

# 安装指南

## CA Application Delivery Analysis

10.1



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內容。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限内。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 © 2014 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。

## 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

---

<b>第 1 章：简介</b>	<b>5</b>
<b>第 2 章：系统要求</b>	<b>7</b>
支持的操作系统.....	8
受支持的 Web 浏览器.....	8
硬件要求.....	9
虚拟计算机要求.....	10
防火墙要求.....	11
Adobe 应用程序.....	11
安装服务器角色和角色服务.....	12
安装 SNMP 服务和 SMTP 服务器.....	14
配置回收站.....	15
禁用不需要的 Windows 服务.....	15
创建 TrapConfiguration 键.....	16
<b>第 3 章：配置硬件</b>	<b>19</b>
配置管理控制台服务器.....	19
配置 Standard Monitor 服务器.....	20
为 NIC 配置网络连接.....	20
为管理 NIC 分配 IP 地址.....	22
<b>第 4 章：安装软件</b>	<b>23</b>
先决条件.....	23
安装管理控制台.....	24
安装 Standard Monitor.....	25
安装虚拟监视器.....	26
<b>第 5 章：安装后配置</b>	<b>27</b>
安装 CA Application Delivery Analysis 更新.....	27
防病毒扫描时排除目录.....	27
同步系统时间和时区.....	27
从管理控制台执行配置任务.....	29
<b>附录 A：部署最佳实践</b>	<b>31</b>
如何确定服务器的位置.....	31

---

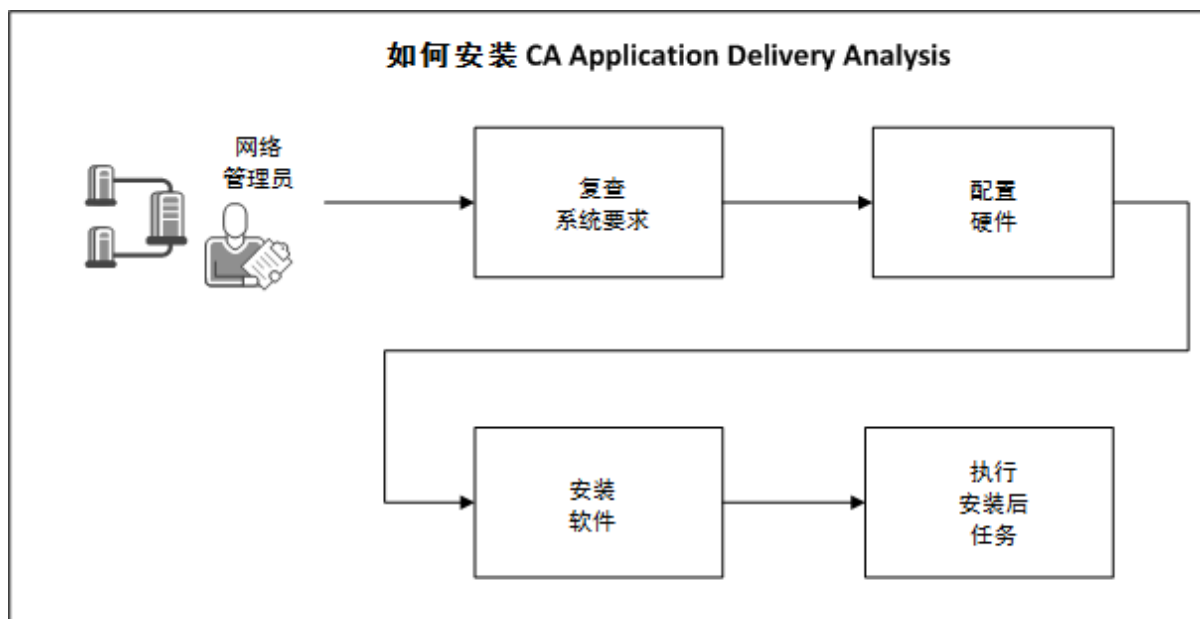
如何监视单向数据流 .....	31
如何镜像交换机端口 .....	32

# 第 1 章：简介

---

CA Application Delivery Analysis (CA ADA) 通过报告页面和视图提供端到端性能监视。CA ADA 收集故障排除信息，并帮助您确定应用程序、网络或服务器性能问题的源头。

下图说明 CA ADA 的安装过程。



详细信息：

[系统要求](#) (p. 7)

[安装后配置](#) (p. 27)

[安装软件](#) (p. 23)

[配置硬件](#) (p. 19)



