



HUAWEI ATIC 管理中心

V200R001

安装指南

文档版本 06

发布日期 2014-10-25

版权所有 © 华为技术有限公司 2014。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： <http://www.huawei.com>

客户服务邮箱：support@huawei.com

客户服务电话：4008302118

目录

1 安装规划	1
1.1 部署规划	2
1.1.1 集中式部署	2
1.1.2 分布式部署	5
1.2 NTP 服务规划	10
1.3 端口列表	11
1.4 安全规划	12
2 安装准备	13
2.1 检查环境要求	14
2.2 收集安装信息	14
2.3 检查硬件连接	16
2.4 验证软件包完整性	17
3 安装操作系统	18
3.1 配置 Windows 操作系统的预安装参数	19
3.1.1 激活 Windows	19
3.1.2 修改操作系统管理员用户 SWMaster 的密码	22
3.1.3 修改操作系统的主机名	22
3.1.4 修改操作系统的 IP 地址	24
3.1.5 设置操作系统自动更新方式	28
3.1.6 (可选) 修改操作系统的时间和时区	30
4 (可选) 安装趋势防毒软件	33
4.1 申请防毒软件 License	34
4.2 安装防毒软件服务器	34
4.2.1 安装步骤	34
4.2.2 验证安装正确性	48
4.3 安装防毒软件客户端	50
4.3.1 安装步骤	50
4.3.2 验证安装正确性	52
4.4 防病毒检查	53
4.5 更新防病毒组件	55

5 配置 NTP 组件	59
6 安装 ATIC 管理中心服务器	64
6.1 安装前检查.....	65
6.2 安装步骤.....	65
6.3 启动 ATIC 管理中心.....	70
6.4 验证安装正确性.....	70
6.5 登录 ATIC 管理中心.....	71
6.6 安装失败处理.....	72
7 安装 Anti-DDoS 采集器	74
7.1 安装前检查.....	75
7.2 安装步骤.....	75
7.3 启动 Anti-DDoS 采集器.....	80
7.4 验证安装正确性.....	80
8 卸载 ATIC 管理中心	82
8.1 卸载 ATIC 管理中心服务器.....	83
8.1.1 关闭 ATIC 管理中心.....	83
8.1.2 卸载 ATIC 管理中心服务器软件.....	83
8.1.3 卸载异常处理.....	86
8.2 卸载 Anti-DDoS 采集器.....	86
8.2.1 关闭 Anti-DDoS 采集器.....	87
8.2.2 卸载 Anti-DDoS 采集器软件.....	87
8.2.3 卸载异常处理.....	89
8.3 卸载趋势防毒软件.....	90
8.3.1 卸载防毒软件客户端.....	90
8.3.2 卸载防毒软件服务器.....	91
9 附录	95
9.1 如何查看 Windows 操作系统中某端口的占用情况及释放端口.....	96
9.2 ping 程序被禁用导致安装服务器至 33%时进程自动结束.....	98
9.3 使用 HTTPS 协议登录 ATIC 管理中心时，如何安装安全证书.....	104
9.4 修改 ATIC 管理中心服务器或采集器软件中 IP 地址的配置信息.....	110
9.5 修改 ATIC 管理中心服务器软件中 WEB 端口的配置信息.....	113
9.6 修改 ATIC 管理中心服务器和采集器软件中 MySQL 数据库的配置信息.....	114

1 安装规划

关于本章

介绍在安装前如何规划ATIC管理中心的部署方式、软硬件配置、网络的路由和带宽、使用的端口和服务、安全方案等。

1.1 部署规划

您需要根据现网情况，选择ATIC管理中心服务器和Anti-DDoS采集器的部署方式，并进行相应的规划。

1.2 NTP服务规划

为了确保ATIC管理中心服务器、采集器与所管理的网元时间一致，需要规划NTP（Network Time Protocol）服务。

1.3 端口列表

为了保证ATIC管理中心的正常运行，各组件的进程所使用的端口不能被其他软件占用。

1.4 安全规划

为了保证ATIC管理中心的安全运行，建议进行安全规划，包括操作系统和数据库的安全。

1.1 部署规划

您需要根据现网情况，选择ATIC管理中心服务器和Anti-DDoS采集器的部署方式，并进行相应的规划。

1.1.1 集中式部署

集中式部署即ATIC管理中心服务器和Anti-DDoS采集器同时安装在同一台物理服务器上。

集中式组网成本较低，适用于Anti-DDoS设备集中部署的网络，具体组网请参见[组网](#)。选择该组网方式需要考虑以下因素：

- **Anti-DDoS设备的组网**
集中式组网要求Anti-DDoS设备部署在相同的局域网，如果设备部署在广域网，集中式部署会导致大量的日志信息占用广域网的带宽，影响正常的业务。另外，广域网的不稳定性也可能导致数据丢失。
- **Anti-DDoS设备的部署场景**
 - 直路部署，所有流量都经过Anti-DDoS设备进行检测清洗，一台Anti-DDoS采集器大约可以处理10000个IP地址的Anti-DDoS业务日志。如果防护对象的IP地址数量达到10000个以上，建议单独配置一台Anti-DDoS采集器。
 - 旁路部署，只有异常流量才引流到Anti-DDoS设备进行检测清洗，异常流量的比例大约占10%，可以大量减少采集器的数量。比如100000个防护IP地址配置一台采集器。设备旁路部署时，如果多台Anti-DDoS设备部署地比较分散，仍然建议配置多台Anti-DDoS采集器。

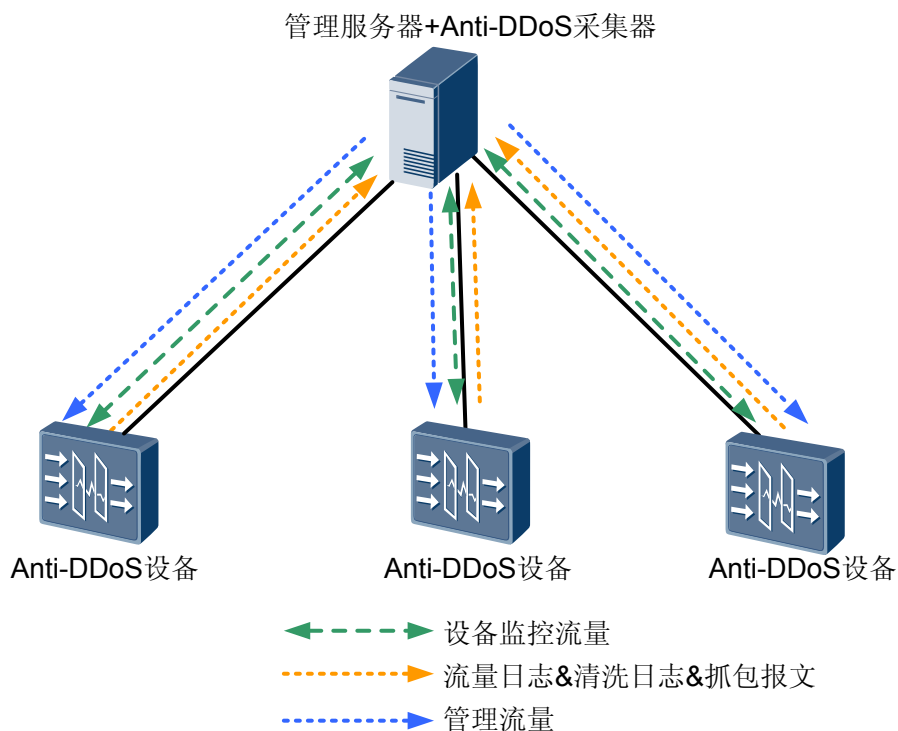
需要规划的项目如下：

- 为了确保ATIC管理中心的正常运行，建议按照推荐的软/硬件配置对服务器进行规划，具体请参见[服务器软件规划](#)、[服务器硬件规划](#)。
- 为了确保ATIC管理中心能正常管理网元、进行Anti-DDoS业务配置和Anti-DDoS业务分析，需要根据实际网络情况规划服务器的IP地址和路由，具体请参见[IP地址规划](#)、[路由规划](#)。
- 为了确保Anti-DDoS采集器和网元之间的正常通信、服务器和网元之间的正常通信以及管理员能够登录服务器，需要提前对带宽进行规划，具体请参见[服务器和Anti-DDoS设备之间的带宽规划](#)、[服务器和访问服务器的PC（即客户端）之间的带宽规划](#)。

组网

ATIC管理中心服务器与Anti-DDoS采集器集中部署的组网如[图1-1](#)所示。

图 1-1 ATIC 管理中心服务器与 Anti-DDoS 采集器集中部署组网图



服务器软件规划

安装ATIC管理中心时，MySQL数据库会自动安装，操作系统和浏览器的规划请参见表 1-1。

表 1-1 服务器软件规划

硬件平台	软件类型	软件版本
x86 (Windows 64bit)	操作系统	Windows Server 2008 R2 Standard
	访问服务器的浏览器	Internet Explorer 6.0/7.0/8.0 Mozilla Firefox 3.6.X至4.X

服务器硬件规划

说明

- 建议Anti-DDoS业务单独部署在一台服务器上，如果和其他业务共用一台服务器，可能会降低Anti-DDoS业务的处理性能。
- 为确保ATIC管理中心能够正常启动，服务器的可用物理内存最低要求是2.5GB。

硬件规划包括推荐配置和最低配置，具体请参见表1-2。

表 1-2 服务器硬件规划

项目	要求
标准配置	<p>华为Tecal RH2288H V2服务器</p> <ul style="list-style-type: none"> ● CPU: 2*E5-2630V2 ● 内存: 2*8GB ● 磁盘: 3*300G SAS <p>建议为安装操作系统的磁盘配置RAID5。</p> <p>为了提高系统可靠性和安全性, 建议将磁盘至少划分为两个分区: 一个分区的容量为50GB, 用于安装操作系统; 剩余空间分配给另一分区, 用于安装数据库软件和ATIC管理中心, 存储数据库文件。</p>

其中, Anti-DDoS日志和报表占用磁盘空间比较多, 可按照如下举例估计数据量:

- Anti-DDoS日志的数据量按照10000个IP地址, 一年的数据量估计如下:

 说明

此处考虑的是Anti-DDoS设备直路部署的情况, 旁路部署时清洗设备只有在流量异常时才会产生数据量, 可以根据实际网络情况减少预留磁盘空间。

1. 每个IP地址各种类型流量数据的记录条数。
 - 原始流量数据5分钟会产生1条记录, 一年的数据量为 $12 \times 24 \times 365 = 105120$ 。
 - 业务流量数据每个IP地址承载1个服务, 5分钟会产生1条记录, 一年的数据量为 $12 \times 24 \times 365 = 105120$ 。
 - 汇总流量数据每小时产生1条记录、每天也会产生1条记录, 一年的数据量为 $24 \times 365 + 365 = 9125$ 。
 - 攻击流量数据按受攻击比例为5%计算, 一年的数据量为 $105120 \times 5\% = 5256$ 。
 - 其他的汇总数据较少, 不做估计。
2. 每个IP每年数据量总条数为 $105120 + 105120 + 9125 + 5256 = 224621$ 。
3. 每条记录的大小约为200Byte, 每个IP地址每年的总数据量为 $200\text{Byte} \times 224621 = 43\text{MB}$ 。
4. 所有IP地址总的的数据量为 $10000 \times 43\text{MB} = 430000\text{MB} = 430\text{GB}$ 。

- Anti-DDoS报表按照2000个防护对象, 仅输出月报表, 一年的数据量估计如下:

1. 报表个数为 $12 \times 2000 = 24000$ 。
2. 每个报表可能会生成两种文件格式Excel和PDF; 报表的大小和Anti-DDoS设备数量有关, 按照1台设备计算Excel和PDF格式共计1MB。
3. 报表总数据量为 $24000 \times 1\text{MB} = 24\text{GB}$ 。

IP 地址规划

在安装ATIC管理中心之前需要规划服务器的IP地址, 该IP地址的主要功能:

- 用于ATIC管理中心服务器的配置和管理。
- 用于ATIC管理中心的对外服务。如：管理员使用浏览器访问ATIC管理中心服务器、ATIC管理中心服务器与网元之间的通信。

IP地址规划的原则：

- ATIC管理中心仅支持IPv4地址，请勿使用IPv6地址。
- 一个网口只能规划一个IP地址。
- 如果服务器上有多个网口且未配置IPMP（IP Network Multipathing），网口的IP地址不能处于同一网段。

例如：服务器的IP地址为129.9.1.1，子网掩码为255.255.255.0，网关为129.9.1.254。

路由规划

路由规划的原则：ATIC管理中心服务器和Anti-DDoS采集器部署在同一台物理服务器上，和Anti-DDoS设备路由可达即可。

推荐在ATIC管理中心上使用默认路由，在路由器或交换机上配置到网元的路由和到ATIC管理中心的回程路由。

服务器和 Anti-DDoS 设备之间的带宽规划

ATIC管理中心服务器和Anti-DDoS设备之间至少保证2M的可用带宽，建议保留10M带宽。

服务器和访问服务器的 PC（即客户端）之间的带宽规划

服务器和客户端之间的带宽需满足访问服务器通信的需要。

规划原则：单个客户端与服务器间推荐通信带宽为2Mbit/s以上。最低带宽不能低于128Kbit/s（如笔记本终端），在128Kbit/s带宽的情况下，可能会使ATIC管理中心的操作效率降低。

计算方法：服务器与客户端通信的带宽 = 单个客户端与服务器间的带宽 × 客户端数量。

例如：一台ATIC管理中心服务器需要与10个客户端通信，则服务器用于客户端通信的带宽推荐为20Mbit/s。

1.1.2 分布式部署

分布式部署即ATIC管理中心服务器和Anti-DDoS采集器分别安装，通常是安装在不同的物理服务器上。

分布式部署适用于Anti-DDoS设备分布部署的网络，具体组网请参见[组网](#)。选择该组网方式需要考虑以下因素：

- Anti-DDoS设备的组网
Anti-DDoS设备分布在多个区域，区域间需要通过广域网连接。每个区域部署所需的Anti-DDoS采集器，可以避免大量的日志信息占用带宽，节约租用带宽的成本。另外，广域网的不稳定性也可能导致数据丢失。
- Anti-DDoS设备的部署场景

- 直路部署，所有流量都经过Anti-DDoS设备进行检测清洗，一台Anti-DDoS采集器大约可以处理10000个IP地址的Anti-DDoS业务日志，如果防护对象的IP地址数量达到10000个以上，建议为每台Anti-DDoS设备单独配置一台采集器。
- 旁路部署，只有异常流量才引流到Anti-DDoS设备进行检测清洗，异常流量的比例大约占10%，可以大量减少采集器的数量，比如100,000个防护IP地址配置一台采集器。设备旁路部署时，如果多台设备部署地比较分散，仍然建议配置多台采集器。

需要规划的项目如下：

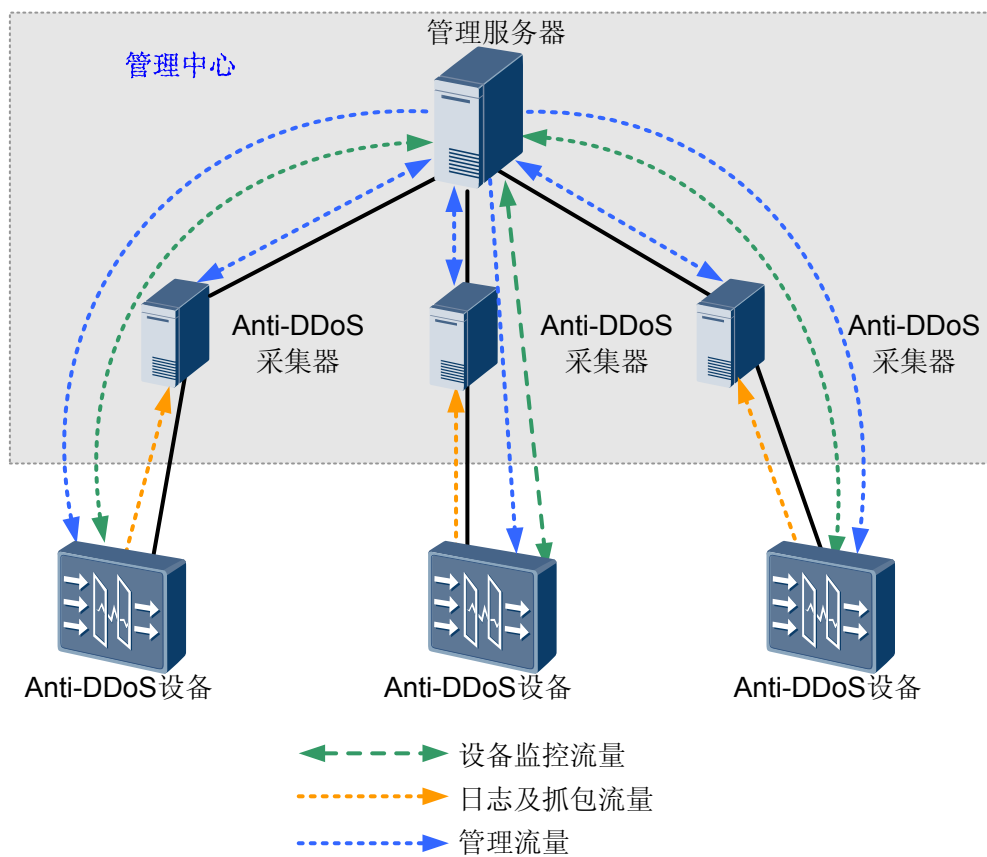
- 为了确保ATIC管理中心的正常运行，建议按照推荐的软/硬件配置对服务器和Anti-DDoS采集器进行规划，具体请参见[服务器软件规划](#)、[服务器硬件规划](#)、[Anti-DDoS采集器软件规划](#)、[Anti-DDoS采集器硬件规划](#)。
- 为了确保ATIC管理中心能正常管理网元、进行Anti-DDoS业务配置和Anti-DDoS业务分析，需要根据实际网络情况规划服务器和Anti-DDoS采集器的IP地址和路由，具体请参见[IP地址规划](#)、[路由规划](#)。
- 为了确保ATIC管理中心服务器、Anti-DDoS采集器和网元之间的正常通信以及管理员能够登录服务器，需要提前对带宽进行规划，具体请参见[服务器、Anti-DDoS采集器和Anti-DDoS设备之间的带宽规划](#)、[服务器和访问服务器的PC（即客户端）之间的带宽规划](#)。

组网

ATIC管理中心服务器与Anti-DDoS采集器分布部署的组网如[图1-2](#)所示。

Anti-DDoS采集器和ATIC管理中心服务器安装在不同的物理服务器上，多台Anti-DDoS采集器可以共用一台ATIC管理中心服务器，一台ATIC管理中心服务器最多可管理20台Anti-DDoS采集器。

图 1-2 ATIC 管理中心服务器与 Anti-DDoS 采集器分布部署组网图



服务器软件规划

安装 ATIC 管理中心时，MySQL 数据库会自动安装，操作系统和浏览器的规划请参见表 1-3。

表 1-3 服务器软件规划

硬件平台	软件类型	软件版本
x86 (Windows 64bit)	操作系统	Windows Server 2008 R2 Standard
	访问服务器的浏览器	Internet Explorer 6.0/7.0/8.0 Mozilla Firefox 3.6.X至4.X

服务器硬件规划

说明

- 建议 Anti-DDoS 业务单独部署在一台服务器上，如果和其他业务共用一台服务器，可能会降低 Anti-DDoS 业务的处理性能。
- 为确保 ATIC 管理中心能够正常启动，服务器的可用物理内存最低要求是 1.5GB。

硬件规划包括推荐配置和最低配置，具体请参见表 1-4。

表 1-4 服务器硬件规划

项目	要求
标准配置	<p>华为Tecal RH2288H V2服务器</p> <ul style="list-style-type: none"> ● CPU: 2*E5-2630V2 ● 内存: 2*8GB ● 磁盘: 3*300G SAS <p>建议为安装操作系统的磁盘配置RAID5。</p> <p>为了提高系统可靠性和安全性, 建议将磁盘至少划分为两个分区: 一个分区的容量为50GB, 用于安装操作系统; 剩余空间分配给另一分区, 用于安装数据库软件和ATIC管理中心, 存储数据库文件。</p>

其中, 报表数据保存在服务器上, Anti-DDoS报表按照2000个防护对象, 仅输出月报表, 一年的数据量估计如下:

1. 报表个数为 $12 \times 2000 = 24000$ 。
2. 每个报表可能会生成两种文件格式Excel和PDF; 报表的大小和Anti-DDoS设备数量有关, 按照1台设备计算Excel和PDF格式共计1MB。
3. 报表总数据量为 $24000 \times 1MB = 24GB$ 。

Anti-DDoS 采集器软件规划

安装Anti-DDoS采集器时, MySQL数据库会自动安装, 操作系统的规划请参见[表1-5](#)。

表 1-5 Anti-DDoS 采集器软件规划

硬件平台	软件类型	软件版本
x86 (Windows 64bit)	操作系统	Windows Server 2008 R2 Standard

Anti-DDoS 采集器硬件规划

说明

为确保Anti-DDoS采集器能够正常启动, Anti-DDoS采集器的可用物理内存最低要求是1.5GB。

硬件规划包括推荐配置和最低配置, 具体请参见[表1-6](#)。

表 1-6 Anti-DDoS 采集器硬件规划

项目	要求
标准配置	<p>华为Tecal RH2288H V2服务器</p> <ul style="list-style-type: none"> ● CPU: 2*E5-2630V2 ● 内存: 2*8GB ● 磁盘: 3*300G SAS <p>建议为安装操作系统的磁盘配置RAID5。</p> <p>为了提高系统可靠性和安全性, 建议将磁盘至少划分为两个分区: 一个分区的容量为50GB, 用于安装操作系统; 剩余空间分配给另一分区, 用于安装数据库软件和ATIC管理中心, 存储数据库文件。</p>

其中, 原始日志数据保存在Anti-DDoS采集器上, Anti-DDoS日志的数据量按照10000个IP地址, 并且都有流量, 一年的数据量估计如下:

说明

此处考虑的是Anti-DDoS设备直路部署的情况, 旁路部署时清洗设备只有在流量异常时才会产生数据量, 可以根据实际网络情况减少预留磁盘空间。

1. 每个IP地址各种类型流量数据的记录条数。
 - 原始流量数据5分钟会产生1条记录, 一年的数据量为 $12 \times 24 \times 365 = 105120$ 。
 - 业务流量数据每个IP地址承载1个服务, 5分钟会产生1条记录, 一年的数据量为 $12 \times 24 \times 365 = 105120$ 。
 - 汇总流量数据每小时产生1条记录、每天也会产生1条记录, 一年的数据量为 $24 \times 365 + 365 = 9125$ 。
 - 攻击流量数据按攻击比例为5%计算, 一年的数据量为 $105120 \times 5\% = 5256$ 。
 - 其他的汇总数据较少, 不做估计。
2. 每个IP每年数据量总条数为 $105120 + 105120 + 9125 + 5256 = 224621$ 。
3. 每条记录的大小约为200Byte, 每个IP地址每年的总数据量为 $200\text{Byte} \times 224621 = 43\text{MB}$ 。
4. 所有IP地址总的的数据量为 $10000 \times 43\text{MB} = 430000\text{MB} = 430\text{GB}$ 。

IP 地址规划

在安装ATIC管理中心之前需要规划ATIC管理中心服务器/采集器的IP地址, 该IP地址的主要功能:

- 用于服务器/采集器的配置和管理。
- 用于ATIC管理中心服务器/采集器的对外服务。如: 管理员使用浏览器访问ATIC管理中心服务器; ATIC管理中心服务器与Anti-DDoS采集器之间的通信; Anti-DDoS采集器与网元之间的通信。

IP地址规划的原则:

