerHA
9. VMware vCloud Director
10. Red Hat Enterprise Virtualization
11. Huawei GalaX
12. Citrix XenDesktop
0.  返回上一个菜单
*******************************
输入选择：4
为 VMware vCenter 节点输入以下信息...

（要在任一点返回到上一个菜单，请按 CTRL + Q 键）。

1. 服务器名称：myvc5
2. 用户名：administrator
3. 密码：*********
4. 端口 [默认=443]:
5. 协议 [默认=https]:

CAAC1016 正在身份验证，请稍候...
CAAC1019 身份验证成功。
CAAC1023 添加节点成功。

按任意键继续...
```

以下示例显示了已成功添加到 ADES AIM 配置的 mydomain 的“安装受管节点”对话框。“管理实体”设置为“Active Directory”。“管理模式”设置为“整个域”。有关详细信息，请参阅 NodeCfgUtil 命令模式。ADES AIM 是多实例 AIM。因此可以重复该步骤，并可以添加更多想要使用该 AIM 管理的实体。

```
****  选择受管节点  ****
1. Microsoft 群集服务
2. Microsoft Active Directory 和 Exchange Server
0. 返回上一个菜单 ********************************
输入选择：2
为“Microsoft Active Directory 和 Exchange Server”节点输入以下信息...

（要在任一点返回到上一个菜单，请按 CTRL + Q 键）。

1. 域名：mydomain
2. 用户名：administrator
3. 密码：************
4. 管理实体：0
5. 管理模式：0

CAAC1016 正在身份验证，请稍候...
CAAC1018 凭据身份验证成功。

按任意键继续...
```

以下示例显示了已成功添加到 LPAR AIM 配置的 HMC1 服务器的“受管系统”对话框。AIM 发现与 HMC 服务器相关的所有虚拟 I/O 服务器后，这些服务器在 NodeCfgUtil 中均可见，并且可以修改每个服务器以指定其凭据。AIM 将第一个完全配置的 VIO 服务器的凭据用作所有尚未配置的 VIO 服务器的默认凭据。因此，如果所有 VIO 服务器共享凭据，则只需指定一个 VIO 服务器的凭据。否则，需要使用不同凭据配置每个 VIO 服务器。AIM 现在已准备好管理 HMC 服务器。

```
****  选择受管节点  ****
1. IBM PowerVM
0. 返回上一个菜单
********************************
输入选择：1
现有条目列表...
1. hmc：HMC1.company.com
2. vio：ibm101.company.com
```

```
选择要修改的条目（0 表示返回上一个菜单）：2
输入 IBM LPAR 节点的以下信息...
（要在任一点返回到上一个菜单，请按 CTRL + Q 键）。
1. 服务器名称：ibm101
2. 用户名：admin
3. 密码：*********

CAAC1016 正在身份验证，请稍候...
CAAC1019 身份验证成功。
CAAC1024 修改节点成功。

按任意键继续...
```

以下示例显示了已成功添加到 GalaX AIM 配置的 *myserver* 的“安装受管节点”对话框。有关详细信息，请参阅 NodeCfgUtil 命令模式。GalaX AIM 是多实例 AIM。因此可以重复该步骤，并可以添加更多想要使用该 AIM 管理的实体。

注意：要配置 Huawei GalaX 组件，需要指定证书文件名。

```
****  选择受管节点  ****
1. Huawei GalaX
0. 返回上一个菜单
*******************************
输入选择：1
输入 Huawei GalaX 节点的以下信息...

（要在任一点返回到上一个菜单，请按 CTRL + Q 键）。

1. 服务器名称：myserver
2. 证书文件名：certificatename123.p12
3. 密码：************
4. 端口 [默认值 = 8773]：
5. 协议 [默认值 = http]：

CAAC1016 正在身份验证，请稍候...
CAAC1018 凭据身份验证成功。

按任意键继续...
```

在命令模式下使用 NodeCfgUtil 配置 AIM

通过 NodeCfgUtil.exe，可以修改 IBM PowerVM、IBM PowerHA、Solaris Zones、VMware vCenter、VMware vCloud、Microsoft 群集、Cisco UCS、Citrix XenServer、Citrix XenDesktop、RHEV、Active Directory 和 Exchange Server (ADES) 或 Huawei GalaX 的 AIM 配置。该实用工具将相应 AIM 的配置文件写入 *sysedge_InstallLpath\plugins\AIPCommon* 目录。还可使用 NodeCfgUtil 实用工具编辑或删除现有条目。

在命令模式下使用该实用工具时，只能将受管节点添加到 AIM 配置。

注意：以 Windows 管理员身份运行 NodeCfgUtil.exe。

此命令具有以下格式：

```
(1) nodecfgutil -help
(2) nodecfgutil {lpar|zone|mscs} -u user -p password -h
{pvmname|hostname/cluster_name}
(3) nodecfgutil {vc|ucs} -u user -p password -h hostname -t port -c protocol
(4) nodecfgutil ades -u user -p passwd -d domainname -e entity -o option
(5) nodecfgutil {xen|vcloud|xenserver} -u user -p passwd -h hostname
(6) nodecfgutil {powerha|kvm} -u user -p password -h {cluster_name/hostname} [-t
port]
(7) nodecfgutil galax -u usercertificate -p password -h hostname [-t port] [-c
protocol]
```

-help

显示有关控制台的用法信息。

lpar|ucs|vc|zone|mscs|ades|xen|vcloud|powerha|kvm|galax|xendesktop

指定虚拟环境或物理环境。

-u *user*/*usercertificate*

相应地指定管理用户或用户证书的名称。

-p *password*

指定该用户的密码。

-h *hostname*

指定通过相应 AIM 管理的服务器的名称。

-d *domainname*

指定通过 ADES AIM 监控的域的名称。

-h *pvmname*

指定通过 LPAR AIM 管理的 IBM PowerVM 服务器（HMC 或 IVM）的名称。

- h *cluster_name*

指定群集的名称。

-t *port*

（可选）指定端口号。

-c *protocol*

（仅限于 vCenter、UCS）指定协议（HTTP、https）。

返回代码：0 成功，-1 失败

-e *entity*

指定受管实体。

0

指定要监控 Active Directory。

1

指定要监控 Exchange Server。

2

指定要监控 Active Directory 和 Exchange Server。

-o *option*

指定用于提供管理的选项。

0

指定要监控整个域。

1

指定要监控域的特定主机。

遵循这些步骤:

1. 在安装 AIM 的系统上打开命令提示符。

   将显示命令提示符。

2. 输入以下命令之一：

