

CA Virtual Assurance for Infrastructure Managers

安装指南

版本 12.7.1



本文档包括内嵌帮助系统和以电子形式分发的材料（以下简称“文档”），其仅供参考，CA 随时可对其进行更改或撤销。

未经 CA 事先书面同意，不得擅自复制、转让、翻印、透露、修改或转录本文档的全部或部分内容。本文档属于 CA 的机密和专有信息，不得擅自透露，或除以下协议中所允许的用途，不得用于其他任何用途：(i) 您与 CA 之间关于使用与本文档相关的 CA 软件的单独协议；或者 (ii) 您与 CA 之间单独的保密协议。

尽管有上述规定，但如果您为本文档中所指的软件产品的授权用户，则您可打印或提供合理数量的本文档副本，供您及您的雇员内部用于与该软件相关的用途，前提是所有 CA 版权声明和标识必须附在每一份副本上。

打印或提供本文档副本的权利仅限于此类软件所适用的许可协议的有效期内。如果该许可因任何原因而终止，您应负责向 CA 书面证明已将本文档的所有副本和部分副本已退还给 CA 或被销毁。

在所适用的法律允许的范围内，CA 按照“现状”提供本文档，不附带任何保证，包括但不限于商品适销性、适用于特定目的或不侵权的默示保证。CA 在任何情况下对您或其他第三方由于使用本文档所造成的直接或间接的损失或损害都不负任何责任，包括但不限于利润损失、投资受损、业务中断、信誉损失或数据丢失，即使 CA 已经被提前明确告知这种损失或损害的可能性。

本文档中涉及的任何软件产品的使用均应遵照有关许可协议的规定且根据本声明中的条款不得以任何方式修改此许可协议。

本文档由 CA 制作。

仅提供“有限权利”。美国政府使用、复制或透露本系统受 FAR Sections 12.212、52.227-14 和 52.227-19(c)(1) - (2) 以及 DFARS Section 252.227-7014(b)(3) 的相关条款或其后续条款的限制。

版权所有 © 2012 CA。保留所有权利。此处涉及的所有商标、商品名称、服务标识和徽标均归其各自公司所有。

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	9
范围.....	9
读者.....	9
相关出版物.....	9
约定.....	10
第 2 章：安装 CA Virtual Assurance	13
安装要求和注意事项.....	13
安装和配置 SQL Server Express.....	13
验证使用 SQL Server 的要求.....	14
安全注意事项.....	14
优化 Windows 内存管理.....	15
SystemEDGE 与 CA Systems Performance LiteAgent 之间的比较.....	15
CA Virtual Assurance 的安装.....	17
为安装做准备.....	17
运行安装.....	19
取消安装.....	22
初始安装之后的组件安装.....	22
无提示管理器安装.....	22
从安装介质中复制无提示安装文件.....	22
编辑 silent.properties 文件.....	23
执行无提示管理器安装.....	23
多个服务器上的安装.....	24
多个服务器上的安装准则.....	24
通信端口.....	26
如何将 SQL Server 用户权限调整到最小必要权限.....	29
查看要求.....	30
以 dbcreator 角色创建数据库用户.....	30
使用新的数据库用户安装产品.....	30
将 aom2 和 dpm 数据库的所有者更改为 sa.....	31
将新数据库用户的权限调整到最小必要权限.....	31
登录用户界面并管理您的环境.....	32
如何更新 CA Virtual Assurance.....	33
检查更新.....	33
下载并应用更新 (PTF).....	34
代理部署.....	35
创建部署作业.....	36

各个代理安装	37
SystemEDGE 组件的依存关系	38
通过 CA Virtual Assurance 管理器安装程序进行 SystemEDGE 安装	39
在 Windows 系统上安装	39
在 UNIX 和 Linux 系统上进行安装	50
配置和使用响应文件	61
以传统模式安装代理	61
安装 AIM	62
安装 CA Systems Performance LiteAgent	64

第 3 章：升级 CA Virtual Assurance 65

支持的升级	65
如何升级 CA Virtual Assurance	66
查看升级文档	67
准备要升级的环境	68
建立维护窗口	69
应用重要修补程序	69
备份整个系统	69
将多 Apache 配置还原到单 Apache	70
停止服务	71
查看升级限制	71
手动升级远程 Embedded Entitlements Manager	72
运行管理器安装	72
查看未自动升级的旧配置	73
手动应用旧配置	74
升级受管节点和 AIM 服务器	74
代理和 AIM 升级	75
将 SystemEDGE 监视器导入策略	77
验证环境中的 CA Virtual Assurance 升级	78

第 4 章：用户界面入门 79

启动 CA Virtual Assurance	79
功能概述	80
启动 AutoShell	80
有效 AutoShell 用户	82
启动 CA Virtual Assurance 命令提示符	82
启动总目录和联机帮助	82

第 5 章：卸载 CA Virtual Assurance 85

卸载选项	85
卸载管理器	85

执行完全卸载.....	86
从命令提示符卸载管理器.....	86
以无提示模式卸载管理器.....	87
卸载 SystemEDGE	87
在 Windows 上卸载 SystemEDGE 和 AIM.....	87
在 UNIX 系统上卸载 SystemEDGE 和 AIM.....	89

第 6 章： 备份与还原 91

备份与还原概述.....	91
备份整个系统.....	92
备份配置和数据.....	93
备份数据库.....	93
备份目录和数据.....	94
还原整个系统.....	97
还原配置和数据.....	97
还原数据库.....	98
还原目录和数据.....	99

第 7 章： 可扩展性最佳实践 101

扩展性概述.....	101
硬件规格.....	102
数据库注意事项.....	102
网络注意事项.....	102
远程部署和策略配置概述.....	103
可扩展性建议.....	105
vCenter AIM 监控建议	105
CA Virtual Assurance vCenter 管理建议.....	106
LPAR AIM 监控建议	108
Solaris Zones AIM 监控建议	109
远程部署和策略配置建议.....	110

词汇表 117

索引 119

第 1 章：简介

CA Virtual Assurance 是基于策略的产品，用于管理虚拟数据中心基础架构的性能。

CA Virtual Assurance 构建于面向服务的体系结构之上，可持续分析这些基础架构，以确保开通 UNIX、Linux 和 Windows 服务器执行所需任务并自动检测更改。

通过增强虚拟和动态环境的性能和工作负载，CA Virtual Assurance 可改进运行效率和端到端的数据中心自动化。

此部分包含以下主题：

[范围](#) (p. 9)

[读者](#) (p. 9)

[相关出版物](#) (p. 9)

[约定](#) (p. 10)

范围

本指南说明了如何安装和实现 CA Virtual Assurance 以及如何开始使用本产品，还提供了有关产品体系结构、组件和要求的简要概述。

本指南介绍了在不同模式下 CA Virtual Assurance 的逐步安装，并详细介绍了安装后任务。

词汇表解释了在虚拟化技术中使用的特定术语。

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 属性以及性能度量标准的详细信息。

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： 安装 CA Virtual Assurance

此部分包含以下主题：

[安装要求和注意事项](#) (p. 13)

[CA Virtual Assurance 的安装](#) (p. 17)

[无提示管理器安装](#) (p. 22)

[多个服务器上的安装](#) (p. 24)

[如何将 SQL Server 用户权限调整到最小必要权限](#) (p. 29)

[如何更新 CA Virtual Assurance](#) (p. 33)

[代理部署](#) (p. 35)

[各个代理安装](#) (p. 37)

安装要求和注意事项

本部分提供了有关安装 CA Virtual Assurance 的要求和注意事项的信息。

安装和配置 SQL Server Express

如果未安装 SQL Server，则还可以从 DVD1 安装 SQL Server Express。

遵循这些步骤：

1. 转到 DVD1 上的 Installers\Windows\External\MSSQLExpress 目录并运行安装程序。
2. 安装后，使用 SQL Server 配置管理器来启用 TCP/IP。
3. 通过 SQL Server 配置管理器确定静态 TCP 端口号（网络配置/协议/TCP/IP 属性/IP 地址）。
4. 在 CA Virtual Assurance 安装期间应用端口号和实例名（默认为 SQLEXPRESS）以连接到 SQL Server Express。

如果计划访问 *远程 SQL Server*：

- 在 CA Virtual Assurance 管理器计算机上安装 SQL Server 客户端。
- 在远程 SQL Server 上启用远程连接。

详细信息

[验证使用 SQL Server 的要求](#) (p. 14)

验证使用 SQL Server 的要求

CA Virtual Assurance 要求为管理数据库和性能数据库使用 SQL Server。CA Virtual Assurance 提供以下 SQL Server 支持：

- 本地或远程 SQL Server
- 默认 SQL Server 实例或命名实例
- 静态 SQL Server TCP/IP 端口
- Windows 身份验证和 SQL Server 身份验证

遵循这些步骤：

1. 验证 SQL Server 要求

- 确定 TCP/IP 已启用。
- 确定已为计划使用的实例指定静态 TCP/IP 端口。不支持动态端口。
- 验证不存在用作本地数据库的服务器名称的 IP 地址。
- 如果希望从远程计算机进行连接，则需确定远程连接已启用。
- 确定已指定所需的身份验证模式（混合模式或 Windows 身份验证）。
- 确定您计划用于新的典型安装或自定义安装的实例不包含名为 AOM2 或 DPM 的数据库。CA Virtual Assurance 会在安装期间创建这些数据库。

2. 验证 SQL Server 客户端要求

确定已在本地 CA Virtual Assurance 管理器系统上安装 SQL Server 客户端。CA Virtual Assurance 管理器要求使用 SQL Server 客户端连接到本地或远程 SQL Server。CA Virtual Assurance 管理器安装程序使用可用的系统 PATH 条目来访问 SQL Server 客户端程序。

安全注意事项

使用 CA Embedded Entitlements Manager (Embedded Entitlements Manager) 保护 CA Virtual Assurance 的安全。安装 CA Virtual Assurance 时，可以选择下列身份验证方法之一。

本地安全性

如果您是 Embedded Entitlements Manager 管理员，可以专门针对 CA Virtual Assurance 创建自己的一组用户、用户组和策略，因为所有这些信​​息都保存在本地存储中。但是，这需要您手动定义自己的一套用户和用户组，可以不与目录服务中当前可用的内容保持一致。

Active Directory 用户

在与现有的 Active Directory 配置集成时，您所有的用户和用户组均已预先定义，并与中央用户存储库保持一致。但可使用 Active Directory 来创建新用户或修改现有用户，而不能使用 CA Virtual Assurance 或 Embedded Entitlements Manager 进行这些操作。

评估您的要求并选择最适合的设置。

优化 Windows 内存管理

要在 CA Virtual Assurance 管理器或 CA Virtual Assurance AIM 服务器上优化 Windows 内存管理性能，您可以应用 Microsoft 知识库文章 <http://support.microsoft.com/kb/Q315407> 中介绍的设置。

SystemEDGE 与 CA Systems Performance LiteAgent 之间的比较

CA Virtual Assurance 附带有两个监控代理，即 SystemEDGE 和 CA Systems Performance LiteAgent。

SystemEDGE 是一个符合 SNMP 标准的代理，可使用行业标准 MIB 提供对受监控元素的访问。SystemEDGE 还提供了一个可扩展的插件 (AIM) 接口，该接口允许进行其他监控，如 vCenter 服务器、Solaris Zones 或服务响应监控。SystemEDGE 向 CA Virtual Assurance 管理器提供状态和性能数据。SystemEDGE 对于管理虚拟环境和服务器是必不可少的。

CA Systems Performance LiteAgent 是一个轻量级监控代理，可提供对 Windows、UNIX 以及 Linux 上的许多性能度量标准的访问。在 Windows 中，能够监控性能注册表中包括的几乎所有度量标准。监控基于管理器组件的请求按需执行。CA Systems Performance LiteAgent 向 CA Virtual Assurance 管理器提供性能数据。

有关 SystemEDGE 与 CA Systems Performance LiteAgent 之间差异的更多详细信息，请参阅下表：

特性	SystemEDGE 代理	CA Systems Performance LiteAgent
SNMP-compliant 代理	Y	N
SNMP-based 陷阱	Y	N
零配置代理	N	Y
SNMP v1/v2 通信	Y	N
SNMP v3 通信	Y	N

特性	SystemEDGE 代理	CA Systems Performance LiteAgent
计算机名称/地址的监控限制	Y	N
基于 CAM 的通信	仅配置操作	Y
支持多个管理器实例	Y	Y
支持 Spectrum IM	Y	N
支持 eHealth	Y	N
支持 NSM	Y	Y
支持第三方管理器	Y	N
支持 UI “资源” 选项卡	Y	N
支持 UI “策略” 选项卡	Y	Y
数据存储性能数据库	Y	Y
基于文件的配置	Y	N/A
基于管理器 UI 的配置	Y	N/A
分层对象模型	Y	N
基于代理的阈值监控	Y	N
支持主机资源 MIB	Y	N
Windows 性能度量标准	部分 ¹	Y
可扩展性能度量标准	N	Y ²
宽幅 UNIX 或 Linux 监控	Y	Y
真实平均性能监控	Y	N
支持 vCenter 服务器管理	Y (AIM)	N
支持 Hyper-V 管理	Y (AIM)	N
支持 Solaris Zones 管理	Y (AIM)	N
支持 LPAR 监控	Y (AIM)	Y
支持 UCS 管理	Y (AIM)	N
对 Exchange Server 和 Active Directory 的支持	Y (AIM)	N
支持 IBM High Availability Cluster Multiprocessing AIM	Y (AIM)	N
支持 VMware vCloud AIM	Y (AIM)	N

特性	SystemEDGE 代理	CA Systems Performance LiteAgent
支持 Citrix XenServer AIM	Y (AIM)	N
支持 KVM AIM	Y (AIM)	N

(1) SystemEDGE 支持有限的一组性能度量标准。请参阅《SystemEDGE 用户指南》。

(2) CA Systems Performance LiteAgent 可以动态监控 Windows 性能度量标准。

CA Virtual Assurance 的安装

本部分详细介绍了在 Windows 操作环境中安装 CA Virtual Assurance 的组件、安装选项和程序。

为安装做准备

通过该安装，可以选择要安装的组件或指定凭据。在安装期间，向导仅显示安装所选组件需要的对话框。根据您的选择，安装向导将请求以下与环境相关的数据（圆括号内为默认值）：

组件	服务器	用户	密码	协议	端口
管理数据库 (1)	X	X (sa)	X	-	X (1443)
性能数据库 (1)	X	X (sa)	X	-	X (1443)
Embedded Entitlements Manager 身份验证 (2)	X	EiamAdmin	X	-	-
以服务登录的 Apache 用户 (3)	-	X	X	-	-
以服务登录的 Tomcat 用户 (4)	-	X	X	-	-
本地安全用户 (5)	-	X	X	-	-
Active Directory 安全性 (5, 6)	X	X	X	-	-
系统用户	-	sys_service	X	-	-

组件	服务器	用户	密码	协议	端口
网络发现网关	-	-	-	-	X (8082)
Apache HTTP Server	-	-	-	-	X (443)
Apache Tomcat 服务 器	-	-	-	-	X (8443)
Apache Tomcat 关闭	-	-	-	-	X (8005)
ActiveMQ	-	-	-	-	X (61616)

(1) 选择“Windows 身份验证”(默认)或“SQL 身份验证”。如果选择了“SQL 身份验证”，请输入数据库管理员 (sa) 的名称和密码。选择管理数据库的适当初始大小：

初始大小	系统数	磁盘空间
小	1,000	1 GB - 核心组件 500 MB - 日志文件
中	5,000	5 GB - 核心组件 1 GB - 日志文件
大	10,000	10 GB - 核心组件 5 GB - 日志文件

SQL Server 数据库在默认情况下设置为完全恢复模式，因此事务日志在备份之前会增大。定期排定数据库备份。

性能数据库默认为 500 MB 并会根据需要自动增加。

(2) Embedded Entitlements Manager 仅支持一个 AIP 实例。如果指定的 EEM 安装中已存在 AIP 实例，请执行以下选项之一：

- 在没有 AIP 实例的情况下指定 Embedded Entitlements Manager 安装。
- 删除 AIP 实例（如果不再需要它）。依次打开 <EMM> 用户界面和“配置”选项卡，选择 AIP，然后单击“取消注册”。
- 允许 CA Virtual Assurance 在本地系统上安装 Embedded Entitlements Manager。

(3) 输入用户名和密码以向 Windows 管理域用户授予 Apache 的“以服务登录”权限。如果将 Windows 身份验证用于远程 SQL Server，则需要此用户。另请参阅本章中的[多个服务器上的安装](#) (p. 24)。

(4) 输入用户名和密码以向 Windows 管理域用户授予 Tomcat 的“以服务登录”权限。如果将 Windows 身份验证用于远程 SQL Server，则需要此用户。可以为 Tomcat 和 Apache 指定相同用户。另请参阅本章中的[多个服务器上的安装](#) (p. 24)。

(5) 选择“Active Directory 安全性”或“本地安全性”（默认）。

(6) 选择“Active Directory 安全性”，提供外部目录主机名、用户和密码。

注意：如果安装在与分发服务器相同的系统上安装 SystemEDGE，则会将 SystemEDGE 的配置管理器主机名设置为 localhost。

详细信息

[通过 CA Virtual Assurance 管理器安装程序进行 SystemEDGE 安装](#) (p. 39)

运行安装

在确定满足所有先决条件后，请执行该过程。

遵循这些步骤：

1. 将安装介质插入 DVD 驱动器。

如果启用了自动运行，安装向导将自动启动。如果安装向导未启动，请双击 setup.hta，或导航到安装介质上的 DVDdrive:\Installers\Windows 目录并双击 install.exe。

此时将显示“预安装检查”对话框。

2. 验证预安装检查项是否已成功完成。

如果某项失败，请修复要求并重新启动安装。

3. 单击“继续”。

此时会出现“许可协议”对话框。

4. 阅读协议并滚动到协议底部，直到“我接受此许可协议的条款”选项处于活动状态。选择该选项，然后单击“下一步”。

此时将显示“选择要安装的功能”对话框。

5. 选择要安装的 CA Virtual Assurance 组件，然后单击“下一步”。

此时将显示“所需配置”对话框。

6. 查看带有绿色勾选标记的项以及带有红色 x 图标的项。

- 安装路径

注意：目标路径中不支持下列字符：感叹号 (!)、左方括号 ([)、右方括号 (])、左括号 “(”、右括号 “)” 和分号 (;)。

- 数据库

验证管理和性能数据库设置，并在必要时更改数据库服务器名称、实例、身份验证类型或端口号 (1433)。单击“确定”。

默认：Windows 身份验证

如果选择了 SQL 身份验证，请输入数据库管理员 (sa) 的名称和密码。

注意：如果数据库登录凭据、服务器名称或端口无效，将显示错误消息，您可以输入正确信息。如果错误无法解决，安装程序将退出，不会对您的计算机做任何更改。有关详细信息，请参阅 [“验证使用 SQL Server 的要求”](#) (p. 14) 一节。

- Embedded Entitlements Manager

如果不参考现有 Embedded Entitlements Manager 安装，则 CA Virtual Assurance 会在本地系统上安装 Embedded Entitlements Manager。在安装期间，CA Virtual Assurance 会在 Embedded Entitlements Manager 中创建 AIP 实例。Embedded Entitlements Manager 仅支持一个 AIP 实例。

如果参考现有 Embedded Entitlements Manager 安装，则安装程序会检查 Embedded Entitlements Manager 是否存在注册的 AIP 实例。如果安装程序发现 AIP 实例，则安装过程会停止。如果不再使用 AIP 实例，则可以对其取消注册。要从 Embedded Entitlements Manager 中删除 AIP 实例：请依次打开 Embedded Entitlements Manager 用户界面和“配置”选项卡，选择 AIP，然后单击“取消注册”。

- 网络端口

可以为列出的组件指定网络端口，或接受以下默认值：

- 网络发现网关端口：8082
- Apache 端口：443
- Tomcat 服务器端口：8443
- Tomcat 关闭端口：8005
- Apache ActiveMQ 消息代理端口：61616

- 其他运行时区域设置

如有必要，请指定另一个要激活的区域设置，然后单击“确定”。

默认：英语(美国)

- SNMP 管理

除默认公共团体和管理员及其关联的 SNMP 端口 161、1691 和 6665 之外，可以指定自己的只读和读写团体和端口。

默认：public、snmp_admin

在安装期间指定的所有团体在安装的产品中用作全局（默认）SNMP 设置。如有必要，可以在 CA Virtual Assurance 用户界面中指定其他 SNMP 设置。请参阅《*管理指南*》的如何配置 SNMP 和访问控制列表部分。

7. 输入必要信息，然后单击“下一步”。

带有要安装的组件列表的“预安装摘要”对话框打开。

8. 单击“安装”开始安装。

此时将显示“安装进度”对话框。

注意：如果安装成功，则安装程序将在 *Install_Path\productname\log\install* 目录中为每个安装的组件创建日志文件。

9. 单击“完成”。

此时将显示“产品状态检查”对话框。

10. 验证产品状态检查项是否已成功完成。

如果某项失败，请验证要执行的操作。例如，安装可用修补程序。

注意：

- 要安装 CA Virtual Assurance 的更新，请参阅[如何更新 CA Virtual Assurance](#) (p. 33) 部分。
- 如果安装不成功，将显示“安装完成但有错误”对话框。有关详细信息，请参阅安装日志 (*Install_Path\productname\log\install\install.log*) 和错误列表 (*Install_Path\productname\log\install\install_error_detected.log*)。