## 第 2 章： 系统要求

---

如果您购买的是来自 *CA Technologies* 的硬件，交货时所有组件都带有操作系统，安全设置也已配置好。请按照本节主题中的描述验证设置，或根据自己组织的需要进行相应的更新。

如果只购买了软件，请按照本节中描述的步骤来配置操作系统及其安全设置。

服务器管理员应安装 CA Application Delivery Analysis。

开始之前，请将需要的所有文件复制到安装服务器中。配置好操作系统安全设置后，您可能无权访问包含这些文件的共享文件夹。

此部分包含以下主题：

[支持的操作系统](#) (p. 8)

[受支持的 Web 浏览器](#) (p. 8)

[硬件要求](#) (p. 9)

[虚拟计算机要求](#) (p. 10)

[防火墙要求](#) (p. 11)

[Adobe 应用程序](#) (p. 11)

[安装服务器角色和角色服务](#) (p. 12)

[安装 SNMP 服务和 SMTP 服务器](#) (p. 14)

[配置回收站](#) (p. 15)

[禁用不需要的 Windows 服务](#) (p. 15)

[创建 TrapConfiguration 键](#) (p. 16)

## 支持的操作系统

CA Application Delivery Analysis 组件需要 Microsoft Windows 2008 R2 Standard Edition，该操作系统要有：

- 最新的 Service Pack 和重要更新。
- Microsoft .NET Framework 3.5.1.
- Java Runtime Environment (JRE).

**注意：** CA ADA 安装程序会安装 JRE。我们不建议单独安装 JRE。

- 英语、简体中文或日语。

**注意：** 区域设置必须使用句点 (.) 来表示小数值。例如，葡萄牙（巴西）区域设置默认情况下使用逗号来表示小数值。自定义区域设置以将小数符号更改为句点。

- 最小显示器分辨率 1024x768 (XGA)。
- ASP.NET 2.0，包括 COM+ 网络访问、IIS 和 ASP。
- 操作系统按本文档中所述得到了配置。
- 启用 SNMP 和 SMTP 服务。
- （推荐）启用远程桌面连接，以允许管理员进行远程访问。
- IPv4 主机地址。目前不支持在具有 IPv6 地址的服务器上进行安装。

## 受支持的 Web 浏览器

以下浏览器支持访问管理控制台：

- Microsoft Internet Explorer 7 或 8

通过 Internet Explorer 8 访问管理控制台时，页面顶端格式可能出现问题。要避免这种情况，请在 Internet Explorer 中按 F12，然后设置“浏览模式”为 IE8，“文档模式”为 Quirks。

- Mozilla Firefox 11.x

其他浏览器或版本可能也可以与 CA Application Delivery Analysis 一起使用，但尚未进行测试。



## 硬件要求

在不同的服务器上安装管理控制台和 **Standard Monitor**。通过一个管理 NIC 来配置管理控制台，以接收来自监视设备（如 **CA Standard Monitor**）的响应时间度量标准。

### 管理控制台

CA 已通过以下规范对服务器上的管理控制台进行了测试。只要服务器满足以下最低规格，管理控制台在任何供应商的服务器上都受支持。

- 两个 Intel® E5520 Xeon 四核 2.66 GHz、1333 MHz FSB 处理器
- 24 GB RAM
- 六个采用 RAID 5 配置的 146 GB SAS 硬盘驱动器
- 配有多达八个 SAS 端口的电池供电缓存的 RAID 控制器
- 10/100/1000 Mbps 以太网 RJ-45 端口
- Intel 82576 Gigabit 以太网控制器

### Standard Monitor

CA 已通过以下规范对服务器上的 **CA Standard Monitor** 进行了测试。只要服务器满足以下最低规格，**Standard Monitor** 在任何供应商的服务器上都受支持。

- Intel® E5520 Xeon 四核 2.66 GHz、1333 MHz FSB 处理器
- 3 GB RAM
- 三个采用 RAID 5 配置的 146 GB SAS 硬盘驱动器
- 配有多达八个 SAS 端口的电池供电缓存的 RAID 控制器
- 两个 10/100/1000 Mbps 以太网 RJ-45 端口  
(可选) 要监视 2 个监视器 NIC 上的 TCP 通信量，请开通额外的以太网 RJ-45 端口。
- Intel 82576 Gigabit 以太网控制器

## 虚拟计算机要求

CA Application Delivery Analysis 在 VMware ESX® 和 VMware ESXi® 3.5、4.0 或 5.0 上支持管理控制台和 CA Standard Monitor。