```
(1) nodecfgutil -help
(2) nodecfgutil {lpar|zone|mscs} -u user -p password -h
{pvmname|hostname/cluster_name}
(3) nodecfgutil {vc|ucs} -u user -p password -h hostname -t port -c protocol
(4) nodecfgutil ades -u user -p passwd -d domainname -e entity -o option
(5) nodecfgutil {xen|vcloud|xenserver} -u user -p passwd -h hostname
(6) nodecfgutil {powerha|kvm} -u user -p password -h {cluster_name/hostname}
[-t port]
(7) nodecfgutil galax -u usercertificate -p password -h hostname [-t port]
[-c protocol]
```

(1) 显示有关控制台的用法信息。

(2) 验证并存储为 Solaris Zones、IBM PowerVM 或 MSCS 传递的凭据。

(3) 验证并存储为 vCenter 或 Cisco UCS 传递的凭据。

(4) 验证并存储为 Active Directory 和 Exchange Server (ADES) 传递的凭据。

(5) 验证并存储为 Citrix XenServer、Citrix XenDesktop 或 VMware vCloud 传递的凭据。

(6) 验证并存储为 IBM PowerHA 或 Red Hat Enterprise Virtualization (KVM) 传递的凭据。

(7) 验证并存储为 HUAWEI Galax 传递的凭据和用户证书。

支持代理

支持代理收集诊断结果信息。要访问支持代理，请使用以下地址：

http://<Manager Server>:8556

用户界面无需加以说明并提供以下信息：

- 系统重要部件的性能度量标准
- 详细的 Web 服务使用率统计信息
- 日志文件监控
- 长期运行的 SQL 查询

附录 C： 故障排除

此部分包含以下主题：

调整适用于 Solaris Zones 环境的轮询间隔设置

症状：

我不知道如何调整适用于 Solaris Zones 环境的轮询间隔设置。

解决方案：

如果系统数和区域数增加，则增大 Solaris Zones AIM 的轮询间隔。例如，如果主机和区域的计数大于 100，则将默认轮询间隔设置为 240。

属性显示零值

症状：

属性显示零值。

解决方案：

如果值小于一，SystemEDGE 会将值向下舍入为零。

注意：zoneAimStatHostDiskSvc MIB 属性始终显示零值。

浏览器不在事件中显示连续空格

症状：

浏览器不在事件描述中显示一个以上的连续空格字符。

解决方案：

浏览器不显示一个以上的连续空格，这是因为根据 HTML 规格，额外的空格会被截断。将事件从浏览器中剪切并粘贴到规则中时应十分小心，因为事件说明可能会不同。

用户界面中未显示 Cisco UCS 文件夹

症状：

安装产品并配置了 Cisco UCS 服务之后，用户界面中未显示 Cisco UCS 文件夹。

解决方案：

打开配置了 UCS AIM 的服务器上的服务，验证 SystemEDGE 是否正在运行；如果 SystemEDGE 服务已停止，则重新启动该服务。启动 nodecfgtutil.exe 以验证 UCS 管理器节点的访问信息。使用 MIB 浏览器验证从 UCS 管理器轮询的数据。如果未填充 UCS 访问信息，请查看 sysedge 日志以获取其他信息。

数据库事务日志大小意外增大

症状：

在包含大量受管对象、配置更改和度量标准数据收集活动的数据中心中，管理数据库和性能数据库事务日志可能会意外增大。该问题可能会导致在资源有限的环境中磁盘空间变少。

解决方案：

要解决此问题，请参阅 Microsoft 支持网站上有关排除全部事务日志故障的知识库文章。

在默认 Microsoft SQL Server 安装中，事务日志文件 aom2.ldf 和 dpm.ldf 位于目录 C:\Program Files\Microsoft SQL Server\...\MSSQL\Data。

注意：如果数据库日志文件大小变小，请重新启动 Apache 服务来提高性能。

过时的 Solaris Zones AIM 属性始终显示为 N/A 或零

症状：

某些 Solaris Zones AIM MIB 的值始终显示为 N/A 或零。

解决方案：

Solaris Zones AIM 的以下 MIB 属性已过时，但保持向后兼容性。过时的 MIB 属性包括：

- zoneAimStatHostDiskMode
- zoneAimStatProcessorSetContainerList
- zoneAimStatProcessorSetResourcepoolId
- zoneAimStatProcessorSetResourcePoolIdList
- zoneAimStatProcessorSetResourcepoolName
- zoneAimStatProjectFSSEnabled
- zoneAimStatResourcePoolContainerList

域服务器不可用

症状：

域服务器不可用、已停止、无法正常运行或不在处理请求，并且服务控制器 (SC) 显示组件已启动并正在运行。

解决方案：

此行为是由于数据库连接失败或 AIM 密码过期所引起的，并且可能会影响策略配置和远程部署组件的行为。监控支持服务 Web 服务 (ISM) 可定期监控域服务器的功能。ISM 发现异常行为时，将向用户发送以下消息，通知状态中的更改：*CA SM 域服务已关闭或没有响应。*

可以使用以下命令监控状态：

```
Caaipscutil /status /id=ISM /user=<user> /password=<password>
```

“管理”面板指示域服务器状态以确保基础架构状态和功能正常。

eHealth 未发现 LPAR 物理磁盘

症状：

eHealth 未发现任何带有 版本 12.8 LPAR AIM 的 LPAR 物理磁盘。

解决方案：

如果使用 版本 12.8 LPAR AIM，请将您的 eHealth 升级到以下版本：

- 6.2.2 D11（如果您具有 eHealth 6.2.2.10 或更低版本）
- 6.3.0.06 或更高版本（如果您具有 eHealth 6.3.0.05 或更低版本）

dpmvc virtualswitch 命令的任务 ID 为空

症状：

当运行 dpmvc virtualswitch 命令时，结果显示任务 ID 为空。

解决方案：

此操作不会异步运行，并且会立刻返回结果。但是，PMM 将该操作视为任务操作。因此响应中包含任务 ID，但该 ID 始终是空字符串（“”）。

例如，从 CLI 运行以下命令时，将得到一个空的任务 ID：

```
dpmvc virtualswitch -vs_add -vc_server MYVC5 -switch_name XYZ
-esx_host_name MYESX -ws_user admin -ws_password ca_admin
```

CLI 输出：