11. 依次导航到“开始”、“程序”、“CA”和“CA Virtual Assurance”，启动 CA Virtual Assurance，并使用已在安装期间指定的凭据进行登录。

详细信息

[为安装做准备](#) (p. 17)

[验证使用 SQL Server 的要求](#) (p. 14)

取消安装

在运行 CA Virtual Assurance 安装程序时，当程序将产品文件解压缩到系统中的临时目录时，将显示进度条。如果在出现第一个安装对话框之前取消安装过程，进度条将消失，并且不会安装产品。但由于无法中断解压缩过程，安装程序将继续解压缩文件，直至完成。然后，程序将删除临时目录，并使系统保持不变。解压缩文件和删除临时目录可能会临时降低 CPU 性能。

初始安装之后的组件安装

如果在初始安装期间未安装所有组件，则可以重新运行安装程序以安装缺失组件。

无提示管理器安装

本节介绍了如何执行无提示管理器安装。完成每个部分中的一个或多个过程。

注意：在开始无提示安装之前，请验证目标计算机是否满足《版本说明》中指定的先决条件。

详细信息

[从安装介质中复制无提示安装文件](#) (p. 22)

[执行无提示管理器安装](#) (p. 23)

从安装介质中复制无提示安装文件

在编辑响应文件并运行实际安装程序之前，将其和其他支持文件从安装介质复制到管理器或代理所在的受支持服务器上。

DVD1 是在 Windows 中完成管理器安装所必需的，其中包括 SystemEDGE 和 SystemEDGE AIM。

在 AIX、HP-UX、Linux 或 Solaris（SPARC、x86）上进行 CA Virtual Assurance 受管节点安装需要 DVD2。

遵循这些步骤：

1. 将 DVD1 安装程序目录复制到目标计算机。
2. 导航到下载的安装介质的根目录，并转到 *ResponseFileTemplates* 目录。
silent.properties 文件将出现在列表中。
3. 将 silent.properties 文件复制到目标计算机上的 \Installers\Windows 目录。
可以根据要求在主机服务器上编辑 silent.properties 文件。

编辑 silent.properties 文件

无提示安装程序使用 silent.properties 文件获取在受支持的 Windows 计算机上安装管理器组件的首选项的相关信息。编辑该文件以执行无提示安装。

重要信息！ 对于 silent.property 文件，我们仅支持 UTF-8 字符编码。有关 UTF-8 字符支持和国际化的详细信息，请参阅《版本说明》。

遵循这些步骤：

1. 导航到目标计算机上的 \Installers\Windows 目录，然后在文本编辑器中打开 silent.properties 文件。
将显示文件的内容。
2. 按照文件中包含的有关在注释中指定安装选项部分的说明进行操作。例如：
`USER_INSTALL_DIR=C:\\Program Files\\CA\\productname`
使用双反斜杠 (\\) 定义路径。
注意： 更新必要的部分，但即使是用不到的部分，也不要删除。
3. 保存并关闭该文件。

在运行无提示安装程序时，将使用您的设置来安装指定的管理器组件。

执行无提示管理器安装

使用 DVD1 中的文件在 Windows 系统中执行无提示管理器安装。

遵循这些步骤：

1. 在目标系统上打开命令提示符。
将显示命令提示符窗口。
2. 转到 \Installers\Windows\ 目录，然后输入以下命令：
`install.exe -i silent -f path_to_silent.properties_file\silent.properties`
安装开始并在系统中安装管理器。
3. 在安装完成之后，请检查 `install_path\productname\log\install` 目录中的文件是否包含错误和警告。
注意： 在分布式无提示安装中，服务控制器必须保持运行才会安装其他组件，以便对其进行验证。

详细信息

[从安装介质中复制无提示安装文件](#) (p. 22)

[编辑 silent.properties 文件](#) (p. 23)

多个服务器上的安装

基于默认设置的安装会导致集中式安装。所有 CA Virtual Assurance 管理器组件、数据库、SystemEDGE 以及所有 AIM 都在单个 Windows 服务器上运行。但是，可以在不同服务器上安装所有必需的 CA Virtual Assurance 组件。

本节介绍涉及多个服务器的安装方案。

详细信息

[多个服务器上的安装准则](#) (p. 24)

[各个代理安装](#) (p. 37)

多个服务器上的安装准则

要在不同服务器上安装 CA Virtual Assurance 组件，必须在每个服务器上运行安装。安装期间从组件树中分别选择相应组件。由于组件之间的依存关系，请考虑以下准则：

- 如果安装范围跨越防火墙，请打开受影响组件之间的相应通信端口。
- 要想实现无缝时区运行，请验证您的分布式计算环境是否已同步到通用的时间源（例如，NTP 服务器、GPS）。
- 验证 SQL 管理工具（OSQL、BCP）在运行 Automation Management Framework 的服务器上是否可用。SQL 管理工具（OSQL、BCP）是 SQL Server 安装的一部分，并且是用于访问本地或远程 SQL Server 的必需工具。Automation Management Framework 以及访问管理数据库和性能数据库的所有 CA Virtual Assurance 管理器组件必须驻留在一个服务器上。
- 验证是否已为 SQL Server 启用 TCP，以及是否已设置静态端口（默认值：1433）。如果连接到远程 SQL Server，则 SQL Server 中允许远程访问。CA Virtual Assurance 允许在访问管理数据库和性能数据库时选择 Windows 身份验证或 SQL Server 身份验证。
- 如果对远程 SQL Server 进行 Windows 身份验证，请验证以下要求：CA SM Domain Server、Apache HTTP Server 和 Apache Tomcat 服务必须在非本地系统帐户下运行。非本地系统帐户（域用户帐户）必须对管理器服务器和数据库服务器拥有必要的访问权限。如果将 Windows 身份验证用于远程 SQL Server，则安装程序会自动提示您输入有关该用户的信息。

SQL Server 身份验证不需要满足这些条件。

- 当在远程系统上安装分发服务器时，请配置分发服务器，以便连接到关联的 CA SM Domain Server。

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 Distribution Server 的“属性”对话框。
3. 停止服务
4. 将以下参数添加到“启动参数”字段：
`-m <运行 CA SM Domain Server 服务的系统的名称>`
5. 启动服务，然后单击“确定”。

方案：最大分布式安装

本方案列出了可在不同服务器上安装的所有 CA Virtual Assurance 组件。

服务器 1

CA Virtual Assurance 管理器组件
SQL Server 管理工具（OSQL、BCP）

服务器 2

Embedded Entitlements Manager

服务器 3

管理数据库

服务器 4

性能数据库

服务器 5

分发服务器

服务器 6

SystemEDGE 和 AIM

根据您的实施，少量服务器可能已足够。

示例

位于一个服务器、远程分发服务器、本地 Embedded Entitlements Manager、SystemEDGE 和 AIM 上的远程数据库：

服务器 1

CA Virtual Assurance 管理器组件
SQL Server 管理工具（OSQL、BCP）
Embedded Entitlements Manager
SystemEDGE 和 AIM

服务器 2

管理数据库
性能数据库

服务器 3

分发服务器

详细信息

[通信端口](#) (p. 26)

通信端口

CA Virtual Assurance 需要打开多个端口才能正常运行。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。

Active Directory 和 Exchange Server (ADES)

PowerShell 端口：80、443、5985 和 5986

ADSI 端口：3268 和 389

Apache 服务器

HTTPS（端口：443）

Embedded Entitlements Manager 服务器

iGateway 端口：5250

SystemEDGE

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

CA Systems Performance LiteAgent

CAM UDP 端口: 4104

CAM TCP 端口: 4105

Cisco UCS

HTTP 端口: 80

HTTPS (端口: 443)

Citrix XenServer

HTTPS (端口: 443)

SNMP 端口: 161

Huawei Galax

HTTP 端口: 8773

Hyper-V 和 SCVMM

WMI 端口: 135

IBM HACMP

安全外壳 TCP 端口: 22

IBM PowerVM

安全外壳 TCP 端口: 22

基于内核的虚拟机 (KVM)

REST API 端口: 8443

Microsoft SQL Server

管理数据库 TCP 端口: 1433

性能数据库 TCP 端口: 1433

MSCS AIM

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

安全外壳 TCP 端口: 22

策略配置

CAM UDP 端口: 4104 (入站/出站)

CAM TCP 端口: 4105 (入站)

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)

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)

远程监控 AIM

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

SNMP 堆栈

UDP 端口: 161、1691、162 (陷阱、入站)

Tomcat (用户界面)

HTTPS (端口: 8443)

关闭端口: 8005

VMware vCenter

HTTPS (端口: 443)

VMware vCloud

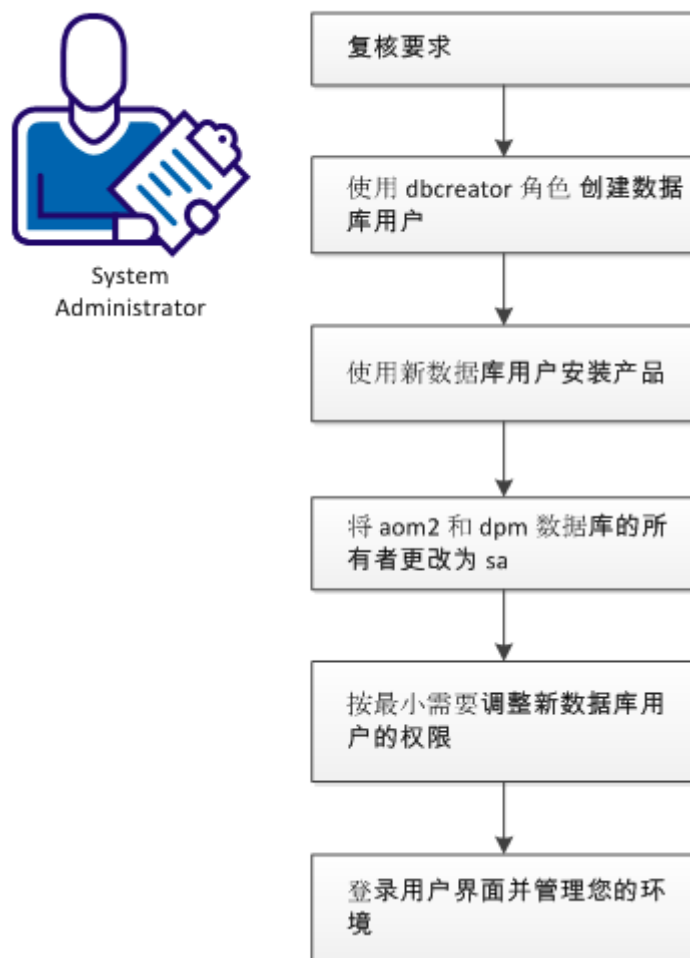
REST API 端口: 8443

如何将 SQL Server 用户权限调整到最小必要权限

作为系统管理员，您希望尽量减小 CA Virtual Assurance 针对访问其 SQL Server 数据库要求的权限。

下图说明了调整权限的必要步骤。

如何按最小需要调整 SQL Server 用户权限



请执行以下步骤：

[查看要求](#) (p. 30)

[以 dbcreator 角色创建数据库用户](#) (p. 30)

[使用新的数据库用户安装产品](#) (p. 30)

[将 aom2 和 dpm 数据库的所有者更改为 sa](#) (p. 31)

[将新数据库用户的权限调整到最小必要权限](#) (p. 31)

[登录用户界面并管理您的环境](#) (p. 32)

查看要求

在开始更改 CA Virtual Assurance 的数据库用户的用户权限之前，请查看以下要求：

- 已根据《安装指南》中指定的要求安装 SQL Server。
- SQL 身份验证（sa 用户）已启用。

以 dbcreator 角色创建数据库用户

在安装产品期间以要使用的 dbcreator 角色创建 CA Virtual Assurance 数据库用户。安装后，CA Virtual Assurance 可以在运行时使用具有其他权限的同一用户。

遵循这些步骤：

1. 以管理员 (sa) 权限登录 SQL Server。
 2. 在导航树中展开“安全”文件夹。
 3. 右键单击“登录”文件夹，然后选择“新建登录名”。
“新建登录名”对话框将打开。
 4. 在“常规”部分下指定以下设置：
 - 输入登录名，例如 causer。
 - 选择“SQL Server 身份验证”，然后输入此用户的密码。
 - 取消选中“用户必须在下次登录时更改密码”。
 5. 转到“服务器角色”部分，添加 dbcreator 角色，然后单击“确定”。
- 新的数据库用户具有足够的权限来安装产品。

使用新的数据库用户安装产品

您可以使用新的数据库用户来安装产品。

遵循这些步骤：

1. 启动 CA Virtual Assurance 的产品安装程序，并启动安装向导。
2. 在“所需配置”对话框中单击“数据库”条目。
此时将显示数据库配置对话框。
3. 选择“SQL Server 身份验证”，输入新的用户名 (causer) 和密码，然后单击“确定”。

4. 开始安装。
5. 安装成功后，依次单击“开始”(Windows)、“管理工具”、“服务”。
将打开“服务”窗口。
6. 向下滚动到 CAAIPApache 和 CAAIPTomcat，停止这些服务。

将 aom2 和 dpm 数据库的所有者更改为 sa

在安装过程中，创建两个 CA Virtual Assurance 数据库：dpm 和 aom2。将这些数据库的所有权更改为 sa 用户所有。

遵循这些步骤：

1. 以 sa 用户身份登录 SQL Server。
2. 单击“新建查询”。
此时将打开 SQL 控制台。
3. 输入以下 SQL 命令：

```
use dpm
exec sp_changedbowner 'sa', 'true'
use aom2
exec sp_changedbowner 'sa', 'true'
```
4. 单击“执行”。
sa 用户拥有 aom2 和 dpm 数据库。

将新数据库用户的权限调整到最小必要权限

CA Virtual Assurance 要求数据库用户必须具有足够的权限才能使用 aom2 和 dpm 数据库。以下过程将介绍如何将这些权限调整至最低。

遵循这些步骤：

1. 在 SQL Server Management Studio 的对象资源管理器中展开“安全”、“登录”。
2. 右键单击新用户（例如 causer），然后打开“属性”、“用户映射”。
此时将显示“用户映射”对话框。
3. 在对话框中选择 aom2 和 dpm 数据库，并向它们分配 db_datareader 和 db_datawriter 角色成员身份。单击“确定”。

4. 单击“新建查询”。

此时将打开 SQL 控制台。

5. 输入以下 SQL 命令，以允许新的数据库用户 (causer) 执行存储过程：

```
use dpm
GRANT EXECUTE TO causer
use aom2
GRANT EXECUTE TO causer
```

6. 在对象资源管理器中右键单击新用户 (causer)，然后打开“属性”、“服务器角色”。

此时将显示“服务器角色”对话框。

7. 删除 db_creator 角色，然后单击“确定”。

新的数据库用户可向 CA Virtual Assurance 提供足够的权限以使用 aom2 和 dpm 数据库。

登录用户界面并管理您的环境

要使用 CA Virtual Assurance 用户界面，首先需要启动 CAAIPApache 和 CAAIPTomcat 服务。

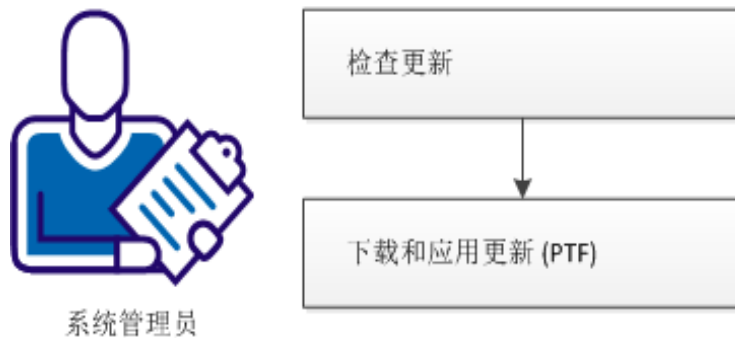
遵循这些步骤：

1. 依次单击“开始”(Windows)、“管理工具”、“服务”。
将打开“服务”窗口。
2. 向下滚动到 CAAIPApache 和 CAAIPTomcat，启动这些服务。
成功启动服务后，即可使用 CA Virtual Assurance。
3. 启动 CA Virtual Assurance 用户界面并管理您的环境。

如何更新 CA Virtual Assurance

作为系统管理员，您的作业包括在管理器系统上应用适用于 CA Virtual Assurance 的 PTF（程序临时修复）。应用 PTF 包括下载并安装可通过一个应用程序处理的 PTF。

如何应用更新 (PTF)



遵循这些步骤：

1. [检查更新](#) (p. 33)。
2. [下载并部署更新 \(PTF\)](#) (p. 34)。

检查更新

下载并应用更新之前，验证该版本适当的更新是否可用。

遵循这些步骤：

1. 右键单击系统托盘中的  图标，然后单击“检查更新”。
工具提示将显示结果。

另外，可以指定自动检查更新的时间设置。

遵循这些步骤：

1. 右键单击系统托盘中的  图标，然后单击“设置”。
此时将显示“设置”对话框。
2. 指定对话框中的字段，然后单击“确定”。
“检查更新”日程表已设置。

下载并应用更新 (PTF)

下载并应用 PTF，以保持管理器系统上的 CA Virtual Assurance 处于最新状态。

遵循这些步骤:

1. 转到“开始”、“所有程序”、CA、CA Virtual Assurance，然后单击“CA Virtual Assurance 更新”。
此时将显示“CA Virtual Assurance 更新”窗口。
2. 将打开适用的页面。
将列出适用于该版本的 PTF。
3. 选择所需的 PTF，单击“下载所选更新”，然后单击“应用所有下载的更新”。
更新实用工具会将 PTF 下载到 %INSTALL_PATH%\productname\CAPTFS 目录，并启动应用程序进程。应用程序进度对话框将显示状态。
4. 成功应用 PTF 后，退出应用程序进度对话框。
“CA Virtual Assurance 更新”窗口的“已应用”页列出了已应用的 PTF。
5. 单击“退出”。

代理部署

CA Virtual Assurance 提供了全面的解决方案，用于将 SystemEDGE 代理远程部署到所有受管系统。您可以基于提供的包含自定义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多个受管系统。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。

CA Virtual Assurance 提供了以下基本部署软件包：

- SystemEDGE 代理核心
- SystemEDGE 高级加密
- CA Citrix XenServer AIM
- SystemEDGE 远程监控 AIM
- SystemEDGE 服务响应监视器 AIM
- CA Systems Performance LiteAgent
- CA IBM LPAR AIM
- CA IBM High Availability Cluster Multiprocessing AIM
- CA KVM AIM（不适用于 CA Server Automation）
- CA Cisco UCS AIM
- CA Microsoft Hyper-V AIM
- CA Microsoft 群集服务支持 AIM
- CA Solaris Zones AIM
- CA VMware vCenter 服务器 AIM
- CA VMware vCloud AIM
- CA Exchange Server 和 Active Directory AIM（不适用于 CA Server Automation）

CA Virtual Assurance 支持以下 SystemEDGE 部署方案：

- 您可以将 SystemEDGE 版本 5.7.1 代理部署到没有预先存在的 SystemEDGE 代理的系统中。
- 您可以将 SystemEDGE 版本 5.7.1 代理部署到具有预先存在的 SystemEDGE 4.3 代理的系统中。部署会自动将现有代理升级到版本 5.7.1。
- 您可以对单个系统或通过配置模板进行配置更改。使用后面的选项可对现有的受管 SystemEDGE 代理或一组受管 SystemEDGE 代理应用更改。

注意：有关如何进行部署的详细信息，请参阅 *CA Virtual Assurance 联机帮助* 和 *《管理指南》*。

CA Virtual Assurance 不支持以下 SystemEDGE 部署方案：

- 您不能部署早于 SystemEDGE 5.0.0 的代理版本。
- 您不能在 CA Virtual Assurance 管理器系统上部署 SystemEDGE 代理。代理会通过 CA Virtual Assurance 管理器安装进行自动安装。

注意：有关部署支持的详细信息，请参阅《CA Virtual Assurance 管理指南》。

创建部署作业

您可以从 CA Virtual Assurance 管理器中通过远程部署在支持的 AIX、HP-UX、Linux、Solaris 或 Windows 系统上安装 SystemEDGE 和 AIM。

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。

- 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。

- （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。

- 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。

- （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。

- 单击“下一步”。

此时将显示“摘要”页面。

- 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。

有关远程部署的详细信息，请参阅《*CA Virtual Assurance 管理指南*》。

各个代理安装

本节详细介绍了用于在受管节点上安装 CA Virtual Assurance 代理的组件和程序。

SystemEDGE 组件的依存关系

CA Virtual Assurance 使用配有适当 Application Insight Module (AIM) 的 SystemEDGE 管理物理环境和虚拟环境。AIM 是扩展该代理功能范围的 SystemEDGE 插件。

可用的 AIM 如下所示：

- 适用于远程监控的 AIM (Windows)
- 适用于服务响应监控的 AIM (Windows、UNIX、Linux)
- 适用于 IBM LPAR 的 AIM (Windows)
- 适用于 IBM High Availability Cluster Multiprocessing 的 AIM (Windows)
- 适用于 KVM 的 AIM (Windows、Linux)
- 适用于 Microsoft Hyper-V 的 AIM (Windows)
- 适用于 Microsoft 群集服务支持的 AIM (Windows)
- 适用于 Solaris Zones 的 AIM (Windows)
- 适用于 Cisco UCS 的 AIM (Windows)
- 适用于 Cisco XenServer 的 AIM (Windows)
- 适用于 VMware vCenter 服务器的 AIM，用于管理 VMware Infrastructure 或 vSphere (Windows)
- 适用于 VMware vCloud 的 AIM (Windows)
- Exchange Server 和 Active Directory 的 AIM (Windows)
- 适用于 HUAWEI GalaX8800 的 AIM