为了在物理服务器不足的环境中实现同等性能，与物理服务器相比，VMware 需要更多内存。在磁盘输入/输出方面，物理服务器优于虚拟机。CA Application Delivery Analysis 服务器的磁盘输入/输出任务量很大。您可能无法期望 VMware 计算机达到更高的性能。

部署于 VMware 的 CA Standard Monitor 可以接收来自 CA GigaStor Connector 和 WAN 优化设备（如 Cisco WAE）的数据。

**重要信息：**请在承载 CA Application Delivery Analysis 的虚拟机上安装 VMware 工具。从虚拟机配置中去除 CD/DVD 驱动器。

### Standard Monitor

CA 已通过以下规范对虚拟机上的 Standard Monitor 进行了测试。我们建议您的虚拟机至少满足以下最低规格。

- 一台虚拟处理器
- 4 GB RAM
- 300 GB 可用磁盘空间
- 两个虚拟网络适配器（最小 1 Gbit）。在其中一个虚拟网络适配器上需要一个上行链路端口（传出 ESX Host 的物理端口）。  
（可选）要监视 2 个监视器 NIC 上的 TCP 通信量，请开通额外的以太网 RJ-45 端口。

### 管理控制台

CA 已通过以下规范对虚拟机上的管理控制台进行了测试。我们建议您的虚拟机至少满足以下最低规格。

- 一台虚拟处理器
- 30 GB RAM
- 700 GB 可用磁盘空间
- 一个虚拟网络适配器（最小 1 Gbit）。网络适配器上必须有一个上行链路端口（离开 ESX 主机的物理端口）。

## 防火墙要求

以下列表汇总了为允许 CA ADA 组件间通信而必须打开的防火墙端口。

### 从管理控制台

- 通过 TCP 1000、1001、3308 和 8080 到 CA Standard 或 Virtual Monitor
- 通过 TCP 80 和 TCP 8080 到 CA ADA Multi-Port Monitor

### 从 Standard 或 Virtual Monitor

- 通过 TCP 3308 到管理控制台

### 从 CA ADA Multi-Port Monitor

- 通过 TCP 80、TCP 3308 和 TCP 8381 到管理控制台。

CA Application Delivery Analysis 上的 CA Single Sign-On 设置使用不同的端口 (TCP 8381) 对用户进行身份验证。登录到 CA Multi-Port Monitor 后，它将重定向到在 CA ADA Manager 的 TCP 8381 上运行的 CA Single Sign-On 应用程序。确认您的防火墙配置允许执行此操作。

安装后，若有必要，可以更新 CA ADA 上的 CA Single Sign-on 设置，以使用不同的 TCP 端口。有关详细信息，请与 CA 技术支持联系。

### 从 Cisco NAM 上的度量标准引擎

- 通过 TCP 9996 到管理控制台

### 从 Cisco WAE 上的 FlowAgent

- 通过 TCP 7878 到 CA Standard 或 Multi-Port Monitor
- 通过 TCP 7878 到管理控制台

### 从 CA GigaStor 连接程序

- 通过 UDP 9995 到 CA Standard 或 Multi-Port Monitor
- 通过 TCP 1001 到管理控制台

## Adobe 应用程序

Adobe® Acrobat Reader 和 Flash Player 是查看报告、图表以及产品文档所必需的。

- 可以从 <http://get.adobe.com/reader/> 安装最新版本的 Acrobat Reader。
- 可以从 <http://get.adobe.com/flashplayer/> 安装最新版本的 Flash Player。

## 安装服务器角色和角色服务

安装所需的 Windows 服务器角色和角色服务。

### 遵循这些步骤:

1. 以管理员身份登录到服务器。
2. 依次选择“开始”、“管理工具”、“服务器管理器”。  
将打开“服务器管理器”窗口。
3. 选择左侧的“控制台”树中的“角色”。
4. 单击“添加角色”。  
此时将打开“添加角色”向导。
5. 单击“下一步”。
6. 从“选择服务器角色”列表中选择“应用程序服务器”。  
“应用程序服务器”角色包括 .NET Framework 3.5.1。
7. 单击“下一步”。
8. 单击“下一步”。  
此时将显示应用程序服务器的“选择角色服务”页面。
9. 添加“Web 服务器 (IIS) 支持”角色服务:
  - a. 选中“Web 服务器(IIS)支持”复选框。  
随后将出现一条确认消息。
  - b. 单击确认消息中的“添加必需的角色服务”。  
“选择角色服务”页面上将突出显示“Web 服务器(IIS)支持”选项。
10. 添加 COM+ 角色服务:
  - a. 选中“COM+ 网络访问”复选框。
  - b. 单击“下一步”。
11. 启用 IIS 6 管理兼容性:
  - a. 再次单击“下一步”。  
此时将显示 Web 服务器 (IIS) 的“选择角色服务”页面。
  - b. 选择该列表“管理工具”部分中的“IIS 6 管理兼容性”复选框，然后单击“下一步”。  
“确认安装选择”页面概述应用程序服务器角色、Web 服务器 (IIS) 角色以及 .NET Framework 3.5.1 功能的配置。