```
...
SC URL: https://VASManager/aip/sc
VC URL: https://VASManager:443/aip/vc
任务 ID:
Command execution successful
```

其他命令（如 dpmvc faulttolerance 或 dpmvc distributedswitch）异步运行，您会得到一个任务 ID。

本地监视器和远程监视器不显示相同的值

症状：

本地监视器和远程监视器对于相同属性不显示相同的值。

解决方案：

对于无缝的本地和远程监控，可以选择相同的受监控对象名。然而，不同的 API 可能返回不同的值。

远程计算机上的 SystemEDGE 独立于服务器上的 RM AIM 运行，其轮询排定程序的起点无法进行同步。所监控的度量标准非常易变，样本可能有所不同。

IBM 逻辑分区的命名限制

症状：

在指定逻辑分区的名称时，CA Virtual Assurance 不支持所指定的名称。

解决方案：

提供给 IBM 创建 LPAR 请求的 LPAR 名称区分大小写。但是，本产品不支持在同一 PowerVM 服务器中管理两个仅名称大小写不同的逻辑分区。例如，在 PowerServer1 中不支持以下 LPAR 名称：

LPAR1 和 lpar1

LPAR 名称不能包含“/”字符，因为该字符用作监控器对象实例中实体的分隔符。“/”字符会生成模糊的监控器对象实例。例如，不支持 LPAR 名称“lpar/blue”。

AIX 系统上 SystemEDGE 安装程序中的导航问题

症状：

在 AIX 6.1 和 7.1 上安装 SystemEDGE 时，导航在 lsm（UNIX 安装程序）文本用户界面中不起作用。高级加密和 SRM AIM 也会出现该问题。

解决方案：

与在其他 UNIX 操作系统和较旧的 AIX 版本上不同，在 AIX 6.1 和 7.1 上，将 TERM 设置为（通用）值 xterm 时，使用键盘箭头键无法在 lsm 文本用户界面中导航。使用基于 Java 的图形 lsm UI 时，不会出现该问题。

变通方法是，在开始安装之前将 TERM 设置为其他值（例如，vt100），使用 + 和 - 键导航，或者（特定于 PuTTY）设置“禁用应用程序光标键模式”。

NodeCfgUtil 无法验证与 XenDesktop 控制器的连接

症状：

NodeCfgUtil 无法验证与 XenDesktop 控制器的连接。

解决方案：

确认以下组件安装在安装 XenDesktop AIM 的计算机上：

- Microsoft .NET Framework 4.0
- Windows 管理框架核心（Windows PowerShell 2.0、Windows 远程管理 (WinRM) 2.0）

性能图表显示在 LPAR 级别上内存使用率为零

症状：

当我在 LPAR 级别上监控内存使用率时，性能不表显示为零。

解决方案：

平台仅提供内存利用率度量，如果内存正以共享模式使用，则意味着，内存处于虚拟化状态。

对于专用内存而言，因为利用率度量信息无法收集，导致利用率图表上报出的利用率值为 0。

PMM 停止轮询 AIM

症状：

PMM 停止轮询 AIM（AIM 的所有实例）并发送 CAAM6504 消息。此外，UI 还在“AIM”面板的“管理”选项卡中将受影响的实例显示为“严重”。

对监控多个实例的 Cisco UCS、Microsoft 群集、IBM PowerVM 以及 Solaris Zones AIM 的轮询将停止。

原因是 PMM 无法继续轮询 AIM。当重新启动处于该状态的 AIM 时，不会使用受影响实例中的数据填充 MIB。PMM 将假定数据不再可用并将其从管理数据库中删除。

解决方案：

- 验证实例为何未处于“就绪”状态。您可以检查以下内容：
  - 证书无效或过期
  - 网络连接
  - 服务器上的硬件问题
- 在相应平台的“管理”选项卡中禁用实例（在 Cisco UCS 上不可用）。
- 从 AIM 中删除实例。

远程部署到 Solaris 时会列出 SPARC 和 x86 系统

症状：

在部署 UI 中列出的计算机通常被筛选到您正在为其部署的所选操作环境。不过，在下列情况下，您可以看到还列出了除所选操作环境以外的其他计算机：

- 当您部署到 Solaris x86 或 Solaris SPARC 服务器时，不管您选择 Solaris x86 还是 Solaris SPARC 作为目标操作环境，列出的服务器适合于所有 Solaris 体系结构。
- 当您部署到任何未分类的计算机时。

解决方案：

验证目标计算机与所选代理体系结构匹配，才能成功进行部署。如果您通过选择列出的所有计算机进行下一步操作，则匹配的体系结构上的部署将成功，而不匹配的体系结构上的部署将失败。

升级后空“查询结果”选项卡

症状：

远程监控查询结果显示升级后的空值。

解决方案：

添加系统时，RM PMM 要求远程系统名称符合完全限定域名 (FQDN) 表示法。但是，RM AIM 使现有系统保留非 FQDN 名称。该名称不匹配将显示空查询结果。您可以按如下方式修复名称不匹配：

在升级转换之前

- 登录到 refresh UI 并从远程监控中删除所有非 FQDN 系统。

  从管理器（数据库）和带有 RM AIM 插件的 SystemEDGE 代理中删除任何关联的系统、查询、实例以及监视器。
- 重新添加使用 FQDN 表示法的这些系统，并指定相同的配置集以重新创建关联的查询、实例和监视器。
- 升级。

在升级转换之后

- 登录到 SystemEDGE 代理计算机并运行刷新 RM AIM 插件。
- 在数据目录路径中查找包含当前远程监控配置的 rmonwbem.cf 文件并复制该文件。例如，另存为 rmonwbem-upgrade.cf
- 登录到 Refresh UI 并从远程监控中删除所有非 FQDN 系统。

  从管理器（数据库）和 RM AIM 代理计算机中删除任何关联的系统、查询、实例以及监视器。
- 立即升级。在代理计算机上，运行 *rmonwatch add* 命令，将 rmonwbem-upgrade.cf 作为输入文件。该过程重新添加 FQDN 表示法的所有系统及关联的查询、实例和监视器。

  注意：“在升级转换之后”方法具有自动重新添加系统并配置 UI 中系统的优势。

查询结果显示升级转换之后的值。

删除 vCenter 服务器使其他受管 vCenter 服务器的对象消失

症状：

删除一台 vCenter 服务器使其脱离管理时，另一台受管 vCenter 服务器的对象意外消失。

解决方案：

要避免出现产品管理问题，请不要在管理其他 vCenter 服务器的虚拟机上安装 vCenter AIM。如果从 CA Virtual Assurance 中删除与该虚拟机相关的 vCenter 的监控和管理，将删除与 vCenter 相关的对象，包括正在运行 AIM 的虚拟机系统。

重置 vCenter 服务器密码导致数据收集失败

症状：

在重置用户的 VMware vCenter 服务器密码（CA Virtual Assurance 正在使用该密码与 VMware vCenter 服务器进行通信）之后，无法进行数据收集。

解决方案：

使用新密码更新 vCenter AIM 配置。您可以从用户界面的“管理”选项卡或通过运行 vCenter AIM 的服务器上的 NodeCfgUtil 来更新密码。

如果受监控系统关闭，Solaris Zones AIM 将重置

症状：

如果受监控系统关闭，Solaris Zones AIM 将重置。

解决方案：

如果在其受监控系统之一关闭时重置 AIM，AIM 将按每个轮询间隔轮询该系统。在系统再次启动之前，AIM 不更新属性。

组件的状态图标显示“未配置”

症状：

CA Virtual Assurance 安装组件后，该组件的状态图标将显示  （未配置）。如果 CA Virtual Assurance 注册了一个已连接到未配置服务器的组件，则显示该状态。

解决方案：

要将组件的状态更改为就绪，请添加缺失的服务器连接设置和验证。

升级 SystemEDGE

症状：

将 SystemEDGE 升级到 r11.6 时，先前 CA Virtual Assurance 版本的 AIM 未运行。

解决方案：

将高级加密和所有 AIM 升级到 CA Virtual Assurance 版本 12.8。SystemEDGE r11.6 不加载先前 CA Virtual Assurance 版本的 AIM。

无法连接到 Microsoft SQL Server

症状：

在产品安装期间尝试验证 Microsoft SQL Server 评估版本的凭据失败。将显示错误消息“无法建立与 MSSQL 的连接”。

解决方案：

发生该问题的原因是默认情况下评估版本中禁用 TCP/IP。启用 TCP/IP。

用户界面未反映出产品升级

症状：

在我升级新版 CA Virtual Assurance 之后，用户界面并未显示出新版本。

解决方案：

如果您在升级前后均使用同一个浏览器窗口，那么用户界面可能显示不出新版本。请关闭浏览器会话，打开新的浏览器会话，清除浏览器缓存，然后登录到用户界面。

在开通和策略屏幕中用户界面无响应

症状：

如果在您位于开通页面或策略页面时重新启动了数据库服务器，则用户界面会变成空白或无响应。

解决方案：

注销 CA Virtual Assurance 用户界面并重新登录。

用户界面将不起作用

症状：

当结合使用远程 SQL Server 和 Windows 身份验证时，用户界面无法正常工作。

解决方案：

在安装期间，系统提示您添加适当的域用户，并授予“以服务登录”的权限。验证是否已为该域用户帐户配置 CAAIPTOMCAT、CAAIAPACHE 和 CA SM Domain Server 服务。如果无法重新配置服务，CA Virtual Assurance 用户界面将不起作用（显示板为空或功能不起作用）。

SQL Server 身份验证不需要满足这些条件。

遵循这些步骤:

1. 从“控制面板”的“管理工具”中打开“服务”对话框。

   将显示可用服务列表。

2. 打开 CA SM Domain Server、CAAIAPACHE 和 CAAIPTOMCAT 服务的“属性”对话框。
3. 在每个对话框中，转到“登录”选项卡，选择“该帐户”，并输入可以浏览的有效凭据（域用户帐户）。
4. 将该域用户帐户添加到两个系统（管理器服务器和数据库服务器）的本地管理员组中。
5. 将该域用户帐户添加到 SQL Server 的 sysadmin（或至少 dbcreator）服务器角色中。

vCenter 服务器 AIM 属性显示为零

症状：

vCenter 服务器属性显示为零。

解决方案：

只有当 vCenter 服务器 AIM 安装在本地 vCenter 服务器实例上时，才能检索以下对象的值。AIM 安装在远程服务器实例上时，这些参数显示为零 (0)。

- vmvcAimStatServerCPUUsage [1.3.6.1.4.1.546.16.52.2.2.12.0]
- vmvcAimStatServerMemUsage [1.3.6.1.4.1.546.16.52.2.2.17.0]
- vmvcAimStatServerTotalPhysMem [1.3.6.1.4.1.546.16.52.2.2.18.0]
- vmvcAimStatServerUsedPhysMem [1.3.6.1.4.1.546.16.52.2.2.19.0]

vCenter 服务器连接失败

症状：

在“管理”、“配置”下添加 vCenter 服务器连接之后，对 vCenter 服务器连接的验证失败。

解决方案：

以下步骤可解决导致连接失败的最常见问题：

- 验证使用的 vCenter 服务器连接数据（服务器名称、用户、密码、协议、端口）是否仍然有效。如有必要，请更新连接数据。
- 验证 vCenter 服务器系统是否正在运行并且可以访问。
- 验证 vCenter 服务器系统中的 VMware 管理服务是否正常运行。

更新 vCenter 服务器连接数据：

1. 单击与失败的连接关联的  （添加）或  （编辑）。

   此时将显示“新建 vCenter 服务器”或“编辑 vCenter 服务器”对话框。

2. 添加有效的服务器名称、用户、密码、协议和端口。启用“受管状态”，然后单击“确定”。

   将更新连接数据。

3. 单击右上角的  （验证）以验证新设置。

   如果无法建立与 vCenter 服务器的连接，请继续执行下一个步骤。

验证 vCenter 服务器系统是否正在运行并可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   ```
   nslookup <vCenter Server Name>
   ping <IP Address of vCenter Server>
   ```