- ATIC管理中心仅支持IPv4地址, 请勿使用IPv6地址。

- 一个网口只能规划一个IP地址。
- 如果服务器上有多个网口且不配置IPMP（IP Network Multipathing），网口的IP地址不能处于同一网段。

例如，服务器的IP地址为129.9.1.1/255.255.255.0，网关为129.9.1.254；采集器的IP地址为129.9.1.10/255.255.255.0，网关为129.9.1.254。

说明

现网实施时，如果需要从外网访问ATIC管理中心，ATIC管理中心服务器和Anti-DDoS采集器都需要配置公网IP地址。

路由规划

路由规划的原则：ATIC管理中心服务器、Anti-DDoS采集器、Anti-DDoS设备之间都要路由可达。

服务器、Anti-DDoS 采集器和 Anti-DDoS 设备之间的带宽规划

服务器、Anti-DDoS采集器和Anti-DDoS设备之间分别至少保证2M的可用带宽，建议保留10M带宽。

服务器和访问服务器的 PC（即客户端）之间的带宽规划

服务器和客户端之间的带宽需满足访问服务器通信的需要。

规划原则：单个客户端与服务器间推荐通信带宽为2Mbit/s以上。最低带宽不能低于128Kbit/s（如笔记本终端），在128Kbit/s带宽的情况下，可能会使ATIC管理中心的操作效率降低。

计算方法：服务器与客户端通信的带宽 = 单个客户端与服务器间的带宽 × 客户端数量。

例如：一台ATIC管理中心服务器需要与10个客户端通信，则服务器用于客户端通信的带宽推荐为20Mbit/s。

1.2 NTP 服务规划

为了确保ATIC管理中心服务器、采集器与所管理的网元时间一致，需要规划NTP（Network Time Protocol）服务。

NTP服务用于对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟保持一致。

NTP服务规划的目的：

- 为了确保ATIC管理中心能够正确管理网元上报的告警和性能数据，要求网元和ATIC管理中心服务器的时间必须保持一致。
- 安装Anti-DDoS业务组件后，为了确保Anti-DDoS业务分析的准确性，要求Anti-DDoS设备、Anti-DDoS采集器和ATIC管理中心服务器的时间必须保持一致。

NTP服务规划的原则：

- 如果存在标准的外部时钟源，建议将ATIC管理中心服务器、Anti-DDoS采集器、网元配置为NTP客户端，跟踪该外部时钟源。

- 如果无标准的外部时钟源，建议将ATIC管理中心服务器配置为NTP服务器，Anti-DDoS采集器、网元配置为NTP客户端。



注意

当网络中管理网元较多时，建议采用标准的外部时钟源作为NTP服务器，或者手工调整网元的时间与ATIC管理中心服务器一致。如果将ATIC管理中心服务器作为NTP服务器，会影响ATIC管理中心服务器的运行效率。

1.3 端口列表

为了保证ATIC管理中心的正常运行，各组件的进程所使用的端口不能被其他软件占用。

ATIC管理中心所使用的端口如表1-7所示。

表 1-7 端口列表

组件及其进程		端口	说明	
组件	进程			
数据库	mysqld.exe	3306	MySQL数据库的默认端口。	
网管基础组件	legowebsrv.exe	8080	HTTP服务端口。	
		443	HTTPS服务端口。	
		8005	系统内部通信端口。	
		8009		
	legosrv.exe	61616		
		10091		
legosrv.exe	162	SNMP trap端口。		
Anti-DDoS 业务组件	服务器	legosrv.exe	11098	服务器的通信端口，用于服务器和Anti-DDoS采集器的通信。
	采集器	DDoSCollector.exe	11099	Anti-DDoS采集器的通信端口，用于Anti-DDoS采集器和服务器的通信。
			9110	接收流量日志、抓包日志的端口。
			8213	Anti-DDoS采集器内部的JMX服务端口，用于监控采集器自身是否在线。
			10324	下载抓包文件的端口。

1.4 安全规划

为了保证ATIC管理中心的安全运行，建议进行安全规划，包括操作系统和数据库的安全。

操作系统安全

使用操作系统加固工具，对操作系统进行加固，主要加固工作有：

- 关闭不使用的端口。
- 停止不使用的服务。
- 禁止使用简单密码。
- 及时安装Microsoft安全补丁（3个月之内）和SP补丁（6个月之内）。

数据库安全

使用数据库加固工具，对数据库进行加固，主要加固工作有：

- 更改知名端口。
- 禁止使用简单密码。
- 及时安装SP补丁（6个月之内）。

2 安装准备

关于本章

介绍安装ATIC管理中心之前，需要了解的环境要求、典型组网；需要收集的安装信息；需要检查的软硬件的准备工作等。

2.1 检查环境要求

介绍安装ATIC管理中心前必须检查的环境条件，包括机房环境、线路状况、机房网络状况等。

2.2 收集安装信息

在安装前，请按照规划结果，收集整理安装信息，包括：服务器和采集器的主机名、IP地址、磁盘分区方案、所在时区和时间、各种软件的用户名和密码、安装路径。

2.3 检查硬件连接

在安装ATIC管理中心前，必须检查硬件安装和连线的正确性，否则将会在安装过程中出现不可预知的错误。

2.4 验证软件包完整性

介绍如何使用工具验证软件包的完整性。

2.1 检查环境要求

介绍安装ATIC管理中心前必须检查的环境条件，包括机房环境、线路状况、机房网络状况等。

在安装ATIC管理中心前，参见[表2-1](#)对环境进行检查。

表 2-1 安装环境要求

检查项	要求
温度	长期工作条件：15° C~30° C，短期工作条件：0° C~45° C。
湿度	长期工作条件：40%~65%，短期工作条件：20%~90%。
灰尘	直径大于5 μ m的灰尘的浓度 $\leq 3 \times 10^4/m^3$ 。
地板	使用防静电活动地板，地板必须接地。
空间	机房中按每一台设备说明书的要求为其预留有足够通风空间。为了后续对设备进行维护 and 操作，需要为人员活动预留空间。
电源	独立的外部供电系统，并且要求供电稳定，建议使用不间断电源UPS（Uninterrupted Power Supply）。
网络	连接所有设备所需的路由器已完成配置，设备可以被访问，设备所处的网络运行正常。

2.2 收集安装信息

在安装前，请按照规划结果，收集整理安装信息，包括：服务器和采集器的主机名、IP地址、磁盘分区方案、所在时区和时间、各种软件的用户名和密码、安装路径。

前提条件

完成ATIC管理中心的安装规划工作，具体内容请参见[1 安装规划](#)。

背景信息

为了便于后续使用和存档，建议使用“任务示例”中的表格记录安装信息。

操作步骤

步骤1 收集服务器、采集器的主机名。

步骤2 收集服务器、采集器的IP地址。

IP地址规划原则：

- IP地址在网络中必须唯一。

- ATIC管理中心仅支持IPv4地址，请勿使用IPv6地址。
- 服务器端与所管网元能正常通信。
- 服务器端与客户端能正常通信。
- 一个网口只能规划一个IP地址。

步骤3 确定服务器、采集器物理位置所在时区和时间。

步骤4 收集服务器、采集器安装的操作系统、数据库的用户名和密码，以及ATIC管理中心软件的用户名和密码。

步骤5 确定服务器磁盘分区原则和方案。

磁盘分区基本原则如下：

- C 盘用作系统盘，主要用于安装操作系统。
- D 盘用作安装ATIC管理中心软件、数据库软件和存储数据库数据。
- 剩余空间自由分配，可以用来保存网管的备份数据。

步骤6 规划安装路径。

ATIC管理中心软件安装路径名称，只能包含字母、数字、下划线，不能包含空格、括号、中文字符等，否则将无法成功安装。

---结束

任务示例



在实际安装中，使用下表前请删除“规划内容”中的信息并打印。

表 2-2 服务器安装信息表

规划项目	规划内容
服务器主机名	ATICserver
服务器IP地址	IP地址：129.9.1.1 子网掩码：255.255.255.0 网关：129.9.1.254
时区	GMT+08:00
时间	14:00
操作系统超级用户 administrator 密码	Changeme123
ATIC管理中心用户 admin 密码	Admin@123（系统默认值）
操作系统安装路径	C:\
ATIC管理中心服务器软件安装路径	D:\VSM

表 2-3 分布式方案采集器安装信息表

规划项目	规划内容
采集器主机名	ATICcollector
采集器IP地址	IP地址：129.9.1.2 子网掩码：255.255.255.0 网关：129.9.1.254
时区	GMT+08:00
时间	14:00
操作系统超级用户administrator密码	Changeme123
操作系统安装路径	C:\
采集器软件安装路径	D:\VSM

2.3 检查硬件连接

在安装ATIC管理中心前，必须检查硬件安装和连线的正确性，否则将会在安装过程中出现不可预知的错误。

前提条件

此处以IBM服务器为例进行说明。

服务器硬件安装以及设备线缆连接已经完成。

操作步骤

步骤1 检查各部件的电源线、地线均连接牢固、极性正确、接触良好。

步骤2 所有电缆要绑扎，外皮均无损伤。

步骤3 检查硬件连接线和网线。

步骤4 检查插头和插座。

1. 各电缆插头的锁扣应扣紧。
2. 检查各个插座是否有缺针或插针弯曲短路现象。

---结束

后续处理

不应有扎带、线头、干燥剂袋等施工遗留物，施工现场应整齐、干净。

将多余的物品从机房内清除掉，需要放置于机房内的物品应摆放整齐，操作台应干净、整洁，活动地板应平整、干净。

2.4 验证软件包完整性

介绍如何使用工具验证软件包的完整性。

背景信息

软件在发布、传输或使用过程中，有可能遭到病毒、木马和黑客的恶意篡改和破坏，从而在客户的系统上运行后造成恶性后果。因此，有必要提供有效的软件完整性保护机制。

操作步骤

- 步骤1** 下载MD5校验工具（MD5 verification tools for windows.rar）和软件完整性验证操作指导书。该工具为华为公司编写。登录<http://support.huawei.com>，下载地址为：“软件中心 > 受控工具（小工具软件） > 业务与软件 > 业务与软件公共 > 平台中间件公共”。
- 步骤2** 解压MD5校验工具，分别得到md5_trans.vbs，md5sum.exe两个文件。
- 步骤3** 将安装包软件及其md5摘要文件“.md5”以及MD5校验工具（“md5_trans.vbs”，“md5sum.exe”）放置同级目录下。
- 步骤4** 双击“md5_trans.vbs”文件之后，当前目录下的摘要文件格式“.md5”会自动转换为可在windows环境下校验的摘要文件格式“.md5.temp”，同时会校验这些“.md5.temp”摘要文件。
- 如果返回OK，则说明hash值匹配，该软件包为原始包。
 - 如果返回FAILED，则说明hash值不匹配，该软件包被篡改过。

----结束

3 安装操作系统

关于本章

介绍ATIC管理中心服务器、采集器操作系统的安装过程

3.1 配置Windows操作系统的预安装参数

缺省情况下，发货服务器上已经安装好Windows操作系统和安全加固组件，用户需要根据实际情况修改操作系统参数的配置。

3.1 配置 Windows 操作系统的预安装参数

缺省情况下，发货服务器上已经安装好Windows操作系统和安全加固组件，用户需要根据实际情况修改操作系统参数的配置。

3.1.1 激活 Windows

在预安装场景下，Windows操作系统未被激活。请您在30天的期限内，激活Windows保证您的正常使用。

前提条件

请您准备好Windows Server 2008 R2标准版的产品密钥。



您可以在Windows包装盒或服务器机身上找到产品密钥。

背景信息

Windows支持以下激活方式：

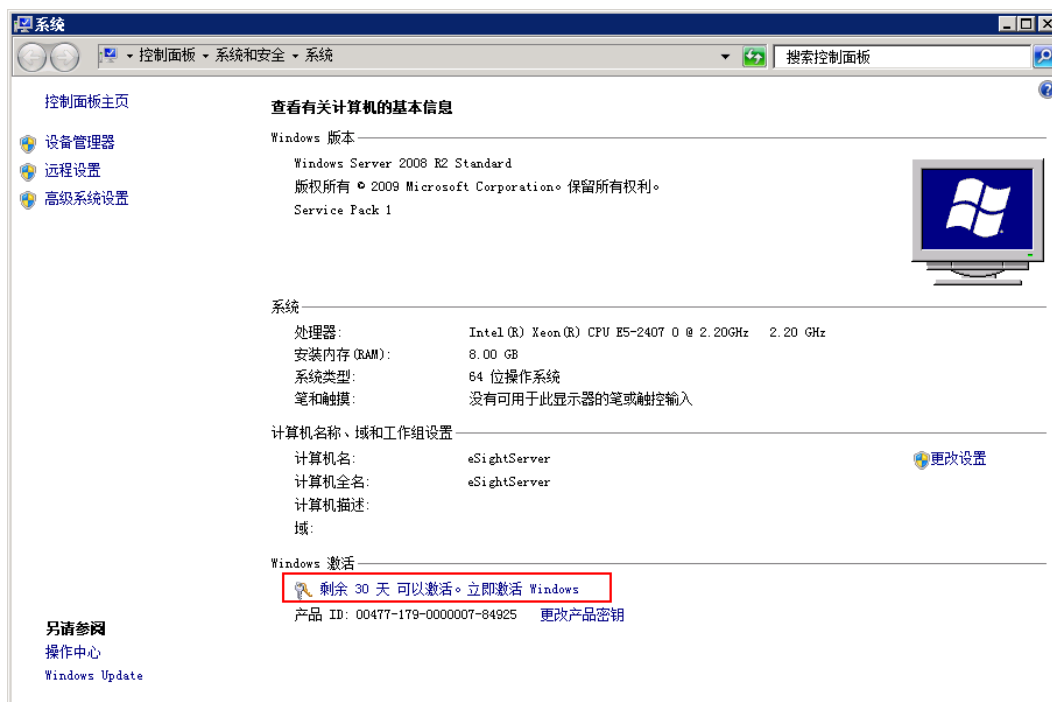
- 通过Internet进行激活
- 通过电话激活

操作步骤

步骤1 以管理员用户登录服务器。

步骤2 右键单击“计算机”，选择“属性”。

系统弹出“系统”窗口。



步骤3 单击“立即激活Windows”。

系统弹出“Windows激活”对话框。



步骤4 选择激活方式。

- 如果您通过Internet进行激活，选择“现在联机激活Windows”。
- 如果您通过电话激活，选择“显示其他激活方法”。

步骤5 输入产品密钥，单击“下一步”，根据提示，完成Windows激活。



---结束

验证激活结果

1. 右键单击“计算机”，选择“属性”。
2. 在“系统”窗口查看Window激活情况。



3.1.2 修改操作系统管理员用户 SWMaster 的密码

介绍修改操作系统管理员用户SWMaster密码的方法。

操作步骤

- 步骤1** 以SWMaster用户登录操作系统。
- 步骤2** 按“Ctrl+Alt+Delete”组合键锁定当前登录用户界面。
- 步骤3** 在弹出的对话框中单击“更改密码”。
- 步骤4** 在弹出的对话框中依次输入SWMaster用户的旧密码、新密码并再次输入新密码。
- 步骤5** 单击“确定”。

----结束

3.1.3 修改操作系统的主机名

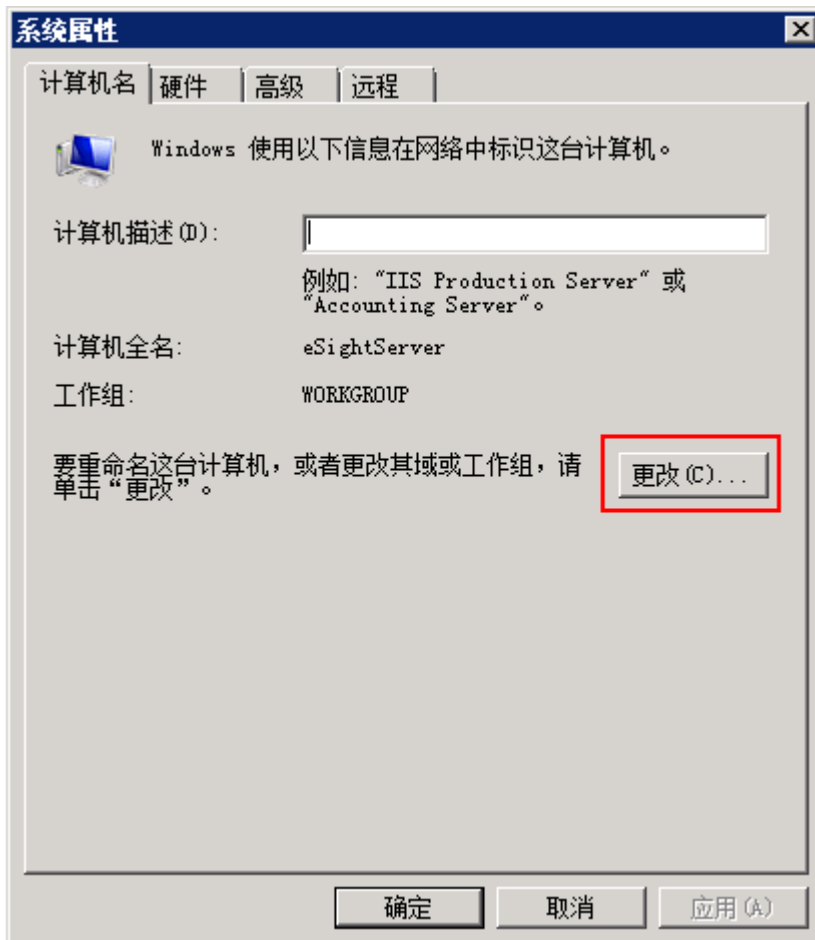
介绍修改操作系统主机名的方法。下面以Windows Server 2008 R2 Standard为例。

操作步骤

- 步骤1** 右键单击桌面上“计算机”图标，选择“属性”。
- 步骤2** 在“计算机名称、域和工作组设置”栏，单击“更改设置”。



步骤3 在“计算机名”页签中，单击“更改”。



步骤4 在弹出对话框中，修改计算机名，单击“确定”。

步骤5 重新启动Windows操作系统，完成主机名的修改。

---结束

3.1.4 修改操作系统的 IP 地址

介绍修改操作系统IP地址的方法。下面以Windows Server 2008 R2 Standard为例。

操作步骤

步骤1 选择“开始 > 控制面板”。

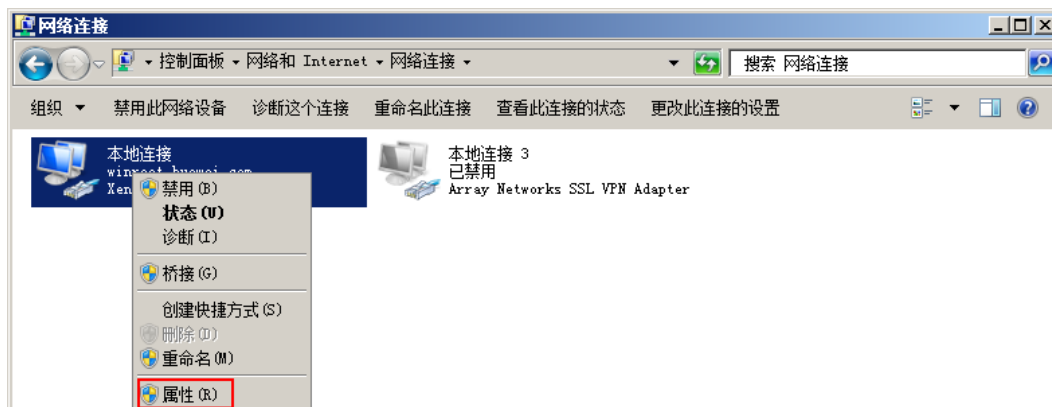
步骤2 在“控制面板”窗口中，单击“网络和共享中心”。



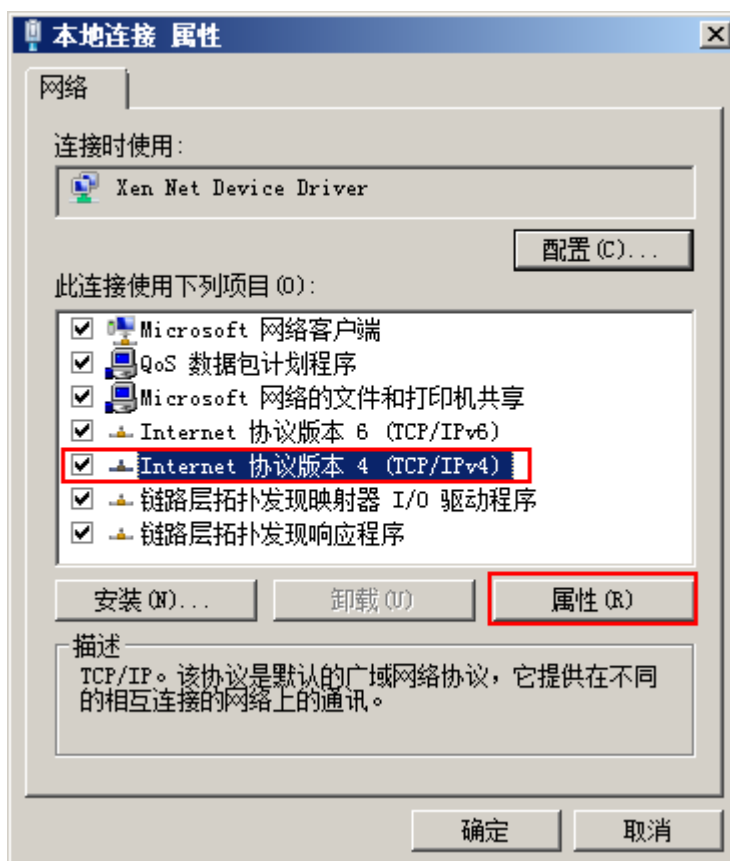
步骤3 在“网络和共享中心”对话框中，单击“更改适配器设置”。



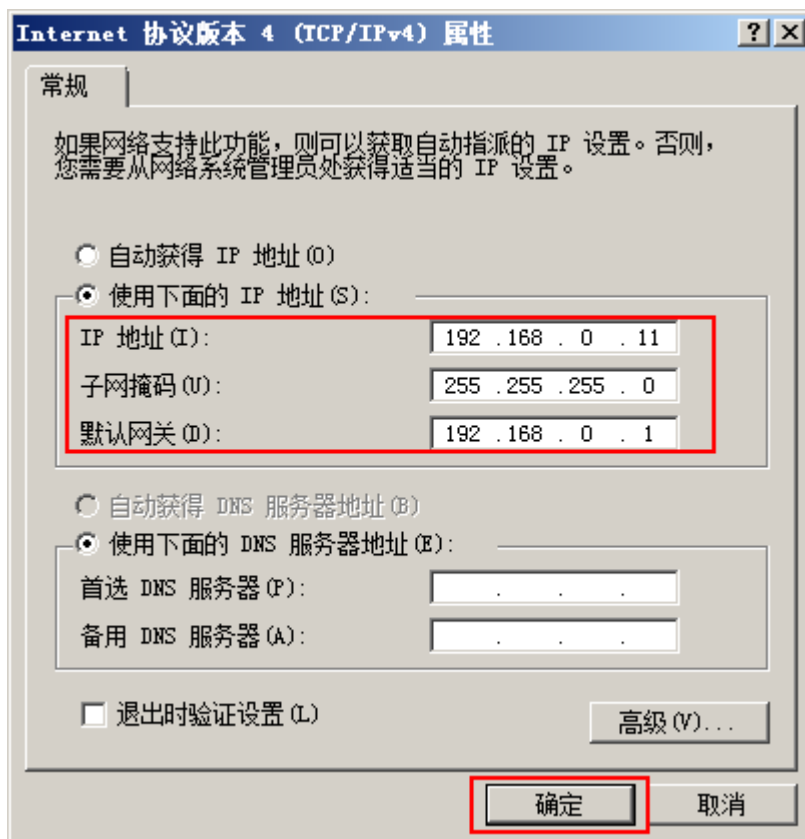
步骤4 在“网络连接”页面中，右键单击要配置的网络连接，然后单击“属性”。



步骤5 在“本地连接 属性”对话框中，单击“Internet 协议版本 4 (TCP/IPv4)”，然后单击“属性”。



步骤6 在“Internet 协议版本 4（TCP/IPv4）属性”对话框中，输入新的IP地址、子网掩码和默认网关。



步骤7 单击“确定”。

---结束

3.1.5 设置操作系统自动更新方式

为了保证操作系统能够安装最新发布的补丁，建议设置操作系统自动更新方式。

前提条件

确保硬件服务器能够连接微软官方网站或企业内部的补丁服务器。

背景信息

某些操作系统补丁在安装完成之后，需要重新操作系统才会生效。请不要选择“自动下载并推荐的更新，并安装它们”。操作系统发现长时间不重新启动，会自动重新启动以便最新的补丁生效。此时，自动重新启动操作系统会停止ATIC业务，导致网络意外中断。建议由系统管理员在业务空闲期手工开始安装补丁，并重新启动操作系统。