12. 安装您选择的 IIS 和 COM+ 角色服务及选项:

- a. 单击“安装”。

“进度”页面显示。完成安装后，将打开“结果”页面。
- b. (可选)单击“打印、保存或通过电子邮件发送安装报告”，复查信息，然后关闭该页面。

“安装报告”页面将显示摘要信息，包括您所做的更改、有关这些更改的重要信息以及完整安装日志的位置。
- c. 单击“关闭”。

“添加角色”向导关闭。

13. 添加并安装 ASP 角色服务:

- a. 在左侧的“控制台”树中的“角色”下，单击“Web 服务器 (IIS)”链接。

将在右窗格中打开“Web 服务器(IIS)”视图。
- b. 在“角色服务”部分，单击“添加角色服务”链接。

“添加角色服务”向导将打开“选择角色服务”页面。
- c. 在列表中的“应用程序开发”下选中“ASP”复选框，然后单击“下一步”。

“确认安装选择”页面概述您的操作及相关消息。
- d. 单击“安装”。

将一直显示“进度”页面，直到安装完成后打开“结果”页面。
- e. (可选)单击“打印、保存或通过电子邮件发送安装报告”，复查信息，然后关闭该页面。

“安装报告”页面将显示摘要信息，包括您所做的更改、有关这些更改的重要信息以及完整安装日志的位置。
- f. 单击“关闭”。

将关闭“安装结果”页面。

14. 将从“服务器管理器”窗口退出。

## 安装 SNMP 服务和 SMTP 服务器

安装 SNMP 服务和 SMTP 服务器。

CA ADA Watchdog 服务需要简单网络管理协议 (SNMP)。简单邮件传输协议 (SMTP) 服务是一个 IIS 组件，用于传送传出电子邮件。

### 遵循这些步骤:

1. 以管理员身份登录到服务器。
2. 导航到“管理工具”、“服务器管理器”。  
将打开“服务器管理器”窗口。
3. 单击左侧“控制台”树中的“功能”。  
“服务器管理器”窗口将显示服务器上已安装功能的列表。
4. 在“功能摘要”下单击“添加功能”。  
添加功能向导的“选择功能”页面中将显示已安装功能和可用功能列表。
5. 在“功能”列表中选择“SNMP 服务”。  
随后将出现一条确认消息。
6. 单击“添加必需的功能”。  
“确认安装服务”页面将标识要安装的功能。该页面还显示了有关安装的重要消息。
7. 单击“安装”。  
“安装进度”页面将显示安装的进度。完成安装后，“安装结果”页面会标识新功能，并指示是否需要重新启动服务器。
8. 单击“关闭”。  
将显示一条消息，询问您是否要立即重新启动服务器。
9. 单击“否”。
10. 对 SMTP 服务器重复步骤 5 至 8。  
将显示一条消息，询问您是否要立即重新启动服务器。
11. 单击“是”。  
重新启动服务器后，“服务器管理器”窗口中的“功能”视图会显示新安装的功能。

## 配置回收站

还可以配置回收站以立即从服务器中删除已删除的文件。系统的默认行为是在回收站中保存已删除文件的副本，占用较多的空间。

**请执行以下步骤：**

1. 以对 CA Network Flow Analysis 具有管理员权限的用户身份登录。
2. 右键单击桌面上的“回收站”图标。
3. 从菜单选择“属性”。  
打开“回收站属性”对话框。
4. 在“常规”选项卡上选择“本地磁盘(C:)”。
5. 选择标记为“不将文件移到回收站中。移除文件后立即将其删除。”的选项。
6. 单击“应用”。
7. 对要配置的每个其他驱动器重复这些步骤。
8. 单击“确定”。