2. 验证命令的输出，以确定 vCenter 服务器是否具有有效的 DNS 条目和 IP 地址。

   如果 vCenter 服务器不在 DNS 中，将 vCenter 服务器添加到 CA Virtual Assurance 管理器系统的 Windows 主机文件中。继续执行步骤 3。

   如果 vCenter 服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   ```
   ipaddress <vCenter Server Name>
   ```

   输入正确的 IP 地址和 vCenter 服务器名称。例如：

   ```
   192.168.50.50 myvCenter
   ```

4. 单击右上角的（验证）。

   即使 vCenter 服务器凭据和连接数据正确并且您可以 ping vCenter 服务器，连接仍然可能失败。在这种情况下，可能是 vCenter 服务器引起该问题。如果无法建立与 vCenter 服务器的连接，请继续执行下一个步骤。

验证 vCenter 服务器系统中的 VMware 管理服务是否正常运行

1. 联系 vSphere 管理员来访问 vCenter 服务器系统。
2. 登录到 vCenter 服务器系统，从“开始”菜单中打开“管理工具”、“服务”。

   将打开“服务”窗口。

3. 选择服务 *VMware VirtualCenter Server*。启动或重新启动该服务。
4. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“vCenter 服务器”窗格，并单击右上角的（验证）。

   CA Virtual Assurance 将验证 vCenter 服务器连接。

   如果与 vCenter 服务器的连接失败，请验证根据该方案的要求收集的数据是否仍然有效。

   与 vSphere 管理员或 VMware 技术支持合作，解决 vCenter 服务器连接问题。

vCenter AIM 实例状态图标显示已禁用

症状：

CA Virtual Assurance 在网络中发现了 vCenter AIM 实例之后，几个实例的状态图标将显示  （已禁用）。该 vCenter AIM 实例未受管理。

如果 CA Virtual Assurance 已发现具有以下关系的 vCenter AIM，则会显示此状态：

- 为有效连接到 CA Virtual Assurance 管理器但处于未受管状态的 vCenter 服务器配置了 vCenter AIM。
- AIM 已连接到未在“vCenter 服务器”窗格中配置的 vCenter 服务器。

解决方案：

要将 AIM 实例的状态更改为就绪，请执行以下操作之一：

- 将缺少的 vCenter 服务器连接添加到 CA Virtual Assurance 管理器中。
- 编辑现有的 vCenter 服务器连接并将其受管状态更改为已启用。

vCenter AIM 实例状态图标显示发现正在进行

症状：

在“管理”、“配置”下为 vCenter 服务器添加 vCenter AIM 实例之后，状态图标将显示  （发现正在进行）。

解决方案：

等到 vSphere 环境的发现过程完成。发现持续时间取决于与 vSphere 中的虚拟和物理资源相关的受管对象数量。可将光标悬停于图标上方，以显示用于指示未完成的发现请求数的工具提示。当发现作业完成时，CA Virtual Assurance 会将 vCenter 服务器文件夹添加到“资源”树。然后，您可以开始管理 vSphere 及其整个虚拟基础架构。

vCenter AIM 实例状态图标显示错误

症状：

在“管理”、“配置”下为 vCenter 服务器添加 vCenter AIM 实例之后，状态图标将显示  （错误）。无法连接到 AIM。

解决方案：

以下步骤可解决导致与 vCenter AIM 的连接失败的最常见问题：

- 验证 vCenter AIM 服务器是否可以访问。
- 验证 SystemEDGE 是否正在运行。如有必要，请启动或重新启动 SystemEDGE。

验证 vCenter AIM 服务器系统是否可以访问：

1. 在 CA Virtual Assurance 管理器系统上打开命令提示符并运行以下命令：

   `ping servername`

2. 验证命令的输出，以确定 vCenter AIM 服务器是否具有有效的 DNS 条目和 IP 地址。

   如果 vCenter AIM 服务器未在 DNS 中，请将 vCenter AIM 服务器添加到 CA Virtual Assurance 管理器系统上的 Windows 主机文件中。继续执行步骤 3。

   如果 vCenter 服务器位于 DNS 中，继续执行第 4 步。

3. 使用 ASCII 编辑器打开 %windir%\system32\drivers\etc 目录中的主机文件，并添加以下行：

   `ipaddress servername`

   输入正确的 IP 地址和 vCenter AIM 服务器名称。例如：

   `192.168.50.51 myvCenterAIM`

4. 在“vCenter AIM 服务器”窗格的右上角，单击  （验证）。

   如果错误状态保持不变，请继续执行下一个步骤。

验证 SystemEDGE 是否正在运行：

1. 登录到 vCenter AIM 服务器，并从 %windir%\Program Files\CA\SystemEdge\bin 目录运行 sysedge.cpl。

   将出现 SystemEDGE 控制面板，其中显示 SystemEDGE 的运行状态。

2. 启动或重新启动 SystemEDGE。

   等到 SystemEDGE 控制面板指示 SystemEDGE 正在运行。

3. 切换到管理器系统上的 CA Virtual Assurance 用户界面、“vCenter AIM 服务器”窗格，并单击右上角的  （验证）。

   CA Virtual Assurance 将验证 vCenter AIM 服务器连接。

   如果错误状态保持不变，请验证根据该方案的要求收集的数据是否仍然有效。

vCenter AIM 实例状态图标显示无轮询

症状：

在“管理”、“配置”下为 vCenter 服务器添加 vCenter AIM 实例之后，状态图标将显示  （无轮询）。

解决方案：

关联实例不需要特定的操作。此图标通知您 CA Virtual Assurance 管理器未轮询此 AIM。AIM 不是首选。

如果将多个 AIM 配置为管理特定 vCenter 服务器，则 PMM 会选择 AIM 之一作为当前 AIM。如果想要使用其他 AIM，则可以在“管理”、“配置”、“开通”下设置首选 AIM。单击服务器条目的“编辑”并选择首选 AIM。首选 AIM 将成为当前 AIM。

断开电源后，VM 使用值未立即更新

症状：

断开电源后，VM 使用值未立即更新。

解决方案：

关闭 VM 电源之后，直至下一次轮询成功之前，使用值不会下降到 0。轮询将花费 5 分钟，这是默认数据收集和记录间隔。

词汇表

application insight module，AIM

SystemEDGE 代理提供了插件体系结构，代理可在初始化时通过该体系结构加载可选的 *application insight module (AIM)*。AIM 是 SystemEDGE 代理的功能扩展。例如，vCenter AIM 允许 SystemEDGE 通过 VMware vCenter 服务器管理 vSphere 环境。