“下载更新，但是由我来决定什么时候安装”

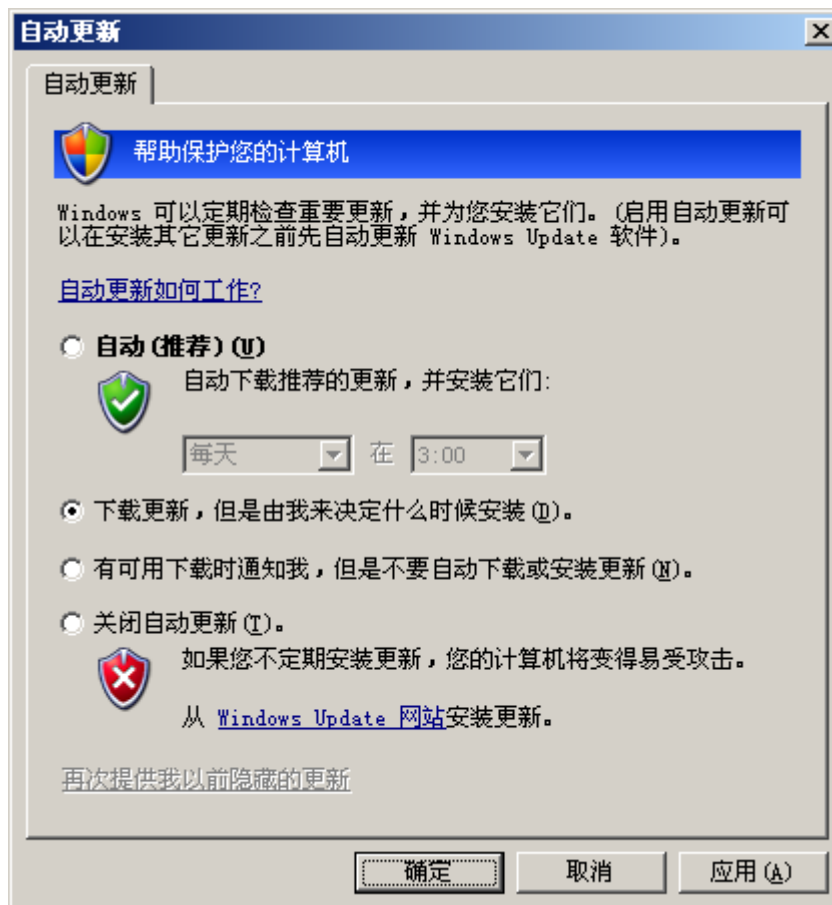
操作步骤

步骤1 以SWMaster账号登录操作系统。

步骤2 根据不同的操作系统进行设置。

- Microsoft Windows Server 2003

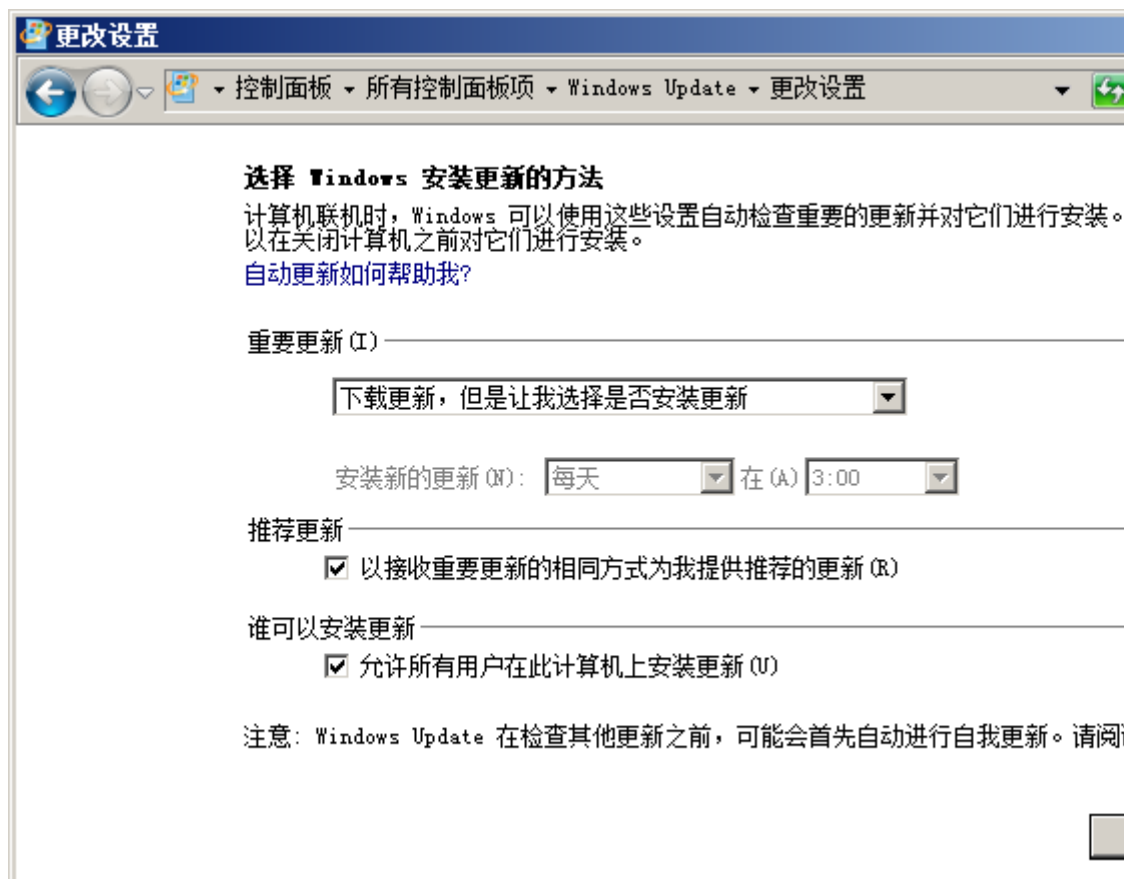
1. 选择“开始 > 控制面板 > 自动更新”。
2. 选择“下载更新，但是由我来决定什么时候安装”。



3. 单击“确定”。
收到更新通知时，请管理员选择业务空闲期安装更新并重新启动操作系统。

● Microsoft Windows Server 2008

1. 选择“开始 > 控制面板 > Windows Update”。
2. 在窗口左边单击“更改设置”。
3. 选择“下载更新，但是由我选择是否安装更新”。



- 单击“确定”。
收到更新通知时，请管理员选择业务空闲期安装更新并重新启动操作系统。

---结束

3.1.6（可选）修改操作系统的时间和时区

如果发货服务器上配置的时间和时区与实际场景有差异，为了保证您的正常使用，请与实际保持一致。本章节介绍修改操作系统时间和时区的方法。

操作步骤

- 步骤1** 选择“开始 > 控制面板”。
- 步骤2** 在“控制面板”窗口中，单击“日期和时间”。



步骤3 在弹出的对话框中单击“时间和日期”页签，设置当前系统时间和时区，单击“确定”。



---结束

4（可选）安装趋势防毒软件

关于本章

为提升Windows操作系统的安全性，需安装趋势防毒软件OfficeScan，包括安装防毒软件服务器和客户端。防毒软件服务器支持独立部署于一台服务器上，也支持和ATIC管理中心服务器同机部署。建议防毒软件服务器独立部署，ATIC管理中心服务器作为防毒软件服务器的客户端，以降低对ATIC管理中心运行性能的影响。

4.1 申请防毒软件License

在趋势防毒软件安装过程中需要使用到趋势防毒软件的License。

4.2 安装防毒软件服务器

防毒软件服务器能够自动从趋势科技官方网站更新防病毒组件，并为杀毒软件客户端提供防病毒组件更新源。

4.3 安装防毒软件客户端

趋势防毒软件客户端用于保护操作系统免受病毒侵害，提高安全性。

4.4 防病毒检查

使用EICAR测试脚本测试防毒墙网络版。EICAR是专用于测试的病毒，不具备真正病毒的传播性和破坏性。

4.5 更新防病毒组件

通过配置防毒软件服务器和客户端的更新源并预设更新周期，可以令防毒软件自动更新防病毒组件，使防毒能力保持最新状态。

4.1 申请防毒软件 License

在趋势防毒软件安装过程中需要使用到趋势防毒软件的License。

操作步骤

步骤1 请联系当地技术支持工程师申请趋势防病毒软件License。

技术支持工程师收到您的请求后会立即处理，并将License发给您。请您将License文件妥善保存，以备安装时使用。

---结束

4.2 安装防毒软件服务器

防毒软件服务器能够自动从趋势科技官方网站更新防病毒组件，并为杀毒软件客户端提供防病毒组件更新源。

4.2.1 安装步骤

介绍趋势防毒软件服务器安装步骤。

背景信息

本章节以在Windows Server 2003环境下安装趋势防毒软件服务器为例介绍安装过程，如果在Windows Server 2008系统上安装，可能会有部分界面差异，请根据实际情况进行安装。

操作步骤

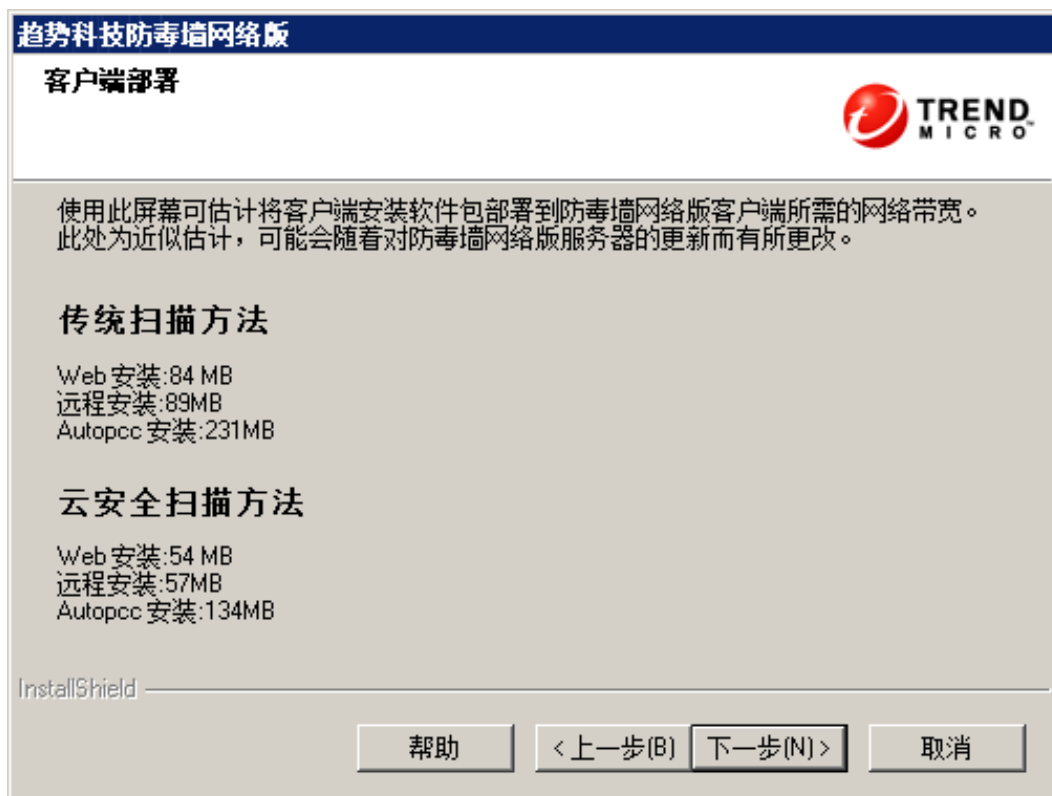
步骤1 运行安装光盘或安装软件包中的“Trend_OfficeScan\OfficeScan_CN\OSCE_10.5_B1103_SC_GM.exe”，启动安装程序。