## 禁用不需要的 Windows 服务

您可选择禁用 CA ADA 不需要的服务。删除不需要的服务有助于保护您的服务器，但这不是必需的。如果出于其他原因需要以下服务，请不要将其禁用。

**请执行以下步骤：**

1. 以对服务器具有管理员权限的用户身份登录。
2. 打开“服务”窗口：依次单击“开始”、“管理工具”、“服务”。  
将打开“服务”窗口。
3. 右键单击以下服务，然后选择“手动”或“已禁用”。  
不要选择“停止”，否则服务器重启时，这些服务会再次启动。

**您可以禁用的 Windows 服务器服务**

- Application Layer Gateway Service
- Distributed Link Tracking Client
- Function Discovery Resource Publication
- Link-Layer Topology Discovery Manager
- Netlogon
- Portable Device Enumerator Service
- Remote Access Connection Manager
- Secondary Logon
- Special Administration Console Helper
- Telephony
- Windows Audio Endpoint Builder
- WinHTTP Web Proxy Auto-Discovery Service
- Application Management
- Distributed Transaction Coordinator
- Human Interface Device Access
- Microsoft Iscsi Initiator Service
- Network List Service
- Print Spooler
- Remote Registry
- Smart Card
- SSDP 发现
- Volume Shadow Copy
- Windows CardSpace
- WMI Performance Adapter
- Certificate Propagation
- DNS 客户端
- IP Helper
- Multimedia Class Scheduler
- Network Location Awareness
- Remote Access Auto Connection Manager
- Resultant Set of Policy Provider
- Smart Card Removal Policy
- Tablet PC Input Service
- Windows Audio
- Windows Color System

## 创建 TrapConfiguration 键

建议您在 Windows 注册表中创建空 TrapConfiguration 键，以便防止 SNMP 服务记录误报事件。

请执行以下步骤：

1. 以对服务器具有管理员权限的用户身份登录。
2. 打开命令提示符窗口。



3. 运行以下命令：

```
reg add  
HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapC  
onfiguration
```