注意：有关平台的更多详细信息，请参阅《版本说明》。

仅在安装有 SystemEDGE 和高级加密的系统上使用这些 AIM。CA Virtual Assurance 可发现此类系统并根据所安装组件的功能范围对其进行管理。

SystemEDGE 在以下操作系统上运行：

- AIX
- HP-UX
- Linux
- Solaris x86
- Solaris SPARC
- Windows

注意：如果通过图形用户界面进行安装期间指定了带空格字符或分号 (;) 的团体字符串，代理将无法正常运行。

通过 CA Virtual Assurance 管理器安装程序进行 SystemEDGE 安装

通过 CA Virtual Assurance 管理器安装程序，可以安装 SystemEDGE，而无需运行单个 SystemEDGE 安装程序。将 CA Virtual Assurance 管理器安装程序用于 SystemEDGE 时，请考虑下列关于配置管理器主机名的默认行为：

- 典型安装将 SystemEDGE 的配置管理器主机名设置为 localhost。
- 如果自定义安装在与分发服务器相同的系统上安装 SystemEDGE，则会将 SystemEDGE 的配置管理器主机名设置为 localhost。
- 如果自定义安装在没有分发服务器的系统上安装 SystemEDGE，则会将 SystemEDGE 的配置管理器主机名设置为星号 (*)。星号指定发现该系统的第一个 CA Virtual Assurance 管理器是 SystemEDGE 的配置管理器主机。

如果要使用 SystemEDGE 和 AIM 设置和管理远程服务器，建议使用远程部署和策略配置。远程部署可指导您完成部署软件包创建过程。您可以指定一个排定和要将软件包部署到的服务器（Windows、Linux、UNIX）列表。根据配置管理器主机名设置，使用策略配置可以管理网络中 SystemEDGE 代理的配置。有关详细信息，请参阅《*管理指南*》和*联机帮助*。

下列情形要求您手工安装代理，而不是使用建议的 CA Virtual Assurance 远程部署方法：

- 在不支持远程部署的系统上安装代理。
- 想要以传统模式安装代理。
- 想要在设置期间手工指定配置管理器主机名和所有其他设置。

有关支持的版本的列表，请参阅《*版本说明*》。

详细信息

[以传统模式安装代理](#) (p. 61)

在 Windows 系统上安装

本节介绍如何在 Windows 系统上手动安装 SystemEDGE。可以使用交互式向导进行安装，也可以使用命令行以无提示方式进行安装。单独的软件包可用于所有支持的硬件体系结构。安装程序会检测硬件体系结构并运行相应的安装软件包。

下列情形要求您手工安装代理，而不是使用建议的 CA Virtual Assurance 部署方法：

- 在不支持远程部署的系统上安装代理。
- 想要以传统模式安装代理。

在本指南中，术语 *Windows* 涵盖支持的 Windows 版本。有关所支持版本的列表，请参阅《*SystemEDGE 版本说明*》。

详细信息

[以传统模式安装代理](#) (p. 61)

在 Windows 上安装代理

可以使用交互式向导在 Windows 上手工安装 SystemEDGE 代理。

遵循这些步骤:

1. 以管理员身份登录到 Windows 系统，并执行以下操作之一：

- 从 CA Virtual Assurance 安装映像的 DVD1 双击 setup.hta，然后在 CA Virtual Assurance 对话框中单击“安装 SystemEDGE 代理”。
- 打开 DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_Core 文件夹并双击 ca-setup.exe。

注意：对于运行 Windows Vista 或更高版本的系统，您能够以非管理员身份进行安装。操作系统会提示您使用管理员凭据授权安装。

安装向导将打开。安装程序会检测系统的硬件体系结构并运行相应的安装软件包版本。

2. 单击“下一步”。

此时将打开“许可协议”页面。

3. 阅读“许可协议”并滚动到协议底部。选择“我接受此许可协议的条款”选项，然后单击“下一步”。

此时将打开“安装类型”页面。

4. 选择“典型安装”或“自定义安装”，然后单击“下一步”。

注意：以下过程介绍自定义安装。如果选择“典型安装”，单击“下一步”时将打开“检查设置”页面。

此时将显示“目标位置”对话框。

5. 接受默认值或进行浏览以选择安装和数据目录的位置，单击“下一步”，然后继续执行第 9 步。如果要指定其他位置，请单击“高级”并继续执行第 8 步。

目标位置

指定要安装代理的位置。默认情况下，安装目录是

Install_Path\SystemEDGE，运行时程序数据存储在 *config* 子目录中。要指定更多参数，请单击“高级”。

注意：在已安装先前版本代理的系统上安装该代理时，安装程序会选择现有代理的安装目录。

如果跳过“高级”对话框，将出现“配置管理器设置”对话框。

6. 填写“高级目标位置”对话框的以下字段，然后单击“下一步”。

SystemEDGE 二进制路径

为二进制程序和文档指定目录。

SystemEDGE 数据路径

为运行时程序数据指定目录。

CA 共享组件路径

为 CA 共享组件指定目录。一旦由任意 CA 软件设置该目录，就无法对其进行更改并且会禁用用户界面中的相应字段。

此时将显示“配置管理器设置”对话框。

7. 填写以下字段，然后单击“下一步”。

配置管理器主机名

指定要用从其管理该代理的配置管理器的主机名。为该参数输入值，以从运行 CA Virtual Assurance 的系统上配置该代理。输入星号 (*) 可接受第一个发现代理系统的管理器。

默认配置策略名称

指定供代理使用的配置策略文件（由 CA Virtual Assurance 管理器维护）的名称。为该参数输入值，以根据管理器中的现有配置文件设置 SystemEDGE 配置。

如果安装程序检测到系统上正在运行本地 Microsoft SNMP 代理，将显示以下“本地 SNMP 选项”对话框。

8. 如果您的系统上已安装简单网络管理协议 (SNMP)，请选择以下选项之一，然后单击“下一步”。

默认来自现有 SNMP 代理

指定是否使用本地 SNMP 代理的默认设置。取消选中该复选框可使用与本地 SNMP 代理不同的团体字符串和陷阱目标。

禁用本地 SNMP 代理

指定是否停止并禁用本地 SNMP 代理。如果使本地 SNMP 代理处于启用状态，则在其他端口上运行 SystemEDGE。

9. 填写以下字段，然后单击“下一步”。

SNMP 端口号

指定要在其上运行 SystemEDGE 代理的端口。

默认值：161

重要信息！ 该端口号专用于 SystemEDGE 代理。如果其他应用程序使用该端口号，则安装将失败。如果本地 SNMP 代理已使用默认端口，请指定其他端口（例如，1691 或 6665）。

此时将显示“SNMP 系统信息”对话框。

10. 填写以下字段，然后单击“下一步”。

系统说明

指定用于填充 sysDescr MIB-II 对象的系统的信息（如系统名称）。

系统位置

指定用于填充 sysLocation MIB-II 对象的系统位置。

系统联系人

指定用于填充 sysContact MIB-II 对象的系统联系人信息。

此时将显示“SNMP 团体设置”对话框。

11. 填写以下字段，单击“下一步”，然后继续执行第 13 步。如果要指定多个团体字符串，请单击“高级”并继续执行第 12 步。

只读团体

指定 SNMP 只读团体字符串。

默认值：public

读写团体

指定 SNMP 读写团体字符串。

如果跳过“高级”对话框，将显示“SNMP 陷阱设置”对话框。

12. 填写“SNMP 团体设置 - 高级”对话框中的以下字段，然后单击“下一步”。

只读团体

指定 SNMP 只读团体字符串。可以指定多个团体，用分号进行分隔（例如，public1; public2）。还可以包括各团体的 IP 地址列表以限制访问（例如，public 1.2.3.4）。

默认值：public

读写团体

指定 SNMP 读写团体字符串。可以指定多个团体，用分号进行分隔（例如，rwcomm1; rwcomm2）。还可以包括各团体以空格分隔的 IP 地址列表以限制访问（例如，rwcomm1 1.2.3.4）。读写团体字符串对于正确操作某些 AIM（例如，RM）和一些远程使用（例如，创建监视器）是必需的。

此时将显示“SNMP 陷阱设置”对话框。

13. 填写以下字段，单击“下一步”，然后继续执行第 15 步。如果要指定多个陷阱目标，请单击“高级”并继续执行第 14 步。

陷阱团体字符串

指定在发送陷阱消息中编码的 SNMP 团体。

默认值：public

目标主机

指定陷阱消息的目标。

默认：在“配置管理器设置”对话框中设置的配置管理器主机名。

端口号

指定陷阱消息发送到的端口。

默认：162。

如果跳过“高级”对话框，将显示“杂项设置”对话框。

14. 填写“SNMP 陷阱设置 - 高级”对话框中的以下字段，然后单击“下一步”。

陷阱配置

指定一个或多个陷阱目标。可以指定多个条目，用分号进行分隔（例如，public server1; public server2 1162）。

此时将显示“杂项设置”对话框。

15. 填写下列字段，然后单击“下一步”：

安装之后启动

指定安装结束时是否启动代理。

安装文档

指定是否安装文档。

此时将显示“检查设置”页面。

16. 检查安装设置并单击“安装”。

安装完成后将显示“安装完成”页面。

17. 单击“完成”。

安装即会完成。

在 Windows 上从命令行安装代理

可以使用命令行版本的安装程序安装 SystemEDGE Windows 软件包。从命令行安装时，使用参数设置各种安装属性。可从命令行执行以下操作：

- 在预先填写安装参数或不预先填写安装参数的情况下启动安装向导
- 指定安装参数并在不使用交互式向导的情况下运行安装程序

该过程适用第二种方案：从命令行运行无人照管的安装。

遵循这些步骤：

1. 以管理员身份登录到 Windows 系统。

注意：对于运行 Windows Vista 和更高版本的系统，可以非管理员身份进行安装，操作系统会提示您使用管理员凭据授权安装。

2. 打开命令提示符，导航到
DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_Core 文件夹，然后输入以下所需参数（在完成第 3 步之前，请勿运行该命令）：

```
ca-setup CA_SETUP_MODE=UNATTENDED EULA_ACCEPTED="YES" [parameter]
```

注意：有关安装参数的帮助，请在命令提示符下输入 `ca-setup -?` 在命令提示符中。

CA_SETUP_MODE

指定安装模式。将该参数设置为 `UNATTENDED` 以在无提示模式下运行安装。如果省略该参数，则运行该命令后，安装向导打开时会预先填写指定的参数值。

EULA_ACCEPTED

读取许可协议并指定是否接受该许可协议。如果在将安装模式设置为 `UNATTENDED` 时省略该参数或将其设置为除 “**YES**” 以外的任何值，安装将失败。交互式安装中不需要该参数。

3. 根据需要添加可选参数并运行命令。

注意：如果省略以下可选参数，则无需提供这些参数的值：

CA_SETUP_LOG_FILE
CA_SETUP_VERBOSE
CASE_INSTALLDIR
CASE_PUBDATADIR
CASE_SNMP_PORT
CASE_SNMP_SYS_DESC
CASE_SNMP_SYS_LOC
CASE_SNMP_SYS_CONTACT
CASE_SNMP_READ_COMMUNITY
CASE_SNMP_READ_ALLOWED_MANAGERS
CASE_SNMP_WRITE_COMMUNITY
CASE_SNMP_WRITE_ALLOWED_MANAGERS
CASE_SNMP_TRAP_COMMUNITY
CASE_SNMP_TRAP_DESTINATION
CASE_SNMP_TRAP_PORT
CASE_DISABLE_NATIVE_SNMP
CASE_DEFAULT_FROM_NATIVE_SNMP
CASE_MANAGER_HOSTNAME
CASE_MANAGER_POLICY_NAME
CASE_START_AFTER_INSTALL
CASE_INSTALL_DOCS
CASE_LEGACY_MODE

CA_SETUP_LOG_FILE

指定记录安装消息的位置和文件名。

CA_SETUP_VERBOSE

设置为“yes”时将打开详细安装模式。详细模式会将更多信息记录到安装日志文件中。

CASE_INSTALLDIR

指定 SystemEDGE 安装目录。该目录中包含与 SystemEDGE 相关的所有内容（如 AIM 和高级加密），并且绝不会在核心安装程序设置后进行修改。

注意：如果定义非默认的安装目录，安装程序会在不创建 SystemEDGE 子文件夹的情况下将代理文件直接安装到指定的目录。

默认：C:\Program Files\CA\SystemEDGE

CASE_PUBDATADIR

指定 SystemEDGE 数据目录，将在该目录中完成所有配置并存储动态数据（在本文档中称为变量 CASYSEDGE_DATA）。代理的配置文件位于基于 SNMP_PORT 参数值的端口特定的子目录中。

默认：C:\Documents and Settings\All Users\Application Data\CA\SystemEDGE（Windows XP 和 2003），
C:\Users\Public\CA\SystemEDGE（Windows Vista 和 2008）

CASE_SNMP_PORT

指定 SystemEDGE 使用的端口。也可以使用 CASE_DEFAULT_FROM_NATIVE_SNMP 参数从本地 SNMP 代理继承该值。如果使用 CASE_SNMP_PORT 参数指定端口，将会覆盖继承的值。该端口必须唯一，否则安装会失败。如果默认端口 161 已被本地 SNMP 代理使用（并且不打算禁用该代理），必须指定其他的唯一端口（例如，1691 或 6665）。

默认：161

CASE_SNMP_SYS_DESC

指定用于填充 sysDescr MIB-II 对象的系统的信息（如系统名称）。也可以使用 CASE_DEFAULT_FROM_NATIVE_SNMP 参数从本地 SNMP 代理继承该值。如果使用 CASE_SNMP_SYS_DESC 参数指定说明，将会覆盖继承的值。

CASE_SNMP_SYS_LOC

指定用于填充 sysLocation MIB-II 对象的系统位置。也可以使用 CASE_DEFAULT_FROM_NATIVE_SNMP 参数从本地 SNMP 代理继承该值。如果使用 CASE_SNMP_SYS_LOC 参数指定位置，将会覆盖继承的值。

CASE_SNMP_SYS_CONTACT

指定用于填充 sysContact MIB-II 对象的系统联系信息。也可以使用 CASE_DEFAULT_FROM_NATIVE_SNMP 参数从本地 SNMP 代理继承该值。如果使用 CASE_SNMP_SYS_CONTACT 参数指定联系人，将会覆盖继承的值。

CASE_SNMP_READ_COMMUNITY

指定可向代理发送 GET 请求的 SNMP 读团体的名称。可以通过以分号进行分隔来指定多个团体（例如，public1;public2），也可以包含各团体的以空格分隔的 IP 地址列表以限制访问（例如，public 1.2.3.4）。也可以使用 CASE_DEFAULT_FROM_NATIVE_SNMP 参数从本地 SNMP 代理继承该值。如果使用 CASE_SNMP_READ_COMMUNITY 参数指定读团体，将会覆盖继承的值。

默认：snmp_public（仅在全新安装（不是升级）以及未指定读写团体的情况下有效）

CASE_SNMP_READ_ALLOWED_MANAGERS

指定所允许的 SNMP 管理器的以空格分隔的 IP 地址/主机名列表，以使用 SNMP_READ_COMMUNITY 查询代理。指定该项时，SNMP_READ_COMMUNITY 只能包含一个词，即 SNMP 团体。

CASE_SNMP_WRITE_COMMUNITY

指定可向代理发送 GET 和 SET 请求的 SNMP 写团体的名称。可以通过以分号进行分隔来指定多个团体（例如，rwcomm1;rwcomm2），也可以包含各团体的以空格分隔的 IP 地址列表以限制访问（例如，rwcomm1 1.2.3.4）。也可以使用 CASE_DEFAULT_FROM_NATIVE_SNMP 参数从本地 SNMP 代理继承该值。如果使用 CASE_SNMP_WRITE_COMMUNITY 参数指定写团体，将会覆盖继承的值。

CASE_SNMP_WRITE_ALLOWED_MANAGERS

指定所允许的 SNMP 管理器的以空格分隔的 IP 地址/主机名列表，以使用 SNMP_WRITE_COMMUNITY 查询代理。指定该项时，SNMP_WRITE_COMMUNITY 只能包含一个词，即 SNMP 团体。

CASE_SNMP_TRAP_COMMUNITY

指定 SNMP 陷阱团体和陷阱目标地址。可以通过以分号 (;) 进行分隔来指定多个陷阱团体设置。也可以使用

CASE_DEFAULT_FROM_NATIVE_SNMP 参数从本地 SNMP 代理继承该参数的值。如果使用 CASE_SNMP_TRAP_COMMUNITY 参数指定陷阱团体，将会覆盖继承的值。对于该参数，以下值是必需的：

- 团体名称
- 要将陷阱发送到的目标地址

对于该参数，以下值是可选的：

- 要将陷阱发送到的端口号
- 陷阱源编码选项
- 陷阱源主机名

陷阱团体设置的语法：

```
community-string {ip-address/hostname} [port [encoding [source]]]
```

示例：

```
public 1.2.3.4;public 2.3.4.5 1162;trapcom 3.4.5.6 1162 100 4.5.6.7
```

CASE_SNMP_TRAP_DESTINATION

指定要向其发送陷阱的主机名或 IP 地址。指定该项时，SNMP_TRAP_COMMUNITY 只能包含一个词（即 SNMP 团体），同时还必须指定 SNMP_TRAP_PORT。

CASE_SNMP_TRAP_PORT

指定要向其发送陷阱的目标端口号。指定该项时，SNMP_TRAP_COMMUNITY 只能包含一个词（即 SNMP 团体），同时还必须指定 SNMP_TRAP_DESTINATION。

CASE_DISABLE_NATIVE_SNMP

指定是否停止并禁用本地 SNMP 代理。

默认值： no

CASE_DEFAULT_FROM_NATIVE_SNMP

指定是否使用本地 SNMP 代理的默认 SNMP 设置。

默认值： no

CASE_MANAGER_HOSTNAME

指定要用从其管理该代理的配置管理器的主机名。为该参数输入值，可从指定的管理器配置该代理。输入星号 (*) 可接受第一个发现代理系统的管理器。该管理器将可以对代理的配置进行完全控制。默认情况下，未输入（使用）任何管理器主机，并且代理在未受管模式下运行。

CASE_MANAGER_POLICY_NAME

指定代理应使用的配置管理器策略文件的名称。为该参数输入值，可根据管理器中的现有配置文件设置 SystemEDGE 配置。默认情况下，代理使用已安装的策略文件。

CASE_START_AFTER_INSTALL

指定安装完成后是否自动启动代理。

默认值： yes

CASE_INSTALL_DOCS

指定是否要随代理一起安装 SystemEDGE 文档。

默认值： yes

CASE_LEGACY_MODE

指定是否以传统模式安装代理，该模式仅在忽略便于与 CA Virtual Assurance 一起使用的所有材料时才会安装基本代理。如果不希望将代理与 CA Virtual Assurance 一起使用，则使用传统模式进行安装。

通过重新安装或升级并指定 CASE_LEGACY_MODE=no，可以使代理进入受管模式。

默认值： no

在命令行中输入命令以及所有必需的参数和值。按 Enter 键开始安装。安装程序会检测操作系统的硬件体系结构并运行相应的安装程序版本。

注意： 如果不接受安装协议，安装将失败。

要验证是否安装，请确认“Windows 服务”对话框中是否有 CA SystemEDGE 服务、安装目录中是否有 SystemEDGE 文件或者“添加或删除程序”对话框中是否有 CA SystemEDGE Core。还可以检查安装日志文件（如果指定了该文件），以确认成功安装。

注意： 如果是在运行 Windows Vista 或更高版本的系统上进行安装，SystemEDGE 安装程序会自动安装“Microsoft Visual C++ 2005 可再发行软件包”。如果未安装该软件包，SystemEDGE 将无法正常运行。要安装“Microsoft Visual C++ 2005 可再发行软件包”，必须接受所显示的许可协议。“Microsoft Visual C++ 2005 可再发行软件包”的许可协议在交互式版本的 SystemEDGE 安装程序中被删除。

在 UNIX 和 Linux 系统上进行安装

本节介绍如何在 UNIX 和 Linux 系统上手动安装 SystemEDGE 代理。可以使用交互式向导进行安装，也可以使用命令行以无提示方式进行安装。如果 Xserver 可用且正确设置了 DISPLAY 环境，交互式向导将以文本模式显示在控制台上或显示为图形应用程序。

下列情形要求您手工安装代理，而不是使用建议的 CA Virtual Assurance 部署方法：

- 在不支持远程部署的系统上安装代理。
- 想要以传统模式安装代理。

有关支持的 UNIX 和 Linux 平台及版本的详细信息，请参阅《SystemEDGE 版本说明》。

详细信息

[以传统模式安装代理](#) (p. 61)

在 UNIX 和 Linux 系统上安装代理

可以使用交互式向导在 UNIX 和 Linux 上手动安装 SystemEDGE 代理。

注意：

- 本文档将安装目录称为 CASYSEDGE，将数据目录称为 CASYSEDGE_DATA。
- 安装程序不会修改 /etc/profile 中的系统环境设置。

遵循这些步骤：

1. 以 root 用户身份登录到系统并挂接 DVD2。
2. 打开终端控制台并转到 `Installers/platform/Agent/SysMan/CA_SystemEDGE_Core` 目录，选择与您的操作系统对应的 *platform* 目录。
3. 按如下方式从该目录运行安装程序：

```
sh ca-setup.sh
```