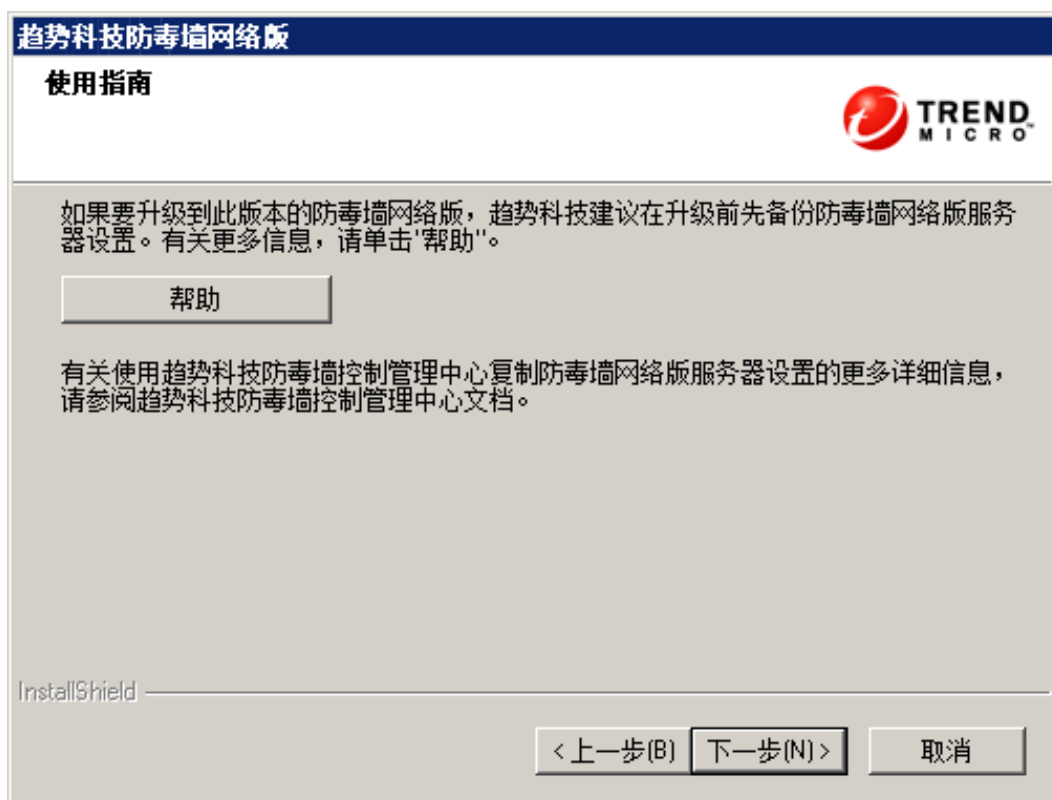
单击“下一步”。

步骤2 选择“我接受许可证协议中的条款”，单击“下一步”。

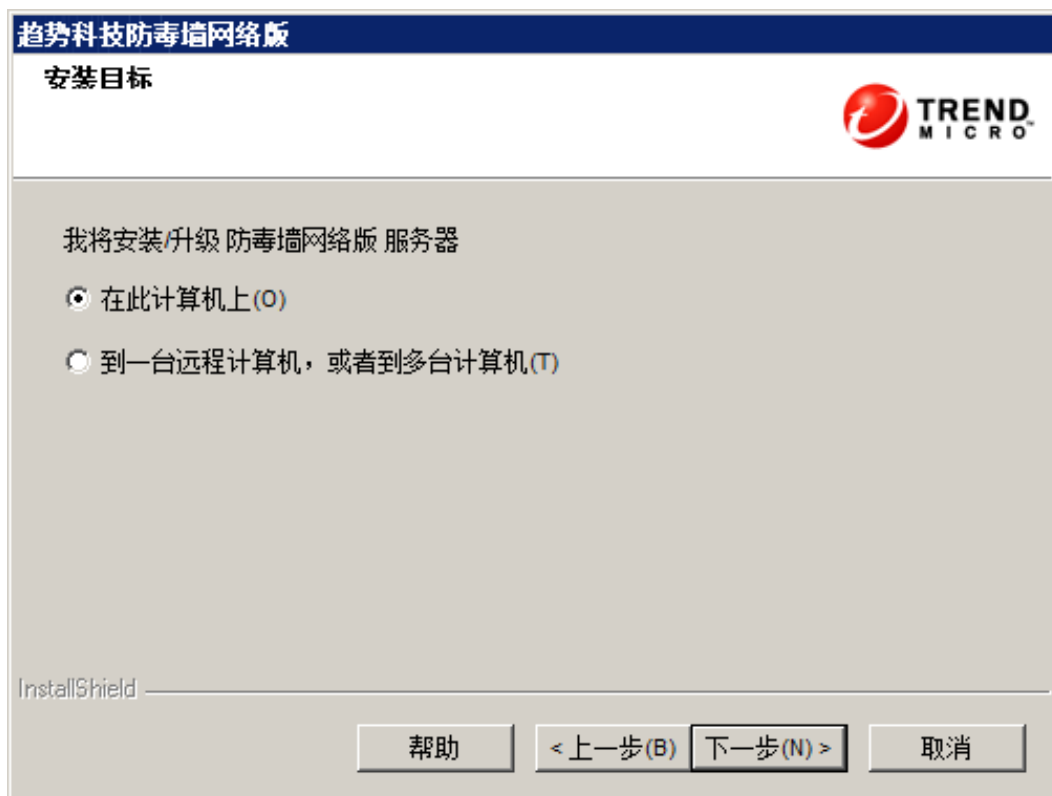
步骤3 弹出“客户端部署”界面，单击“下一步”。



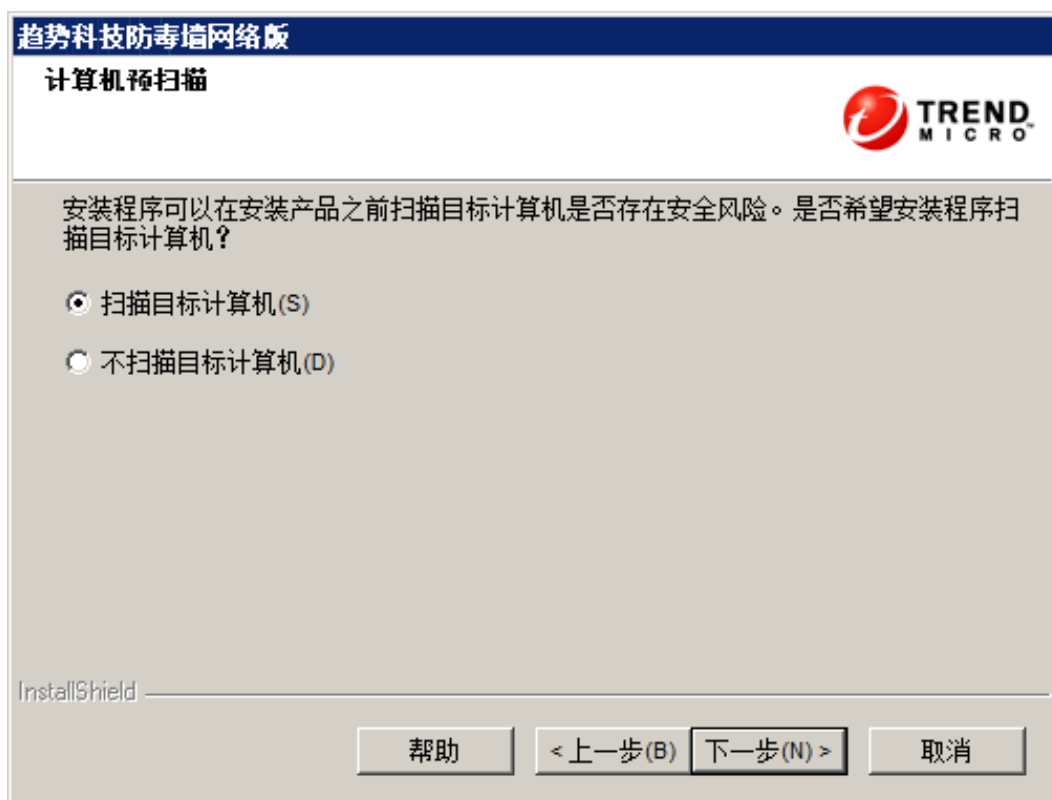
步骤4 弹出“使用指南”界面，单击“下一步”。



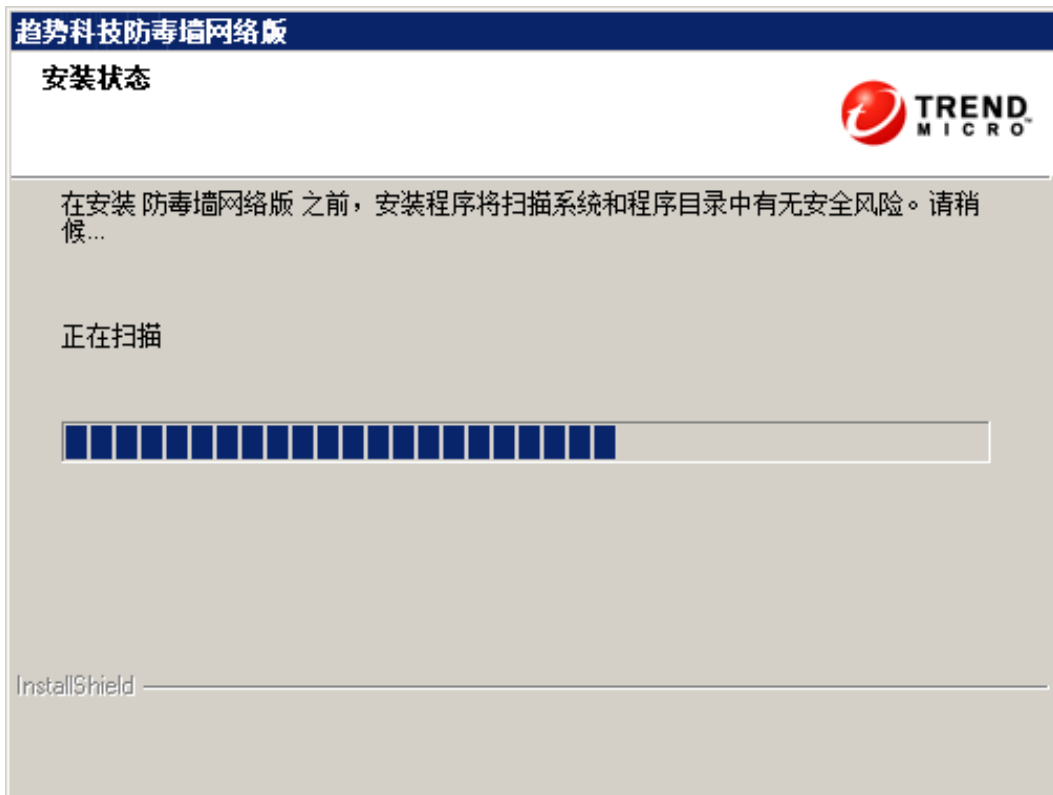
步骤5 弹出“安装目标”界面，选择“在此计算机上”，单击“下一步”。



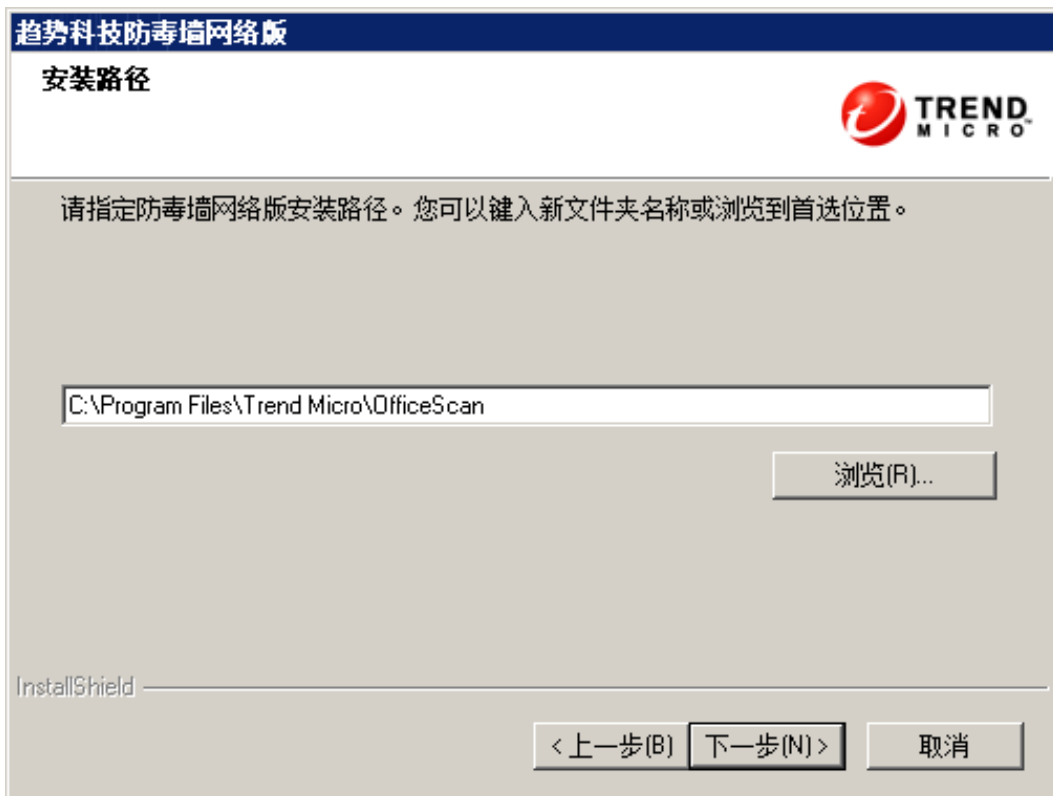
步骤6 弹出“计算机预扫描”界面，选择“扫描目标计算机”，单击“下一步”。



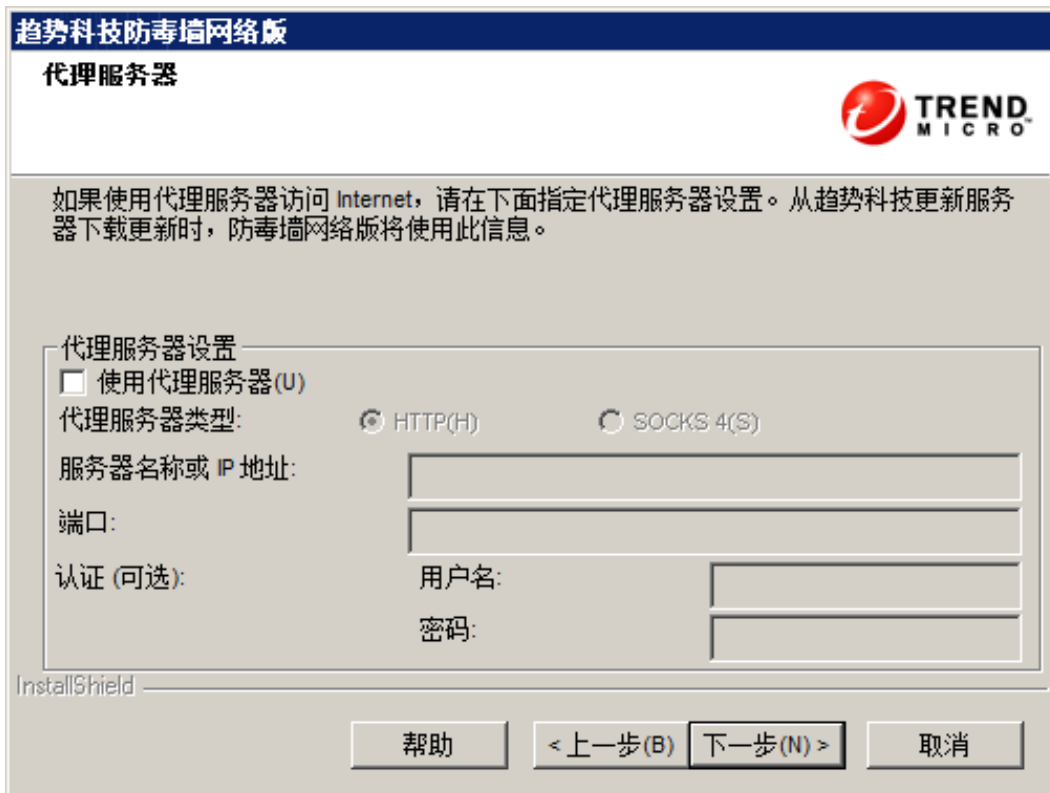
步骤7 弹出“安装状态”界面，请等待。



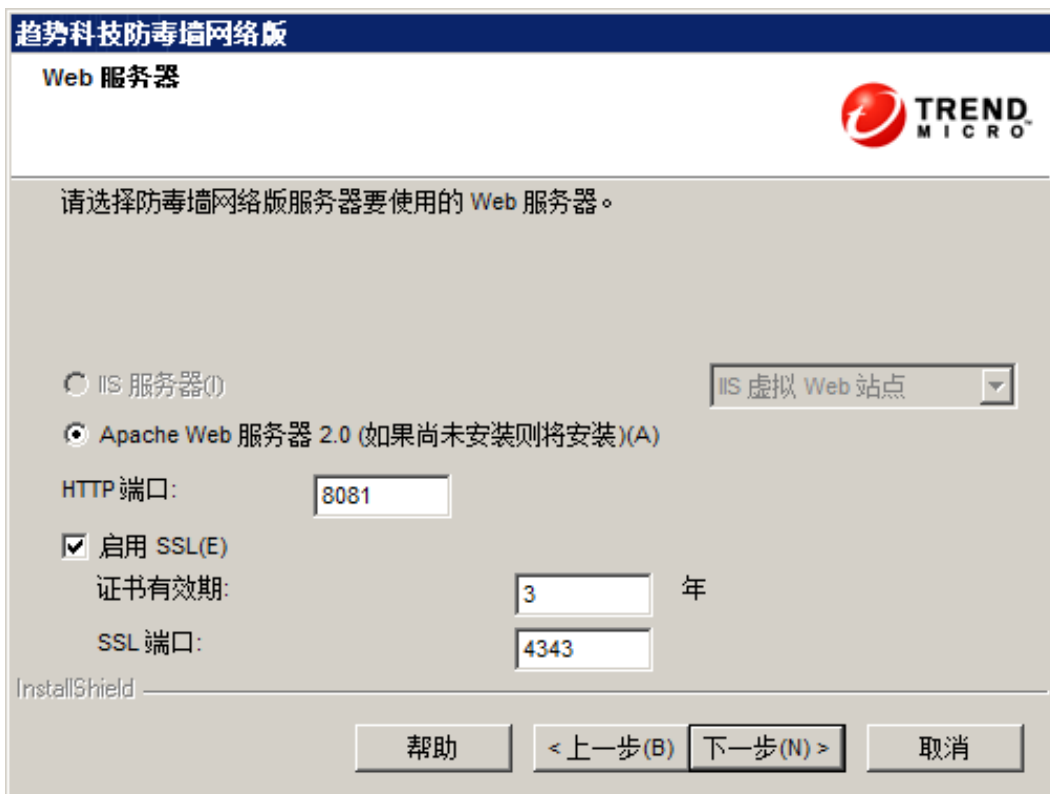
步骤8 弹出“安装路径”界面，请选择安装路径。建议选择默认安装路径“C:\Program Files\Trend Micro\OfficeScan”，单击“下一步”。



步骤9 弹出“代理服务器”界面，单击“下一步”。



步骤10 弹出“Web服务器”界面，选择“Apache Web服务器2.0”，并设置HTTP端口为“8081”。SSL证书参数使用默认值。单击“下一步”。



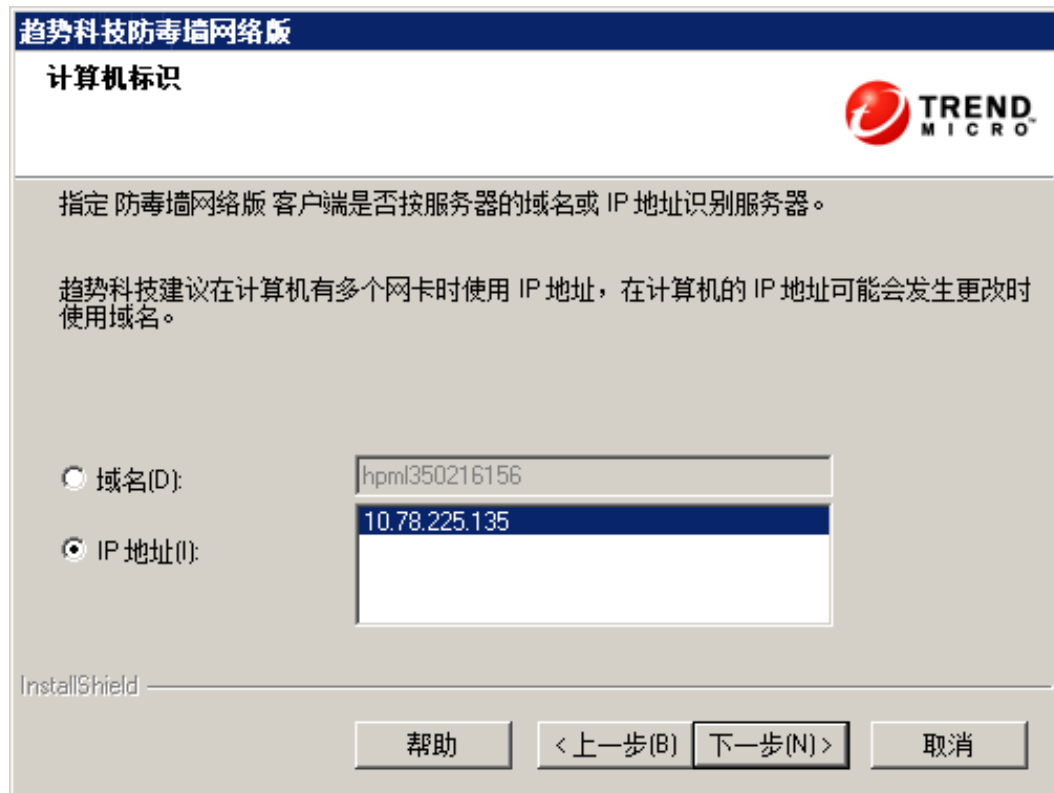


ATIC管理服务器的默认HTTP和SSL端口分别为8080和443，为避免端口冲突，请安装防病毒软件时选择其他端口号，如上图所示。

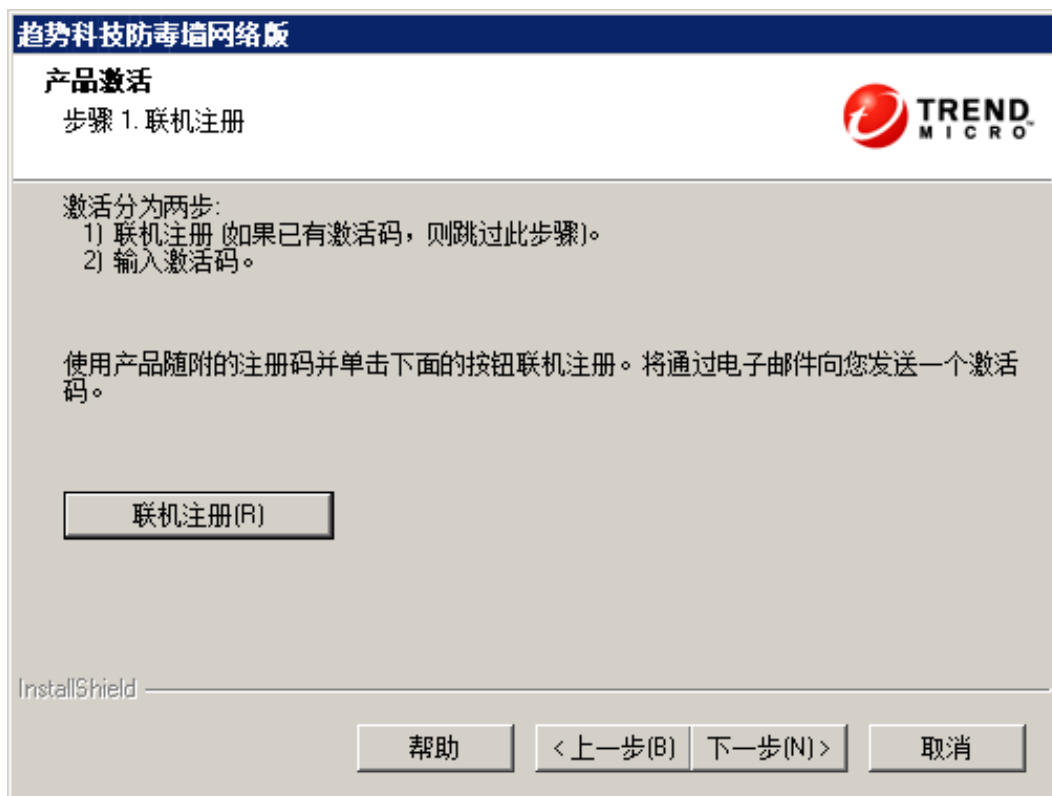
步骤11 弹出“计算机标识”界面，建议选择“IP地址”，指定IP地址后，单击“下一步”。



当服务器存在多个IP地址时，选择可以正常对外通信的IP地址。



步骤12 弹出“产品激活 步骤1.联机注册”界面，单击“下一步”。



步骤13 弹出“产品激活 步骤2.输入激活码”界面，输入激活码，单击“下一步”。

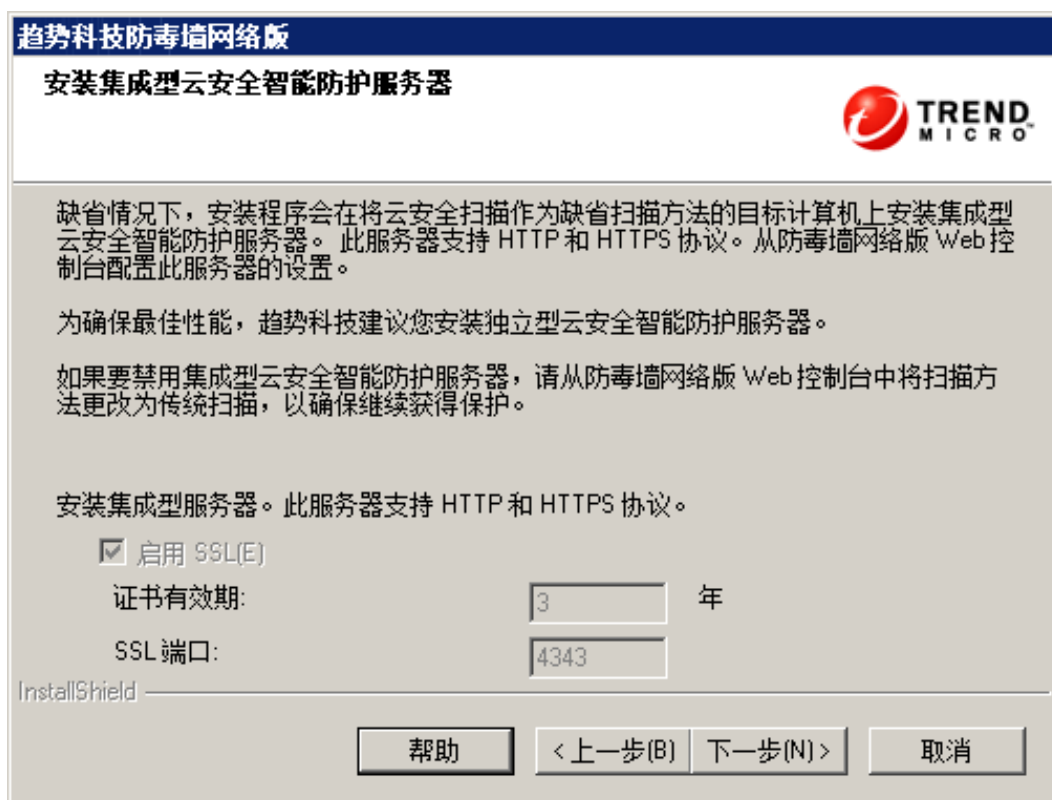
 **说明**

利用趋势防毒软件的License的序列号在华为Support网站: <http://support.huawei.com/support/>申请激活码。

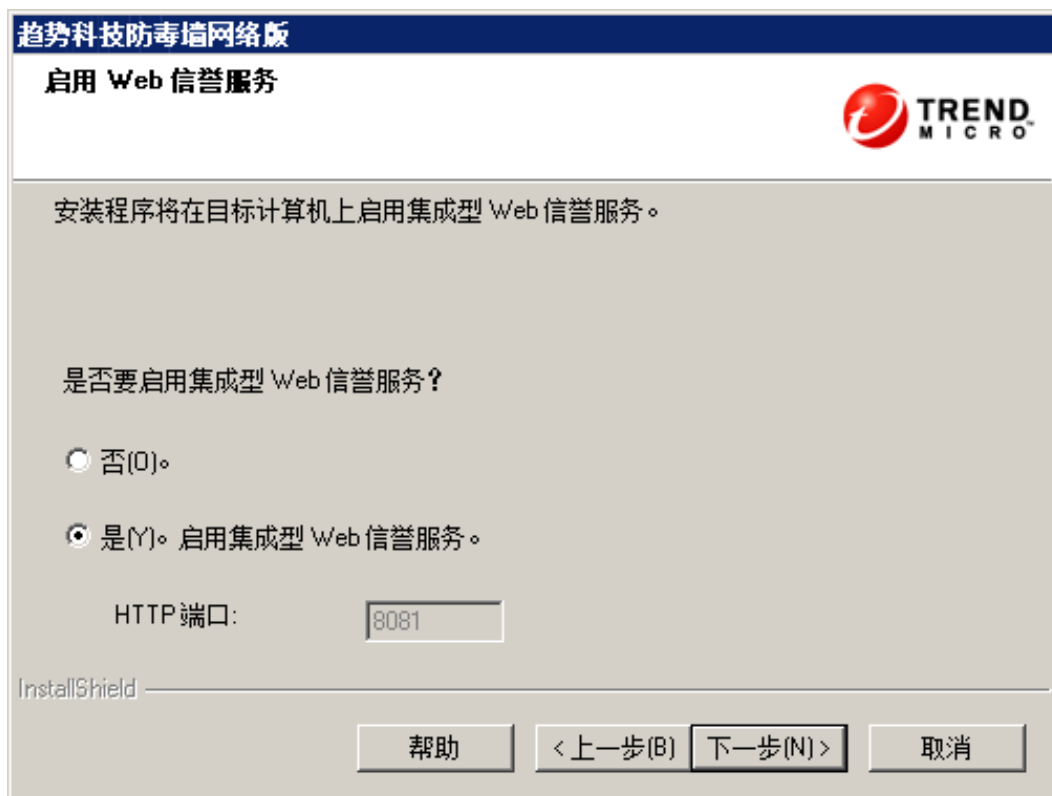
登录网站后，在“软件中心 > 软件License > 外购License > License申请”链接中提交申请后获取。