autoshell

AutoShell 提供命令行和脚本环境，可以用来自动化复杂的重复和管理任务。AutoShell 不是一种编程语言，而是脚本语言和命令行外壳的组合。AutoShell 基于标准的脚本语言 ECMA-脚本 (JavaScript)。虽然 JavaScript 通常被认为是在网页上使用的脚本语言，但它不需要在浏览器中运行。它是实现面向对象、XML 和正则表达式处理支持的独立脚本语言。AutoShell 使用 Mozilla Spidermonkey JavaScript 解析程序的开箱即用版本（它还向 Mozilla Firefox Web 浏览器提供 JavaScript 功能）。

autoshell 可加载模块，ALM

Autoshell 可加载模块 (ALM) 是 AutoShell 核心的扩展。根据 CA Virtual Assurance 安装中选择的组件，会自动安装所需的 ALM。例如，使用 ALM 可以通过 AutoShell 来管理平台，如 LPAR、Solaris Zones 或 vCenter 服务器。

Cisco Nexus 1000V 交换机

*Cisco Nexus 1000V 交换机*是可以在 VMware vSphere 环境中运行的分布式虚拟交换机。Cisco Nexus 1000V 交换机包括虚拟以太网模块 (VEM) 和虚拟监控模块 (VSM)。在与 Cisco Nexus 1000V 交换机相关的每个 ESX 或 ESXi 主机上，VEM 将替换 VMware vSwitch 并且作为管理程序内核中的模块运行。VSM 将多个 VEM 作为一个逻辑交换机进行控制，并在 ESX 或 ESXi 主机上的 VM 中运行。有关更多详细信息，请参阅 http://www.cisco.com/go/1000vdocs 上的 Cisco Nexus 1000V 交换机文档。CA Virtual Assurance VM 开通支持 VMware vNetwork 分布式交换机和 Cisco Nexus 1000V 交换机。

Cisco Unified Computing System (UCS)

Cisco Unified Computing System (UCS) 提供数据中心硬件和虚拟化服务。

cmdlet

cmdlet 是一个命令，必须以行中第一个非空白字符开始。因为该限制，它们只能单独使用，不能作为范围更广的 JavaScript 表达式的一部分进行使用。尤其是无法用作 rvalue（赋值运算符的右侧操作数）。
？ 是 AutoShell cmdlet 的示例。

CPU 上限

*CPU 上限*限制区域的 CPU 资源的数量。

CPU 份额 (VMware)

份额指定为自然数，表示每个虚拟机的比例权重。

指定份额仅可用于层次结构中具有相同父项的同级虚拟机、vApp 或资源池。将份额分配给虚拟机时，始终为该虚拟机指定相对于其他已打开电源的虚拟机的优先级。

例如，发生竞争时，具有 2000 份额的虚拟机接收的 CPU 时间多于具有 1000 份额的虚拟机。份额相对于其他份额进行配置；因此，仅与份额的比例有关，而不是份额的值。份额值为 1000、2000、3000 的三个虚拟机与份额值为 1、2、3 的三个虚拟机作用相同。可以使用您喜欢的任何编号方案。

Dell EqualLogic

Dell EqualLogic 包含虚拟化 iSCSi SAN 解决方案，可将虚拟存储用于虚拟服务器。

dvPort 组 (VMware)

每个 VMware vNetwork 分布式交换机都分配有一个或多个 *dvPort 组*。dvPort 组在通用配置下组合多个端口，并且提供稳定的点，便于虚拟机连接到标记的网络。唯一的网络标签标识每个 dvPort 组。网络标签对于当前数据中心是唯一的。
dvPort 组为 vNetwork 分布式交换机上的每个成员端口指定端口配置选项。dvPort 组定义如何连接网络。

dvUplink 端口 (VMware)

分布式虚拟上行链路 (dvUplink) 为 ESX 主机上的物理 NIC (vmnic) 提供一个抽象层。每个物理 NIC 均映射到 dvUplink。对于每个与 VMware vNetwork 分布式交换机关联的主机，每个物理 NIC（上行链路）通过一个上行链路端口分配到 vNetwork 分布式交换机。

ESX/ESXi 主机 (VMware)

*ESX 或 ESXi 主机*是物理计算机，它使用 ESX 或 ESXi 服务器虚拟化软件来运行虚拟机。主机提供虚拟机使用的 CPU 和内存资源，并向虚拟机提供访问存储和网络连接的权限。

funclet

Funclet 维护详细命令，如具有可选子句的语法、字符串化等。Funclet 通常像 cmdlet 一样使用，也就是说，在单个行中单独使用。它们能够返回可作为范围更广的表达式的一部分进行处理的值。

Huawei SingleCLOUD

Huawei SingleCLOUD 是用于云计算数据中心的云服务解决方案。

Hyper-V

Hyper-V 是适用于 Windows Server 2008 R2 的基于 Microsoft 管理程序的服务器虚拟化技术。单独的虚拟机 (VM) 在单个物理服务器上运行，并且可运行多个不同的操作系统，如 Windows 或 Linux。

I18n（国际化）

*I18N（国际化）*是对软件产品的修改，从而使其可以处理多种语言、时间和日期格式、数字格式（十进制分隔符、数字分组）等书写约定，等等。CA Virtual Assurance 使用 UTF-8 编码显示输入和输出数据中特定于语言的字符，如德语的 ü（元音变音）、法语的 è（重音符）或日文字符。

IBM High Availability Cluster Multiprocessing (HACMP)

IBM High Availability Cluster Multiprocessing (HACMP) 是在 AIX UNIX 和 Linux 上为 IBM System p 平台构建高可用性群集的解决方案。

internet 小型计算机系统接口，iSCSI

iSCSI 用于促进通过内部网进行的数据传输并用于长距离管理存储。iSCSI 将 SCSI 命令封装在 IP 数据包中，这些数据包与网络上的其他任何 IP 数据包一样进行路由。当该 IP 数据包到达目的地时，iSCSi 设备将删除封装并解释 SCSI 命令。

L10n（本地化）

*L10N（本地化）*是已国际化的软件的某种特定语言的实现。

MIB 对象，MIB 属性

*MIB 对象*是在代表一个或多个资源对象或数据项的 MIB 中定义的实体。MIB 对象包括组、表和单个属性，并且必须根据管理信息结构 (SMI) 进行定义。

NetApp 文件管理器

*NetApp 文件管理器*是磁盘存储设备，它拥有和控制一个文件系统，并通过网络向主机提供文件和目录。

onTap

onTap 框架是免费的、面向服务的 Web 应用程序框架。

P12 文件

*P12 文件*是存储私钥及其证书的存档文件。P12 文件用于 Huawei GalaX 环境。

POWER 处理器 (LPAR)

*POWER 处理器*基于 RISC，在许多 IBM 服务器、微型计算机、工作站和超级计算机中用作 CPU。

Red Hat Enterprise Virtualization

Red Hat Enterprise Virtualization (RHEV) 是基于 KVM 管理程序的企业虚拟化产品。

SNMPv3

SNMPv3 是一种协议，具有以下三个通信级别：