此时将显示安装程序的“简介”页面。

4. 单击“下一步”。

此时会出现“许可协议”页面。

5. 阅读许可协议并选择“我接受此许可协议的条款”。单击“下一步”。

此时将显示“安装类型”页面。

6. 选择“典型安装”或“自定义安装”，然后单击“下一步”。

注意：该过程介绍自定义安装。如果选择“典型安装”，单击“下一步”时将显示“检查设置”页面。

此时将显示“目标位置”对话框。

7. 接受默认值或进行浏览以选择安装和数据目录的位置，单击“下一步”，然后继续执行第 9 步。如果要指定其他位置，请单击“高级”并继续执行第 8 步。

目标位置

指定要安装代理的位置。默认情况下，安装目录是
`/opt/CA/SystemEDGE`，运行时程序数据存储在 `config` 子目录中。
要指定更多参数，请单击“高级”。

注意：如果在已安装了代理先前版本的系统上安装该代理，安装程序会自动选择现有代理的安装目录。

如果跳过“高级”对话框，将出现“配置管理器设置”对话框。

8. 填写“高级目标位置”对话框的以下字段，然后单击“下一步”。

SystemEDGE 二进制路径

为二进制程序和文档指定目录。

SystemEDGE 数据路径

为运行时程序数据指定目录。

CA 共享组件路径

为 CA 共享组件指定目录。一旦由任意 CA 软件设置该目录，就无法对其进行更改并且会禁用用户界面中的相应字段。

此时将显示“配置管理器设置”对话框。

9. 填写以下字段，然后单击“下一步”。

配置管理器主机名

指定要用从其管理该代理的配置管理器的主机名。为该参数输入值，以从运行 CA Virtual Assurance 的系统上配置该代理。输入星号 (*) 可接受第一个发现代理系统的管理器。

默认配置策略名称

指定供代理使用的策略文件(由 CA Virtual Assurance 管理器维护)的名称。为该参数输入值，以根据管理器中的现有配置文件设置 SystemEDGE 配置。

如果安装程序检测到系统上正在运行本地 SNMP 代理，将显示“本地 SNMP 选项”对话框。

10. 填写以下字段，然后单击“下一步”。

默认来自现有 SNMP 代理

指定是否使用本地 SNMP 代理的默认设置。取消选中该复选框可使用与本地 SNMP 代理不同的团体字符串和陷阱目标。

禁用本地 SNMP 代理

指定是否停止并禁用本地 SNMP 代理。如果使本地 SNMP 代理处于启用状态，则在其他端口上运行 SystemEDGE。

11. 填写以下字段，然后单击“下一步”。

SNMP 端口号

指定要在其上运行 SystemEDGE 代理的端口。该端口必须未被任何其他应用程序使用，否则安装会失败。如果本地 SNMP 代理已使用默认端口，请指定其他端口（例如，1691 或 6665）。

默认值：161

此时将显示“SNMP 系统信息”对话框。

12. 填写以下字段，然后单击“下一步”。

系统说明

指定用于填充 sysDescr MIB-II 对象的信息（如系统名称）。

系统位置

指定用于填充 sysLocation MIB-II 对象的系统位置。

系统联系人

指定用于填充 sysContact MIB-II 对象的系统联系人信息。

此时将显示“SNMP 团体设置”对话框。

13. 填写以下字段，单击“下一步”，然后继续执行第 15 步。如果要指定多个团体字符串，请单击“高级”并继续执行第 14 步。

只读团体

指定 SNMP 只读团体字符串。

默认值：public

读写团体

指定 SNMP 读写团体字符串。

如果跳过“高级”对话框，将显示“SNMP 陷阱设置”对话框。

14. 填写“SNMP 团体设置 - 高级”对话框中的以下字段，然后单击“下一步”。

只读团体

指定 SNMP 只读团体字符串。可以通过以分号分隔各个团体来指定多个团体（例如，public1;public2）。还可以包括各团体的 IP 地址列表以限制访问（例如，public 1.2.3.4）。

默认值：public

读写团体

指定 SNMP 读写团体字符串。可以通过以分号分隔各个团体来指定多个团体（例如，rwcomm1;rwcomm2）。还可以包括各团体以空格分隔的 IP 地址列表以限制访问（例如，rwcomm1 1.2.3.4）。读写团体字符串对于正确操作某些 AIM（例如，RM）和一些远程使用（例如，创建监视器）是必需的。

此时将显示“SNMP 陷阱设置”对话框。

15. 填写以下字段，单击“下一步”，然后继续执行第 17 步。如果要指定多个陷阱目标，请单击“高级”并继续执行第 16 步。

陷阱团体字符串

指定在发送陷阱消息中编码的 SNMP 团体。

默认值：public

目标主机

指定陷阱消息的目标。

默认：在“配置管理器设置”对话框中设置的配置管理器主机名。

端口号

指定陷阱消息发送到的端口。

默认：162。

如果跳过“高级”对话框，将显示“权限分隔用户”对话框。

16. 填写“SNMP 陷阱设置 - 高级”对话框中的以下字段，然后单击“下一步”。

陷阱配置

指定一个或多个陷阱目标。可以通过以分号分隔各个条目来指定多个条目（例如，`public server1;public server2 1162`）。

此时将显示“权限分隔用户”对话框。

17. 填写以下字段，然后单击“下一步”：

用户名

指定用户名，在 SNMP 通信期间代理使用其凭据运行。

该条目会指示代理（仅限 UNIX）在其他用户帐户下运行 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。

此时将显示“杂项设置”对话框。

18. 填写下列字段，然后单击“下一步”：

安装之后启动

指定安装结束时是否启动代理。

安装文档

指定是否安装文档。

此时将显示“检查设置”页面。

19. 检查安装设置并单击“安装”。

安装完成后将显示“安装完成”页面。

20. 单击“完成”。

安装即会完成。

在 64 位 Linux 版本上安装 SystemEDGE 失败

症状：

在 64 位 Linux 版本上安装 SystemEDGE 时，安装失败。

解决方案：

要在 64 位 Linux 版本上运行并安装 SystemEDGE，请安装必需的 32 位库：

- 在 RedHat 或 SuSE 发行版上有效：

```
yum install glibc.i686
```

- 在 Debian 发行版上有效：

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

在 UNIX 上从命令行安装代理

可以使用命令行版本的安装程序安装 SystemEDGE UNIX 软件包。从命令行安装时，使用参数设置各种安装属性。可从命令行执行以下操作：

- 在预先填写安装参数或不预先填写安装参数的情况下启动安装向导
- 指定安装参数并在不使用交互式向导的情况下运行安装程序

注意：

- UNIX 不支持自动创建响应文件来运行无提示安装。但是，可以手动创建响应文件，并使用该文件进行无人照管的安装。
- 安装程序不会修改 `/etc/profile` 中的系统环境设置。

该过程适用第二种方案：从命令行运行无人照管的安装。

遵循这些步骤：

1. 以 root 用户身份登录到系统。
2. 导航到 `DVD2/Installers/platform/Agent/SysMan/CA_SystemEDGE_Core` 文件夹（指定与您的操作系统对应的 `platform` 文件夹），然后输入以下所需参数（在完成第 3 步之前，请勿运行该命令）：

```
sh ca-setup.sh CA_SETUP_MODE="UNATTENDED" EULA_ACCEPTED="yes" [parameter]
```

注意：有关安装参数的帮助，请在命令提示符下输入 `ca-setup -?` 在命令提示符中。

CA_SETUP_MODE

指定安装模式。将该参数设置为 `UNATTENDED` 以在不显示安装向导的情况下运行安装。如果省略该参数，则运行该命令后，安装向导打开时会预先填写指定的参数值。

EULA_ACCEPTED

读取许可协议并指定是否接受该许可协议。如果在将安装模式设置为 `UNATTENDED` 时省略该参数或将其设置为除 “**YES**” 以外的任何值，安装将失败。交互式安装中不需要该参数。

3. 根据需要添加可选参数并运行命令。

注意：如果省略以下可选参数，则无需提供这些参数的值：

CA_SETUP_LOG_FILE
CA_SETUP_VERBOSE
CASE_INSTALLDIR
CASE_PUBDATADIR
CASE_SNMP_PORT
CASE_SNMP_SYS_DESC
CASE_SNMP_SYS_LOC
CASE_SNMP_SYS_CONTACT
CASE_SNMP_READ_COMMUNITY
CASE_SNMP_READ_ALLOWED_MANAGERS
CASE_SNMP_WRITE_COMMUNITY
CASE_SNMP_WRITE_ALLOWED_MANAGERS
CASE_SNMP_TRAP_COMMUNITY
CASE_SNMP_TRAP_DESTINATION
CASE_SNMP_TRAP_PORT
CASE_DISABLE_NATIVE_SNMP
CASE_DEFAULT_FROM_NATIVE_SNMP
CASE_MANAGER_HOSTNAME
CASE_MANAGER_POLICY_NAME
CASE_PRIVSEP_USER
CASE_START_AFTER_INSTALL
CASE_INSTALL_DOCS
CASE_LEGACY_MODE

CA_SETUP_LOG_FILE

指定记录安装消息的位置和文件名。默认情况下，消息将记录到 /opt/CA/installer/log/CA_SETUP_PACKAGE_NAME.log 中。

CA_SETUP_VERBOSE

设置为“yes”时将打开详细安装模式。详细模式会将更多信息记录到安装日志文件中。

CASE_INSTALLDIR

指定 SystemEDGE 安装目录。该目录中包含与 SystemEDGE 相关的所有内容（如 AIM 和高级加密），并且绝不会在核心安装程序设置后进行修改。

注意：如果定义非默认的安装目录，安装程序会在不创建 SystemEDGE 子文件夹的情况下将代理文件直接安装到指定的目录。

默认： /opt/CA/SystemEDGE

CASE_PUBDATADIR

指定 SystemEDGE 数据目录，将在该目录中完成所有配置并存储动态数据（在本文档中称为变量 `CASYSEDGE_DATA`）。代理的配置文件位于基于 `SNMP_PORT` 参数值的端口特定的子目录中。

默认： `/opt/CA/SystemEDGE/config`

CASE_SNMP_PORT

指定 SystemEDGE 使用的端口。也可以使用

`CASE_DEFAULT_FROM_NATIVE_SNMP` 参数从本地 SNMP 代理继承该值。如果使用 `CASE_SNMP_PORT` 参数指定端口，将会覆盖继承的值。该端口必须唯一，否则安装会失败。如果默认端口 161 已被本地 SNMP 代理使用（并且不打算禁用该代理），必须指定其他的唯一端口（例如，1691 或 6665）。

默认： 161

CASE_SNMP_SYS_DESC

指定用于填充 `sysDescr` MIB-II 对象的信息（如系统名称）。也可以使用 `CASE_DEFAULT_FROM_NATIVE_SNMP` 参数从本地 SNMP 代理继承该值。如果使用 `CASE_SNMP_SYS_DESC` 参数指定说明，将会覆盖继承的值。

CASE_SNMP_SYS_LOC

指定用于填充 `sysLocation` MIB-II 对象的系统位置。也可以使用 `CASE_DEFAULT_FROM_NATIVE_SNMP` 参数从本地 SNMP 代理继承该值。如果使用 `CASE_SNMP_SYS_LOC` 参数指定位置，将会覆盖继承的值。

CASE_SNMP_SYS_CONTACT

指定用于填充 `sysContact` MIB-II 对象的系统联系信息。也可以使用 `CASE_DEFAULT_FROM_NATIVE_SNMP` 参数从本地 SNMP 代理继承该值。如果使用 `CASE_SNMP_SYS_CONTACT` 参数指定联系人，将会覆盖继承的值。

CASE_SNMP_READ_COMMUNITY

指定可向代理发送 GET 请求的 SNMP 读团体的名称。可以通过以分号进行分隔来指定多个团体（例如，`public1;public2`），也可以包含各团体的以空格分隔的 IP 地址列表以限制访问（例如，`public 1.2.3.4`）。也可以使用 `CASE_DEFAULT_FROM_NATIVE_SNMP` 参数从本地 SNMP 代理继承该值。如果使用 `CASE_SNMP_READ_COMMUNITY` 参数指定读团体，将会覆盖继承的值。

默认： `snmp_public`（仅在全新安装（不是升级）以及未指定读写团体的情况下有效）

CASE_SNMP_READ_ALLOWED_MANAGERS

指定所允许的 SNMP 管理器的以空格分隔的 IP 地址/主机名列表，以使用 CASE_SNMP_READ_COMMUNITY 查询代理。指定该项时，CASE_SNMP_READ_COMMUNITY 只能包含一个词，即 SNMP 团体。

CASE_SNMP_WRITE_COMMUNITY

指定可向代理发送 GET 和 SET 请求的 SNMP 写团体的名称。可以通过以分号进行分隔来指定多个团体（例如，rwcomm1;rwcomm2），也可以包含各团体的以空格分隔的 IP 地址列表以限制访问（例如，rwcomm1 1.2.3.4）。也可以使用 CASE_DEFAULT_FROM_NATIVE_SNMP 参数从本地 SNMP 代理继承该值。如果使用 CASE_SNMP_WRITE_COMMUNITY 参数指定写团体，将会覆盖继承的值。

CASE_SNMP_WRITE_ALLOWED_MANAGERS

指定所允许的 SNMP 管理器的以空格分隔的 IP 地址/主机名列表，以使用 CASE_SNMP_WRITE_COMMUNITY 查询代理。指定该项时，CASE_SNMP_WRITE_COMMUNITY 只能包含一个词，即 SNMP 团体。

CASE_SNMP_TRAP_COMMUNITY

指定 SNMP 陷阱团体和陷阱目标地址。可以通过以分号 (;) 进行分隔来指定多个陷阱团体设置。也可以使用 CASE_DEFAULT_FROM_NATIVE_SNMP 参数从本地 SNMP 代理继承该参数的值。如果使用 CASE_SNMP_TRAP_COMMUNITY 参数指定陷阱团体，将会覆盖继承的值。对于该参数，以下值是必需的：

- 团体名称
- 要将陷阱发送到的目标地址

对于该参数，以下值是可选的：

- 要将陷阱发送到的端口号
- 陷阱源编码选项
- 陷阱源主机名

陷阱团体设置的语法：

```
community-string {ip-address/hostname} [port [encoding [source]]]
```

示例：

```
public 1.2.3.4;public 2.3.4.5 1162;trapcom 3.4.5.6 1162 100 4.5.6.7
```

CASE_SNMP_TRAP_DESTINATION

指定要向其发送陷阱的主机名或 IP 地址。指定该项时，CASE_SNMP_TRAP_COMMUNITY 只能包含一个词（即 SNMP 团体），同时还必须指定 CASE_SNMP_TRAP_PORT。

CASE_SNMP_TRAP_PORT

指定要向其发送陷阱的目标端口号。指定该项时，CASE_SNMP_TRAP_COMMUNITY 只能包含一个词（即 SNMP 团体），同时还必须指定 CASE_SNMP_TRAP_DESTINATION。

CASE_DISABLE_NATIVE_SNMP

指定是否停止并禁用本地 SNMP 代理。

默认值：no

CASE_DEFAULT_FROM_NATIVE_SNMP

指定是否使用本地 SNMP 代理的默认 SNMP 设置。

默认值：no

CASE_MANAGER_HOSTNAME

指定要用从其管理该代理的配置管理器的主机名。为该参数输入值，可从指定的管理器配置该代理。输入星号 (*) 可接受第一个发现代理系统的管理器。该管理器将可以对代理的配置进行完全控制。默认情况下，未输入（使用）任何管理器主机，并且代理在未受管模式下运行。

CASE_MANAGER_POLICY_NAME

指定代理应使用的配置管理器策略文件的名称。为该参数输入值，可根据管理器中的现有配置文件设置 SystemEDGE 配置。默认情况下，代理使用已安装的策略文件。

CASE_START_AFTER_INSTALL

指定安装完成后是否自动启动代理。有效值包括：Yes、No 和 PRESERVE。如果安装开始时代理正在运行，此时要升级为仅启动代理，可以使用 PRESERVE。

默认值：PRESERVE

CASE_PRIVSEP_USER

指定用户名，在 SNMP 通信期间代理使用其凭据运行。

该条目会指示代理（仅限 UNIX）在其他用户帐户下运行 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。

CASE_INSTALL_DOCS

指定是否要随代理一起安装 SystemEDGE 文档。

默认值: yes

CASE_LEGACY_MODE

指定是否以传统模式安装代理，该模式仅在忽略便于与 CA Virtual Assurance 一起使用的所有材料时才会安装基本代理。如果不希望将代理与 CA Virtual Assurance 一起使用，则使用传统模式进行安装。

通过重新安装或升级并指定 CASE_LEGACY_MODE=no，可以使代理进入受管模式。

默认值: no

安装开始。如果不接受许可协议，安装将失败。

/opt/CA/installer/log/\$CA_SETUP_PACKAGE_NAME.log 中始终存在 lsm 安装程序日志文件，可以使用该文件检查安装是否成功。

如果要验证是否安装，请确认安装目录中是否有 SystemEDGE 文件。

\$CASYSEDGE 变量的传统支持

Linux/UNIX 上的安装程序不会在 /etc/profile 中修改系统环境设置。因此，\$CASYSEDGE 变量不再可用。

如果您的环境必须支持 \$CASYSEDGE，请执行以下选项之一：

- 在 shell 中创建 \$CASYSEDGE。

在 sh、ksh 或 bash shell 中运行以下命令：

```
./etc/profile.CA
```

如果您使用 csh，请运行以下命令：

```
source /etc/csh_login.CA
```

- 强制安装程序修改 /etc/profile 并创建 \$CASYSEDGE。

打开 shell 并输入以下命令：

```
Update_Profile=1;export Update_Profile  
sh ca-setup.sh
```

如果您使用 csh，请运行以下命令：

```
setenv Update_Profile 1  
sh ca-setup.sh
```

安装程序将安装 SystemEDGE 并在环境中创建 \$CASYSEDGE。

在升级到版本 5.7.1 期间，SystemEDGE 安装程序不会更改现有环境。先前创建的 \$CASYSEDGE 变量依然在环境中。

配置和使用响应文件

可以创建响应文件，以便在没有用户交互的情况下运行无提示安装。使用响应文件的效果与在命令行中指定 `CA_SETUP_MODE=UNATTENDED` 相同。响应文件会使安装进入无提示、无人照管模式。

安装程序使用响应文件中的属性，在不提示用户进行输入的情况下安装代理。

遵循这些步骤:

1. 以管理员或 `root` 用户身份登录到计算机系统。
2. 根据在“从命令行安装代理”部分中指定的参数创建响应文件。响应文件是包含如下所示参数设置的文本文件：

```
parameter1=value1  
parameter2=value2  
...
```

3. 导航到 `DVDdrive\Installers\OperatingSystem\Agent\SysMan\CA_SystemEDGE_Core` 目录，然后根据您的操作系统输入以下命令之一：

```
ca-setup CA_SETUP_RESPONSE_FILE="<响应文件的名称>" (Windows)
```

```
sh ca-setup.sh CA_SETUP_RESPONSE_FILE="<响应文件的名称>" (UNIX、Linux)
```

CA_SETUP_RESPONSE_FILE

指定响应文件的路径和名称。

安装将使用响应文件中的设置以无提示方式运行。

以传统模式安装代理

忽略便于与 CA Virtual Assurance 一起使用的以下组件时，可以在传统模式下安装 SystemEDGE 以获得所有基本代理功能。

- CAM，允许通过 CA Virtual Assurance 进行远程配置。
- IDPrimer，允许通过 CA Virtual Assurance 进行远程部署。

仅当您不打算使用 CA Virtual Assurance 或类似管理应用程序对 SystemEDGE 进行管理时，才以传统模式安装 SystemEDGE。如果以传统模式安装代理并且希望以后使用 CA Virtual Assurance 对其进行管理，您可以升级该代理。

注意：当您升级以前版本的 SystemEDGE 时，它会自动升级到完全代理，除非您另外指定其他代理。

遵循这些步骤:

1. 将 CA_SystemEDGE_Core 目录从安装介质复制到硬盘。
2. 转到 CA_SystemEDGE_Core 目录并使用 ASCII 编辑器打开 ca-setup.dat。
3. 编辑 ca-setup.dat，设置 CASE_LEGACY_MODE=yes。
4. 保存 ca-setup.dat。
5. 如[在 Windows 上安装代理](#) (p. 40)或[在 UNIX 上安装代理](#) (p. 50)中所述运行安装。
6. 完成安装。

要以传统模式从命令行安装代理，请在 ca-setup 命令中包括以下参数：

```
CASE_LEGACY_MODE="yes"
```

安装 AIM

在 SystemEDGE 上安装 AIM 时，请考虑以下指导原则：

- SRM AIM、RM AIM、MSCS AIM 或用于管理虚拟环境的 AIM 依赖于高级加密和 SystemEDGE。
- 高级加密依赖于 SystemEDGE。

根据这些依存关系，安装顺序如下所示：

1. SystemEDGE 核心
2. 高级加密
3. SRM AIM、RM AIM、MSCS AIM 或用于管理虚拟环境的 AIM

安装程序不允许采用其他任何顺序。例如，当尝试在安装高级加密之前安装 SRM 时，将显示错误消息，且安装不会开始。

使用 **ca-setup.exe** 在 Windows 上安装 AIM

1. 导航到包含以下子目录的 DVD1\Installers\Windows\Agent\SysMan 目录:

- CA_SystemEDGE_CXEN
- CA_SystemEDGE_GALAX
- CA_SystemEDGE_HACMP
- CA_SystemEDGE_HYPERV
- CA_SystemEDGE_KVM
- CA_SystemEDGE_LPAR
- CA_SystemEDGE_MSCS
- CA_SystemEDGE_RM
- CA_SystemEDGE_SOLZONES
- CA_SystemEDGE_SRM
- CA_SystemEDGE_UCS
- CA_SystemEDGE_VC
- CA_SystemEDGE_VCLOUD

2. 对于 SRM 或 RM AIM，转到相应目录并运行以下命令:

```
ca-setup
```

按照屏幕说明进行操作并完成安装。

3. 对于 Hyper-V、LPAR、MSCS、Zones、UCS、vCenter、HACMP、vCloud、CXEN 或 KVM AIM，请打开命令提示符，转到相应目录并运行以下命令:

```
ca-setup EULA_ACCEPTED="YES"
```

ca-setup 程序将以无提示方式完成安装。

注意：还可以使用 CA Virtual Assurance 管理器自定义安装在 Windows 服务器上安装 SystemEDGE 组件。

使用 **ca-setup.sh** 在 UNIX 上安装 AIM

1. 打开终端控制台，并转到包含以下子目录的 DVD2/Installers/Platform/Agent/SysMan 目录:

- CA_SystemEDGE_SRM

2. 转到相应目录并运行以下命令:

```
sh ca-setup.sh
```

按照屏幕说明进行操作并完成安装。

在 SRM 安装期间，您可以指定以下参数：

允许运行脚本

指定是否允许运行自定义脚本。这些脚本使用超级用户权限运行。

默认值： 否（典型安装）

允许文件 IO 测试

允许运行文件 IO 测试。由于这些测试使用超级用户权限运行，因此当启用此参数时，可以访问系统中的任何文件。

默认值： 否（典型安装）

允许不信任的 SSL 证书

允许 HTTPS 测试访问具有无效证书（不受信任的证书，或者网站与证书中的名称不匹配）的站点。

默认值： 否（典型安装）

杂项

安装 SRM 文档组件。

默认值： 是

安装 CA Systems Performance LiteAgent

可以在 Windows 和 UNIX 或 Linux 系统上安装 CA Systems Performance LiteAgent。

注意： CA Systems Performance LiteAgent 在 32 位和 64 位操作系统上运行。

在 Windows 系统上安装 CA Systems Performance LiteAgent

从 DVD1 运行自定义安装，以安装 CA Systems Performance LiteAgent。

在 AIX、HP-UX、Linux、Solaris SPARC 或 Solaris x86 系统上安装 CA Systems Performance LiteAgent

使用远程部署在 UNIX 或 Linux 上安装 CA Systems Performance LiteAgent。

注意： 有关远程部署的详细信息，请参阅《管理指南》。

第 3 章： 升级 CA Virtual Assurance

此部分包含以下主题：

[支持的升级](#) (p. 65)

[如何升级 CA Virtual Assurance](#) (p. 66)

[查看升级文档](#) (p. 67)

[准备要升级的环境](#) (p. 68)

[手动升级远程 Embedded Entitlements Manager](#) (p. 72)

[运行管理器安装](#) (p. 72)

[查看未自动升级的旧配置](#) (p. 73)

[手动应用旧配置](#) (p. 74)

[升级受管节点和 AIM 服务器](#) (p. 74)

[验证环境中的 CA Virtual Assurance 升级](#) (p. 78)

支持的升级

您可以将以下 CA Virtual Assurance 版本升级到 版本 12.7.1:

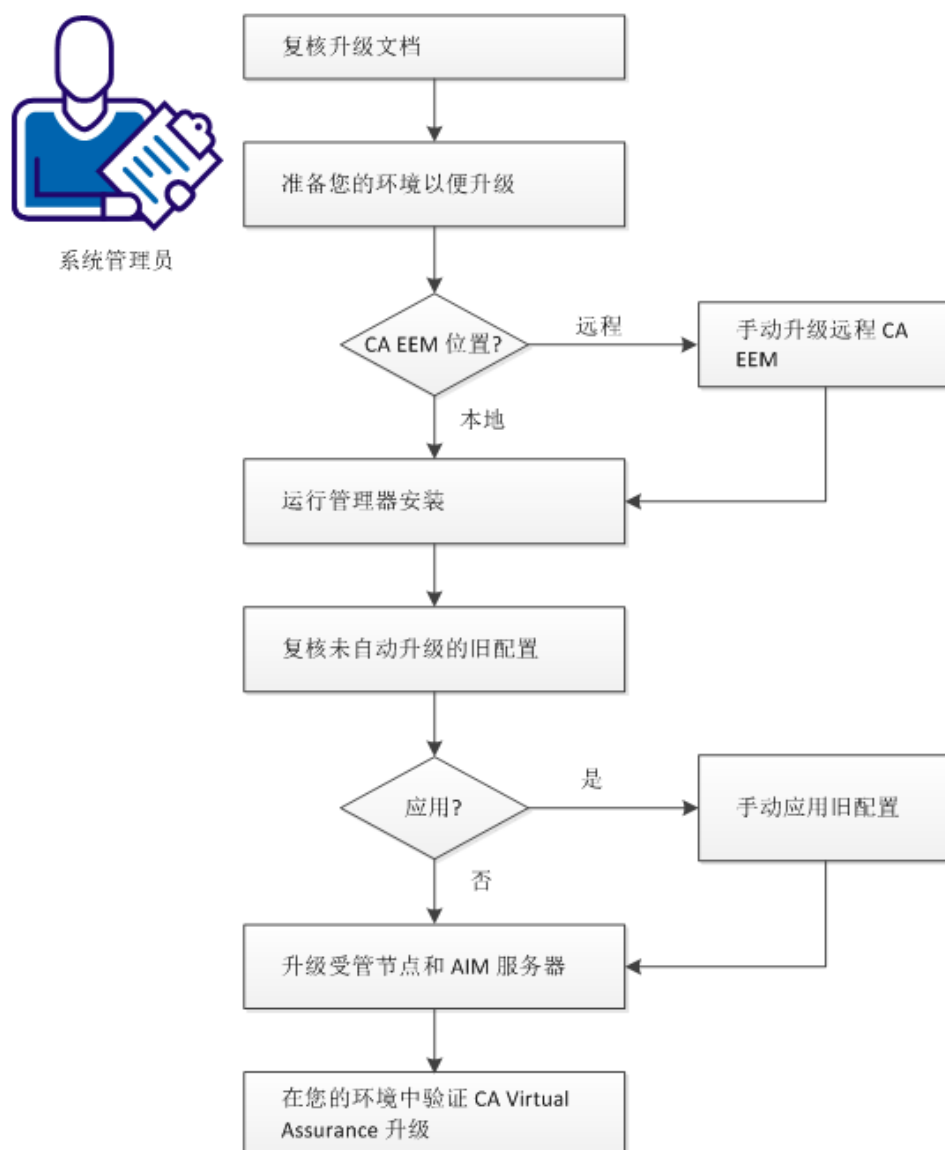
- CA Virtual Assurance 版本 12.5 和 12.6

注意：在升级之前，要获取重要修补程序，请参阅 CA 在线支持上的最新[版本说明](#)和[解决方案和修补程序](#)。

如何升级 CA Virtual Assurance

下图提供有关升级过程的概述。

如何升级 CA Virtual Assurance for Infrastructure Managers



请执行以下步骤：

[查看升级文档](#) (p. 67)

[准备要升级的环境](#) (p. 68)

[手动升级远程 Embedded Entitlements Manager](#) (p. 72)

[运行管理器安装](#) (p. 72)

[查看未自动升级的旧配置](#) (p. 73)

[手动应用旧配置](#) (p. 74)

[升级受管节点和 AIM 服务器](#) (p. 74)

[验证环境中的 CA Virtual Assurance 升级](#) (p. 78)

查看升级文档

开始升级 CA Virtual Assurance 过程之前，请先阅读本章中的升级信息。本章包含有关准备和执行升级所需的步骤的关键信息。

除本章之外，请验证《版本说明》中的硬件和软件要求并阅读本指南中的 [“准备自定义安装”](#) (p. 17)。

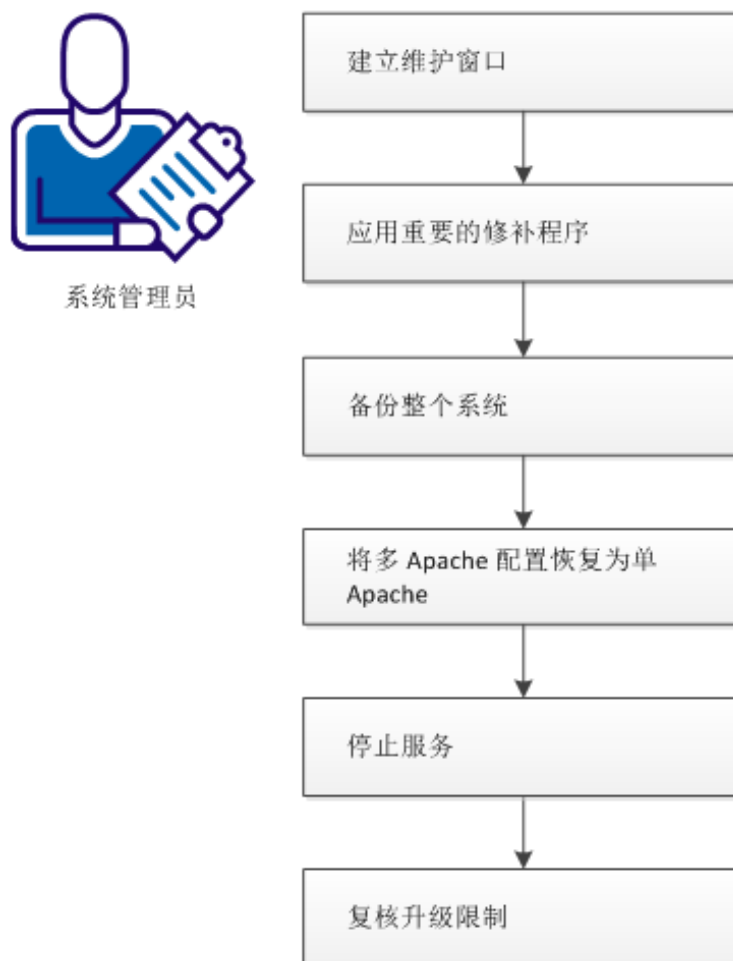
如果使用远程 Embedded Entitlements Manager 安装进行身份验证，请阅读 Embedded Entitlements Manager 文档中的升级说明。

如果使用远程部署来升级网络中的受管节点或 AIM 服务器，请参阅《管理指南》和联机帮助中的远程部署文档了解详细信息。

准备要升级的环境

本节介绍如何在开始升级过程之前准备环境。

如何准备您的环境以便升级



请执行以下步骤：

[建立维护窗口](#) (p. 69)

[应用重要修补程序](#) (p. 69)

[备份整个系统](#) (p. 92)

[将多 Apache 配置还原到单 Apache](#) (p. 70)

[停止服务](#) (p. 71)

[查看升级限制](#) (p. 71)

建立维护窗口

预先与受影响用户建立维护窗口。确认没有管理用户在建立该维护窗口期间尝试执行操作。

应用重要修补程序

要获取更新，请参阅 CA 在线支持上的最新[版本说明](#)和[解决方案和修补程序](#)。

如果已将 CA Virtual Assurance 版本 12.0.2 (SP2) 升级到版本 12.5，请在升级到版本 12.7.1 之前将以下修补程序应用到域服务器管理器 12.5：

- RO36999（VDEPIN—升级部署）

如果从版本 12.6 升级到版本 12.7.1，请将以下修补程序之一应用到 12.6：

- RO48212（LPARAIM - 32 位 - CUMULATIVE FIX 12162）
- RO48213（LPARAIM - 64 位 - CUMULATIVE FIX 12162）

备份整个系统

对管理器节点执行整个系统（完全）备份。管理器节点是包含以下组件的任何服务器：

- 域服务器
- 分发服务器
- 数据库
- EEM 服务器

使用行业标准工具（例如，适用于物理服务器的 ARCserve 或适用于虚拟机的快照）备份管理器节点。如果有多个管理器节点，请确认同时所有服务器上执行备份。

建议在没有用户活动时进行脱机备份。确认在开始备份之前已完成远程部署的所有活动作业。

注意：由于灾难恢复是针对整个系统的，因此请与在系统上安装有软件的其他产品所有者协商。

遵循这些步骤:

1. 依次导航到“资源”、“部署”窗格、“作业”，并确认所有作业都已 100% 完成。
2. 使用这些选项之一停止下列服务：
 - 命令行界面：

```
net stop CASMDmnSrvr
net stop CASMDstrbnSrvr
```
 - Windows 服务控制管理器：
 - CA SM 域服务器
 - CA SM 分发服务器
3. 执行以下操作之一：
 - 抓取整个管理器系统的快照。
 - 抓取整个管理器系统的 Ghost 映像。
4. 使用下列选项之一重新启动已停止的服务：
 - 命令行界面：

```
net start CASMDmnSrvr
net start CASMDstrbnSrvr
```
 - Windows 服务控制管理器。
 - CA SM 域服务器
 - CA SM 分发服务器

注意: 如果备份不是在管理器节点（包含域服务器）上执行的，请仅停止和启动分发服务。

将多 Apache 配置还原到单 Apache

如果已将安装配置为在多 Apache 配置中运行，则在执行就地升级之前更改为单 Apache 配置。在升级之后，您可以还原到多 Apache 配置。

[请与 CA Support 联系](#) (p. 3) 以获取有关如何还原配置的多 Apache 文档和说明。

停止服务

开始升级之前停止以下服务。

遵循这些步骤:

1. 注销 CA Virtual Assurance 用户界面。
2. 停止以下 Windows 服务:
 - CAAIPTomcat
 - CAAIPApache
 - CA Message Queuing Server (ActiveMQ)

查看升级限制

产品升级期间按如下方式对多个组件目录进行重命名:

`<product root>\component` 重命名为 `<product root>\component-old`

在升级完成之后, 将仍保留这些“旧”目录以供参考。如果在升级之前对这些目录树进行任何修改或添加, 则它们将包含在该“旧”目录中。这些修改不会自动与接管 `<product root>\component` 的新运行产品合并。如果要使这些修改对新产品生效, 请手动重新应用自定义设置。

以下列表提供了具有该限制的组件及其目录名称:

- Apache HTTP Server: `<product root>\apache`
- Apache ActiveMQ: `<product root>\activeMQ`
- Apache Tomcat: `<product root>\tomcat`, 包括 `\tomcat\UI`

注意: 虽然该限制适用于 Tomcat 本身, 但事实上, 在升级期间将自动转入 Tomcat 下的某些配置数据。

手动升级远程 Embedded Entitlements Manager

如果在 CA Virtual Assurance 管理器所在的同一服务器上运行 Embedded Entitlements Manager，您可以跳过本节。CA Virtual Assurance 升级过程将自动升级本地安装的 Embedded Entitlements Manager。

如果在单独服务器上运行 Embedded Entitlements Manager，请参阅支持的 Embedded Entitlements Manager 版本的《版本说明》。如果必须升级 Embedded Entitlements Manager，请执行以下过程：

遵循这些步骤：

1. 从 Windows “开始” 菜单中打开 Embedded Entitlements Manager 服务器上的 Embedded Entitlements Manager 文档总目录。
2. 阅读《入门指南》中的升级部分。
3. 将 CA Virtual Assurance 安装介质 (DVD1) 插入 DVD 驱动器。
4. 打开 Windows Explorer 并转到 \Installers\Windows\External\CAEEMServer 目录。
5. 启动 EEMServer_win32.exe 以升级 Embedded Entitlements Manager 并按照 Embedded Entitlements Manager 升级文档的说明操作。

运行管理器安装

将升级之前安装的所有组件。升级之前安装的组件是强制性的，且维护所有现有配置。您也可以选择要随升级一起安装的新组件。安装期间可以配置最新选定的组件。

在确定满足所有先决条件后，请执行该程序。如果您决定在安装期间跳过某个组件配置，请在安装后使用图形用户界面的“管理”选项卡配置该组件。

注意：有关组件配置的详细信息，请参阅《管理指南》。

遵循这些步骤：

1. 将安装介质插入 DVD 驱动器。

如果启用了自动运行，安装向导将自动启动。如果安装向导未启动，请双击 setup.hta，或在安装介质上导航到 DVDdrive:\Installers\Windows 目录并双击 install.exe。

此时将显示“检测到升级”对话框。
2. 单击“继续”。

将显示“简介”对话框。
3. 单击“下一步”。

此时会出现“许可协议”对话框。

4. 阅读协议并滚动到协议底部,直到“*我接受此许可协议的条款*”选项变为活动状态。选择该选项,然后单击“下一步”。

此时将显示“选择要安装的功能”对话框。将升级已安装的所有组件。

5. (可选) 选择要安装的其他组件,然后单击“下一步”。
6. 升级过程请求您为 **Embedded Entitlements Manager**、网络发现网关和任何其他组件提供凭据或其他附加信息。

安装向导最终会显示“安装摘要”对话框,其中列出要安装的组件。

7. 单击“安装”开始升级。

如果安装成功,安装程序将在以下目录中为每个安装的组件创建日志文件:

Install_Path\log\install

将出现“安装完成”对话框。

8. 在退出安装程序之前,请阅读对话框中提供的信息。
9. 导航到“开始”、“程序”、“CA”、“CA Virtual Assurance”、“启动 CA Virtual Assurance”,并登录用户界面。
10. 如果升级不成功,请参阅安装日志 (*Install_Path*\log\install\install.log) 和错误列表 (*Install_Path*\log\install\install_error_detected.log) 了解详细信息。

将出现“安装完成但有错误”对话框。请与 CA Support 联系以解决升级失败问题。

查看未自动升级的旧配置

您可以使用以下目录来验证是否需要先前版本中尚未转入的配置。

- Apache HTTP Server: <product root>\apache-old
- Apache ActiveMQ: <product root>\activeMQ-old
- Apache Tomcat: <product root>\tomcat-old, 包括 \tomcat\UI

注意: 升级期间将自动转入 Tomcat 下的某些配置数据。

手动应用旧配置

如果您具有要在升级的 CA Virtual Assurance 安装中使用但尚未转入的配置数据，请使用以下准则。

遵循这些步骤：

1. 请阅读 Apache、Tomcat 或 ActiveMQ 配置文档。
2. 注销 CA Virtual Assurance。
3. 更改相应的 Apache、Tomcat 或 ActiveMQ 配置文件。
4. 重新启动已更改其配置文件的服务。
5. 登录 CA Virtual Assurance。

升级受管节点和 AIM 服务器

建议的方法是远程部署升级受管节点和远程 AIM 服务器。远程部署允许您升级 SystemEDGE、高级加密和 AIM。

如果系统不支持 SystemEDGE 的受管模式，则您无法使用远程部署。我们建议使用以下选项之一：

- 从安装介质进行手动安装
- 例如，SystemEDGE、高级加密和使用 SSH 的 SRM AIM 的远程安装

请执行以下步骤：

[代理和 AIM 升级 \(p. 75\)](#)

[将 SystemEDGE 监视器导入策略 \(p. 77\)](#)

代理和 AIM 升级

您可以从 SystemEDGE 的任何可升级版本升级到 SystemEDGE 5.7.1 版：

- 4.3.4 及更高版本 (4.3.x)
- 5.1.0 及更高版本 (5.1.x)
- 5.6.0 及更高版本 (5.6.x)
- 5.7.0 及更高版本 (5.7.x)

安装程序会在原始安装路径的根文件夹中创建升级的目录，并将之前版本中的配置文件复制到其中。在代理首次启动时，它会将配置数据迁移到新建的数据目录。将 SystemEDGE 升级到版本 5.7.1 时，高级加密以及所有相应的 AIM 将升级到最新版本。

注意：SystemEDGE 5.7.1 版不会加载先前版本的 CA Virtual Assurance 的 AIM。

您可以通过以下方式之一升级 SystemEDGE：

- 通过 CA Virtual Assurance 远程部署到已安装可升级代理的系统。

注意：如果您想要升级 SystemEDGE、高级加密和 AIM，请使用单个远程部署作业进行升级。将 SystemEDGE、高级加密和所有必需的 AIM 添加到远程部署作业。SystemEDGE 仅加载级别为 5.7.1 的 AIM，或者类似 iddmod 的传统 AIM。也就是说，将隔离 5.7 或更低级别的 AIM。

有关远程部署的详细信息，请参阅《*管理指南*》中的“远程部署”一章。

- Windows 上的自定义管理器安装。该选项升级所有已安装的组件。选择要安装的任何其他代理和 AIM。
- 在已安装可升级代理的系统上的手动安装。

要执行升级，如[在 Windows 上安装代理](#) (p. 40)或[在 UNIX 上安装代理](#) (p. 50)中所述安装代理。

如果不支持升级较旧的代理版本，请执行以下操作：

- 对于 SystemEDGE 的早期版本，请先卸载代理，然后安装 SystemEDGE 版本 5.7.1。您可以在卸载之前保存所有配置数据，并将这些数据应用于 SystemEDGE 版本 5.7.1。

详细信息：

[从 SystemEDGE 4.3.4 升级代理](#) (p. 76)