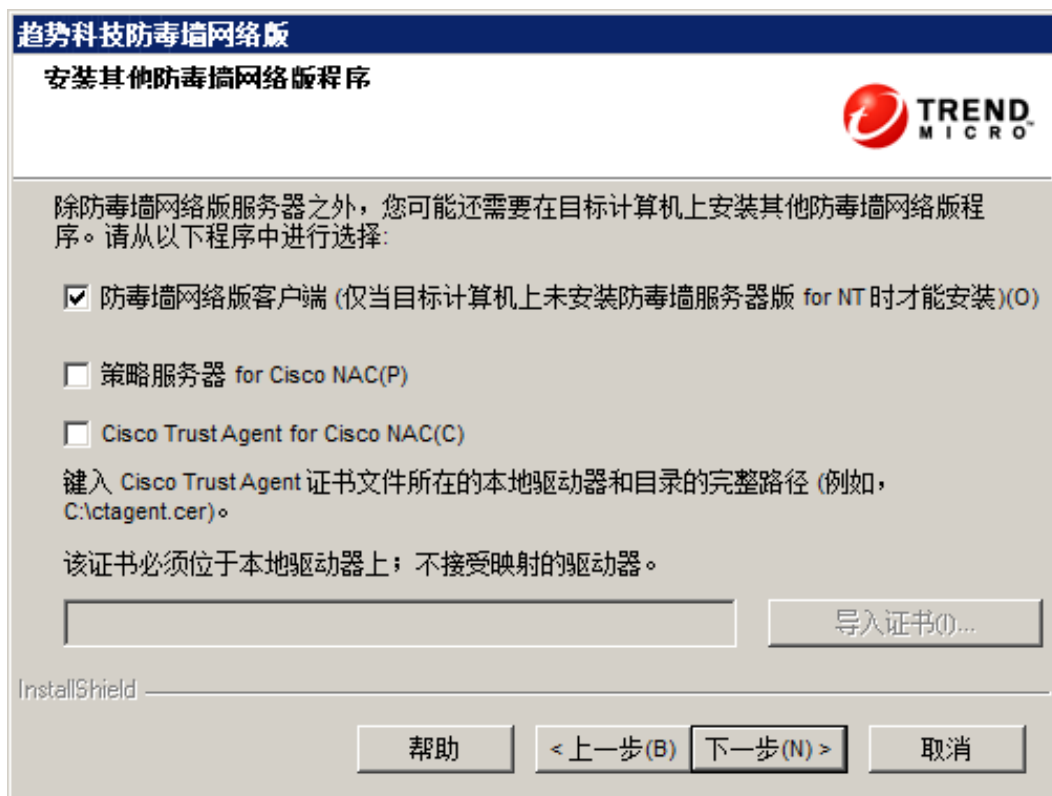
步骤14 弹出“安装集成型云安全智能防护服务器”界面，单击“下一步”。



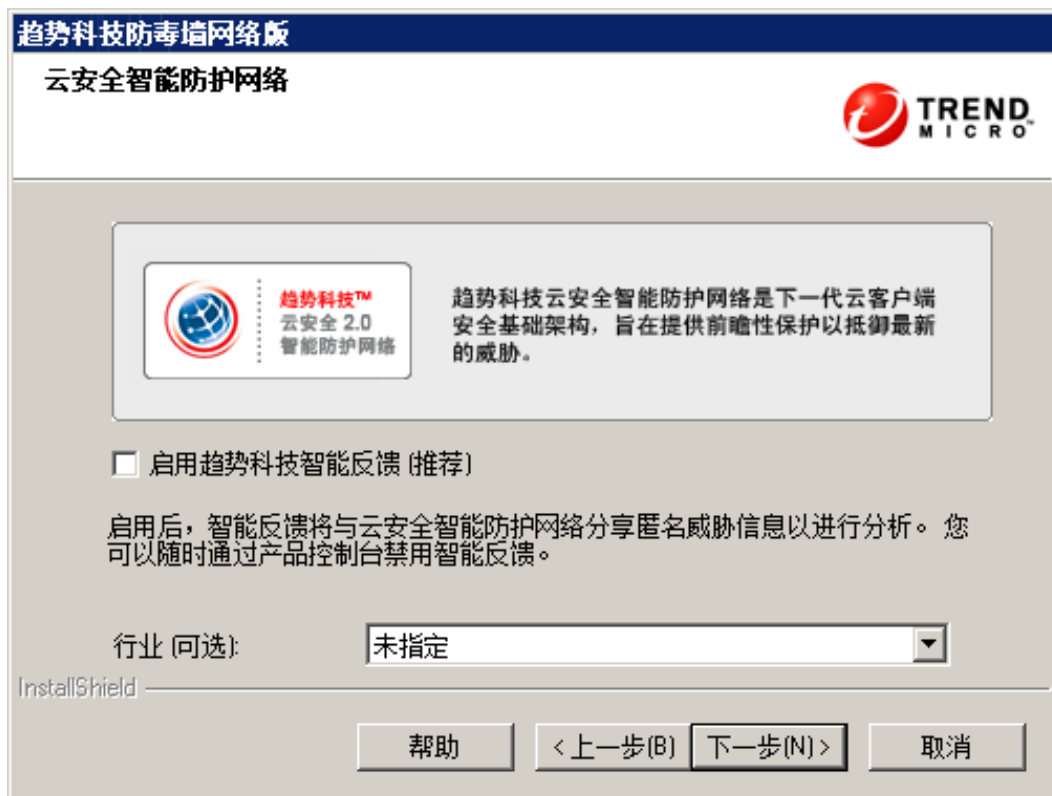
步骤15 弹出“启用Web信誉服务”界面，选择“是”，单击“下一步”。



步骤16 弹出“安装其他防毒墙网络版程序”界面，选择“防毒墙网络版客户端”，单击“下一步”。



步骤17 弹出“云安全智能防护网络”界面，去勾选“启用趋势科技智能反馈”，单击“下一步”。



步骤18 弹出“管理员帐户密码”界面，设置Web控制台密码和客户端退出与卸载密码。单击“下一步”。

Web控制台密码为进入Web控制台的密码，客户端退出与卸载密码为退出或卸载客户端时使用的密码。

说明

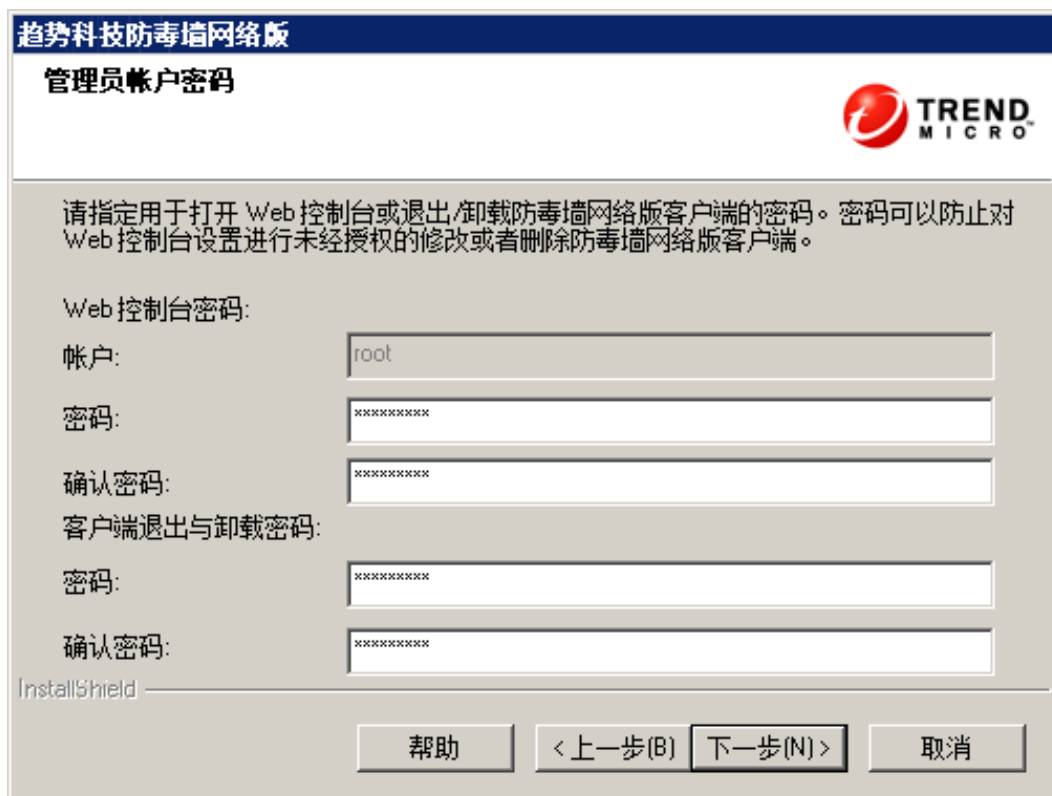
建议密码满足如下条件，如设置缺省值Changeme_123。

- 长度至少8个字符，最大为30个字符。
- 密码必须包含如下四种字符的组合：
 - 至少一个小写字母。
 - 至少一个大写字母。
 - 至少一个数字。
 - 至少一个特殊字符：~@#^*0-_{|}:/?>

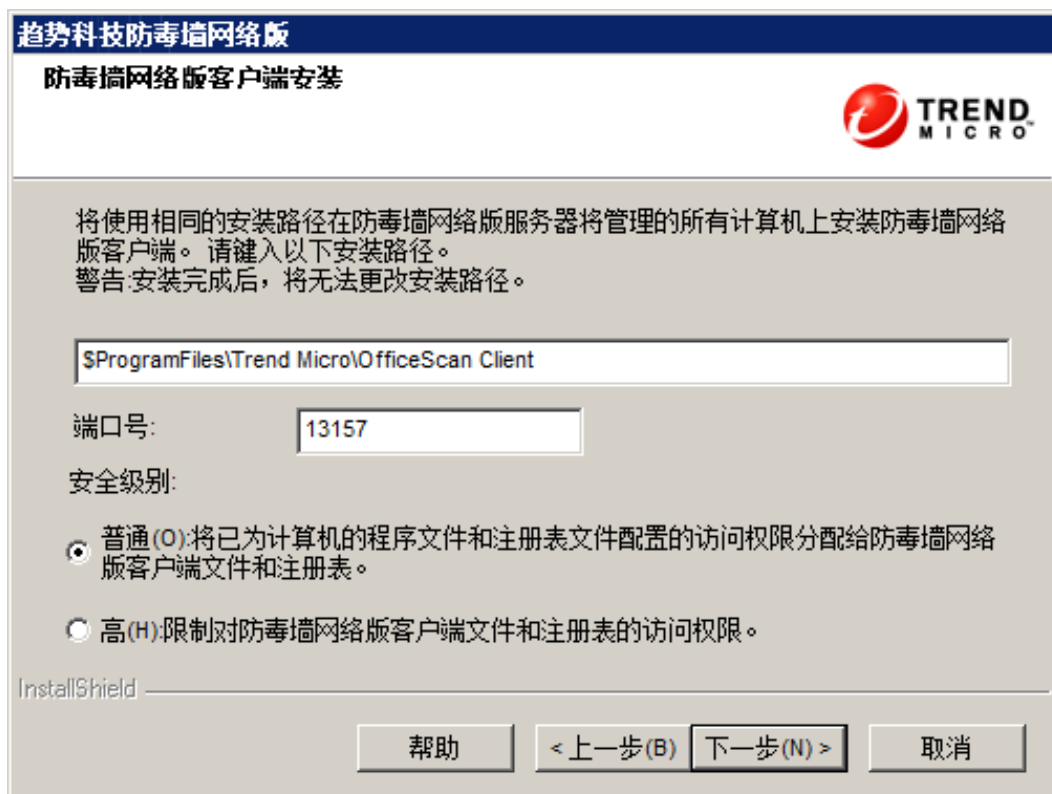
不支持其他特殊字符，请不要尝试使用其他特殊字符作为部分密码信息，例如<>&'!\$"%'=',及空格等。

为保证系统安全，请及时修改密码，定期更新并妥善保管密码。修改方法如下：

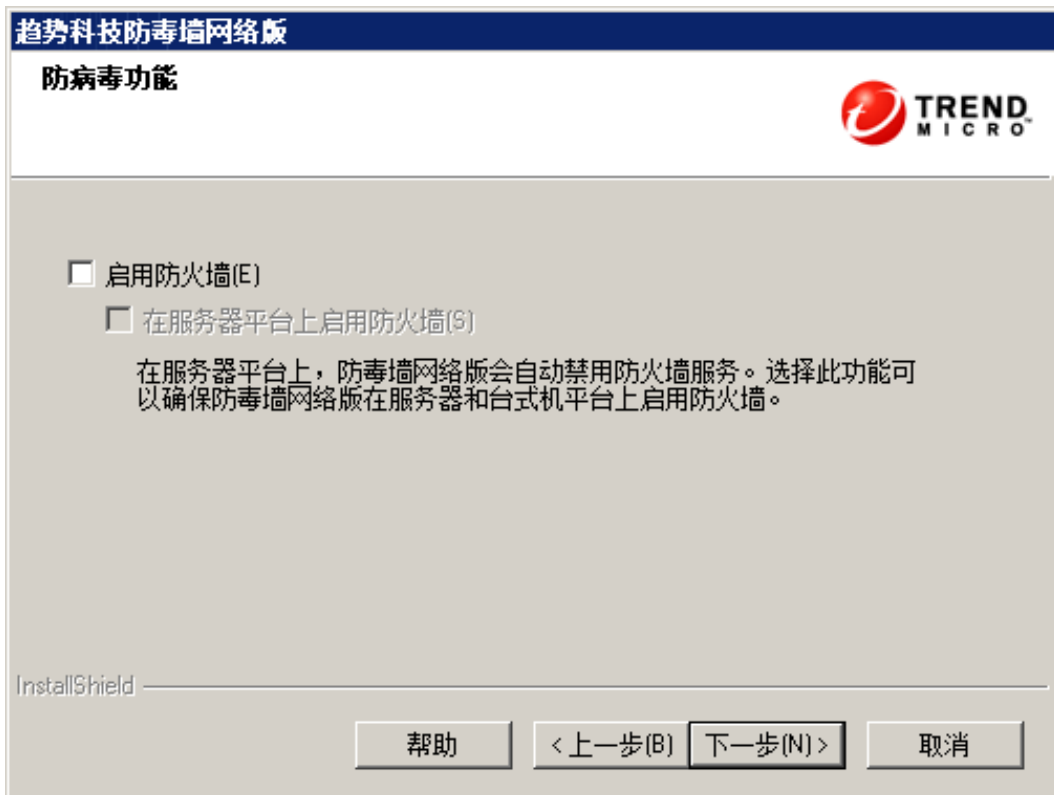
1. 登录趋势Web控制台。
2. 选择“管理>用户帐户”。
3. 可以在右侧窗口更新用户密码。



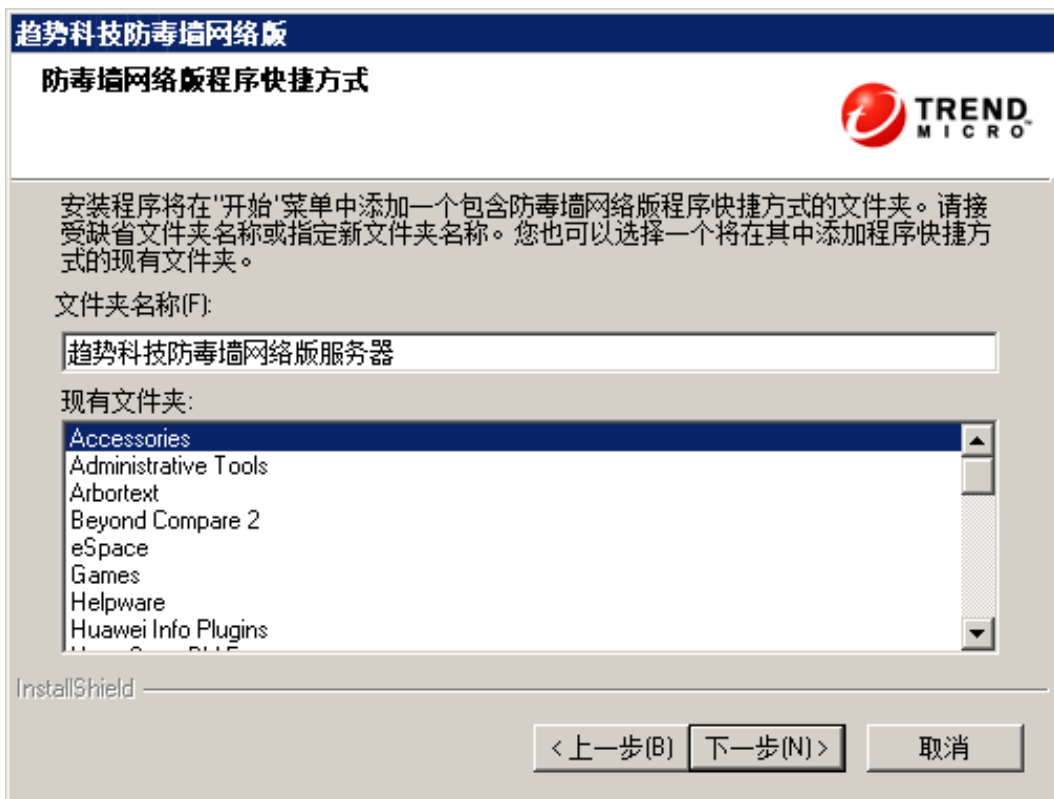
步骤19 弹出“防毒墙网络版客户端安装”界面，为确保网络端口不冲突，请设置“端口号”为“13157”，安全级别选择“普通”。单击“下一步”。



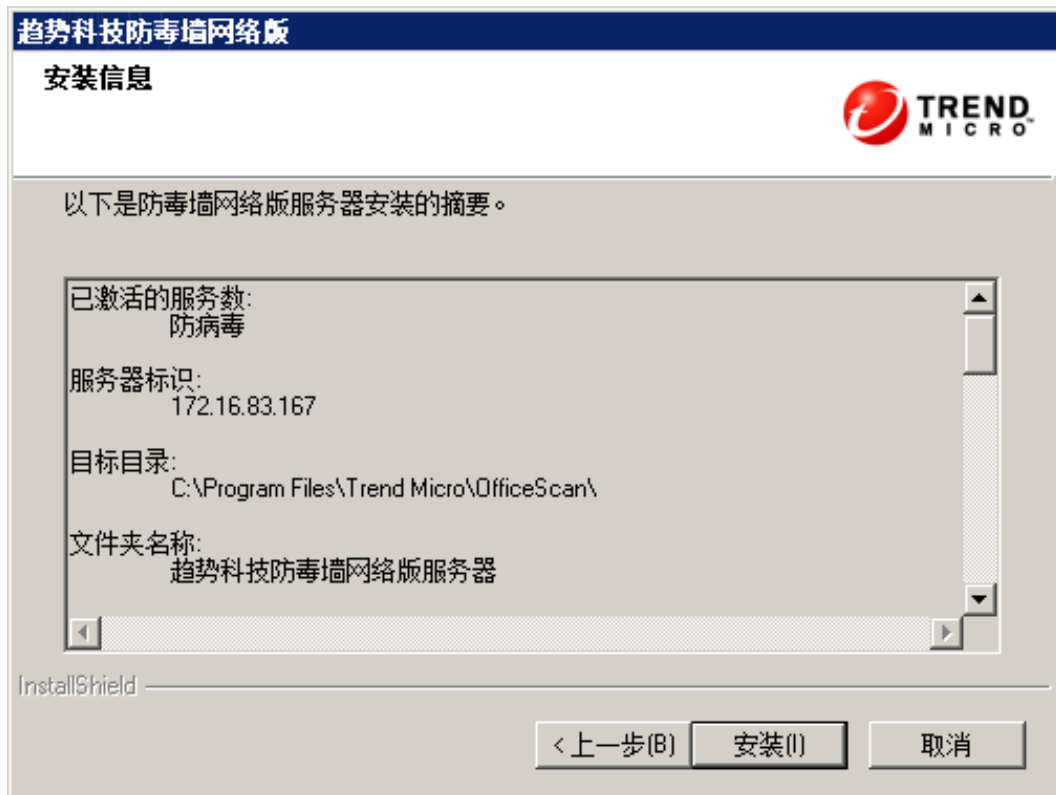
步骤20 弹出“防病毒功能”界面，去勾选“启用防火墙”，单击“下一步”。



步骤21 弹出“防毒墙网络版程序快捷方式”界面，单击“下一步”。



步骤22 弹出“安装信息”界面，确认安装信息，单击“安装”。



步骤23 安装完成后，弹出“安装完毕”界面，单击“完成”。

如果安装失败，请联系技术支持工程师。



---结束

4.2.2 验证安装正确性

介绍如何检查服务器端是否安装正确。

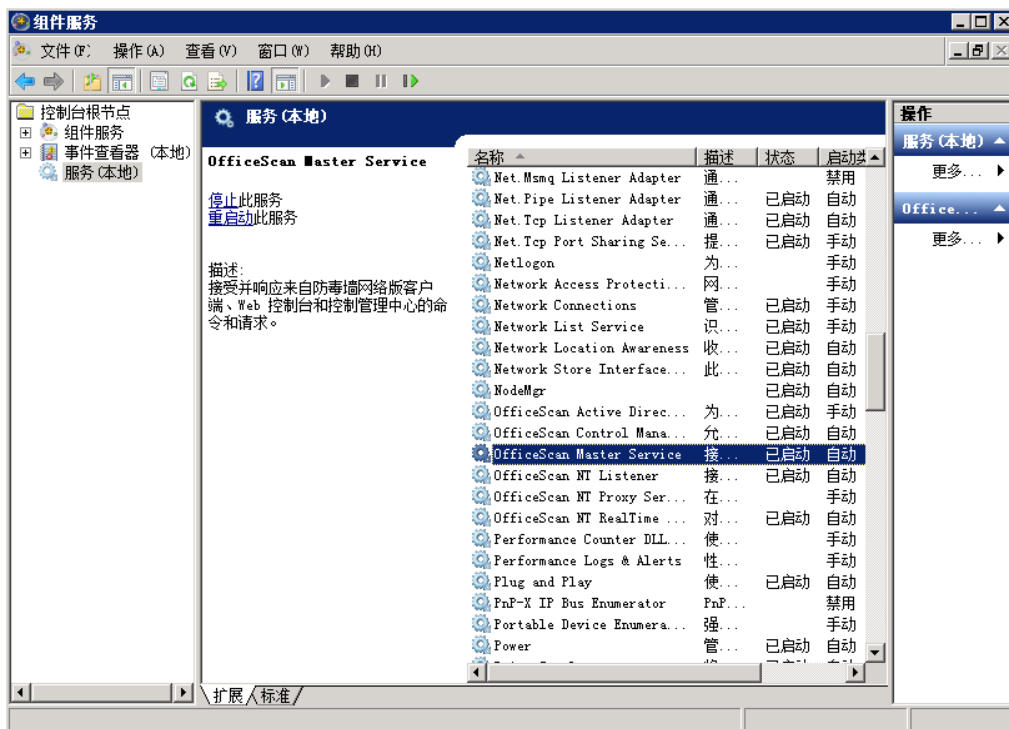
操作步骤

步骤1 查看服务列表。

选择“开始 > 所有程序 > 管理工具 > 组件服务”，单击“服务（本地）”，检查“OfficeScan Master Service”和“OfficeScan Constrol Manager Agent”两服务状态是否为“已启动”，启动类型是否为“自动”。

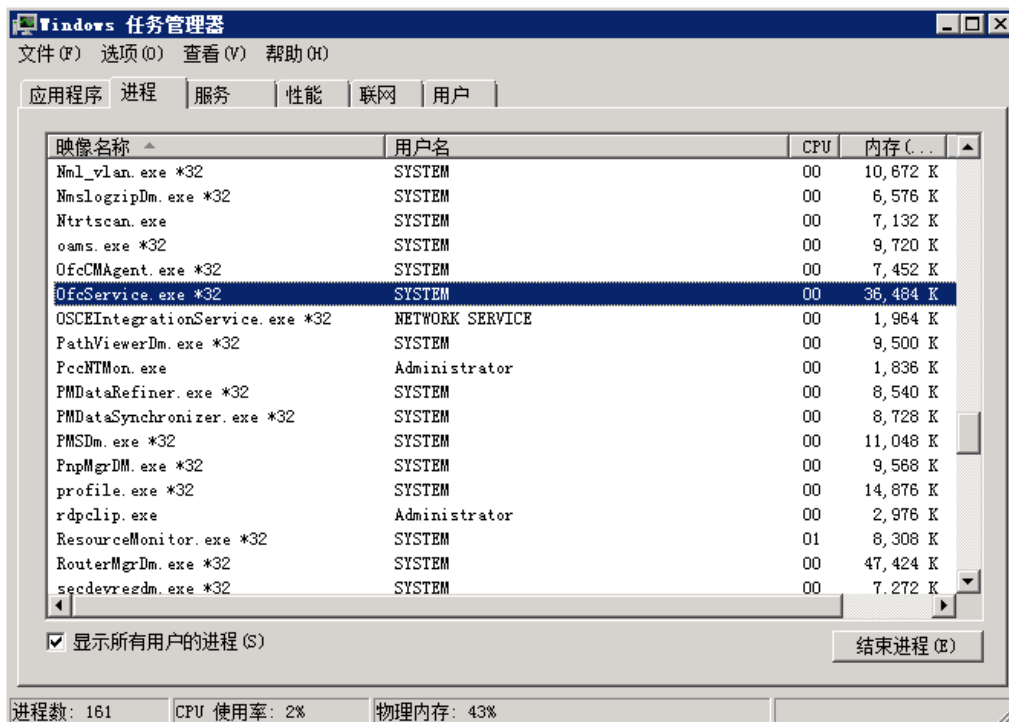
如果服务未处于“已启动”状态，在该服务上单击右键，选择“启动”。

如果服务启动类型不是“自动”状态，在该服务上单击右键，选择“属性”。在“常规”页签内，将“启动类型”修改为“自动”。



步骤2 查看系统进程。

打开Windows任务管理器，查看是否存在“OfcService.exe”进程。

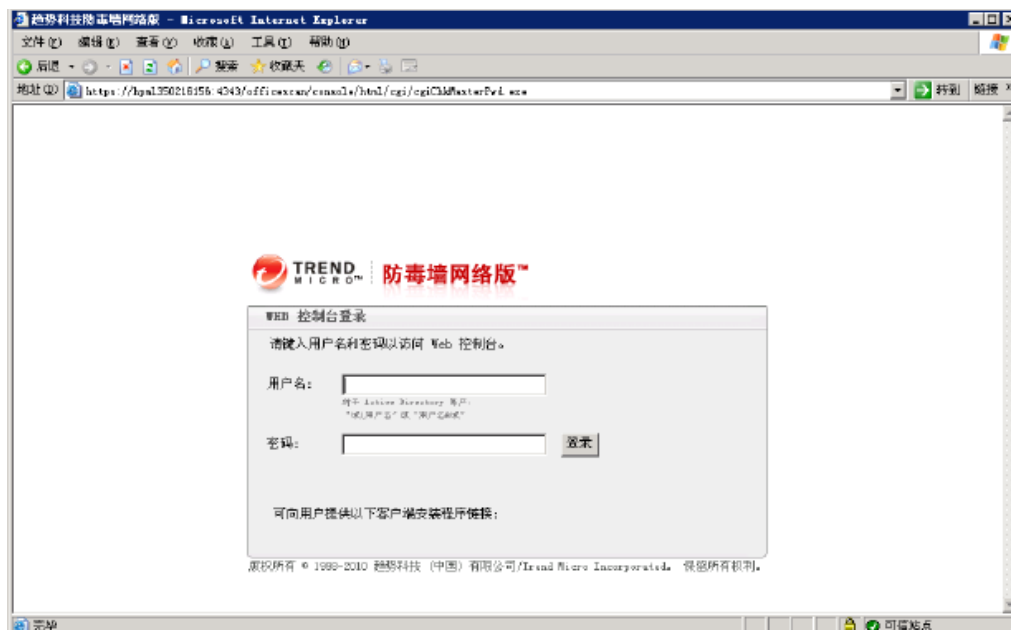


步骤3 登录Web控制台。

选择“开始 > 所有程序 > 趋势科技防毒墙网络版服务器 > 防毒墙网络版Web控制台 (HTML)”，弹出“趋势科技防毒墙网络版”界面。

说明

- 如果弹出安全证书问题，请单击“继续浏览此网站”，单击“确定”。
- 如果弹出关于安装证书的“安全警报”对话框，单击“确定”，继续安装。
- 若弹出提示是否添加可信站点，请单击“添加”，弹出“可信站点”对话框，继续单击“添加”后关闭该窗口。
- 如果有安装ActiveX控件提示，单击“安装”，安装ActiveX控件。
- 如果有下载ActiveX控件下载失败的提示，在IE中选择“工具 > Internet选项”，单击“安全”页签，单击“可信站点”后选择“站点”按钮，弹出“可信任站点”对话框，将趋势服务器的登录站点添加到可信站点。