如果命令成功执行，则返回值为：“操作已成功完成”。

将在以下位置创建空的 TrapConfiguration 注册表键：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Par  
ameters。
```



## 第 3 章：配置硬件

---

配置硬件时，您需要以下类型的电缆：

### 电源电缆

将服务器连接到两个电源，最好是两个独立的 UPS 设备。第二根电缆是为连接备用电源所必需的。

### 管理 NIC 电缆

#### 铜 1-Gb 电缆

插入交换机后，管理 NIC 便提供了到 CA ADA 服务器的网络访问。

管理 NIC 还接收来自 Cisco WAE 设备、NAM 设备以及 CA GigaStor 的性能数据。

### 监视器 NIC 电缆

#### 铜 1-Gb 电缆

从交换机上的镜像端口收集网络通信量。

此部分包含以下主题：

[配置管理控制台服务器](#) (p. 19)

[配置 Standard Monitor 服务器](#) (p. 20)

[为 NIC 配置网络连接](#) (p. 20)

[为管理 NIC 分配 IP 地址](#) (p. 22)

## 配置管理控制台服务器

使用该过程可配置承载管理控制台的服务器。

请执行以下步骤：

1. 将电缆的一端连接到服务器的电源接口上。
2. 将电缆的另一端连接到两个独立的电源。
3. 将管理电缆的一端连接到服务器上的 NIC。
4. 将管理电缆的另一端连接到交换机，启用对管理控制台的网络访问。

5. 打开服务器。
6. 配置来自 CA 的设备时，请使用以下凭据登录到设备：
  - 用户名：netqos
  - 密码：Changepassword1我们建议立即更改默认密码。
7. 为 NIC 配置[网络连接](#) (p. 20)。
8. 为 NIC 分配 [IP 地址](#) (p. 22)。

## 配置 Standard Monitor 服务器

使用该过程可配置承载 Standard Monitor 的服务器。

请执行以下步骤：

1. 将电缆的一端连接到服务器的电源接口上。
2. 将电缆的另一端连接到两个独立的电源。
3. 将监视器电缆和管理电缆的一端连接到服务器上的 NIC。
4. 将监视器电缆的另一端连接到镜像交换机端口。
5. 将管理电缆的另一端连接到管理控制台服务器。
6. 打开服务器。
7. 配置来自 CA 的设备时，请使用以下凭据登录到设备：
  - 用户名：netqos
  - 密码：Changepassword1我们建议立即更改默认密码。
8. 为 NIC 配置[网络连接](#) (p. 20)。
9. 为 NIC 分配 [IP 地址](#) (p. 22)。

## 为 NIC 配置网络连接

在您要安装管理控制台或 CA Standard Monitor 的每台服务器上配置网卡 (NIC)。

- 对于 CA Standard Monitor，为管理和监视 NIC 建立网络连接。请注意，最多可配置 2 个监视器 NIC 来接收通信。
- 对于管理控制台，设置管理 NIC 的优先级。

**请执行以下步骤：**

1. 在“控制面板”中，单击“网络连接”。  
此时“网络连接”窗口将打开。
2. 复查 LAN 或高速 Internet 连接的名称。如有必要，可以按下表中所示将默认名称更改为与接口对应的名称：

**铜制以太网适配器**

默认名称：本地连接 2

要指定的新名称：管理

**铜制以太网适配器**

默认名称：本地连接 3

要指定的新名称：监视器

**千兆位光纤端口**

默认名称：本地连接

要指定的新名称：光纤监视器

**提示：**您可以通过断开设备背面的电缆并检查“网络连接”对话框中哪个接口的状态更改为“已断开”来标识设备。

3. 在管理控制台或 CA Standard Monitor 上禁用未使用的监视器 NIC。
  - a. 右键单击 NIC。
  - b. 选择“禁用”。
4. 依次单击“高级”、“高级设置”、“适配器”和“绑定”。
5. 使用向上箭头将管理 NIC 移至“连接”窗格的顶部。此操作将设置优先级并允许 CA ADA 正确运行。
6. 为所有 NIC 清除以下与 Internet 协议 (TCP/IP) 相关的复选框：
  - Microsoft 网络的文件和打印机共享
  - Microsoft 网络客户端
7. 单击“确定”。

## 为管理 NIC 分配 IP 地址

为管理控制台或 CA Standard Monitor 上的管理 NIC 分配静态 IP 地址、子网掩码和默认网关。

**注意：**管理 NIC 是向网络传送数据的唯一 NIC。分配给其他 NIC（如 Monitor NIC）的 IP 地址不必对其所连接的网络有效，也不必为他们分配默认网关。

**请执行以下步骤：**

1. 打开“控制面板”，然后选择“网络连接”。
2. 右键单击“管理”网络连接并选择“属性”。
3. 单击“常规”选项卡上的“属性”。
4. 清除除“Internet 协议版本 4 (TCP/IPv4)”之外的所有网络组件复选框。
5. 选择“Internet 协议版本 4 (TCP/IPv4)”，然后单击“属性”。
6. 选择“使用下面的 IP 地址”，然后输入 IP 地址、子网掩码和默认网关。
7. 单击“确定”。
8. 对监视器 NIC 重复步骤 5 至 7，并使用以下建议值：

### **监视器 NIC**

IP 地址：1.1.0.2

子网掩码：255.0.0.0

### **光纤监视器 NIC**

IP 地址：1.1.0.1

子网掩码：255.0.0.0

# 第 4 章： 安装软件

---

此部分包含以下主题：