从 SystemEDGE 4.3.4 升级代理

从以前的 4.3.4 版本升级配置文件时，安装程序将执行以下操作。

- 安装程序检测以下文件的以前版本并将其复制到 CASYSEDGE\upgraded 目录：
 - system32\sysedge.cf (Windows) 和 /etc/syedge.cf (UNIX)
 - CASYSEDGE\config\sysedgeV3.cf (Windows 和 UNIX)
 - system32\sysedge.mon (Windows) 和 /etc/sysedge.mon (UNIX)
 - system32\sysedge.lic (Windows) 和 /etc/sysedge.lic (UNIX)
 - CASYSEDGE\plugins\monwin\monwin.cf (Windows 和 UNIX)
- 当代理首次启动时，它会直接把以下文件复制到 CASYSEDGE_DATADIR 目录：
 - CASYSEDGE\config\sysedge.cf (Windows 和 UNIX)
 - CASYSEDGE\config\sysedgeV3.cf (Windows 和 UNIX)
- 作为 sysedge.cf 复制操作的一部分，代理会将升级目录中的 sysedge.cf、sysedge.mon 和 monwin.cf 文件中的配置数据迁移到数据目录中的新 sysedge.cf 文件。
- 作为 sysedgeV3.cf 复制操作的一部分，代理会将升级目录中的 sysedgeV3.cf 文件中的配置数据迁移到数据目录中的新 sysedgeV3.cf 文件。

注意：数据目录存储用于运行时配置更改的 sysedge.cf 文件的版本。

当从以前的版本升级时，代理会自动对配置文件设置进行以下更改：

- procAlive 进程监视器语法已更改，以遵循阈值进程监视器语法。代理会自动将任何现有的 procAlive 条目转换为新格式。

注意：有关 procAlive 条目的语法的更多信息，请参阅“进程和服务监控”一章。
- 禁用 no_process_sets 和 no_remoteshell_group 参数将允许对只有一个 SNMP 写团体的代理系统进行关键访问。因此，代理不迁移这些参数以前的设置并且总是启用它们。
- sysedge_memory 参数不再存在，在升级的 sysedge.cf 文件中已删除。现在通过在 sysedge.mon 文件中存储任何监视器的当前状态来处理显著的警报。现有条目被迁移到新警报处理配置中。
- Tc_publish 参数被重命名为 no_trapcommunity_table（具有反向逻辑）并在默认情况下启用。
- 当您使用远程部署从 SystemEDGE 版本 4.3.4 升级到 SystemEDGE 版本 5.7.1 时，迁移的监视器将存储在 sysedge.cf.bak 文件中。
- 根据您的部署策略，可以使用策略配置来在环境中应用迁移的监视器。

注意：有关详细信息，请参阅 CA Virtual Assurance 总目录。
- 当您在本地系统上从 SystemEDGE 版本 4.3.4 升级到 SystemEDGE 版本 5.7.1 时，安装程序会迁移监视器并在新配置中提供它们。

所有以前的语法均与新版本的代理兼容。但是，可提供许多用于增强代理功能的新选项。我们建议您检查较旧的监视器条目并编辑语法来包含附加选项。

注意：在从 4.3.4 版或更高版本 (4.3.x) 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。

将 SystemEDGE 监视器导入策略

在升级代理之前，请验证是否在“管理”选项卡下的“SNMP”中指定了 SystemEDGE 代理使用的 SNMP 团体字符串。也可以在“策略”、“计算机”、“度量标准”、“SNMP”下逐个计算机指定团体字符串。SystemEDGE 安装程序将 SystemEDGE 文件移至“upgraded”目录，代理将在升级后进行读取。将保留 OID。策略配置只能从现有的 sysedge.cf 文件中读取条目。不会导入 sysedge.mon 文件。

远程部署会将监视器的原始 OID 导入实例。

遵循这些步骤：

1. 验证代理的端口的“管理”选项卡下的“SNMP”中是否包括 SystemEDGE 代理团体字符串。
2. 将 SystemEDGE 升级到版本 5.7.1。
3. 验证是否已正确发现 SystemEDGE 5.7.1（“资源”选项卡）且其包含策略。
4. 单击“资源”选项卡，打开“配置”窗格，展开“策略”，然后单击“SystemEDGE”。

此时将显示“SystemEDGE”窗格。

5. 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。
6. 输入策略的名称，然后单击“导入...”。
此时将显示“SystemEDGE 代理计算机”对话框。
7. 选择已升级的服务器，然后单击“确定”。
将关闭“SystemEDGE 代理计算机”对话框。
8. 在“新建 SystemEDGE”对话框中，单击“确定”。
CA Virtual Assurance 将创建一个包含已导入的监视器的策略。

您可以编辑或更新监视器，并使用 SystemEDGE 版本 5.7.1 状态的模型。

验证环境中的 CA Virtual Assurance 升级

成功升级所有 CA Virtual Assurance 组件后，请验证 CA Virtual Assurance 总体上是否按预期工作。

第 4 章： 用户界面入门

本章简要介绍了 CA Virtual Assurance 图形用户界面、AutoShell 和总目录。在管理器上执行典型安装之后，Windows “开始” 菜单项 “CA”、“CA Virtual Assurance” 下将出现这些组件。

有关进一步的概念、详细信息和管理虚拟环境的具体任务，请参阅《*管理指南*》、《*联机帮助*》或《*参考指南*》。

此部分包含以下主题：

[启动 CA Virtual Assurance](#) (p. 79)

[启动 AutoShell](#) (p. 80)

[启动 CA Virtual Assurance 命令提示符](#) (p. 82)

[启动总目录和联机帮助](#) (p. 82)

启动 CA Virtual Assurance

在进行成功安装和安装后配置后，可以启动 CA Virtual Assurance。

遵循这些步骤：

1. 选择 “CA”、“CA Virtual Assurance”，并启动 CA Virtual Assurance。

将显示 CA Virtual Assurance 登录页。

注意：当您第一次启动 CA Virtual Assurance 用户界面时，浏览器将显示 SSL 证书警告。当浏览器连接到没有签名的 SSL 证书的安全站点时，将显示该警告。必须为特定服务器和证书颁发机构创建 SSL 证书，并且不能自动生成和安装该证书。当显示警告时，请单击 “确定” 以继续。

2. 输入您在安装期间定义的用户名和密码，然后单击 “登录”。

此时将显示产品 “显示板”。

只有在为 Web 浏览器安装 Flash 插件后，CA Virtual Assurance 才能显示图表。如果未安装 Flash 插件，将显示插件下载链接，而不是图表。默认情况下，“显示板” 会显示 “系统状态”、“使用率历史记录”、“服务”、“CA Virtual Assurance 状态” 和 “事件”。可以通过将模块从左侧窗格拖动到右侧窗格来配置显示板。

功能概述

CA Virtual Assurance 图形用户界面由左侧的导航窗格和右侧的数据窗格构成。使用窗格顶部的选项卡可在下列功能区之间切换：

显示板

提供虚拟环境和关联物理资源的当前状态的概括视图。可以将模块从导航窗格拖动到数据窗格来配置显示板。

资源

提供有关在环境中发现的资源的详细信息。有关某个被监控的资源的详细信息，请在导航树中单击该资源。要发现新资源，请从导航树中选择“数据中心”，然后打开“快速启动”选项卡。

您可以从“资源”选项卡使用以下功能：

- 配置监控和管理功能。
- 开通 VM 和 Solaris Zones。
- 远程部署 SystemEDGE 和 AIM。
- 创建并管理 SystemEDGE 和 AIM 配置。
- 管理操作以及可导致操作运行的规则。

报告

用于创建有关环境的特定方面或特征的报告。您可以从左侧窗格中选择预定义或自定义报告。

管理

用于配置 CA Virtual Assurance 组件、管理用户组或访问管理。

注意：有关详细信息，请参阅《*管理指南*》和*联机帮助*。

启动 AutoShell

AutoShell 是可自动完成复杂的周期性任务和管理任务的命令行和脚本环境。它是脚本语言 (JavaScript) 和命令行外壳的组合。它允许您直接在 AutoShell 中将 JavaScript 语法用于 AutoShell 命令、函数和类，或运行 .js 文件中的脚本。

注意：有关 AutoShell 的详细信息，请参阅《*参考指南*》。

遵循这些步骤：

1. 打开 Windows 资源管理器并导航到以下目录：
C:\Program Files\CA\SC\AutoShellManager
2. 双击 caaipaomautoshell.exe。

此时将显示 AutoShell 登录对话框。

3. 输入您在安装期间定义的用户名和密码。

此时将显示 AutoShell 命令提示符。

```
CA AutoShell v1.5.0.1
基于 Mozilla SpiderMonkey 1.7
用户名: ca
密码: *****
VASU::->
```

4. 输入适当的 AutoShell 表达式或命令。
5. 输入 **exit** 以退出 AutoShell。

示例

显示 “Hello World!”:

```
? "Hello World!"
Hello World
```

显示数字 1 到 10:

```
for(i=1;i<11;i++)qout(i);
1
2
3
4
5
6
7
8
9
10
```

显示当前的日期和时间:

```
? "Today is", new Date
Today is Tue Jun 02 2009 14:17:05 GMT-0400 (Eastern Daylight Time)
```

详细信息

[有效 AutoShell 用户](#) (p. 82)

有效 AutoShell 用户

在 CA Virtual Assurance 安装期间，您在安装向导的“本地安全性用户信息”屏幕中定义 CA Embedded Entitlements Manager (Embedded Entitlements Manager) 用户身份和密码。凭据存储在 Embedded Entitlements Manager 数据库中。用户被分配给 CA Virtual Assurance 管理员组，并且可用于登录到 CA Virtual Assurance 用户界面和 AutoShell 管理器。

如果使用 Embedded Entitlements Manager 的 CA Virtual Assurance 组件安装在本地或远程系统上，AutoShell 管理器将始终对比 Embedded Entitlements Manager 数据验证登录凭据。否则，AutoShell 管理器对比 Windows 身份验证验证登录凭据。

启动 CA Virtual Assurance 命令提示符

如果要使用《参考指南》中介绍的 CLI 命令，请启动 CA Virtual Assurance 命令提示符。

遵循这些步骤：

1. 选择“CA”、“CA Virtual Assurance”、“CA Virtual Assurance 命令提示符”。
此时将显示“CA Virtual Assurance 命令提示符”对话框，并打开 `Install_Path\productname\bin` 目录。
2. 输入 CLI 命令。

启动总目录和联机帮助

总目录包含整个 CA Virtual Assurance 文档集。所有指南均以 HTML 和 PDF 格式提供；联机帮助和自述文件仅以 HTML 格式提供。总目录支持跨所有交付文档进行全文搜索。联机帮助系统用户界面中的高级选项卡与上下文相关。

启动联机帮助

1. 打开 CA Virtual Assurance 用户界面，然后单击窗口右上角的“帮助”。
此时将显示与选项卡相关的主题。
2. 如有必要，请使用包含“目录”、“索引”或“搜索”的导航窗格。

从联机帮助中打开总目录

1. 打开 CA Virtual Assurance 用户界面，然后单击窗口右上角的“帮助”。
此时将显示与选项卡相关的主题。
2. 切换到导航窗格中的“目录”。
3. 向上滚动到顶部，然后单击“返回到总目录”。
此时将显示总目录。

从“开始”菜单启动总目录

1. 从 Windows “开始”菜单中选择“CA”、“CA Virtual Assurance”、“总目录”。

此时将显示“总目录”窗口。

2. 执行以下操作之一：
 - 单击“总目录”窗口中的相应链接可打开文档或联机帮助系统。
 - 在“总目录”窗口右上角的字段中键入一个词，并单击“搜索”，可跨所有交付文档执行全文搜索。

第 5 章： 卸载 CA Virtual Assurance

此部分包含以下主题：

[卸载选项](#) (p. 85)

[卸载管理器](#) (p. 85)

[卸载 SystemEDGE](#) (p. 87)

卸载选项

CA Virtual Assurance 提供了以下卸载选项：

- 完全卸载
- 卸载特定功能（仅管理器）
- 以无提示模式卸载

卸载管理器

“完全卸载”选项会删除 CA Virtual Assurance 的所有组件和功能，并提供一个用于删除以下嵌入式组件的选项：

- Embedded Entitlements Manager
- Apache
- Tomcat
- 管理数据库
- 性能数据库

卸载向导允许您仅删除最初在 CA Virtual Assurance 安装过程中安装的嵌入式组件。卸载本产品将不会删除在安装本产品之前存在于系统上的共享组件。

注意：即使您未选择卸载 Apache 和 Tomcat 应用程序，卸载过程也可能会停止这些服务。

详细信息

[执行完全卸载](#) (p. 86)

[从命令提示符卸载管理器](#) (p. 86)

[以无提示模式卸载管理器](#) (p. 87)

执行完全卸载

如果要删除所有 CA Virtual Assurance 功能和组件，请使用“完全卸载”选项。该选项还允许您选择是保留还是删除嵌入式组件。

遵循这些步骤：

1. 从 Windows “开始” 菜单中单击“开始”、“设置”、“控制面板”、“添加或删除程序”。

此时将显示“添加或删除程序”窗口。

2. 选择“CA Virtual Assurance”，然后单击“更改/删除”。

此时将显示“卸载 CA Virtual Assurance”对话框。

3. 单击“下一步”。

此时将显示“卸载选项”对话框。

4. 选择是否要保留管理数据库，然后单击“下一步”。

卸载将开始。将从系统中删除 CA Virtual Assurance 和所有选定组件。

注意：如果嵌入式组件不是在 CA Virtual Assurance 安装期间安装的，则不卸载该组件。

从命令提示符卸载管理器

使用此步骤从 Windows 命令提示符卸载 CA Virtual Assurance。

遵循这些步骤：

注意：该程序中命令语法中的引号是必需的，因为命令名称包含空格。

1. 以管理员身份登录并打开命令提示符。

将显示命令提示符窗口。

2. 转到 `install_path\productname\Uninstall` 目录，并输入以下命令：

`Uninstall.exe`

卸载将开始。

3. 选择以下选项之一，并按照屏幕说明完成卸载：

- 完全卸载
- 卸载选定功能

详细信息

[以无提示模式卸载管理器](#) (p. 87)

以无提示模式卸载管理器

使用该程序可从 Windows 服务器中以无提示方式移除管理器。

遵循这些步骤:

1. 以管理员身份登录并打开命令提示符。
将显示命令提示符窗口。
2. 转到 `install_path\productname\Uninstall` 目录，并输入以下命令以卸载管理器：

```
Uninstall.exe -i silent
```

卸载将开始。CA Virtual Assurance 将从系统中移除。

详细信息

[从命令提示符卸载管理器](#) (p. 86)

卸载 SystemEDGE

本节介绍如何删除与 SystemEDGE 代理相关联的文件和子目录。

在 Windows 上卸载 SystemEDGE 和 AIM

卸载程序可从系统中删除 SystemEDGE。您可以指定是否从数据目录中删除配置数据。您可以从 Windows 的“添加或删除程序”窗口或从命令行卸载代理和 AIM。

卸载时请考虑以下依存关系：

- 虚拟环境的 AIM，RM AIM 和 SRM AIM 依存于高级加密和 SystemEDGE。
- 高级加密依赖于 SystemEDGE。

基于这些依存关系，卸载顺序如下所示：

1. RM AIM、SRM AIM 或虚拟环境的 AIM
2. 高级加密
3. SystemEDGE 核心

如果使用任何其它顺序，则无法完成该卸载。删除最初通过远程部署安装的组件时，不会卸载 Idprimer 和 CAM。

从 Windows 的“添加或删除程序”窗口卸载 SystemEDGE 或 AIM

1. 选择“开始”、“设置”、“控制面板”、“添加或删除程序”。
显示“添加或删除程序”窗口并列以下组件：
 - 虚拟环境的 AIM
 - CA SystemEDGE Core
 - CA SystemEDGE AdvancedEncryption
 - CA SystemEDGE RM
 - CA SystemEDGE SRM
2. 根据卸载顺序，右键单击相应的组件并选择“卸载”。
卸载 SystemEDGE 时，会显示一个对话框，提示您指定是否保留配置文件。
3. 单击“是”或“否”。
对话框中会显示此卸载过程。卸载完成时，对话框将关闭。

从命令行卸载 SystemEDGE 或 AIM

1. 打开命令提示符并转到 DVD1\Installers\Windows\Agent\SysMan 目录。此目录包含以下子目录：
 - CA_SystemEDGE_SRM
 - CA_SystemEDGE_RM
 - CA_SystemEDGE_AdvancedEncryption
 - CA_SystemEDGE_Core
2. 运行下列命令：

```
ca-setup -x
```


卸载 SystemEDGE 时，会显示一个对话框，提示您指定是否保留配置文件。
3. 单击“是”或“否”。
对话框中会显示此卸载过程。卸载完成时，对话框将关闭。

无提示卸载 SystemEDGE 或 AIM

- 请执行以下步骤来卸载 SystemEDGE：
 - a. 打开“命令提示符”窗口，并转到以下目录路径：

```
DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_Core
```
 - b. 运行下列命令：

```
ca-setup.exe CA_SETUP_MODE=UNINSTALL CASE_KEEP_DATA=[YES|NO]
```


SystemEDGE 已从计算机上卸载。
- 注意：**要进行验证，请转到“控制面板”，并查看是否已从控制面板项中删除了 SystemEDGE。

- 请执行以下步骤来删除 AIM：
 - a. 打开“命令提示符”窗口，并转到相应的 AIM 目录路径：

`DVD1\Installers\Windows\Agent\SysMan\AIM`

- b. 运行下列命令：

`ca-setup.exe CA_SETUP_MODE=UNINSTALL`

AIM 已从计算机上卸载。

注意：导航到“程序文件”、“CA”、“SystemEDGE”、“插件”，并验证是否已删除 AIM 文件夹。

在 UNIX 系统上卸载 SystemEDGE 和 AIM

卸载程序可从系统中删除 SystemEDGE 或 AIM。您可以为 SystemEDGE 指定是否从数据目录中删除配置数据。

卸载时请考虑以下依存关系：

- SRM AIM 依存于高级加密和 SystemEDGE。
- 高级加密依赖于 SystemEDGE。

基于这些依存关系，卸载顺序如下所示：

1. SRM AIM
2. 高级加密
3. SystemEDGE 核心

如果使用任何其它顺序，则无法完成该卸载。删除最初通过远程部署安装的组件时，不会卸载 Idprimer 和 CAM。

使用 `ca-setup.sh` 卸载代理或 AIM

1. 打开终端控制台并以 root (su) 登录。
2. 转到 `DVD2/Installers/<Platform>/Agent/SysMan` 目录。此目录包含以下子目录：

- `CA_SystemEDGE_SRM`
- `CA_SystemEDGE_AdvancedEncryption`
- `CA_SystemEDGE_Core`

- 3. 转到相应目录并运行以下命令：

`sh ca-setup.sh -x`

此时会显示一个对话框，提示您指定是否保留配置文件。

- 4. 单击“是”或“否”。

对话框中会显示此卸载过程。卸载完成时，对话框将关闭。

使用 lsm 卸载代理或 AIM

1. 打开终端控制台并以 root (su) 登录。
2. 运行以下列表中相应的命令：

```
lsm -e CA_SystemEDGE_SRM  
lsm -e CA_SystemEDGE_AdvancedEncryption  
lsm -e CA_SystemEDGE_Core
```

卸载 SystemEDGE 时，系统会提示您指定是否保留配置文件。

3. 单击“是”或“否”。
- 卸载完成。

无提示卸载代理或 AIM

- 请执行以下步骤来卸载代理：

- a. 打开终端控制台并以 root (su) 登录。转到以下目录路径：

DVD2/Installers/Platform/Agent/SysMan/CA_SystemEDGE_Core

- b. 运行下列命令：

```
sh ca-setup.sh CA_SETUP_MODE=UNATTENDED_UNINSTALL  
CASE_KEEP_DATA=[YES|NO]
```

代理已从计算机上卸载。

- 请执行以下步骤来卸载 AIM：

- a. 打开终端控制台并以 root (su) 登录。转到相应的 AIM 目录路径：

DVD2/Installers/Platform/Agent/SysMan/AIM

- b. 运行下列命令：

```
sh ca-setup.sh CA_SETUP_MODE=UNATTENDED_UNINSTALL
```

AIM 已从计算机上卸载。

第 6 章： 备份与还原

此部分包含以下主题：

[备份与还原概述](#) (p. 91)

[备份整个系统](#) (p. 92)

[备份配置和数据](#) (p. 93)