输入默认用户名**root**和在安装过程中设置的**root**用户的密码，检查是否可以正常登录。

----结束

4.3 安装防毒软件客户端

趋势防毒软件客户端用于保护操作系统免受病毒侵害，提高安全性。

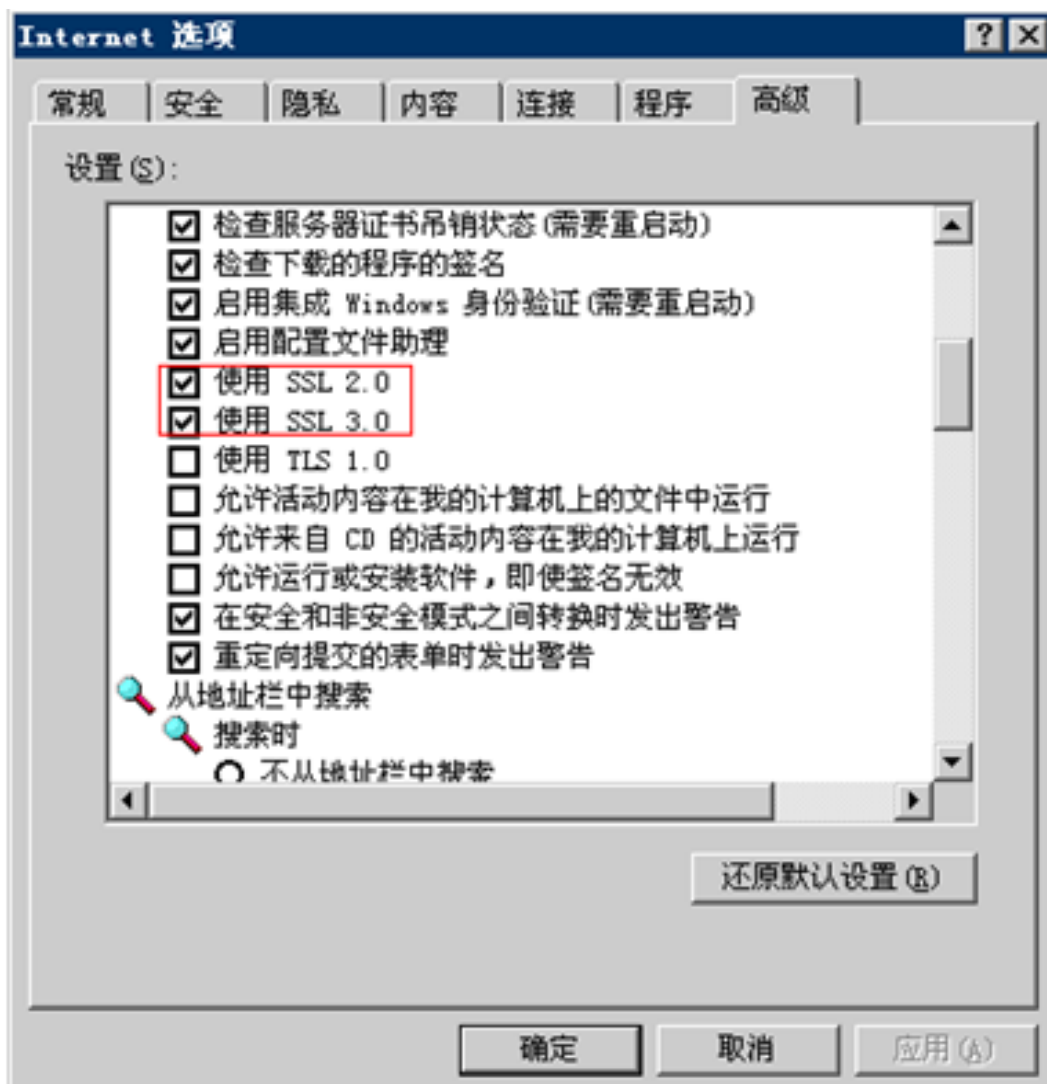
4.3.1 安装步骤

有多种安装趋势防毒软件客户端的方法，Web安装是最简便的一种安装方式。

操作步骤

步骤1 检查客户端的IE浏览器是否安装了安全协议SSL。

在IE浏览器中单击“工具 > Internet选项 > 高级”，检查是否选择“使用SSL 2.0”或者“使用SSL 3.0”，如果已经选择了，就已经安装了安全协议SSL；否则没有安装安全协议SSL。



步骤2 登录趋势服务器。

- 安装了安全协议SSL，趋势服务器的登录地址是（更安全）：**https://防毒墙服务器的IP地址:4343/officescan/console/html/ClientInstall/**。
- 没有安装安全协议SSL，趋势服务器的登录地址是：**http://防毒墙服务器的IP地址:8081/officescan/console/html/ClientInstall/**。

步骤3 单击“立即安装”，开始安装趋势防毒软件客户端程序。

说明

- 如果弹出安全证书问题，请单击“继续浏览此网站”，单击“确定”。
- 如果弹出关于安装证书的“安全警报”对话框，单击“确定”，继续安装。
- 若弹出提示是否添加可信站点，请单击“添加”，弹出“可信站点”对话框，继续单击“添加”后关闭该窗口。
- 如果有安装ActiveX控件提示，单击“安装”，安装ActiveX控件。
- 如果有下载ActiveX控件下载失败的提示，在IE中选择“工具>Internet选项”，单击“安全”页签，单击“可信站点”后选择“站点”按钮，弹出“可信任站点”对话框，将趋势服务器的登录站点添加到可信站点。



步骤4 安装完成后，关闭窗口以结束安装程序。

如果安装失败，请联系技术支持工程师。




步骤5 重启Windows操作系统。

---结束

4.3.2 验证安装正确性

客户端检查目的是验证趋势客户端安装是否成功。

操作步骤

步骤1 选择“开始>所有程序>趋势科技防毒墙网络版客户端>防毒墙网络版客户端”，弹出趋势防毒软件客户端主界面并且桌面右下角出现趋势防毒软件图标.

步骤2 选择“开始>所有程序>管理工具>组件服务>服务(本地)”，查看服务列表（以Windows 2003为例）。

服务列表中应存在如下服务：

- OfficeScan NT Listener
- OfficeScan NT Proxy Service
- OfficeScan NT RealTime Scan

其中OfficeScan NT Listener和OfficeScan NT RealTime Scan已修改为自动启动。

步骤3 在任务管理器中，新增加了系统进程PccNTMon。

----结束

4.4 防病毒检查

使用EICAR测试脚本测试防毒墙网络版。EICAR是专用于测试的病毒，不具备真正病毒的传播性和破坏性。

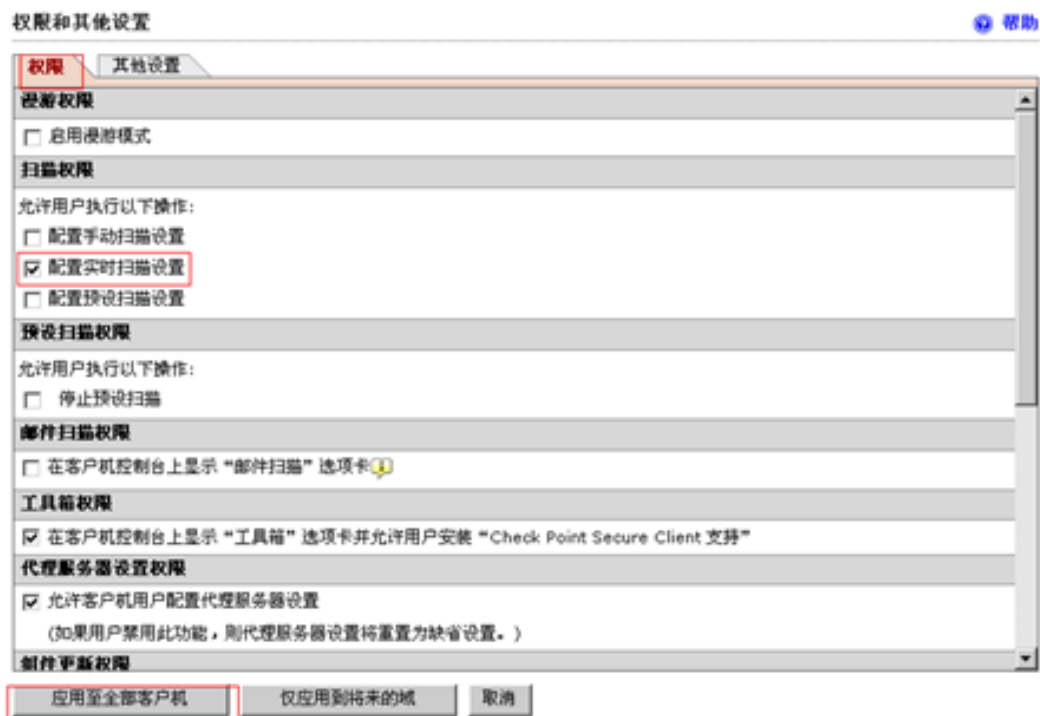
操作步骤

步骤1 启用客户机实时扫描。

1. 登录趋势服务器控制台。
2. 选择“联网计算机 > 客户机管理 > 设置 > 权限和其他设置”，弹出“权限和其他设置”对话框。



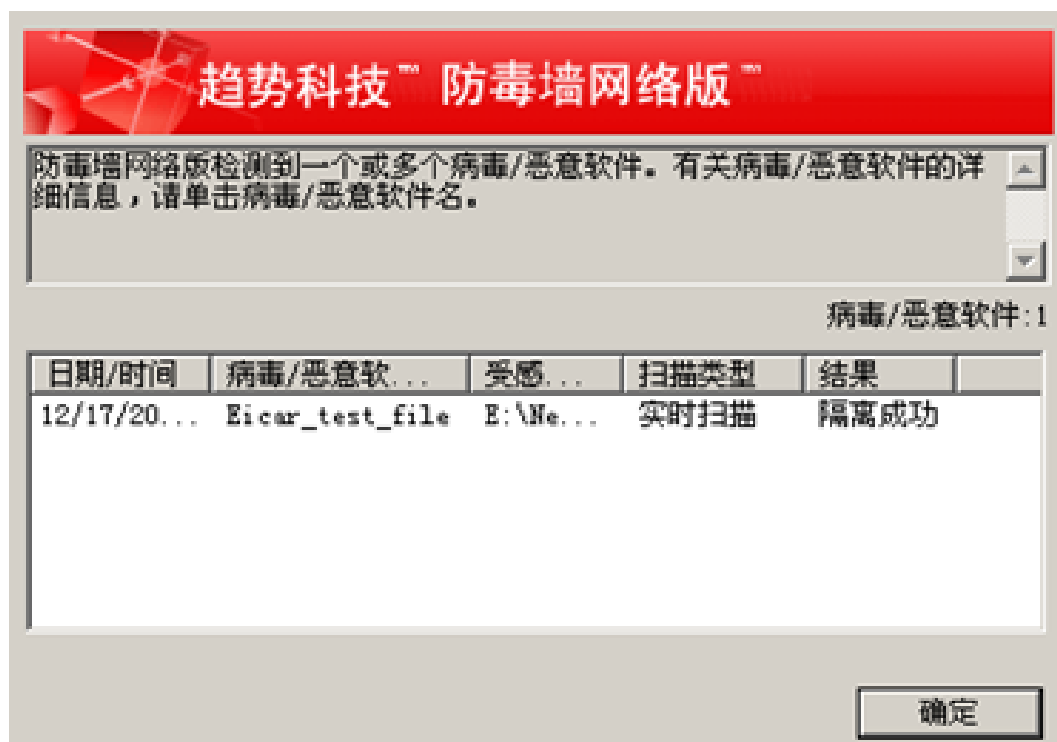
3. 选择“权限 > 配置实时扫描设置 > 应用至全部客户机”，启用客户机的实时扫描功能。



步骤2 将以下字符串X50!P%@AP[4PZX54(P^)7CC)7}SEICAR-STANDARD-ANTIVIRUS-TEST-FILE!SH+H*复制、粘贴到记事本或任何纯文本编辑器。

将该文件另存为EICAR.com，存放到一个临时目录。

防毒墙网络版应当立即检测到该文件。



---结束

4.5 更新防病毒组件

通过配置防毒软件服务器和客户端的更新源并预设更新周期，可以令防毒软件自动更新防病毒组件，使防毒能力保持最新状态。

背景信息

趋势防毒软件分为防毒软件服务器和客户端两部分。防毒软件服务器用于获取病毒码和各防病毒组件的更新，并通知下发给各客户端，以便客户端为操作系统提供最新的实时病毒防护。在更新防毒软件服务器和客户端的防病毒组件之前，要分别为他们配置更新源。

防毒软件服务器和客户端的更新可分为自动更新和手动更新两种。自动更新用于日常更新，手动更新用于特殊情况，例如在病毒爆发时，需要进行手动更新。在更新防毒软件客户端之前，需要先更新服务器的防病毒组件。

操作步骤

步骤1 登录防毒软件服务器的Web控制台。

1. 在防毒软件服务器所在系统中选择“开始>所有程序>趋势科技防毒墙网络版服务器>防毒墙网络版Web控制台（HTML）”，弹出“趋势科技防毒墙网络版”界面。
2. 输入用户名和密码登录。

步骤2 配置防毒软件服务器的更新源。

1. 选择“更新 > 服务器 > 更新源”。

服务器更新源

 帮助

从以下更新源下载更新

趋势科技 ActiveUpdate 服务器
(http://oscel05-p.activeupdate.trendmicro.com.cn/activeupdate/china)

其他更新源:
http:// + -

包含当前文件副本的 Intranet 位置
UNC 路径:
例如: \\server_name\download
用户名:
密码:

2. 选择更新源类型。

- （推荐）若使用趋势科技官方网站提供的服务器作为更新源，请选择“趋势科技 ActiveUpdate服务器”。
- 若使用官方服务器以外的更新源，请确保更新源可提供安全有效的组件更新功能，并选择“其他更新源”添加更新源所在地址。
- 若使用可通过UNC路径访问的服务器作为更新源，请选择“包含当前文件副本的 Intranet位置”，并添加该更新源的UNC路径及具有权限的用户名、密码。

说明

从趋势科技ActiveUpdate服务器上更新防病毒组件时，要求防毒软件服务器所在的计算机连接Internet。

使用其他更新源或Intranet上更新源更新防病毒组件时，要求防毒软件服务器所在的计算机与目标地址保持连通。

3. 单击“保存”。

步骤3 更新防毒软件服务器的防病毒组件。

1. 配置自动更新参数。

- a. 选择“更新 > 服务器 > 预设更新”。
- b. 选中“启用防毒墙网络版服务器的预设更新”。
- c. 选择需要更新的组件。
- d. 配置更新时间表。

更新时间表

每小时一次

每日一次

每周一次，在

每月一次，在每月的 号

开始时间: : (时:分)

以 小时为更新周期

当更新频率为每日、每周或每月时，可以配置在这段时间内的某固定时间点开始更新。

- e. 单击“保存”。

2. （可选）手动更新防毒软件服务器。

在设置好防毒软件服务器的更新源后，如果出现病毒爆发，或自动更新尚未将重要组件更新至服务器时，需要手动更新防病毒组件。

- a. 在Web控制台的主菜单上单击“立即更新服务器”。
- b. 选择需要更新的组件。
- c. 单击“更新”。


步骤4 配置防毒软件客户端的更新源。




1. 选择“更新 > 联网计算机 > 更新源”。

更新源（联网计算机）

 [帮助](#)

可以选择某些客户端使之从防毒墙网络版服务器以外的源进行更新。备用更新源可以是一个更新代理或一台 ActiveUpdate 服务器。

- 标准更新源（从防毒墙网络版服务器更新）
- 定制的更新源 [更新代理分析报告](#)
 - 如果所有定制源均不可用或未找到，则从防毒墙网络版服务器更新组件
 - 如果所有定制源均不可用或未找到，则从防毒墙网络版服务器更新域设置
 - 如果所有定制源均不可用或未找到，则从防毒墙网络版服务器更新客户端程序和 Hotfix
- 更新代理：始终从标准更新源（防毒墙网络版服务器）更新 

定制的更新源列表		
 添加	 删除	
<input type="checkbox"/>	顺序	IP 范围
<input type="checkbox"/>		外部源
 添加	 删除	

[通知所有客户端](#)

2. 选择更新源类型。

- （推荐）若使用防毒软件服务器作为更新源，请选择“标准更新源”。
- 若为防毒软件客户端配置其他更新源，请选择“定制的更新源”，并将该更新源添加到列表中。

 **说明**

在使用其他定制更新源，如直接从ActiveUpdate服务器更新防病毒组件时，会因占用大量网络带宽而影响性能，因此建议选择标准更新源。

3. 单击“通知所有客户端”，将更新源配置下发到各客户端上。

步骤5 更新防毒软件客户端的防病毒组件。

1. 配置自动更新参数。

- a. 选择“更新 > 联网计算机 > 自动更新”。

自动更新（联网计算机）

 帮助

在发生某些事件时或在指定的更新日期期间触发客户端以更新组件。

事件触发更新	
<input checked="" type="checkbox"/> 防毒墙网络版服务器下载完新组件后立即在客户端上启动组件更新。	
<input type="checkbox"/> 包括漫游客户端和脱机客户端	
<input checked="" type="checkbox"/> 使客户端在重新启动并连接到防毒墙网络版服务器时启动组件更新（漫游客户端除外）	
<input type="checkbox"/> 更新后执行“立即扫描”（漫游客户端除外）	
基于预定更新	
<input checked="" type="radio"/> 分钟	10 分钟
<input type="radio"/> 小时	<input type="checkbox"/> 每天只更新一次客户端配置
<input type="radio"/> 每日一次	
<input type="radio"/> 每周一次，在 星期日	

- b. 根据实际需求选择触发防毒软件客户端组件更新的条件。
 - c. 配置更新时间表。
当更新频率为每小时、每日或每周时，可以配置在这段时间内的某固定时间点开始更新。
 - d. 单击“保存”。
- 2.（可选）手动更新防病毒软件客户端。

在配置好防毒软件客户端后，如果客户端组件严重过期，或存在病毒爆发等情况，需要对客户端组件进行更新。

- a. 选择“更新 > 联网计算机 > 手动更新”。
- b. 选择需要更新的防毒软件客户端。
选择客户端有两种方式：
 - 选择带有过期组件的客户端：该选项可以自动为用户选取所有需要更新的客户端。
 - 手动选择客户端：选择此选项后，单击“选择”，在打开的客户端树中选择需要更新的客户端，然后返回。
- c. 单击“开始更新”。

---结束

5 配置 NTP 组件

介绍如何在ATIC管理中心服务器、采集器上安装和配置NTP服务器、NTP客户端。网元的NTP配置，具体请参见网元的相关手册。

前提条件

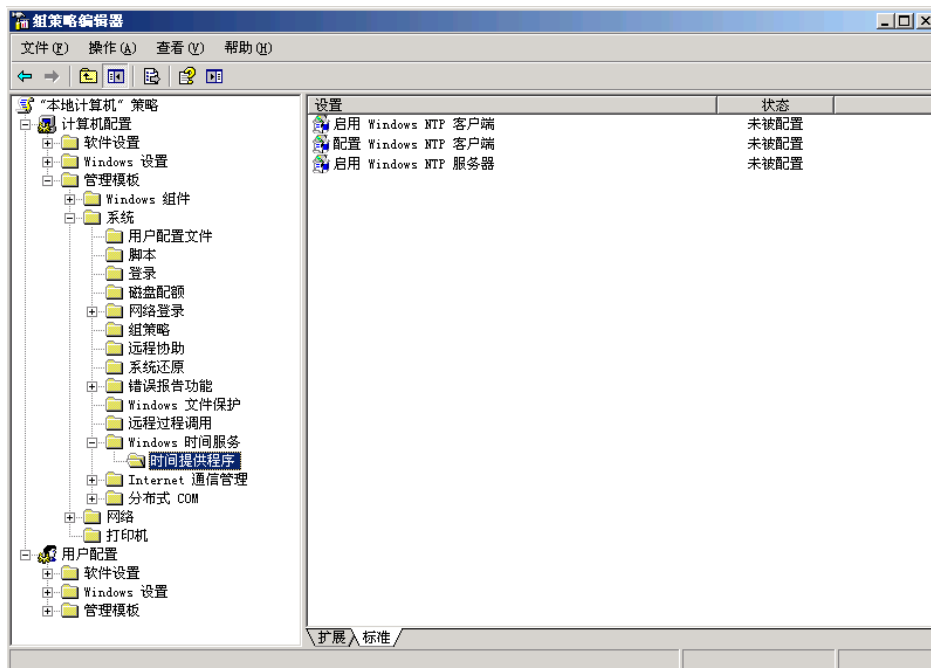
完成NTP服务规划，具体请参见[1.2 NTP服务规划](#)。

背景信息

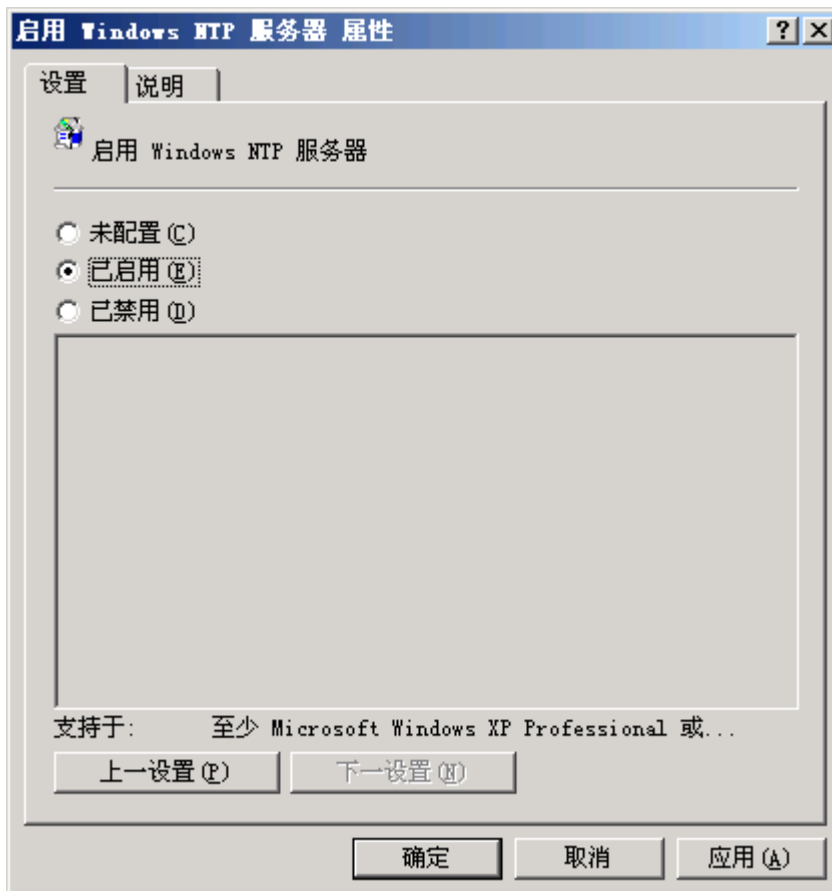
请根据NTP服务规划结果，在ATIC管理中心服务器、采集器上执行操作步骤。以Windows Server 2003为例介绍。