[先决条件](#) (p. 23)

[安装管理控制台](#) (p. 24)

[安装 Standard Monitor](#) (p. 25)

[安装虚拟监视器](#) (p. 26)

## 先决条件

安装 CA ADA 软件之前，请执行以下任务：

- 从 [CA 技术支持网站](#) 下载最新的 CA ADA 安装文件 ADASetup10.1.xxx.exe。
- 如果您使用来自 CA 的 CA ADA 设备，我们建议您确认当前安装的软件版本。如有必要，请升级到最新版本。要确认软件版本，请登录到 CA ADA 控制台并单击“关于”链接。有关升级 CA ADA 的信息，请参阅《*升级指南*》。
- 不要将 CA ADA 与 NetQoS Performance Center 6.1 安装在同一台计算机上。随 CA ADA 提供的 CA Single Sign-on 应用程序与随 CA NetQoS Performance Center 提供的 CA Single Sign-on 不兼容。必要时，在不同的计算机上安装 CA ADA。
- 将安装文件提取或复制到要安装该软件的服务器或虚拟机上。
- 确认安装文件有权运行：
  - a. 右键单击安装文件并选择“属性”。
  - b. 单击“解除锁定”。
  - c. 单击“确定”。

## 安装管理控制台

使用该过程可在物理服务器或虚拟机上安装管理控制台。CA Standard Monitor 也会安装，但不会自动添加为监视设备。安装后，手动[添加监视设备](#) (p. 27)作为响应时间数据的源。

安装程序将其状态记录在 `驱动器:\CA\ADA_Uninstaller\Logs` 中。

### 请执行以下步骤：

1. 以管理员身份登录到服务器。
2. 双击 ADASetup10.1.xxx.exe 文件。  
将打开“欢迎”对话框。
3. 单击“下一步”。  
将打开“许可协议”对话框。
4. 阅读并接受许可协议，然后单击“下一步”。  
将打开“选择安装文件集”对话框。
5. 选择“分布式管理器”，然后单击“下一步”。  
“信息”对话框将提醒您将 CA ADA 注册为 CA SOLVE:Access 或 CA Performance Center 的数据源。
6. 单击“继续”。  
将打开“选择安装文件夹”对话框。
7. (可选)单击“选择”可选择其他位置。默认位置为 C:\CA。
8. 单击“下一步”。  
将打开“安装前摘要”对话框，其概述了安装参数。
9. 单击“安装”。  
将开始安装过程。显示消息，指示安装进度。安装完成后，将打开“安装完成”对话框。
10. 选择“是，重新启动系统”。
11. 单击“完成”。  
服务器重启后，您可以将 CA Standard Monitor 等监视设备添加到管理控制台。

### 详细信息：

[安装后配置](#) (p. 27)



## 安装 Standard Monitor

可以遵照以下过程安装监视设备。

安装程序将其状态记录在 `驱动器:\CA\ADA_Uninstaller\Logs` 中。

**请执行以下步骤：**

1. 以管理员身份登录到服务器。
2. 双击 `ADASetup10.1.xxx.exe` 文件。  
将打开“欢迎”对话框。
3. 单击“下一步”。  
将打开“许可协议”对话框。
4. 阅读并接受许可协议，然后单击“下一步”。  
将打开“选择安装文件集”对话框。
5. 选择“Single-Port Monitor”，然后单击“下一步”。  
“信息”对话框将提醒您将 CA ADA 注册为 CA SOLVE:Access 或 CA Performance Center 的数据源。
6. 单击“继续”。  
将打开“选择安装文件夹”对话框。
7. （*可选*）单击“选择”可选择其他位置。默认位置为 `C:\CA`。
8. 单击“下一步”。  
将打开“安装前摘要”对话框，其概述了安装参数。
9. 单击“安装”。  
将开始安装过程。显示消息，指示安装进度。安装完成后，将打开“安装完成”对话框。
10. 选择“是，重新启动系统”。
11. 单击“完成”。  
重新启动服务器后，您的系统可以继续完成[安装后配置](#) (p. 27)。

## 安装虚拟监视器

使用该过程可以安装 CA Virtual Monitor。

安装程序将其状态记录在 `驱动器:\CA\ADA_Uninstaller\Logs` 中。

**请执行以下步骤：**

1. 以管理员身份登录到虚拟机。
2. 双击 `ADASetup10.1.xxx.exe` 文件。  
将打开“欢迎”对话框。
3. 单击“下一步”。  
将打开“许可协议”对话框。
4. 阅读并接受许可协议，然后单击“下一步”。  
将打开“选择安装文件集”对话框。
5. 选择“Virtual Monitor”，然后单击“下一步”。  
“信息”对话框将提醒您将 CA ADA 注册为 CA SOLVE:Access 或 CA Performance Center 的数据源。
6. 单击“继续”。  
将打开“选择安装文件夹”对话框。
7. （*可选*）单击“选择”可选择其他位置。默认位置为 `D:\CA`。
8. 单击“下一步”。  
将打开“安装前摘要”对话框，其概述了安装参数。
9. 单击“安装”。  
将开始安装过程。显示消息，指示安装进度。安装完成后，将打开“安装完成”对话框。
10. 选择“是，重新启动系统”。
11. 单击“完成”。  
重新启动虚拟机后，您的系统可以继续完成[安装后配置](#) (p. 27)。

# 第 5 章： 安装后配置

---

此部分包含以下主题：

[安装 CA Application Delivery Analysis 更新](#) (p. 27)