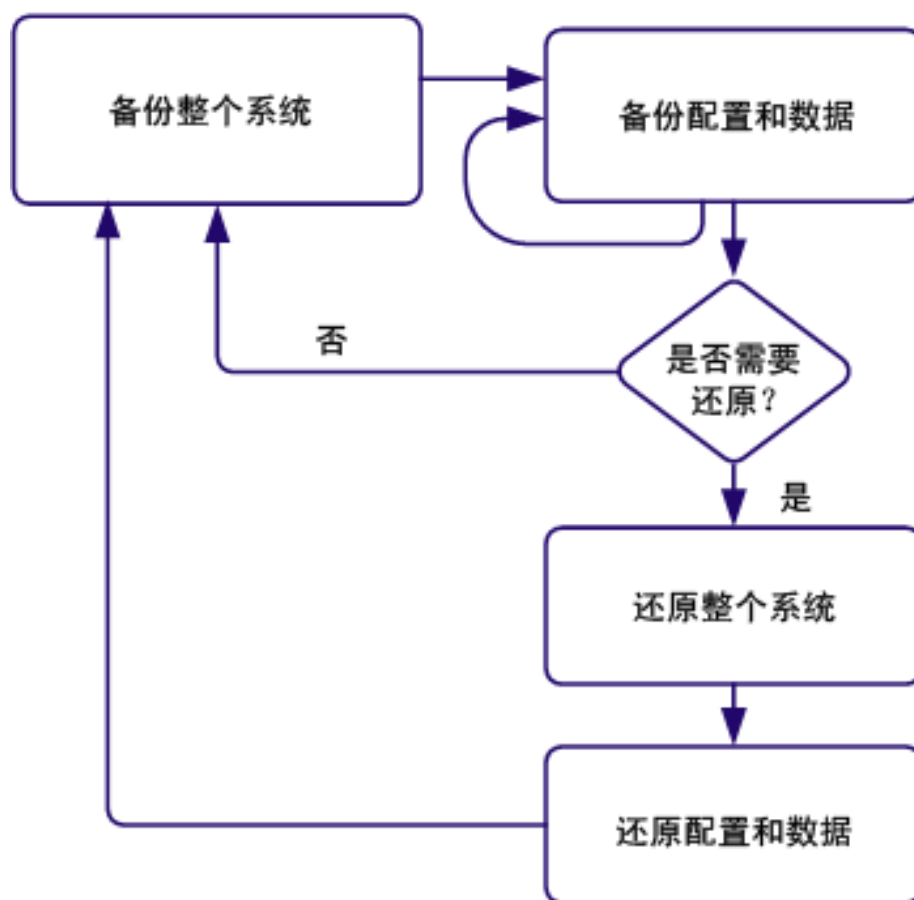
[还原整个系统](#) (p. 97)

[还原配置和数据](#) (p. 97)

备份与还原概述

以下部分提供有关备份的两种模式及其相应的还原过程的信息。该图说明还原您的环境所需的程序。

备份与还原过程



要备份并恢复系统，请执行下列操作：

1. 根据需要[备份整个系统](#) (p. 92)。
2. [备份配置和数据。](#) (p. 93)
3. 如果想还原系统：
 - a. [还原整个系统。](#) (p. 97)
 - b. [还原配置和数据。](#) (p. 97)

备份整个系统

对于管理器节点，我们建议每周至少执行一次整个系统（完全）备份以进行灾难恢复。管理器节点是包含以下组件的任何服务器：

- 域服务器
- 分发服务器
- 数据库
- EEM 服务器

使用行业标准工具（例如，适用于物理服务器的 ARCserve 或适用于虚拟机的快照）备份管理器节点。如果有多个管理器节点，请确认同时也在所有服务器上执行备份。

建议在没有用户活动时进行脱机备份。确认在开始备份之前已完成远程部署的所有活动作业。

注意：由于灾难恢复是针对整个系统的，因此请与在系统上安装有软件的其他产品所有者协商。

遵循这些步骤：

1. 依次导航到“资源”、“部署”窗格、“作业”，并确认所有作业都已 100% 完成。
2. 使用这些选项之一停止下列服务：
 - 命令行界面：

```
net stop CASMDmnSrvr
net stop CASMDstrbnSrvr
```
 - Windows 服务控制管理器：
 - CA SM 域服务器
 - CA SM 分发服务器
3. 执行以下操作之一：
 - 抓取整个管理器系统的快照。
 - 抓取整个管理器系统的 Ghost 映像。

4. 使用下列选项之一重新启动已停止的服务：
- 命令行界面：
net start CASMDmnSrvr
net start CASMDstrbnSrvr
 - Windows 服务控制管理器。
 - CA SM 域服务器
 - CA SM 分发服务器

注意：如果备份不是在管理器节点（包含域服务器）上执行的，请仅停止和启动分发服务。

备份配置和数据

本部分针对数据库、关键配置文件和其他数据的增量备份提供建议。建议每天在非高峰使用时期或系统脱机时至少执行一次差异备份。

本部分介绍以下程序：

- [备份数据库](#) (p. 93)
- [备份目录和数据](#) (p. 94)

备份数据库

使用 SQL Management Studio 可以备份管理和性能数据库。

遵循这些步骤：

1. 启动 SQL Server Management Studio。
2. 展开 AOM2 和 DPM 数据库所在的已注册 SQL Server。
3. 展开“数据库”。
4. 右键单击相应的数据库，然后依次单击“任务”、“备份”。
5. 确认将备份类型设置为“完全”并确定要备份到的路径。
6. 单击“确定”。

下表提供了针对性能和管理数据库的建议：

数据库	描述	建议
AOM2	管理数据库	增量备份

数据库	描述	建议
DPM	性能数据库	性能数据库包含代理收集的性能度量标准。除非从历史的角度来看，认为该数据是至关重要的，否则建议不要备份该数据库。

备份目录和数据

建议每天或根据公司备份策略备份远程部署和配置数据。

下表提供了关键目录、其位置和相应缩写的列表。

目录	查找目录	缩写
产品安装目录* (对 32 位系统有效)	REG QUERY "HKEY_LOCAL_MACHINE\ SOFTWARE\ComputerAsso ciates\DynamicProvisionin gManager" /v InstallDirectory	<INSTALLDIR>
产品安装目录* (对 64 位系统有效)	REG QUERY "HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\ComputerAssociates\Dy namicProvisioningManage r" /v InstallDirectory	<INSTALLDIR>
部署和配置个人数据 目录	Findstr /i "CAISM_PRIVATE_DATA" "<INSTALLDIR>\bin\smglo bals.ini"	<PRIVATEDATADIR>
部署和配置公共数据 目录	Findstr /i "CAISM_PUBLIC_DATA" "<InstallDir>\bin\smglo bals.ini"	<PUBLICDATADIR>
IDManager 安装目录 * (对 32 位系统有效)	REG QUERY "HKEY_LOCAL_MACHINE\ SOFTWARE\ComputerAsso ciates\InfrastructureDeplo yment" /v MgrApiPath	<IDDIR>

目录	查找目录	缩写
IDManager 安装目录 * (对 64 位系统有效)	REG QUERY "HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\ComputerAssociates\Inf rastructureDeployment"/v MgrApiPath	<IDDIR>

(*) 注意：在 64 位系统上使用 32 位命令提示符。

下表中汇总了备份建议：

说明	目录	建议
安装程序配置文件	<INSTALLDIR>\bin\ smglobals.ini	该文件定义 <CAVPM> 目录设置。建议用于增量备份集。
域服务器数据	<PRIVATEDATADIR>\ domainserver	增量备份需要目录及其子目录，但不包括以下目录中的部署软件包 <PRIVATEDATADIR>\domainserver\Deployment\Packages\SM
部署软件包	<PRIVATEDATADIR>\ domainserver\ Deployment\ Packages\SM	不需要进行备份。可以从安装介质获得。
分发服务器数据	<PRIVATEDATADIR>\ distributionserver\	如果域服务器和分发服务停止时备份已完成，则不需要进行备份。
分发服务器上的 IDManager 配置	<IDDIR>\config\SM	对于增量备份为必需。 如果无法在远程分发服务器上备份此信息，且分发服务器已重新安装，请在使用此分发服务器执行下一个部署期间重新输入凭据。
Web 服务数据	<PRIVATEDATADIR>\ caismweb service	不需要进行备份。将从域服务器进行传播。

说明	目录	建议
CA Virtual Assurance 日志文件	<PUBLICDATADIR>\log	如果需要进行参考，请备份。
ID 日志文件	<IDDIR>\logs	如果需要进行参考，请备份。

遵循这些步骤：

1. 验证所有活动远程部署作业是否均已完成。
2. 使用这些选项之一停止下列服务：
 - 命令行界面：


```
net stop CASMDmnSrvr
net stop CASMDstrbnSrvr
```
 - Windows 服务控制管理器：
 - CA SM 域服务器
 - CA SM 分发服务器
3. 备份建议的目录。
4. 使用下列选项之一重新启动已停止的服务：
 - 命令行界面：


```
net start CASMDmnSrvr
net start CASMDstrbnSrvr
```
 - Windows 服务控制管理器。
 - CA SM 域服务器
 - CA SM 分发服务器

还原整个系统

遵循这些步骤:

1. 使用这些选项之一停止下列服务:

- 命令行界面:
`net stop CASMDmnSrvr`
`net stop CASMDstrbnSrvr`
- Windows 服务控制管理器:
 - CA SM 域服务器
 - CA SM 分发服务器

2. 在进行备份的相同计算机上使用相同的备份工具执行还原。

重要信息! 如果已经还原了多个管理器节点, 请将所有系统还原到同一备份级别以避免数据不一致。还原管理器节点, 域服务器最后进行还原。

3. 使用下列选项之一重新启动已停止的服务:

- 命令行界面:
`net start CASMDmnSrvr`
`net start CASMDstrbnSrvr`
- Windows 服务控制管理器。
 - CA SM 域服务器
 - CA SM 分发服务器

注意: 如果备份不是在管理器节点 (包含域服务器) 上执行的, 请仅停止和启动分发服务。

详细信息

[还原配置和数据](#) (p. 97)

还原配置和数据

执行整个系统的还原后, 还原差异备份数据。

本部分介绍以下程序:

- [还原数据库](#) (p. 98)
- [还原目录和数据](#) (p. 99)

详细信息

[还原整个系统](#) (p. 97)

还原数据库

当还原数据库时，请使用 SQL Management Studio。

遵循这些步骤：

1. 关闭服务：CAAIPApache、CAAIPTomcat、CA SM Distribution Server、CA SM Domain Server
2. 启动 SQL Server Management Studio。
3. 展开数据库所在的已注册 SQL Server。
4. 展开“数据库”。
5. 右键单击相应的数据库，然后依次单击“任务”、“还原数据库”。
6. 选择数据库。
7. 确定从其进行还原的设备路径。
8. 单击“确定”。
9. 重新启动服务：CAAIPApache、CAAIPTomcat、CA SM Distribution Server、CA SM Domain Server

还原目录和数据

将来自同一备份介质的配置和数据文件还原到进行备份的相同计算机上。

遵循这些步骤:

1. 转到“资源”、“部署”、“作业”，确认不存在任何正在进行的活动部署作业。
2. 使用这些选项之一停止下列服务：
 - 命令行界面：

```
net stop CASMDmnSrvr
net stop CASMDstrbnSrvr
```
 - Windows 服务控制管理器：
 - CA SM 域服务器
 - CA SM 分发服务器
3. 还原来自同一备份介质的配置和数据文件。

注意：还原操作使信息回到与上次备份时相同的状态。上次备份之后进行的所有更改都将丢失。
4. 如果备份多个管理器节点，请继续还原其他管理器节点。
5. 使用下列选项之一重新启动已停止的服务：
 - 命令行界面：

```
net start CASMDmnSrvr
net start CASMDstrbnSrvr
```
 - Windows 服务控制管理器。
 - CA SM 域服务器
 - CA SM 分发服务器

注意：如果备份不是在管理器节点（包含域服务器）上执行的，请仅停止和启动分发服务。

第 7 章：可扩展性最佳实践

此部分包含以下主题：

[扩展性概述](#) (p. 101)
[硬件规格](#) (p. 102)
[数据库注意事项](#) (p. 102)
[网络注意事项](#) (p. 102)
[远程部署和策略配置概述](#) (p. 103)
[可扩展性建议](#) (p. 105)

扩展性概述

本部分提供用于部署 CA Virtual Assurance 的最佳实践和建议。本文档的目的在于帮助计划在生产环境中大量使用 CA Virtual Assurance，专注于以下方面：

- VMware 环境的监控和 CA Virtual Assurance 管理
- IBM LPAR 环境的监控
- Oracle Solaris Zones 环境的监控
- SystemEDGE 和其他监控软件的部署
- SystemEDGE 的初始配置和正在进行的配置

包括以下部分：

1. [远程部署和策略配置概述](#) (p. 103)
2. [硬件规格](#) (p. 102)
3. [数据库注意事项](#) (p. 102)
4. [网络注意事项](#) (p. 102)
5. [可扩展性建议和限制](#) (p. 105)
6. [可扩展性用例](#) (p. 111)

硬件规格

本部分列出了大规模实施 CA Virtual Assurance 的最低硬件规格。对于更大规模的实施，请考虑增加管理服务器的规格。

- 域服务器：2.6-GHz 双核处理器，4-GB RAM，100-GB 磁盘。
- 分发服务器：1-GHz 单核/处理器/虚拟处理器，2-GB RAM，100-GB 磁盘，100-Mb/秒以太网。
- VC AIM 监控服务器：双核处理器：2.6-GHz CPU，4-GB RAM，100-GB 磁盘。
- LPAR AIM 监控服务器：双核处理器：2.6-GHz CPU，4-GB RAM，100-GB 磁盘。
- Solaris Zones AIM 监控服务器：双核处理器：2.6-GHz CPU，4-GB RAM，100-GB 磁盘。
- 目标系统：1-GHz 单核/处理器/虚拟处理器，512-MB RAM，2-GB 磁盘，单路 100-Mb/秒以太网。

注意：50% 是 CPU 和内存所允许的最大使用率。

数据库注意事项

随着受管环境变得越大，预期的数据库活动就越多。产品数据库的大小会随着产品的使用而增长，可能会占用 30 GB 或更多空间，具体取决于正在执行的维护。我们建议针对数据保留采用以下一般规则：对于受监控环境中的每 1000 台计算机，轮询间隔增加 300 秒。

注意：为数据库使用专用的独立系统可以改进其性能。使数据库接近于网络上（例如，在同一子网上）其他 CA Virtual Assurance 组件以改进响应时间。

网络注意事项

计划批量安装 CA Virtual Assurance 时，请考虑网络连接的质量以决定在何处定位管理组件。以下各项影响解决方案的可扩展性和有效性：

- 网路质量：质量差导致数据丢失，响应迟缓或失败。
- 网络带宽：低带宽会限制在组件之间发送数据的速率。
- 网络延迟：较高的延迟会限制数据传输的速率（其方式与低带宽类似）。
- DNS：配置错误的 DNS 会阻止部署和持续配置监控代理。

我们建议在管理组件之间至少使用 100 Mb/秒的网络链路，尤其是在使用远程数据库时。如果网络速度低于 100 Mb/秒，请考虑引入与目标系统并置的其他分发服务器。

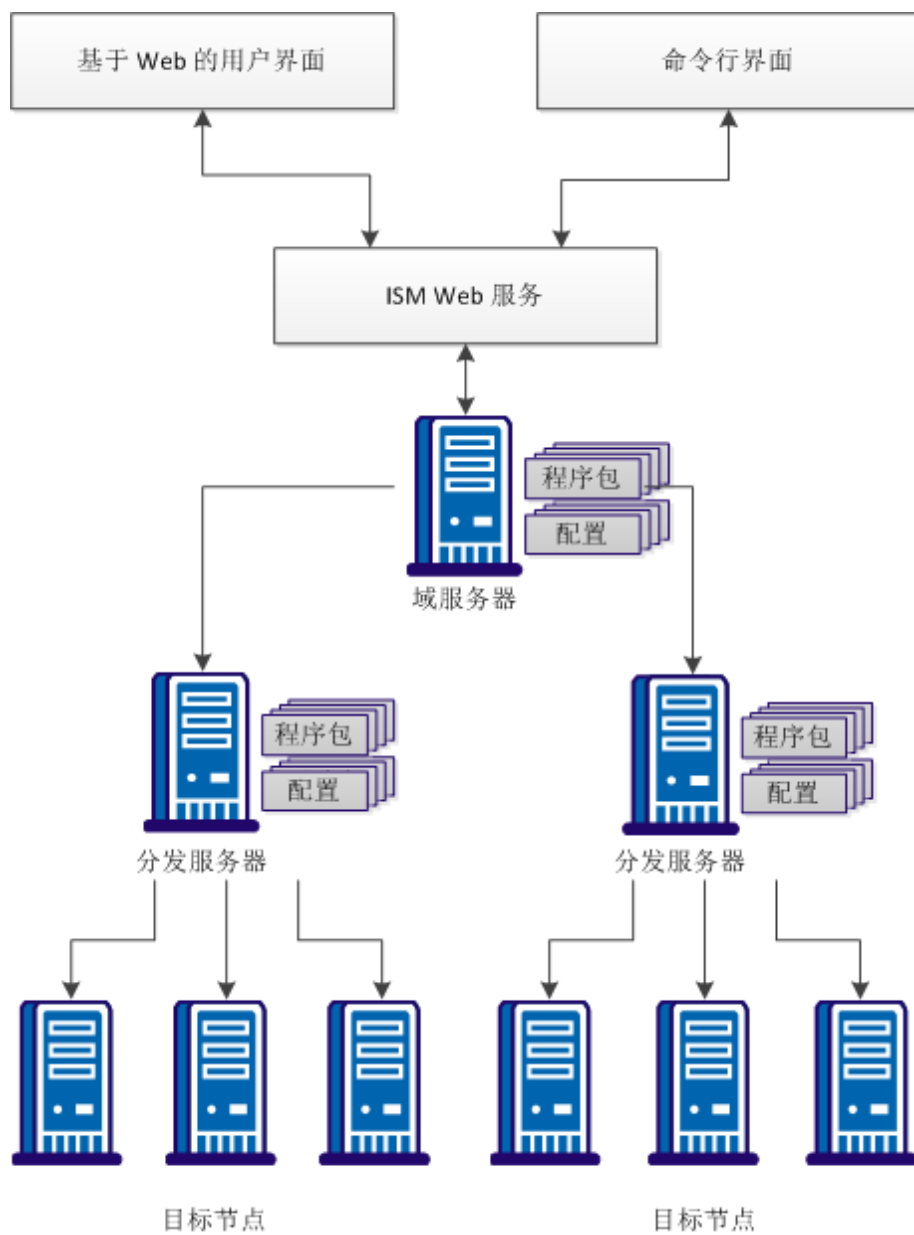
远程部署和策略配置概述

CA Virtual Assurance 提供了全面的解决方案，用于将 SystemEDGE 代理远程部署到所有受管系统。您可以基于包含自定义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多个受管系统。

此外，CA Virtual Assurance 还针对所有受管系统上运行的 SystemEDGE 代理的持续配置提供了全面的解决方案。策略配置允许创建策略库。这些策略应用于一个或多个运行 SystemEDGE 和 SRM AIM 的系统。安装了由策略配置管理的代理后，将自动请求策略。因此，该代理将运行一组受控且一致的策略。然后可以基于代理正在运行的策略或代理所属的服务分别更新每个代理。

远程部署和策略配置共享域服务器和分发服务器技术。该技术提供了一个既可扩展又能够在多个数据中心中进行分发的解决方案。

该图说明了远程部署和策略配置组件的基本体系结构。



可扩展性建议

本部分提供有关可扩展性建议和限制的信息。

考虑下列信息：

- [VMware 环境的监控](#) (p. 105)
- [VMware 环境的 CA Virtual Assurance 管理](#) (p. 106)
- [远程部署和策略配置建议](#) (p. 110)
- [域服务器建议](#) (p. 111)
- [分发服务器建议](#) (p. 111)
- [可扩展性用例](#) (p. 111)

vCenter AIM 监控建议

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。

vCenter AIM (Application Insight Module) 是在 SystemEDGE 框架内实施的可插拔组件。因此，vCenter AIM 发布的数据会提供给多个 SNMP 管理器。CA Virtual Assurance Manager、eHealth 和 Spectrum IM 等产品可以利用该数据。

由于可能在 CA Virtual Assurance 管理器外部使用该组件，因此会分别指定可扩展性建议。下面会讨论两个主要的可扩展性注意事项：

vCenter AIM 监控的一般建议

vCenter AIM 监控的可扩展性限制的一般建议如下所示：

- VM 的最大数目大约是 $240,000 / (x + 6)$
- 对象的最大数目大约是 $2,000,000 / (x + 6)$

其中 x 是每小时针对 AIM 的 SNMP 轮询数。

在受监控对象方面的可扩展性限制

一般情况下，在考虑可扩展性限制时，应首要关注的是 CPU 使用率。对于 vCenter AIM 监控，考虑影响 CPU 使用率的三个主要因素：

- 受监控的 vCenter 服务器的动态性质。
vCenter 服务器的活动级别会影响 CPU 消耗。下列可扩展性建议假定受监控的 vCenter 服务器处于平均活动级别。
- SNMP 管理器的数目，以及那些 SNMP 管理器的轮询间隔。
大量 SNMP 管理器轮询 vCenter AIM，或轮询间隔很短，会导致 CPU 消耗增大。
- 对象计数相对于 VM 计数的比率。
对象是 vCenter AIM 监控的 vSphere 的任何元素。例如，vCenter AIM 监控数据存储、虚拟磁盘、物理网络接口控制器、虚拟交换机、SCSI 控制器、ESX 主机硬件传感器等。对象数目直接影响 CPU 消耗。基于维护 vCenter AIM 缓存的需求以及发布此数据所需的其他开销。在实际的系统中，对象数量通常是给定 vCenter 内虚拟机数量的 6 到 11 倍。

基于上述因素，按照 10 分钟的轮询间隔监控 vCenter AIM 的单个 SNMP 管理器具有大约 20,000 个 VM 的限制。

在受监控服务器方面的可扩展性限制

vCenter AIM 可在多 vCenter 服务器环境中起作用。随着每个 vCenter 服务器的 VM 数量的减少，vCenter AIM 框架会导致 CPU 使用率略有降低。例如，与具有 6,000 个 VM 的单个 vCenter 服务器相比，每个具有 2,000 个 VM 的三个 vCenter 服务器的 CPU 使用率更低。