noAuthNoPriv：该消息中的镜像 SNMPv1 和 SNMPv2 都附带用户名，并且该用户名在发件人和收件人之间必须保持一致。
AuthNoPriv：使用一致的用户名和密码。
AuthPriv：使用用户名、密码以及加密邮件正文的加密密钥。

UCS

请参阅 *Cisco Unified Computing System (UCS)*。

UCS 管理器

管理 UCS 硬件（交换机、机箱和刀片服务器）的软件模块。

vApp (VMware)

vApp 是一个特殊资源池，它将 VM 集合视为单个单元。vApp 使用开放虚拟化格式。*开放虚拟化格式 (OVF)* 是一种标准，用于指定和封装多层应用程序的所有组件以及与该应用程序关联的操作策略和服务级别。CA Virtual Assurance 可对 vApp 执行操作。针对 vApp 执行的操作将传播给 vApp 上的所有 VM。

vCenter 服务器 (VMware)

VMware *vCenter Server* 为配置、开通和管理虚拟 vSphere 环境提供了一个中央控制点。vCenter 服务器作为 Microsoft Windows 服务器和 Linux 服务器上的一项服务来运行。

vCenter 服务器代理 (VMware)

VMware *vCenter Server 代理*将 ESX 服务器与 vCenter 服务器连接。

vCenter 服务器数据库 (VMware)

VMware *vCenter Server 数据库*存储有关 VirtualCenter 管理的物理服务器、资源池、数据中心和虚拟机的永久信息。

vCloud Director (VMware)

使用 *VMware vCloud Director*，您可以通过将虚拟基础架构资源共用到虚拟数据中心，并将其展示给用户来构建安全、多承租人的云。
vCloud Director 资源根据基础 vSphere 资源（例如，CPU、内存、存储或 vNetwork 分布式交换机）来运行虚拟机。您可以使用这些基础 vSphere 资源，以在 vCloud 中创建虚拟机和 vApp。

vCloud 组织 (VMware)

*vCloud 组织*是一个管理单位，表示用户、组和计算资源的集合。关联的虚拟数据中心可提供所需的计算资源。用户在组织级别进行身份验证后，可以创建、使用和管理虚拟机或 vApp。

vNetwork 分布式交换机，vDS (VMware)

*VMware vNetwork 分布式交换机*将虚拟交换机的配置从主机提取到数据中心级别。vNetwork 分布式交换机作为单个虚拟交换机运行，该交换机跨数据中心中与其关联的所有主机。vNetwork 分布式交换机包含同样配置到标准交换机上的端口组的分布式端口组，但跨多个主机。这些属性可使虚拟机在多个主机之中迁移时维持一致的网络配置。

与 vNetwork 标准交换机一样，每个 vNetwork 分布式交换机均是虚拟机可以使用的网络集线器。vNetwork 分布式交换机可以在虚拟机之间内部转发流量，或通过连接到物理 NIC（上行链路适配器）链接到外部网络。有关更多详细信息，请参阅 http://pubs.vmware.com 上的 vNetwork 分布式交换机文档。

CA Virtual Assurance VM 开通支持 VMware vNetwork 分布式交换机和 Cisco Nexus 1000V 交换机。可以通过 vNetwork 面板、AutoShell 或 CLI 命令管理虚拟分布式交换机。

vNetwork 标准交换机，vSwitch (VMware)

CA Virtual Assurance 管理作为抽象网络设备的标准 vSwitch 的策略和属性。*VMware vNetwork 标准交换机 (vSwitch)* 在单个主机上运行，该主机上的虚拟机可以附加到该标准交换机。

vSwitch 可以在 VM 内部之间路由流量并且链接到外部网络。vSwitch 结合多个网络适配器的带宽并在它们之间平衡通信流量。vSwitch 可以处理物理 NIC 故障切换。

XenCenter (XenServer)

XenCenter 是一个用于管理 XenServer 环境的 Windows 客户端应用程序。它必须安装在可以通过网络连接到 XenServer 主机的远程 Windows 计算机中，但无法作为 XenServer 主机在同一个系统中运行。

XenMotion (XenServer)

XenMotion 提供了在资源池内实时迁移 VM 的功能。

XenServer 主机 (XenServer)

*XenServer 主机*对象代表运行 XenServer 及其 VM 的物理主机。XenServer 主机可以是独立主机，也可以与 XenServer 池关联。

刀片服务器 (UCS)

附加到 Cisco UCS 机箱的服务器。

公平份额排定程序，FSS (Solaris)

公平份额排定程序 (FSS) 指定根据份额分配 CPU 时间的排定程序类。份额定义分配给项目的系统 CPU 资源的部分。

区域 (Solaris)

Solaris *Zones* 定义可为 Solaris 10 系统设置的虚拟化操作系统环境。Zones 可虚拟化操作系统服务，并为应用程序提供独立、安全的环境。每个 Solaris 系统包含一个作为系统默认区域的全局区域。例如，您可以创建、删除、修改、暂停或重新引导非全局区域。

双 HMC (LPAR)

双 HMC 是提供高可用性的冗余硬件管理控制台 (HMC) 管理系统。

开放虚拟化格式 (OVF)

开放虚拟化格式 (OVF) 是一种标准，用于指定和封装多层应用程序的所有组件以及与该应用程序关联的操作策略和服务级别。

主机总线适配器，HBA

主机总线适配器 (HBA) 是将主机连接到*存储区域网络 (SAN)* 的接口卡。

处理器池 (LPAR)

*处理器池*是可以跨不同的逻辑分区共享的一组物理处理器。

处理器集，pset (Solaris)

*处理器集*定义 CPU 的非连续组。每个处理器集可以包含零个或多个处理器。它是资源池配置中的资源元素。

平台管理模块，PMM

平台管理模块 (PMM) 是一个 Web 服务，该服务负责为相应的环境提供连接和操作支持。支持的环境如下：VMware vSphere、Microsoft Hyper-V、IBM PowerVM、Solaris Zones、Cisco UCS 或 Microsoft 群集服务。PMM 管理与这些环境的服务器的连接，执行与环境相关的操作，从相应的 AIM 检索数据，以及填充 CA Virtual Assurance 管理数据库。

正则表达式

*正则表达式*是用于匹配的文本模式。正则表达式是由纯文本和特殊字符混合组成的字符串，用于指示所需匹配的类型。

目录 (VMware)

组织提供*目录*来存储 vApp 模板和媒体文件。组织成员可以使用目录中的 vApp 模板和媒体文件来创建自己的 vApp。

任务 (Solaris)

*任务*随着时间推移表示一组工作。每个任务与一个项目关联。

光纤通道，FC

*光纤通道*是用于在计算机设备之间传送数据的标准化千兆位速度技术。光纤通道尤其适用于将计算机服务器连接到共享存储设备以及在存储控制器和驱动器之间进行互连。

全局区域 (Solaris)

*全局区域*是每个 Solaris 系统上均包含的区域。如果系统上存在非全局区域，则全局区域是系统和系统范围管理的默认区域。

全局唯一标识符，UUID

全局唯一标识符 (UUID) 是在分布式系统中使用的标识符标准，以便唯一地标识信息。当信息存储在单个数据库时，标签信息会与 UUID 限制标识符冲突。

共享内存 (Solaris)

*共享内存*定义在项目中运行的进程可使用的内存总量。