[防病毒扫描时排除目录](#) (p. 27)

[同步系统时间和时区](#) (p. 27)

[从管理控制台执行配置任务](#) (p. 29)

## 安装 CA Application Delivery Analysis 更新

从 [CA 在线支持](#) 网站安装任何可用更新。

## 防病毒扫描时排除目录

如果您必须安装防病毒软件，请将以下目录从病毒扫描中排除：

- C:\Windows\Temp
- CA ADA 的安装目录及其子目录。默认情况下，CA ADA 将安装到 C:\CA。

## 同步系统时间和时区

遵循这些步骤：

1. 以具有管理员权限的用户身份登录到服务器。
2. 右键单击任务栏右边缘上的日期或时间，然后选择“调整日期/时间”。  
将打开“日期和时间”对话框。
3. 单击“Internet 时间”选项卡。
4. 单击“更改设置”。  
将打开“Internet 时间设置”对话框。
5. 选中“与 Internet 时间服务器同步”复选框。
6. 选择要与之同步的 NTP 时间服务器。默认选择为 time.windows.com。
7. 单击“立即更新”。  
系统时间将与选定的服务器同步。

8. 在“Internet 时间设置”对话框中，单击“确定”。
9. 在“日期和时间”对话框中，单击“确定”。

**注意：**如果您在其他时区也有 CA Standard Monitor，请将各监视设备设置到当地时区。使用 NTP 服务器来帮助确保时间准确。这些时间将被转换为格林尼治标准时间 (GMT)。

## 从管理控制台执行配置任务

使用管理控制台：

- 将 CA Standard Monitor 添加为监视设备。
- 定义要监视的服务器子网和客户端网络。

**注意：**有关详细信息，请参阅 CA Application Delivery Analysis 联机帮助或《CA Application Delivery Analysis 管理员指南》。

**遵循这些步骤：**

1. 单击“管理配置”页面。
2. 添加监视设备：
  - a. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
  - b. 在“向我显示”菜单下单击“添加 ADA 监视器”。  
将打开“Standard Monitor 属性”。
  - c. 填写“Standard Monitor 属性”中的字段，然后单击“确定”。  
为您在[配置网络接口卡](#) (p. 20)中配置的管理 NIC 和监视器 NIC 提供 IP 地址。有关详细信息，请单击“帮助”。
3. 定义您想要的服务器子网：
  - a. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
  - b. 滚动到“服务器子网列表”，然后单击“添加服务器子网”。
  - c. 将打开“添加服务器子网”。
  - d. 完成“服务器子网”中的字段，然后单击“确定”。  
有关设置服务器子网属性的信息，请单击“帮助”。
4. 定义您想要的客户端网络：
  - a. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。
  - b. 在“向我显示”菜单下，单击“添加网络”。
  - c. 将打开“网络属性”。
  - d. 填写“网络属性”中的字段，然后单击“确定”。
  - e. 有关网络属性的信息，请单击“帮助”。
5. 单击该链接可同步监视设备，并开始基于当前服务器子网络和客户端网络定义收集数据。



# 附录 A： 部署最佳实践

---

该部分的主题提供了一些关于如何配置和放置服务器以便帮助您更好地监视所有相关通信量的建议。

## 如何确定服务器的位置

CA ADA 服务器需要连接到每个网络交换机上的处理您要监视的通信量的 SPAN 或镜像端口。连接通常在访问层发生。将 CA ADA 管理控制台安装在其连接的监视设备的临近位置。

服务器必须能够观测尽可能多的相关网络通信量。请考虑以下问题：

- 要监视哪些应用程序？
- 哪些服务器承载这些应用程序？
- 这些服务器连接到哪些交换机？
- 用户从哪些子网访问监视的应用程序？

## 如何监视单向数据流

可以利用内联光纤分流器查看单向数据流。某些分流器设计有一个入口网卡和两个出口网卡，一个出口网卡负责传送，另一个负责接收。在这种情况下，CA ADA 需要使用一个多 NIC 监视器（如 CA ADA Multi-Port Monitor）才能准确计算通信量。

在非对称路由环境中，一个核心交换机将数据路由到数据中心。另一个核心交换机路由退出数据中心的通信量。捕获服务器场的传输和接收通信量时，必须使用镜像到同一个监视器的两个端口。

CA Standard Monitor 无法监视单向或非对称通信。

## 如何镜像交换机端口

在网络交换机上，*端口镜像*功能用于将来自一个端口的网络数据包的副本发送到另一个交换机或端口以供分析。

端口镜像是将通信量镜像到 CA ADA 监视设备的安全且有效方式。

某些交换机不提供这些方案所需的各种 TCP 数据包镜像功能。

如果不能对通信量进行最佳镜像，请使用其他方式，例如光纤分流器。

**注意：**Cisco 交换机上的端口镜像功能被命名为 **Switched Port Analyzer (SPAN)**。

将用于在受监视服务器上传入或传出通信的交换机端口镜像到 CA ADA 服务器上的监视器 NIC，或镜像到 CA ADA 监视设备所连接到的端口。正确配置镜像端口后，CA ADA 便可以监视客户端和服务器之间的应用程序通信流，无需使用桌面或服务器代理。

有关详细信息，请参阅《*数据采集最佳实践指南*》。