操作步骤

- 配置ATIC管理中心服务器作为NTP服务器。
 1. 以具有administrator权限的操作系统用户登录操作系统。
 2. 选择“开始 > 运行”。
 3. 在“运行”中，输入“gpedit.msc”。
 4. 单击“确定”。
 5. 在“组策略编辑器”的左侧导航树中选择“计算机配置 > 管理模板 > 系统 > Windows时间服务 > 时间提供程序”。



6. 在右侧窗口中，双击“启用Windows NTP服务器”。
7. 在“启用Windows NTP服务器属性”中，单击“设置”页签，选择“已启用”。

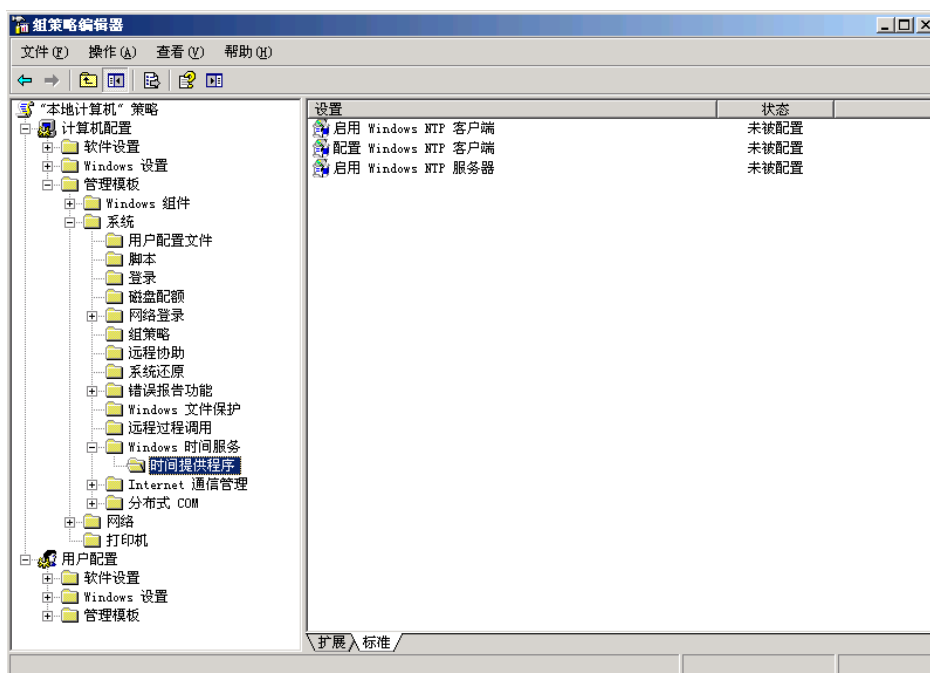


8. 单击“确定”。

9. 设置主机宣布自身为可靠的时钟源。
 - a. 选择“开始 > 运行”。
 - b. 在“运行”中，输入“regedit.exe”。
 - c. 在“注册表编辑器”中，选择“HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > Config > AnnounceFlags”。
 - d. 在右侧窗口中，右键单击“AnnounceFlags”，在快捷菜单中选择“修改”。
 - e. 在“编辑 DWORD 值”的“数值数据”中，键入“5”。
 - f. 单击“确定”。
 - g. 关闭“注册表编辑器”。
 10. 重启W32Time服务。
 - a. 选择“开始 > 运行”。
 - b. 在“运行”中，输入“cmd”。
 - c. 输入以下命令，关闭W32Time服务。

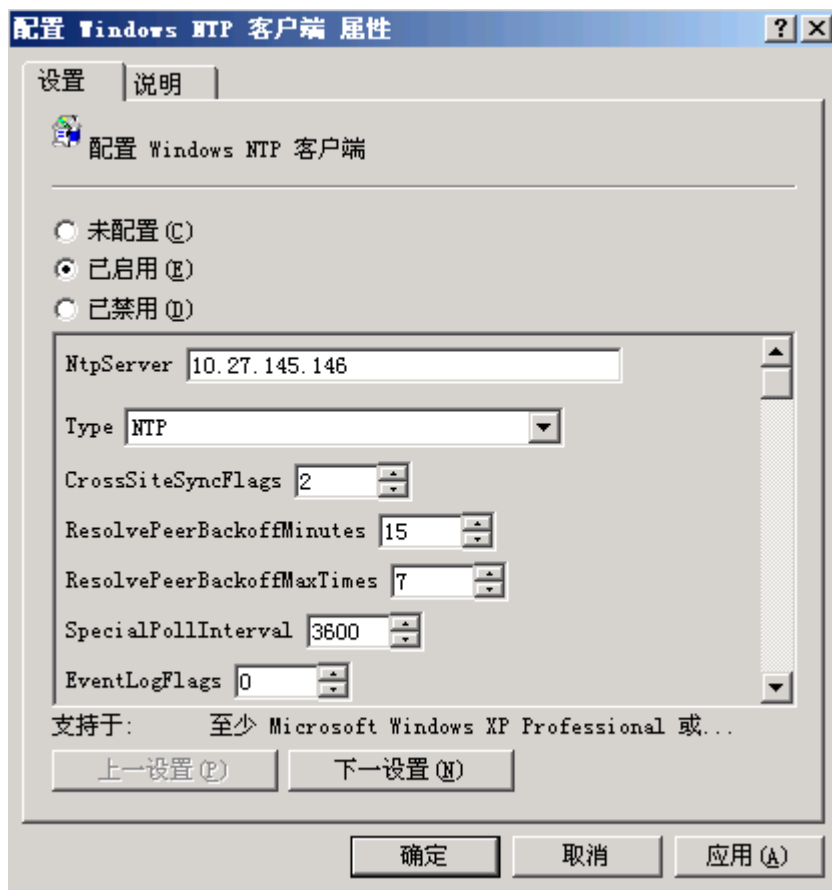
```
net stop w32time
```
 - d. 输入以下命令，启动W32Time服务。

```
net start w32time
```
- 配置ATIC管理中心服务器、采集器作为NTP客户端。
 1. 以具有administrator权限的操作系统用户登录操作系统。
 2. 选择“开始 > 运行”。
 3. 在“运行”中，输入“gpedit.msc”。
 4. 单击“确定”。
 5. 在“组策略编辑器”中，左侧导航树中选择“计算机配置 > 管理模板 > 系统 > Windows时间服务 > 时间提供程序”。

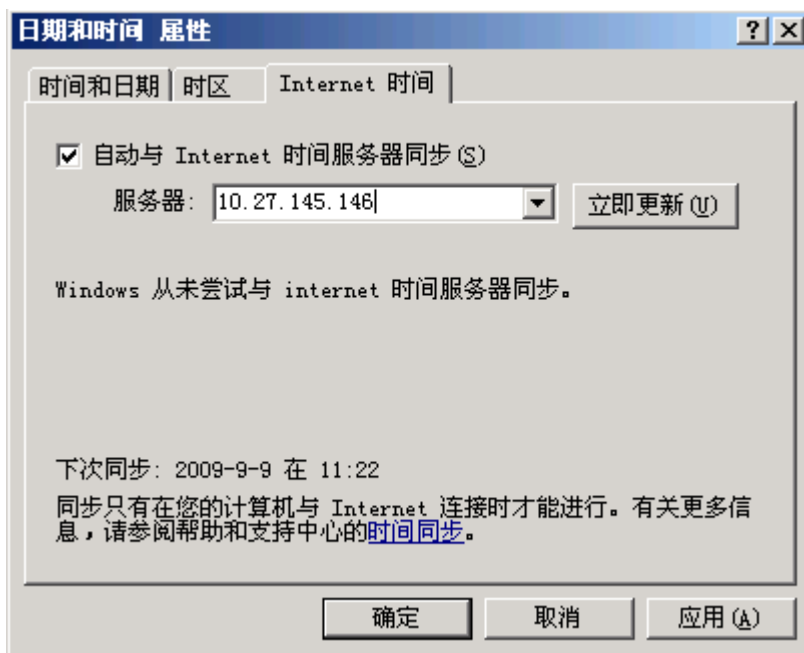


6. 双击“配置Windows NTP客户端”。

- a. 在“配置Windows NTP客户端属性”中，单击“设置”页签。
- b. 选择“已启用”。
- c. 在“NTP Server”中，输入NTP服务器的IP地址。
- d. 在“Type”中，选择“NTP”。
- e. 单击“确定”，返回“组策略编辑器”。



7. 双击“启用Windows NTP客户端”。
 - a. 在“启用Windows NTP客户端属性”中，单击“设置”页签。
 - b. 选择“已启用”。
 - c. 单击“确定”，返回“组策略编辑器”。
8. 设置自动与NTP服务器同步时间。
 - a. 选择“开始 > 控制面板 > 日期和时间”。
 - b. 单击“Internet 时间”页签。
 - c. 选中“自动与Internet时间服务器同步”。
 - d. 在“服务器”中，输入NTP服务器的IP地址。
 - e. 单击“立即更新”，立即执行时间同步。
 - f. 单击“确定”，完成NTP客户端配置。



- 手动调整ATIC管理中心服务器、采集器时间。
 1. 检查屏幕右下角显示的时间与现实时间是否一致。
 2. 选择“开始 > 控制面板”，双击“日期和时间”，调整系统时间为现实时间。

----结束

6 安装 ATIC 管理中心服务器

关于本章

介绍如何安装ATIC管理中心服务器。

6.1 安装前检查

介绍安装前的准备工作。

6.2 安装步骤

介绍安装ATIC管理中心服务器软件的操作步骤。

6.3 启动ATIC管理中心

ATIC管理中心服务器软件安装完成后会提示用户选择是否立即启动程序和服务。如果当时没有立即启动，可使用手动方式启动。如果ATIC管理中心所在的物理服务器因断电、系统软件升级等原因导致操作系统重新启动后，ATIC管理中心将自动启动，请不要手动启动。

6.4 验证安装正确性

ATIC管理中心服务器软件安装完成后，您需要验证安装成功并能够正常运行。

6.5 登录ATIC管理中心

介绍如何登录ATIC管理中心。

6.6 安装失败处理

ATIC管理中心服务器意外掉电、重新启动、系统崩溃或维护人员误操作，导致正在运行的安装程序关闭。

6.1 安装前检查

介绍安装前的准备工作。

操作步骤

- 步骤1** 确认ATIC管理中心服务器操作系统及其补丁已经正确安装。具体请参见[3 安装操作系统](#)。
- 步骤2** 确认操作系统的“区域和语言选项”（Windows 2003）或“时钟、语言和区域”（Windows 2008）与其语言版本一致。
- 步骤3** ATIC管理中心占用的端口列表请参见[1.3 端口列表](#)。如果有其他程序占用端口，请停止占用端口的程序，释放端口，具体请参见[9.1 如何查看Windows操作系统中某端口的占用情况及释放端口](#)。
- 步骤4** 确保至少一个网卡处于启动状态，并且已经连接物理网线。在安装过程中，安装软件需要调用网卡的服务。网络必须处于连通状态。
- 步骤5** 确认正确设置ATIC管理中心服务器的系统时间。具体请参见[5 配置NTP组件](#)。

---结束

6.2 安装步骤

介绍安装ATIC管理中心服务器软件的操作步骤。

前提条件

- 准备ATIC管理中心服务器安装软件。
- 完成服务器安装前检查，并解决所有问题。具体请参见[6.1 安装前检查](#)。

背景信息

建议MySQL数据库与ATIC管理中心服务器软件安装在同一服务器上。

ATIC管理中心有两种安装方式：

- 通过光盘安装。安装文件存放在光盘根目录下。
- 通过软件包安装。解压所有的安装包到同一目录，安装文件存放在此目录下。如“D:\install”。



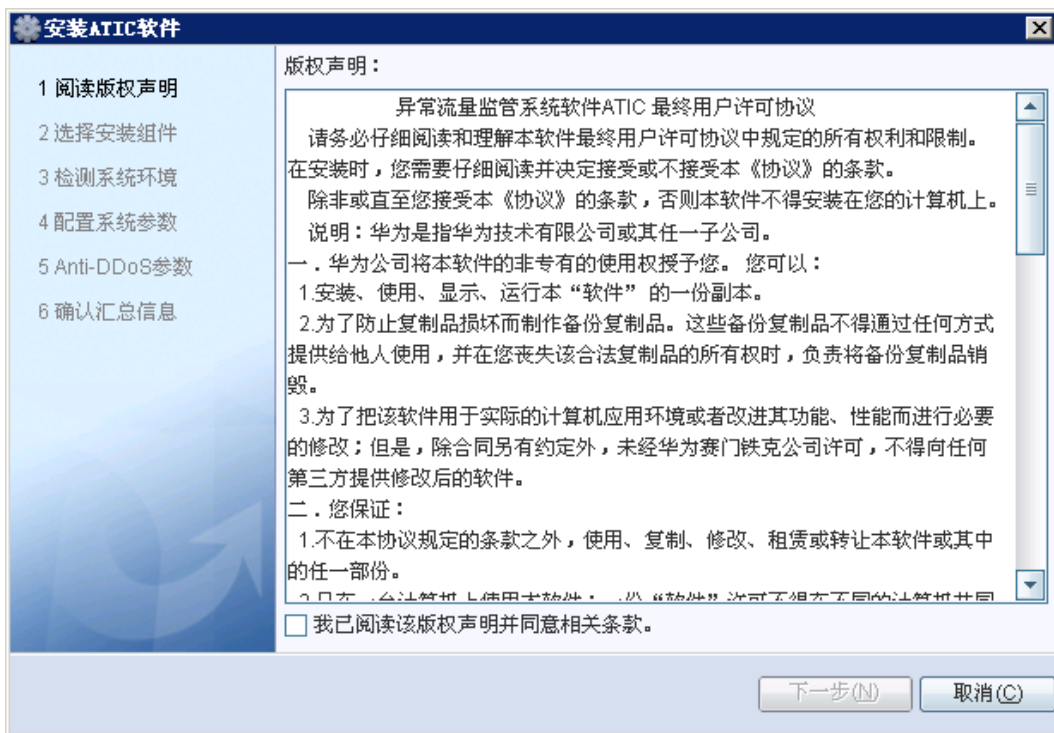
注意

- ATIC管理中心安装路径，只能包含字母、数字、下划线，不能包含空格、括号、中文字符等，否则将无法成功安装。
 - 禁止在安装过程中修改系统时间。
-

操作步骤

步骤1 以具有administrator权限的操作系统用户登录操作系统。

步骤2 运行安装光盘或安装软件包中的“ATIC\install.exe”文件，启动安装程序。请阅读安装许可协议，并且确认同意该协议后，选中“我已阅读该版权声明并同意相关条款”。



步骤3 单击“下一步”，显示需要安装的组件。



步骤4 单击“下一步”，安装程序将自动检测系统环境，检查HTTP、HTTPS端口是否被占用。只有端口检查结果均为“可用”时，才可以继续安装。

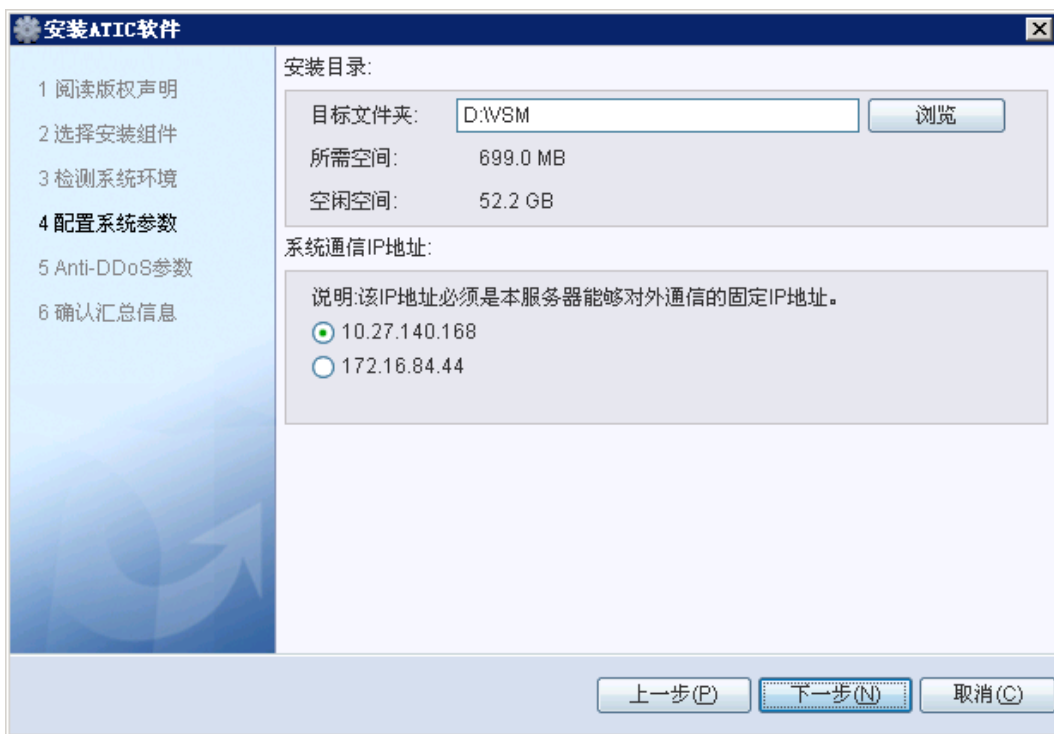
ATIC管理中心默认使用的HTTP端口为8080、HTTPS端口为443。如上述端口已经被其他程序使用，将提示“被占用”。此时可以选择：

- 修改ATIC管理中心使用的端口。在“HTTP 端口”或“HTTPS 端口”中输入新端口号，单击“重新检测”，查看检查结果。
- 释放被系统其他应用程序占用的端口。具体方法请参见该应用程序的使用说明。



步骤5 单击“下一步”，配置系统参数。

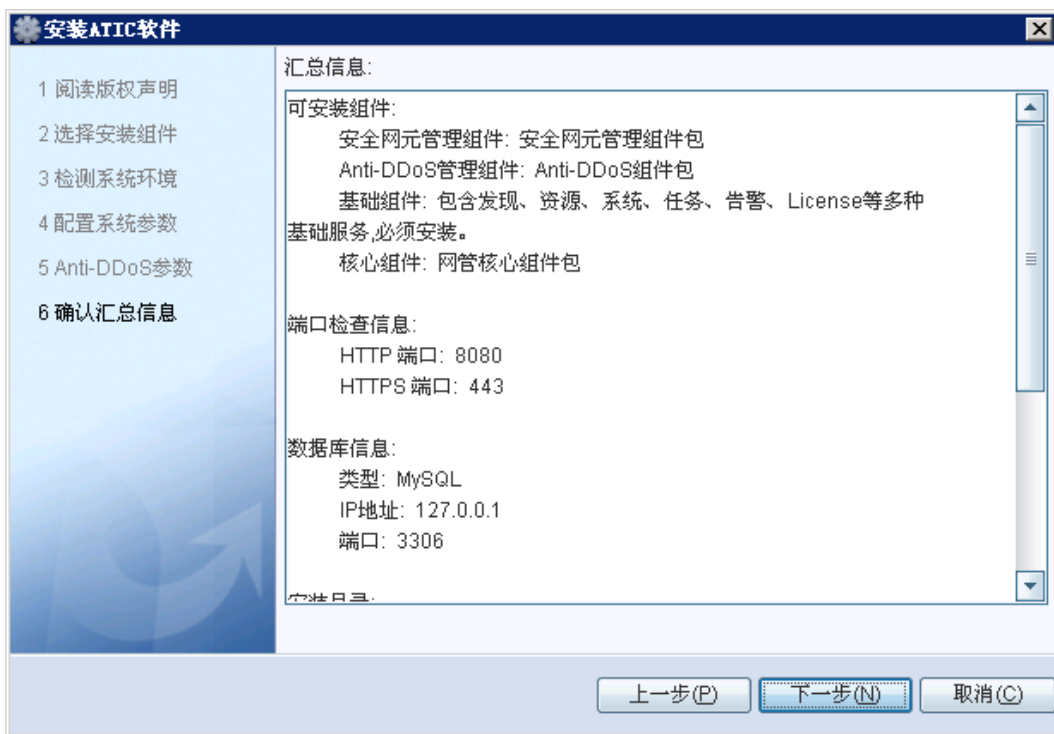
1. 设置ATIC管理中心的安装目录，默认安装目录为：D:\VSM。
2. 选择系统通信IP地址。请务必保证设置的IP地址为固定IP，能够与采集器、被管理的网元路由互通，能够被管理员通过网络访问。



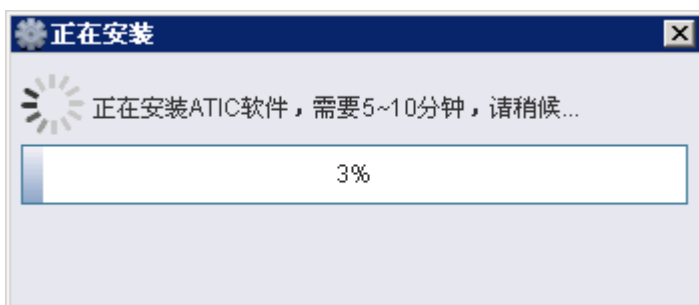
步骤6 单击“下一步”，设置Anti-DDoS采集器参数。如果采用集中式部署方案，请选中“安装Anti-DDoS采集器”。



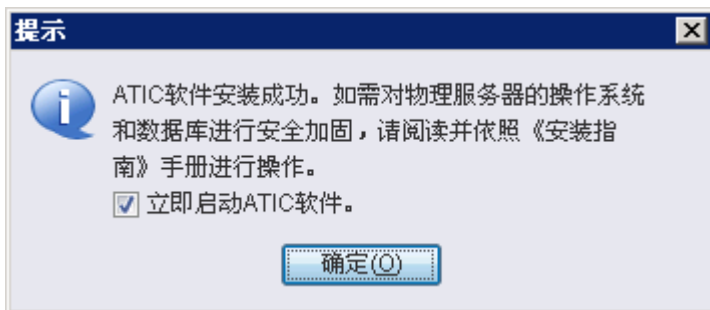
步骤7 单击“下一步”。确认汇总信息。



步骤8 单击“下一步”，开始安装，以进度条形式显示安装进度。安装过程中，将会弹出命令行窗口，请不要手动关闭。



步骤9 安装完成后，弹出“提示”，表明软件安装成功。单击“确定”，立即启动ATIC管理中心。



如果不需要立即启动ATIC管理中心，取消选中“立即启动ATIC软件”，单击“确定”。

----结束

后续处理

安装完成后请进行正确性验证，具体请参见[6.4 验证安装正确性](#)。

如需要手动方式启动ATIC管理中心，具体请参见[6.3 启动ATIC管理中心](#)。

安装过程因意外终止或安装失败，后续处理请参见[6.6 安装失败处理](#)。

6.3 启动 ATIC 管理中心

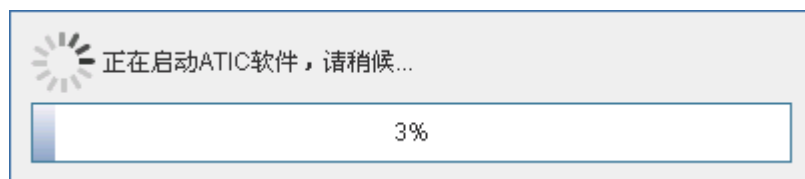
ATIC管理中心服务器软件安装完成后会提示用户选择是否立即启动程序和服务。如果当时没有立即启动，可使用手动方式启动。如果ATIC管理中心所在的物理服务器因断电、系统软件升级等原因导致操作系统重新启动后，ATIC管理中心将自动启动，请不要手动启动。