有时，vCenter AIM 的响应速度成为可扩展性限制。通常，vCenter AIM 能监控多达 10 个 vCenter 服务器。

CA Virtual Assurance vCenter 管理建议

CA Virtual Assurance 管理器的功能远不止监控和发布 vCenter 数据。该管理器负责存储和管理历史数据，针对 vCenter 执行活动操作，运行自动化策略，报告等。因此，VA-IM 管理器通常需要比 vCenter AIM 更多的资源，VA-IM 管理器将此用作其主要的收集数据机制。

在虚拟机方面的 vCenter 管理限制

由于大多数 CA Virtual Assurance 管理器位于单个进程空间内，因此操作系统限制往往是可扩展性的首要障碍。请考虑以下限制因素：

- 可用内存：随着受管对象数目的增加，缓存数据以及处理消息所需的内存量会快速增加。建议将管理器的内存增加到至少 8 GB。
- 可用 CPU：CA Virtual Assurance 管理器需要大量的 CPU 资源，特别是在环境快速变化时或在初始启动期间。我们建议为中等大小的受管环境提供附加的 CPU（3.2 GHz 或更大）来加快自动化进程的响应速度。
- 操作系统限制：大多数 CA Virtual Assurance 管理器位于单个进程空间内。因此，32 位操作系统的内存地址空间可能会用尽，即使系统内存未用尽。要避免此问题，我们建议为中等大小的受管环境使用 64 位处理器和操作系统。

示例：

下列示例提供了 CA Virtual Assurance 管理器的要求和可扩展性限制建议：

- 最低要求（32 位，2.6-GHz CPU，4-GB RAM，100-GB 磁盘）
可扩展性限制：2500 个计算机系统（即，VM 和 ESX 主机）。
- 建议的系统（64 位处理器和操作系统，3.2-GHz CPU，8-GB RAM，100-GB 磁盘）
可扩展性限制：8,000 个计算机系统（即，VM 和 ESX 主机）。

在初始发现期间的性能注意事项

执行您需要管理的 vCenter 环境的初始发现和数据库加载可能是一个耗时的过程。在该过程中，会执行下列操作：

1. vCenter AIM 解析整个 vCenter 环境并发布管理器的结果。
2. CA Virtual Assurance 管理器从 vCenter AIM 检索已发布的数据，并创建内部缓存以进行处理。
3. 会将内部缓存与当前 CA Virtual Assurance 管理器数据库内容同步，为计算机系统执行的发现当前不在数据库内。

在 vCenter 服务器的初始管理期间，该数据库在数据库中没有计算机系统，因此会发现并创建所有这些对象。考虑完成初始发现所需的估计时间。根据基准测试，平均吞吐量是：每分钟 8 至 9 个计算机系统。

示例：

下列示例提供环境的规模和完成初始发现所需的相应估计时间：

- 2500 个计算机系统—大约五个小时
- 8000 个计算机系统—大约 15 个小时

在该初始填充期间，CPU 使用率可能在较长的时间内保持很高。

注意：初始发现进程会占用此时间的绝大多数。但是，初始发现在产品的生存期内仅进行一次。vCenter AIM 和 CA Virtual Assurance 内部缓存进程会快得多。例如，2500 个计算机系统通常是通过 vCenter AIM 发布的，并且在大约 5 分钟内由 CA Virtual Assurance 管理器进行缓存。

LPAR AIM 监控建议

LPAR AIM (Application Insight Module) 是在 SystemEDGE 框架内实施的可插拔组件。因此，vCenter AIM 发布的数据会提供给多个 SNMP 管理器。CA Virtual Assurance、eHealth 和 Spectrum IM 等产品可以利用该数据。

以下部分指定了 LPAR AIM 监控的可扩展性建议。

LPAR AIM 监控的可扩展性建议

一个 LPAR AIM 可以处理以下范围内的 P 系统环境配置：

- HMC 服务器数：1 到 4 个
- 每个 HMC 服务器的 Power 系统数：2 到 10 个
- 每个 Power 系统的虚拟 I/O 服务器数：1 到 2 个
- 每个 Power 系统的 LPAR 数：10 到 100 个

LPAR AIM 监控的一般建议提供了 LPAR 环境的典型配置：

- 受监控的 Power 系统：多达 20 个
- 受监控的 VIO 服务器：多达 30 个
- 受监控的 LPAR：多达 300 个

AIM 消耗的 CPU 和内存大致上对应于 LPAR 数。如果 LPAR 的最大数目为 300，sysedge 进程的 CPU 消耗将小于 10%。

注意：提供的 CPU 消耗对不运行任何其他 AIM 的专用 SystemEDGE 代理有效。

如果将 300 个 LPAR 添加到 LPAR AIM，sysedge 进程的内存消耗将增加约 8 MB。

Solaris Zones AIM 监控建议

Solaris Zones AIM (Application Insight Module) 是在 SystemEDGE 框架内实施的可插拔组件。因此，vCenter AIM 发布的数据会提供给多个 SNMP 管理器。CA Virtual Assurance、eHealth 和 Spectrum IM 等产品可以利用该数据。

以下部分指定了 Solaris Zones AIM 监控的可扩展性建议。

Solaris Zones AIM 监控的可扩展性建议

一般建议是使一个 Zones AIM 监控以下配置：

- 受监控的 Zones 服务器：多达 20 个
- 受监控的 Zones：多达 1000 个

AIM 根据 Zones 的数量按比例消耗 CPU 和内存。但是，前几个 Zones 的初始内存消耗较高，随着添加的 Zones 增多，内存消耗会降低。

如果 Zones 的数量为 1000，sysedge 进程的 CPU 消耗将小于 5%。

注意：提供的 CPU 消耗对不运行任何其他 AIM 的专用 SystemEDGE 代理有效。

如果将 1000 个 Zones 添加到 Zone AIM，sysedge 进程的内存消耗将增加约 20 MB。

远程部署和策略配置建议

请考虑以下方面和建议来改进远程部署和策略操作：

- 目标计算机数

为获得最佳性能，请将每批次中的部署作业大小限制为 500 个目标计算机。

- 分发服务器数

使用多个分发服务器时，部署吞吐量更好。

- 部署软件包大小

部署软件包越小，吞吐量越好。建议的数目假定要求所有受管服务器都具有 SystemEDGE 和高级加密。

注意：典型软件包大小的范围在 10MB 到 20MB 之间。

- 网络的质量和速度

低带宽、高数据包丢失，以及分发服务器和目标服务器之间的高延迟影响部署和配置操作的速率和可靠性。

- 监控软件批量安装到目标系统的时间刻度

使用并置的部署服务器交错监控软件的部署。交错会降低网络基础架构上的负荷。可通过创建大量作业或使用内置到解决方案的“交错”功能来降低该负荷。

如果必须在短时间内部署监控软件，建议在环境中部署更多分发服务器。

- 代理重新配置的频率（通过策略配置）

在典型网络环境中，对于每个代理来说，重新配置 SystemEDGE 代理预计需要大约 30 秒加上 2 到 10 秒的时间。如果必须频繁地重新配置代理，我们建议在该环境中部署其他分发服务器。

- 目标系统在多个站点之间的地理分布

目标系统跨多个站点分布时，我们建议在每个位置部署一个分发服务器。如果远程数据中心使用较慢的（慢于 100 Mb/秒）或不可靠的链路，该建议尤其有效。部署本地分发服务器允许通过现场分发服务器对所有部署和配置请求进行定向。该操作会限制中心站点与远程站点之间的网络通信。

- 通信端口

远程部署和策略配置依赖于域服务器的 CA 消息传递到分发服务器之间的通信以及分发服务器到代理之间的通信。CA 消息传递通过端口 4104 (UDP) 和 4105 (TCP) 进行通信。对于受防火墙保护的远程站点，将分发服务器置于该站点上将允许所有 CA 消息传递通信被设置为点对点。

注意：对于代理发现和持续监控，将使用 SNMP 通信（通常为端口 161）。打开此端口以从受管系统与管理器直接进行通信。

- 策略配置策略和模板的管理

我们建议根据环境中不同的工作负荷将监控要求编入模板。每个策略或模板最多使用 1000 个监视器。可以将任意数量的模板应用于系统，但我们建议将模板的数量限制于每个系统 100 个。

- 服务成员身份

为了减轻配置操作，我们建议将服务器组织到服务中，上限为每个服务大约 500 个服务器。服务器可能是多个服务的成员，因此我们建议创建服务来代表不同的工作负荷。然后可以直接将模板应用于服务。

- 测试部署

域服务器建议

部署和配置域服务器（域服务器）管理和控制所有部署和策略配置操作。

如果目标系统的数目超过 10,000，我们建议运行 CA Virtual Assurance 的多个实例。

分发服务器建议

*部署和配置分发（可扩展性）服务器*确保以有效及时的方式执行部署和策略配置操作。

安装了 CA Virtual Assurance 管理器后，远程部署和策略配置批量安装的下一步是考虑分发服务器的数目。

对于部署操作，我们建议在典型 100 Mb/秒网络环境中，每 2000 个目标系统使用一个分发服务器。

注意：如果使用策略配置但不使用远程部署，则每台分发服务器最多可以用于 3000 台服务器。

重要信息！在执行较大的部署操作之前，建议对每个分发服务器的至少一个系统执行测试部署。我们建议使用分发服务器部署所有可能的软件包，确保较大规模的部署不存在任何故障。

可扩展性用例

本部分提供的用例旨在呈现典型的生产环境。我们建议将这些用例与自己的环境进行比较，并按照与您的环境最匹配的建议操作。

部门数据中心

在此用例中，需要监控包含在一个数据中心内的 1000 个系统。所有系统均位于防火墙内且处于同一位置，计算机之间存在快速链路。

针对该环境的建议是：

- 组件安装

所有 CA Virtual Assurance 管理器组件可安装在同一系统上。

- 初始部署

可以创建两个作业以将监控软件部署到所有目标节点。SystemEDGE（必要时还包含高级加密）的初始部署预计需要 8 到 12 个小时完成，具体取决于网络负载。

完成到远程系统的部署之后，CA Virtual Assurance 管理器会立即发现 SystemEDGE。策略配置向每个代理发送初始策略。预计初始策略发送会在该作业完成后约 8 小时内完成。

- 服务成员身份

为了便于维护，建议将受监控服务器调整到服务中，每个服务大约可以容纳 200 台服务器。可以根据需要使服务与业务职能、网络拓扑结构或其他类别相匹配。

- 应用策略

在必要时，可以通过单次操作将策略应用于所有受监控的系统。

多个数据中心

在此用例中，将管理分布在多个数据中心中的 10,000 个系统。每个数据中心包括的系统数从 500 到 2,500 不等。数据中心分布在多个地理位置。数据中心之间的链路包括低于 100 Mb/秒的租用链路。系统运行各种工作负荷，并且受众多不同部门（应用程序所有者）所管理。

针对该环境的建议是：

- 组件安装

将 CA Virtual Assurance 管理器组件安装在专用服务器上。此服务器必须满足支持的最低规格，但建议使用至少具有 8 GB RAM 的四核服务器。

我们建议将数据库安装在单独的专用服务器上，且其具有更高的规格（四核处理器加 8 GB RAM）。

要支持远程数据中心，我们建议在每个数据中心分别安装一台分发服务器。对于包含 2,000 台以上服务器的数据中心，我们建议安装第二台分发服务器。

注意：如果使用策略配置但不使用远程部署，则每台分发服务器最多可以用于 3000 台服务器。

- 初始部署

在规划使用多台分发服务器进行部署时，需要考虑以下相关因素：

- 如果可能的话，请将单个部署作业大小限制为最多 500 个目标系统。
- 确保为部署操作选择最近的分发服务器。
- 虽然在单台分发服务器内支持并发部署，但建议只在多台分发服务器之间使用并发部署。如果您有 4 台分发服务器，则可以启动作业针对每台分发服务器部署到 500 台计算机。
- 使用同一分发服务器执行并发部署时，请确保第二个作业不向与第一个作业相同的一组目标计算机进行部署。
- 如果将多个软件包交付给许多系统，请考虑将软件包交付拆分为多个作业。例如，通过首先部署 SystemEDGE 和高级加密。
- 如果在大规模部署期间出现故障，请验证所有先决条件，然后使用“重新提交作业”来重试部署。
- 为了帮助执行未来的部署，我们建议将部署保存为模板。

- 服务成员身份

为了便于维护，建议将受监控服务器调整到服务中，每个服务最多可以容纳 500 台服务器。对于远程数据中心，我们建议创建一个或多个服务（取决于数据中心规模）来表示数据中心。

如果多个部门各自使用特定的系统，可以将这些系统添加到多个服务，以便于各个部门进行管理。

- 应用策略

在该用例中，服务器运行各种工作负荷。因此，我们建议基本策略仅包含控制设置。根据不同的监控要求，将监控配置保存在模板中。稍后可以将这些模板应用到所需的系统，此操作可以通过手工选择系统或将模板应用于服务来实现。

将监控要求分成多个模板可以将模板应用于所需的系统，而彼此不会互相影响。手工选择系统，或将模板应用于服务。我们建议按每批 2,000 到 2,500 个系统分批应用模板。

如果需要更改基本策略，我们建议按照每批 2,000 到 2,500 个系统分批将该策略应用到这些系统。

注意：在使用模板时，每次模板或策略的交付均包含将所有已分配模板与基本策略相合并。下一步是将结果配置交付到代理。因此，将多个模板应用于系统时，交付的时间可能会略有增加。

大型环境

在此用例中，受管理的代理大约有 21,000 个。这些代理分布在三个数据中心，每个数据中心包含 2,000 到 10,000 个目标。数据中心虽然分布在不同位置，但它们之间具有快速链路。受管系统大部分都被虚拟化，运行各种工作负荷，并且不时被重新开通。

针对此环境的建议将是：

- 组件安装

强烈建议在每个数据中心中运行一个 CA Virtual Assurance 实例，以便每个实例最多管理 10,000 个系统。

在每个数据中心中，我们建议在专用服务器上安装 CA Virtual Assurance 管理器组件。此服务器必须满足支持的最低规格，但建议再增加 8 GB RAM。

我们建议将数据库安装在具有 8 GB RAM 的单独专用服务器上。

如果需要 CA Virtual Assurance 的单个实例，我们建议使用具有四核处理器以及 16 GB RAM 的管理器服务器和数据库服务器。

为了支持远程部署和策略配置操作，我们建议在每个数据中心安装一台分发服务器（安装在管理器系统上）。

- 初始部署

在此用例中，数据中心中有一台额外的分发服务器。除了在设置方面的这一差异之外，前一方案中强调的所有因素同样适用于本方案。

- 服务成员身份

为了便于维护，建议将受监控服务器划分到多个服务中，每个服务最多可以容纳 500 台服务器。

■ 应用策略

我们建议限制基本策略，以控制设置和“基础 OS”监视器。如果将不同的映像用作虚拟机的基础，则可以为每个操作系统映像创建一个基本策略。确认将 SystemEDGE 配置为在注册时请求该策略。

对于应用程序特定的监视器，请基于具体监控要求创建模板。为了避免模板之间产生索引冲突，我们建议事先为每个应用程序定义“索引范围”。或者，可以在“控制设置”部分下将基本策略配置为“自动解决索引”。

将监控要求分成多个模板可以将模板应用于所需的系统，而彼此不会互相影响。您可以手工选择系统，也可以将模板应用于服务。我们建议按每批 2,000 到 2,500 个系统分批应用模板。

如果需要更改基本策略，我们建议按照每批 2,000 到 2,500 个系统分批将该策略应用到这些系统。

注意：在使用模板时，每次模板或策略的交付均包含将所有已分配模板与基本策略相合并。下一步是将结果配置交付到代理。因此，将多个模板应用于系统时，交付的时间可能会略有增加。

重要信息！如果已部署 CA Virtual Assurance 的多个实例，并且希望在不同的实例之间共享创建的策略，请与 CA 支持部门联系。CA 支持部门可以帮助在 CA Virtual Assurance 实例之间导出和导入策略和模板。

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。

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。

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。

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。

VA--ADES AIM

通过 Active Directory 和 Exchange Server AIM，您可以监控外部和内部基础架构上的 Active Directory 和 Exchange Server 环境。通过该 AIM 可配置 AD 和 ES 环境，以及监控关键性能指标。

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。

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。

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。

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 and 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。

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。

索引

符号

\$CASYSEDGE 变量的传统支持 - 63

A

application insight module, AIM - 123

C

CA Technologies 产品引用 - 3

CA Virtual Assurance vCenter 管理建议 - 112

CA Virtual Assurance 的安装 - 17

H

Hyper-V - 123

I

internet 小型计算机系统接口, iSCSI - 123

L

LPAR AIM 监控建议 - 114

LPAR AIM 监控的可扩展性建议 - 115

P

POWER 处理器 (LPAR) - 123

S

Solaris Zones AIM 监控建议 - 115

Solaris Zones AIM 监控的可扩展性建议 - 116

SystemEDGE 与 CA Systems Performance
LiteAgent 之间的比较 - 15

SystemEDGE 组件的依存关系 - 39

V

VA--ADES AIM - 123

vCenter AIM 监控建议 - 111

vCenter AIM 监控的一般建议 - 111

三划

下载并应用更新 (PTF) - 35

大型环境 - 121

四划

为安装做准备 - 17

从 SystemEDGE 4.3.4 升级代理 - 80

从安装介质中复制无提示安装文件 - 22

从命令提示符卸载管理器 - 90

分发服务器建议 - 118

升级 CA Virtual Assurance - 69

升级受管节点和 AIM 服务器 - 78

手动升级远程 Embedded Entitlements
Manager - 76

手动应用旧配置 - 78

支持的升级 - 69

无提示管理器安装 - 22

五划

代理和 AIM 升级 - 79

代理部署 - 36

四划

以 dbcreator 角色创建数据库用户 - 31

以无提示模式卸载管理器 - 91

以传统模式安装代理 - 64

五划

功能概述 - 84

可扩展性用例 - 118

可扩展性建议 - 111

可扩展性最佳实践 - 107

平台管理模块, PMM - 123

正则表达式 - 123

用户界面入门 - 83

六划

优化 Windows 内存管理 - 15

创建部署作业 - 37

动态重新配置连接器索引, DRC 索引 (LPAR)
- 123

各个代理安装 - 39

在 64 位 Linux 版本上安装 SystemEDGE 失败
- 57

在 UNIX 上从命令行安装代理 - 57
在 UNIX 系统上卸载 SystemEDGE 和 AIM - 93
在 UNIX 和 Linux 系统上安装代理 - 52
在 UNIX 和 Linux 系统上进行安装 - 52
在 Windows 上从命令行安装代理 - 46
在 Windows 上安装代理 - 41
在 Windows 上卸载 SystemEDGE 和 AIM - 91
在 Windows 系统上安装 - 41
在初始发现期间的性能注意事项 - 114
在受监控对象方面的可扩展性限制 - 112
在受监控服务器方面的可扩展性限制 - 112
在虚拟机方面的 vCenter 管理限制 - 113
多个服务器上的安装 - 24
多个服务器上的安装准则 - 24
多个数据中心 - 119
如何升级 CA Virtual Assurance - 70
如何更新 CA Virtual Assurance - 34
如何将 SQL Server 用户权限调整到最小必要权限 - 30
安全注意事项 - 14
安装 AIM - 65
安装 CA Systems Performance LiteAgent - 67
安装 CA Virtual Assurance - 13
安装和配置 SQL Server Express - 13
安装要求和注意事项 - 13
执行无提示管理器安装 - 23
执行完全卸载 - 90
扩展性概述 - 107
有效 AutoShell 用户 - 86
约定 - 10
网络注意事项 - 109

七划

初始安装之后的组件安装 - 22
启动 AutoShell - 85
启动 CA Virtual Assurance - 83
启动 CA Virtual Assurance 命令提示符 - 86
启动总目录和联机帮助 - 87
应用重要修补程序 - 73
运行安装 - 19
运行管理器安装 - 76
还原目录和数据 - 105
还原配置和数据 - 103
还原数据库 - 104
还原整个系统 - 103

远程部署和策略配置建议 - 116
远程部署和策略配置概述 - 109

八划

使用新的数据库用户安装产品 - 31
取消安装 - 22
备份与还原 - 97
备份与还原概述 - 97
备份目录和数据 - 100
备份配置和数据 - 99
备份数据库 - 99
备份整个系统 - 73, 98
建立维护窗口 - 73
范围 - 9
轮询时间间隔 - 124

九划

卸载 CA Virtual Assurance - 89
卸载 SystemEDGE - 91
卸载选项 - 89
卸载管理器 - 89
将 aom2 和 dpm 数据库的所有者更改为 sa - 32
将 SystemEDGE 监视器导入策略 - 81
将多 Apache 配置还原到单 Apache - 74
将新数据库用户的权限调整到最小必要权限 - 32
查看升级文档 - 71
查看升级限制 - 75
查看未自动升级的旧配置 - 77
查看要求 - 31
相关出版物 - 10

十划

准备要升级的环境 - 72
读者 - 9
通过 CA Virtual Assurance 管理器安装程序进行 SystemEDGE 安装 - 40
通信端口 - 27
部门数据中心 - 118
配置和使用响应文件 - 64
验证使用 SQL Server 的要求 - 14
验证环境中的 CA Virtual Assurance 升级 - 82

十一划

停止服务 - 75

域服务器建议 - 117

检查更新 - 34

虚拟 I/O 服务器，VIOS (LPAR) - 124

逻辑分区，LPAR - 124

十二划

登录用户界面并管理您的环境 - 33

硬件规格 - 108

编辑 `silent.properties` 文件 - 23

联系技术支持 - 3

十三划

数据库注意事项 - 108

简介 - 9