动态重新配置连接器索引，DRC 索引 (LPAR)

物理系统单元中的每个插槽都会分配有一个 *DRC 索引*。部署过程需要使用该数字来执行 LPAR 的实际创建。管理控制台 (HMC) 和系统使用该索引来唯一地标识系统中的每个插槽。在单元通电之前，不会为插槽分配 DRC 索引。

多个共享处理器池 (MSPP)

“多个共享处理器池 (MSPP)” 功能在 Power6 和更高版本的服务器上受支持。使用此功能可创建多个处理器池，从而使 CPU 资源分配更为灵活。

多个虚拟 I/O 服务器

*多个虚拟 I/O 服务器*可通过启用虚拟 I/O 服务器维护提供增加应用程序可用性的功能，且不会针对客户端分区宕机。

字符串化

*字符串化*获取一个字符序列，并且将其转变为适当的 JavaScript 文字字符串。

存储区域网络，SAN

存储区域网络 (SAN) 是一种将远程计算机存储设备连接到服务器的体系结构，在该连接方式中，设备看上去是从本地连接到操作系统。

存储库，SR (XenServer)

存储库 (SR) 描述了存储虚拟磁盘映像 (VDI) 的特定存储目标。存储硬件的接口允许在多个 SR 类型中支持 VDI。

有上限的逻辑分区 (LPAR)

“有上限的逻辑分区” 无法使用比分配到的处理单元更大的处理器能力。为有上限分区分配了最大容量，确保无法超过此容量且不会影响物理系统的整体行为。

机箱 (UCS)

支撑 Cisco UCS 交换机和刀片服务器的硬件框架。

网络对象 (XenServer)

每个 XenServer 主机均具有一个或多个*网络对象*，这些是虚拟以太网交换机。网络对象具有名称和说明、全局唯一 UUID 和可以连接到的虚拟网络接口和物理网络接口（VIF 和 PIF）的集合。附加到特定网络对象的 VM 和主机对象可以相互发送网络数据包。

将与 PIF 没有关联的网络视为*内部网络*，仅在 XenServer 主机上的 VM 之间提供连接，但对外界没有任何连接。将具有 PIF 关联的网络视为*外部网络*，并在 VIF 和连接到网络的 PIF 之间提供网桥。

网络安装管理器，NIM (LPAR)

网络安装管理器 (NIM) 提供了一个中心管理点，用于为 LPAR 和各服务器安装和维护 AIX 映像。它还便于从同一主映像、不同映像、安装介质或该实例的前一个 mksysb 安装所有这些实例。实例是指 OS 映像，无论是在 LPAR 上还是物理服务器上。

访问控制列表

访问控制列表或 ACL 将指定 IP 地址的空格分隔列表以将团体使用仅限于那些地址。如果保留列表为空，代理将授予对任何使用关联团体名称的系统的访问权限。

时间份额排定程序，TS (Solaris)

时间份额排定程序 (TS) 指定一个排定程序类，该类试图向每个进程提供对可用 CPU 的平等访问。它根据优先级分配 CPU 时间。

服务配置文件

有关 Cisco UCS 硬件的配置信息集合，包括接口、光纤连接以及网络和服务器身份。

物理网络接口，PIF (XenServer)

物理网络接口 (PIF) 对象表示在 XenServer 主机上的物理网络接口。PIF 对象具有名称和说明、全局唯一 UUID、表示 NIC 的参数，并指定该对象可连接到的网络和服务器。PIF 对象同时提取物理接口和 VLAN。

物理块设备，PBD (XenServer)

物理块设备 (PBD) 对象表示在主机与存储库对象之间的连接。PBD 存储用于连接到给定的存储目标并与其进行交互的设备配置字段。

轮询时间间隔

*轮询时间间隔*是资源组连续轮询之间的时间长度。

非全局区域 (Solaris)

*非全局区域*在 Solaris 操作系统的单个实例中提供虚拟化的操作系统环境。Solaris Zones 软件分区技术虚拟化操作系统服务。

轻量级进程，LWP (Solaris)

轻量级进程 (LWP) 属于 Solaris 10 内核线程模型。通过将用户线程与内核线程进行关联，LWP 为用户线程形成执行上下文。在 Solaris 10 内核中，内核服务和任务作为内核线程运行。创建用户线程时，也会创建关联的 LWP 和内核线程，并链接到用户线程。资源控制允许为 LWP 设置边界。

项目 (Solaris)

*项目*定义与主机关联的容器。它是抽象层，帮助组织和管理物理系统资源的集合。

项目是任务的集合，任务是进程的集合。当 login、cron、newtask、setproject 或 su 命令打开新会话时，将在项目中启动新任务。每个进程仅属于一个任务，每个任务仅属于一个项目。

项目和任务是基本实体，用于在 Solaris 10 操作系统中标识工作负荷。一个项目与一组用户和一组组关联。用户和组可以在它们所属的项目的上下文中运行其进程，但它们可以是多个项目的成员。项目是基本实体，可针对其限制资源的使用。任务是与进程关联的实体，而项目与一组任务关联。

容错，FT (VMware)

通过 VMware vSphere，可以在 VM 上启用*容错 (FT)*，该虚拟机定义到配置用于高可用性 (HA) 的群集。容错会在群集中的其他 ESX 服务器上创建辅助 VM。辅助 VM 以锁步模式与正在执行工作负荷的主 VM 协同运行。如果发生故障，辅助 VM 将立即从故障点接管工作负荷执行。CA Virtual Assurance 发现和管理群集中的主 VM 和辅助 VM。

容器 (Solaris)

Solaris *容器*为应用程序提供完整的运行时环境。资源管理和 Solaris Zones 是容器的一部分。

资源池 (Solaris)

*资源池*定义分区系统资源的配置机制。资源池是能够进行分区的资源组之间的关联。

资源池 (VMware)

*资源池*定义物理计算的分区和单个主机或群集的内存资源。您可以将任何资源池分割成更小的资源池，从而将资源分开并分配给具体的组或用于特殊目的。您也可以分层组织和嵌套资源池。

资源池，过量分配 (XenServer)

*资源池*包含多个 XenServer 主机安装，并将其绑定到可以托管 VM 的单个受管实体中。与共享存储组合时，资源池支持 VM 在任何具有足够内存的 XenServer 主机上启动，然后在 XenServer 主机之间动态移动 (XenMotion)。

如果当前在资源池中运行的 VM 在达到用户定义的失败次数后无法在别处重新启动，则会过量分配资源池。XenServer 将动态维护一个故障转移计划以应对资源池中的一组主机在任何给定时间发生故障的情况。将可接受的主机故障次数值定义为高可用性 (HA) 配置的一部分可确定允许出现故障但没有任何服务丢失的故障次数。如果计划不可用，则该池将被视为过量分配。基于 VM 生命周期操作和移动，将动态重新制定该计划。

资源池主服务器 (XenServer)

资源池至少由一个物理节点*资源池主服务器*构成。而加入现有池的其他物理节点均被视为成员。只有主服务器节点显示通过 XenCenter 和 CLI 使用的管理界面。必要时主服务器可以从池外部将命令或请求转发给各个成员。

资源控制 (Solaris)

通过为工作负荷定义特定资源消耗的限制，可以直接为 Solaris Zones 设置*资源控制*。工作负荷是一个应用程序或一组应用程序的所有进程的合计。

资源控制通过 zonecfg(1M) 中描述的 zonecfg 命令存储在 /etc/project 文件或区域的配置中。

陷阱

*陷阱*是未经请求的信息，SNMP 代理可以将其发送给一个或多个管理器，以通知代理和资源事件的管理应用程序。SNMP 陷阱分常规（所有类型的 SNMP 代理通用）或特定于企业（发送它的代理独有）两种。

基于内核的虚拟机 (KVM)

基于内核的虚拟机 (KVM) 是 Linux 内核的硬件辅助虚拟化基础架构。

基于策略的配置

通过*基于策略的配置*，可创建通过一次操作即可部署到一组受管计算机的代理配置策略。

弹性服务控制器 (ESC)

弹性服务控制器 (ESC) 是 Huawei 控制器，提供对虚拟资源、计算、存储和其他服务的集中管理。

虚拟 I/O 服务器，VIOS (LPAR)

虚拟 I/O 服务器 (VIOS) 是一个配置为拥有所有物理 I/O 资源的特殊逻辑分区，它向其他 LPAR 提供其虚拟化功能。LPAR 作为虚拟设备通过虚拟 I/O 服务器访问磁盘、网络和光学设备。具有虚拟化输入输出设备的每个 PowerVM 系统均具有一个或多个虚拟 I/O 服务器。

虚拟 NIC (VMware)

虚拟 NIC 是虚拟机上的虚拟以太网适配器。来宾操作系统通过设备驱动程序与虚拟以太网适配器（将虚拟以太网适配器看作物理以太网适配器）进行通信。虚拟以太网适配器有其自己的 MAC 地址、一个或多个 IP 地址，并响应标准以太网协议（就像物理 NIC）。

虚拟交换机 (VMware)

*虚拟交换机*的工作方式和物理交换机类似。每个 ESX 服务器均有自己的虚拟交换机，它们通过端口组连接到虚拟机。这些虚拟交换机还有指向 ESX 服务器上物理以太网适配器的上行链路连接。虚拟机通过连接到虚拟交换机上行链路的物理以太网适配器与外界进行通信。

虚拟机，VM (VMware)

虚拟机 (VM) 是一个基于软件的计算机，运行操作系统和应用程序的方式和物理计算机类似。虚拟机根据其工作负荷，在其物理主机上动态消耗资源。因为虚拟机是灵活的计算单元，所以其部署包含各种各样的环境，如数据中心、群集、云计算、测试环境、台式计算机或便携式计算机。它们的主要优势体现在数据中心，在数据中心内，它们用于服务器整合、工作负荷优化和能效。

虚拟机，VM (XenServer)

虚拟机 (VM) 指定了来宾操作系统和应用程序可以运行的虚拟化 x86 环境。可使用模板创建 VM。模板包含多种配置设置以实例化指定的 VM。XenServer 提供了一组基本模板，从引导 OS 供应商安装 CD 或从网络存储库中运行安装的常规原始 VM 到完整的预配置 OS 实例均包含在内。XenServer 支持 Linux 和 Windows 来宾操作系统。

虚拟机硬件版本 7 (VMware)

虚拟机硬件版本 7 指定从 VMware 生成虚拟硬件，是使用 vSphere 创建的虚拟机默认版本。它支持对 CPU 和内存等进行热插拔。如果在虚拟机中启用了热插拔，CA Virtual Assurance 也支持对 CPU 和内存进行热插拔。**注意：**有关 VMware 虚拟机硬件版本 7 的信息，请参阅 VMware 文档。

虚拟网络接口，VIF (XenServer)

虚拟网络接口 (VIF) 对象表示在 VM 和网络对象之间的连接。VIF 对象具有名称和说明、全局唯一 UUID，并指定其可以连接到的网络和 VM。启动 VM 时，将查询其 VIF 对象以确定必须创建哪些网络设备。

虚拟块设备，VBD (XenServer)

虚拟块设备 (VBD) 对象表示虚拟机 (VM) 与虚拟磁盘映像 (VDI) 之间的连接。启动 VM 时，查询其 VBD 对象以确定应附加哪些磁盘映像。

虚拟局域网，VLAN (XenServer)

虚拟局域网 (VLAN) 允许单个物理网络支持多个逻辑网络。要将 VLAN 与 XenServer 结合使用，必须将主机的 NIC 连接到 VLAN 中继端口。

虚拟私有云 (VPC)

虚拟私有云 (VPC) 是具有多个虚拟机及相关虚拟磁盘的 Huawei SingleCLOUD 用户的私有本地网络。

虚拟数据中心，vDC (VMware)

虚拟数据中心 (vDC) 向 vCloud 组织提供虚拟计算资源。您可以在虚拟数据中心中开通、运行和存储虚拟系统。一个 vCloud 组织可以具有多个虚拟数据中心。

虚拟磁盘 (VMware)

*虚拟磁盘*在虚拟来宾操作系统中定义磁盘驱动器。虚拟磁盘是位于本地主机或远程文件系统上的一个特定文件或一组文件。它在操作系统中的运行方式类似于物理磁盘驱动器。

虚拟磁盘映像，VDI (XenServer)

虚拟磁盘映像 (VDI) 是提供给 VM 的虚拟磁盘在磁盘上的表示形式。VDI 是 XenServer 中虚拟化存储的基本单元。

逻辑内存块，LMB (LPAR)

逻辑内存块 (LMB) 用于指定分配给 LPAR 的物理和逻辑内存的粒度（例如：256 MB）。

逻辑分区，LPAR

逻辑分区 (LPAR) 是硬件资源的子集，虚拟化为单独的系统。一个物理系统可以分区为多个 LPAR，每个 LPAR 都提供单独的操作系统和应用程序。逻辑分区的数目取决于系统的硬件配置。LPAR 通常用于不同的环境，如数据库、Web 服务器等。LPAR 作为单独的系统在网络中进行通信。

硬件管理控制台，HMC (LPAR)

硬件管理控制台 (HMC) 是一个外部组件，用于在 IBM PowerVM 系统上执行管理任务。HMC 可用于创建或更改逻辑分区，包括为分区动态分配资源。HMC 与 POWER 系统的服务器固件层进行通信，在大型 PowerVM 环境中提供单一控制点。

集成虚拟化管理器（IVM、LPAR）

集成虚拟化管理器 (IVM) 是虚拟 I/O 服务器 (VIOS) 的增强，使用 IVM 可以管理单个 POWER 系统。使用 IVM 可以创建和管理 LPAR。IVM 支持 VIOS 功能的管理并提供基于 Web 的用户界面。

数据中心 (VMware)

*数据中心*用作主机、虚拟机、资源池或群集的容器。如果它们的虚拟配置符合特定部门的要求，则数据中心可以表示组织结构（如地理区域或单独的业务功能）。您也可以使用数据中心创建隔离的虚拟环境用于测试，或用于组织环境。

数据存储 (VMware)

*数据存储*指定数据中心中基础物理存储资源组合的虚拟表示。这些物理存储资源可由服务器上的本地磁盘、SAN 磁盘阵列等提供。

简单网络管理协议 (SNMP)

简单网络管理协议 (SNMP) 是 Internet 的标准管理协议。SNMP 管理应用程序和代理使用 Get 请求、Set 请求、Get-Next 请求、Get-Response 以及陷阱 PDU 来进行通信。MIB 跟踪网络和系统资源以及应用程序，定义它们交换的数据。

群集

*群集*由链接在一起并作为单个实体运行的两个或多个独立的计算机系统构成。群集用于并行处理、负载平衡和容错。

模板 (XenServer)

*模板*是将 *is_a_template* 参数设置为 true 的 VM。模板包含多种配置设置以实例化指定的 VM。XenServer 附带了一组基本模板，从引导 OS 供应商安装 CD 或从网络存储库中运行安装的常规原始 VM 到完整的预配置 OS 实例均包含在内。

使用 XenServer 可以创建 VM，并根据特定的需求使用标准格式对其进行配置，然后将 VM 的副本另存为模板以供将来在部署中使用。

管理信息库 (MIB)

管理信息库 (MIB) 是描述资源属性的数据存储。MIB 用 ASN.1 编写，ASN.1 是由管理标准指定的语言，并且符合 OSI 定义 SNMP MIB 的管理信息结构 (SMI) 标准。

额定池容量 (LPAR)

共享处理器池的*“额定池容量”*用于定义保证可用于处理器池中分区组的处理器容量。

索引

符号

A

C

D

E

F

H

I

L

M

N

O

P

R

S

U

V

W

X

二划

三划

四划

五划

四划

五划

六划

七划

八划

九划

八划

九划

十划

十一划

十二划

十三划

十四划

十五划

十六划