前提条件

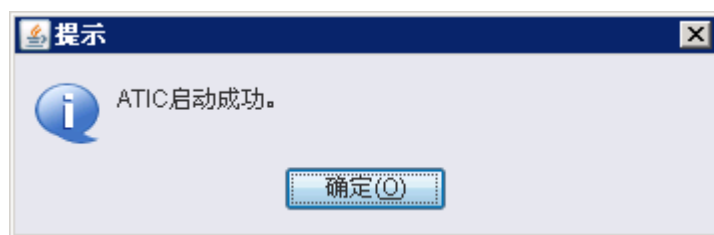
已经完成ATIC管理中心服务器软件安装。

操作步骤

步骤1 选择“开始 > 所有程序 > ATIC > Start ATIC”。界面显示如下图所示。



步骤2 当界面显示如下图所示，表示已经正常启动。单击“确定”，关闭窗口。



----结束

6.4 验证安装正确性

ATIC管理中心服务器软件安装完成后，您需要验证安装成功并能够正常运行。

操作步骤

步骤1 以安装ATIC管理中心服务器的操作系统用户登录操作系统。

步骤2 打开操作系统本地用户文件夹（Windows 2003操作系统为“C:\Documents and Settings\administrator”，Windows 2008操作系统为“C:\Users\Administrator”），确认以下文件是否存在：

- “legoInstalled.xml”，记录ATIC管理中心安装信息，包括：安装目录、数据库类型、数据库基本信息等。
- “ddosCollectorInstalled.xml”，记录Anti-DDoS采集器软件的安装信息，仅在采用集中式部署方式时生成本文件。

如果文件不存在，请重新安装ATIC管理中心。

步骤3 选择“开始 > 控制面板 > 管理工具 > 服务”。

步骤4 确认以下服务是否存在，并且已经启动。

表 6-1 系统服务列表

服务名称	使用对象
LEGOService	ATIC管理中心服务器软件
LEGOWebSrv	ATIC管理中心服务器软件
LEGOMonitor	ATIC管理中心服务器软件
mysqservice	ATIC管理中心服务器软件
Anti-DDoS Collector Monitor Service	Anti-DDoS采集器软件
Anti-DDoS Collector Service	Anti-DDoS采集器软件

- 如果服务存在并且已经启动，说明ATIC管理中心服务器软件安装正确。
- 如果服务存在但是没有启动，请右键单击该服务，在弹出的快捷菜单中选择“启动”。
- 如果服务不存在，请重新安装ATIC管理中心服务器软件。

---结束

6.5 登录 ATIC 管理中心

介绍如何登录ATIC管理中心。

前提条件

完成ATIC管理中心服务器软件安装。

背景信息

首次登录时，请使用系统缺省超级管理员admin，初始密码为Admin@123。



小心

ATIC管理中心不支持使用IPv6地址作为登录服务器IP地址。如果操作系统中已安装IPv6组件，请勿使用localhost作为服务器IP地址。

操作步骤

步骤1 打开浏览器。

ATIC管理中心支持IE 6.0、IE 7.0、IE 8.0，FireFox 3.6至4.X版本浏览器。

步骤2 输入系统登录地址**https://服务器IP地址:端口号**（ATIC管理中心默认使用443端口。如果安装时修改为其他端口，请输入端口号），按“Enter”。

- 建议把ATIC管理中心主页加入“受信任的站点”。
- 如果使用**http://服务器IP地址:端口号**（ATIC管理中心默认使用8080端口。如果安装时修改为80端口，可以不输入端口号）方式登录，系统将自动跳转为**https://服务器IP地址:端口号**方式。

步骤3 可选：如果提示安全证书问题，请参见**9.3 使用HTTPS协议登录ATIC管理中心时，如何安装安全证书**解决。

步骤4 在登录页面，选择界面语言，输入用户名、密码和验证码。

用户名为admin，初始密码为Admin@123。

步骤5 单击“登录”。

步骤6 页面提示“第一次登录，请修改密码”。输入新密码并确认密码，单击“确定”。



说明

请牢记admin密码，一旦丢失无法重置。

步骤7 在“成功”提示框中，单击“确定”。

----结束

6.6 安装失败处理

ATIC管理中心服务器意外掉电、重新启动、系统崩溃或维护人员误操作，导致正在运行的安装程序关闭。

操作步骤

步骤1 检查ATIC管理中心服务器是否已掉电。如果服务器电源指示灯灭，则表明已掉电，请重新打开电源开关。

步骤2 选择“开始 > 所有程序 > ATIC > Uninstall ATIC”。或者双击打开安装路径下“D:\VSM\Runtime\bin\uninstall.vbe”文件。请依据界面提示，选择“完全卸载”。

- 卸载成功，重新执行安装操作。
- 卸载失败，请执行后续步骤。

步骤3 选择“开始 > 控制面板 > 管理工具 > 服务”。

步骤4 按表6-2顺序，停止服务。右键单击该服务，在弹出的快捷菜单中选择“停止”。

表 6-2 停止系统服务顺序

服务名称	使用对象
LEGOMonitor	ATIC管理中心服务器软件
LEGOWebSrv	ATIC管理中心服务器软件
LEGOService	ATIC管理中心服务器软件
mysqservice	ATIC管理中心服务器软件
Anti-DDoS Collector Monitor Service	Anti-DDoS采集器软件
Anti-DDoS Collector Service	Anti-DDoS采集器软件

步骤5 选择“开始 > 运行”，输入cmd，打开命令行窗口。

步骤6 按表6-2顺序，删除服务。输入命令sc delete *ServiceName*。其中*ServiceName*为服务名称。

步骤7 打开操作系统本地用户文件夹（Windows 2003操作系统为“C:\Documents and Settings\administrator”，Windows 2008操作系统为“C:\Users\Administrator”），删除以下文件：

- “legoInstalled.xml”
- “ddosCollectorInstalled.xml”

步骤8 手动删除安装目录，如“D:\VSM”。

步骤9 重新执行安装操作，具体请参见6 安装ATIC管理中心服务器。

----结束

7 安装 Anti-DDoS 采集器

关于本章

介绍如何安装ATIC管理中心的Anti-DDoS采集器。Anti-DDoS采集器用于采集、解析、汇总、入库Anti-DDoS设备流量和日志，存储抓包文件。

7.1 安装前检查

介绍安装Anti-DDoS采集器需要进行的准备工作。

7.2 安装步骤

介绍安装ATIC管理中心的Anti-DDoS采集器软件的操作步骤。

7.3 启动Anti-DDoS采集器

Anti-DDoS采集器安装完成后会提示用户选择是否立即启动程序和服务。如果当时没有立即启动，可使用手动方式启动。如果Anti-DDoS采集器所在的物理服务器因断电、系统软件升级等原因导致操作系统重新启动后，Anti-DDoS采集器将自动启动，请不要手动启动。

7.4 验证安装正确性

Anti-DDoS采集器安装完成后，您需要验证Anti-DDoS采集器安装是否成功、运行是否正常。

7.1 安装前检查

介绍安装Anti-DDoS采集器需要进行的准备工作。

前提条件

在安装Anti-DDoS采集器之前，请先关闭Windows自带的防火墙。

操作步骤

- 步骤1** 确认Anti-DDoS采集器操作系统及其补丁已经正确安装。具体请参见[3 安装操作系统](#)。
- 步骤2** 确认操作系统的“区域和语言选项”（Windows 2003）或“时钟、语言和区域”（Windows 2008）与其的语言版本一致。
- 步骤3** 确保Anti-DDoS采集器安装需要使用的端口没有被其他程序占用。具体请参见[1.3 端口列表](#)。
如果有其他程序占用端口，请停止占用端口的程序，释放端口，具体请参见[9.1 如何查看Windows操作系统中某端口的占用情况及释放端口](#)。
- 步骤4** 确保至少一个网卡处于启动状态，并且已经连接物理网线。在安装过程中，安装软件需要调用网卡的服务。
- 步骤5** 当ATIC管理中心系统采用分布式部署方案时，确保ATIC管理中心服务器所在的物理服务器与Anti-DDoS采集器所在的物理服务器网络互通。
- 步骤6** 确保ATIC管理中心服务器所在的物理服务器与Anti-DDoS采集器所在的物理服务器时间一致，保持同步。具体请参见[5 配置NTP组件](#)。
- 步骤7** 确保已经完成ATIC管理中心服务器安装。具体请参见[6 安装ATIC管理中心服务器](#)。

----结束

7.2 安装步骤

介绍安装ATIC管理中心的Anti-DDoS采集器软件的操作步骤。

前提条件

完成服务器安装前检查，并解决所有问题。具体请参见[7.1 安装前检查](#)。

背景信息



注意

所有软件安装路径名称，包括安装包路径和ATIC管理中心安装路径，只能有字母、数字、下划线，不能有空格、括号、中文字符等，否则将无法成功安装。

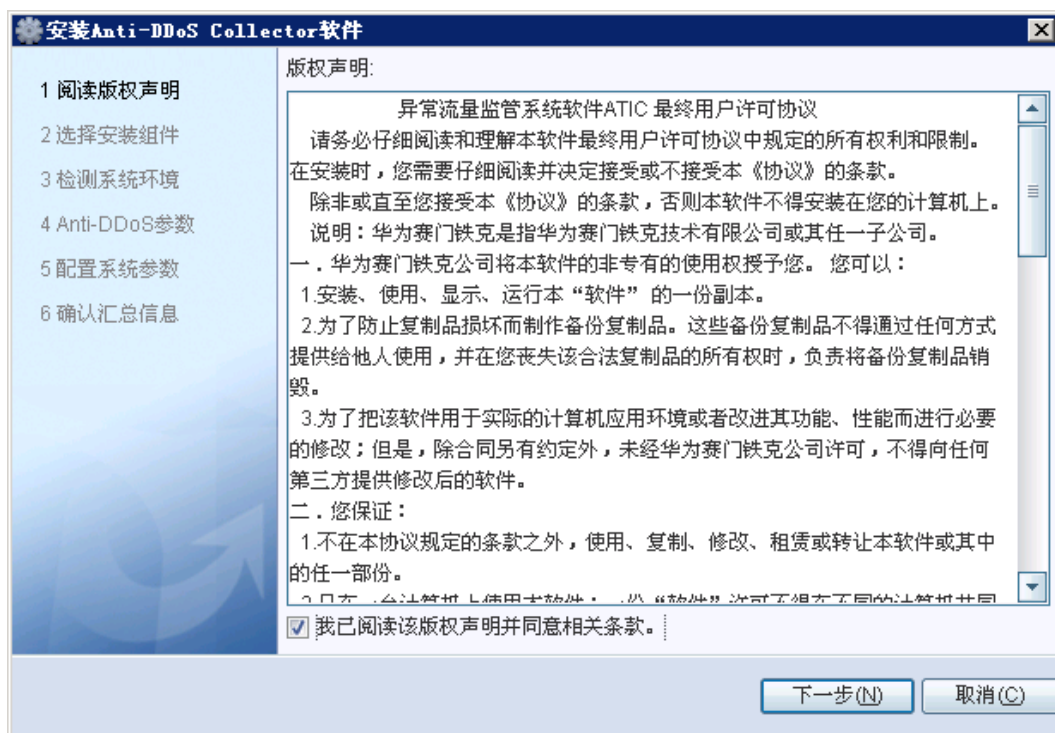
ATIC管理中心采集器有两种安装方式：

- 通过光盘安装。安装文件存放在光盘根目录下。
- 通过软件包安装。解压所有的安装包到同一目录，安装文件存放在此目录下。

操作步骤

步骤1 以具有administrator权限的操作系统用户登录操作系统。

步骤2 运行安装光盘或安装软件包中的“ATIC\antiddos_collector\DDoS-Collector-install.exe”文件启动安装程序。请阅读安装许可协议，并且确认同意该协议后，选中“我已阅读该版权声明并同意相关条款”。



步骤3 单击“下一步”，显示需要安装的组件。



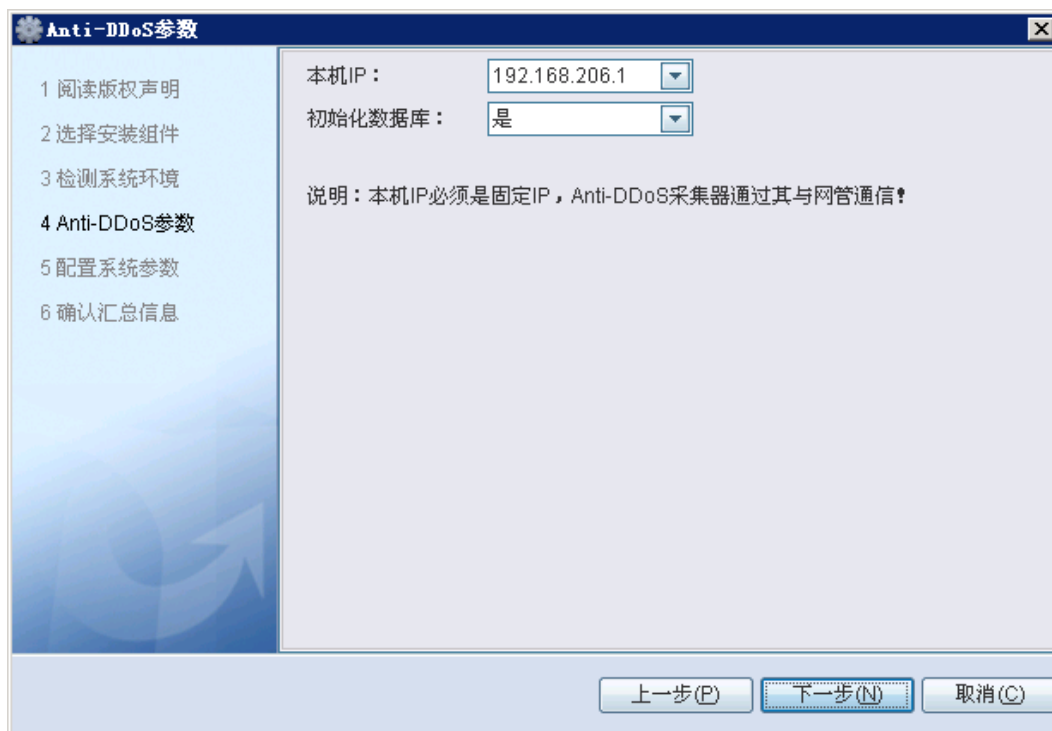
步骤4 单击“下一步”，显示系统基本信息。



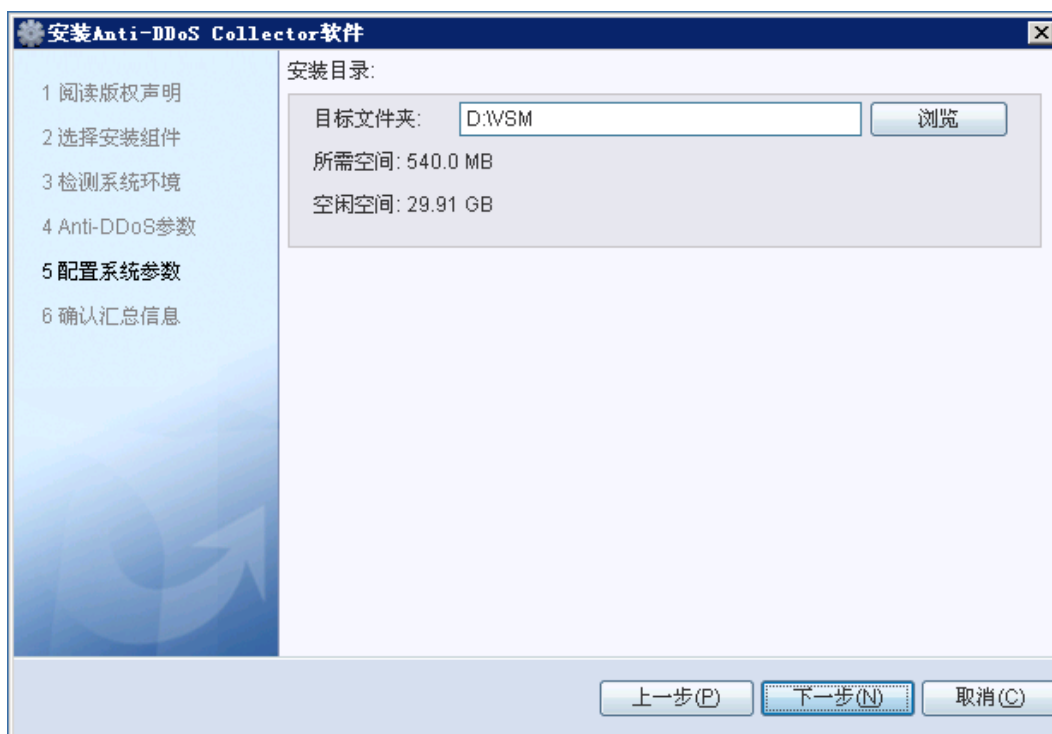
步骤5 单击“下一步”，设置Anti-DDoS采集器的IP地址，并初始化数据库。

请务必保证设置的IP地址为固定IP，能够与服务器、被管理的网元路由互通，能够被管理员通过网络访问。

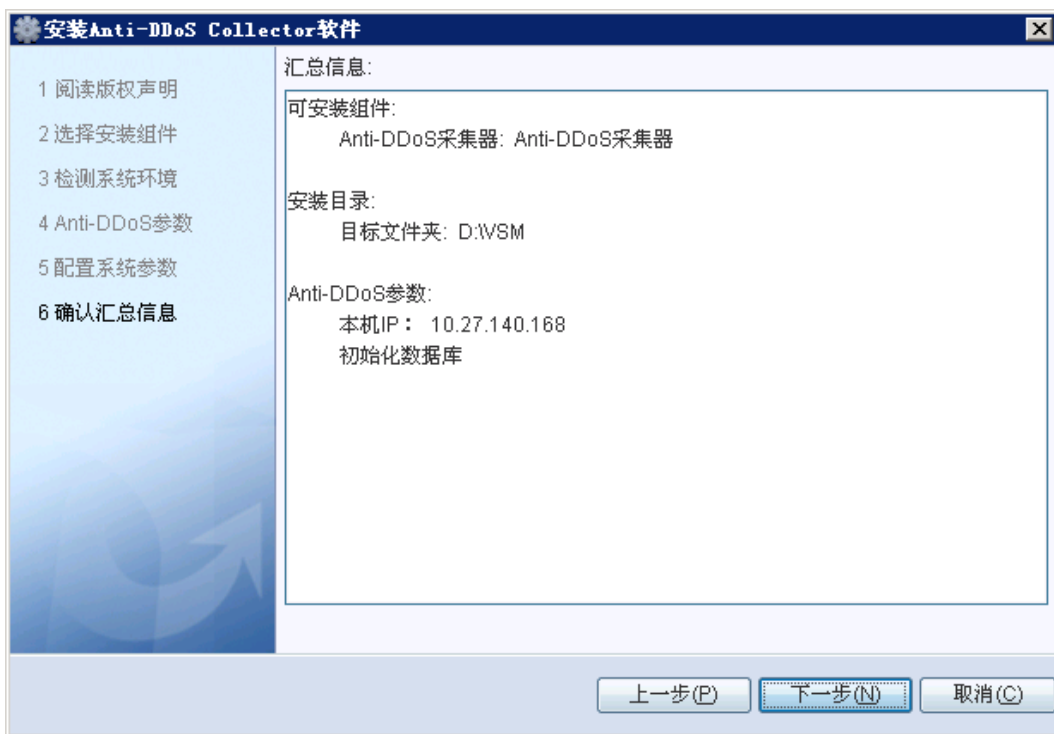
如果之前安装过Anti-DDoS采集器，并且卸载时选择保留数据文件以备后续使用，此时在“初始化数据库”中要选择“否”。



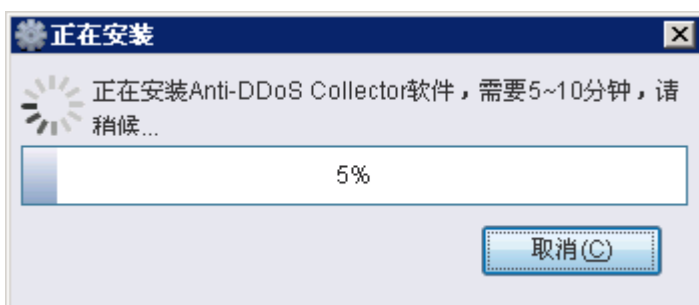
步骤6 单击“下一步”，设置ATIC管理中心的安装目录，默认安装目录为：“D:\VSM”。



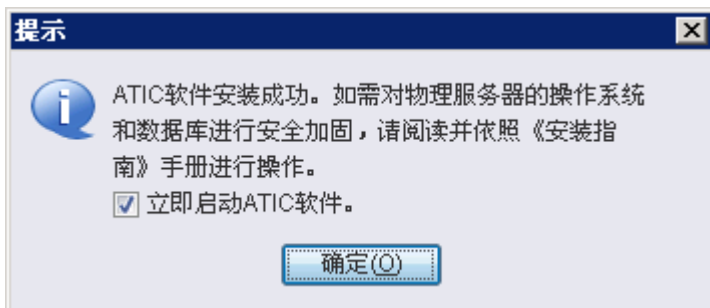
步骤7 单击“下一步”。确认汇总信息。



步骤8 单击“下一步”，开始安装，以进度条形式显示安装进度。安装过程中，将会弹出命令行窗口，请不要手动关闭。



步骤9 安装完成后，弹出“提示”，表明软件安装成功。单击“确定”，立即启动Anti-DDoS采集器软件。



如果不需要立即启动Anti-DDoS采集器软件，取消选中“立即启动Anti-DDoS Collector软件”，单击“确定”。

---结束

后续处理

安装完成后请进行正确性验证，具体请参见[7.4 验证安装正确性](#)。

如需要手动方式启动Anti-DDoS采集器软件，具体请参见[7.3 启动Anti-DDoS采集器](#)。

如果安装过程因意外终止或安装失败，请重新安装Anti-DDoS采集器。

7.3 启动 Anti-DDoS 采集器

Anti-DDoS采集器安装完成后会提示用户选择是否立即启动程序和服务。如果当时没有立即启动，可使用手动方式启动。如果Anti-DDoS采集器所在的物理服务器因断电、系统软件升级等原因导致操作系统重新启动后，Anti-DDoS采集器将自动启动，请不要手动启动。

前提条件

已经完成Anti-DDoS采集器软件安装，具体请参见[7.2 安装步骤](#)。

背景信息

Anti-DDoS采集器软件安装完成后，会提示用户是否立即启动。如果当时没有选择启动，可使用手工启动方式。

操作步骤

步骤1 选择“开始 > 所有程序 > Anti-DDoS Collector > Start Collector”。界面显示如下图所示。



步骤2 当界面显示如下图所示，表示已经正常启动。单击“确定”，关闭窗口。



---结束

7.4 验证安装正确性

Anti-DDoS采集器安装完成后，您需要验证Anti-DDoS采集器安装是否成功、运行是否正常。

操作步骤

步骤1 以具有administrator权限的操作系统用户登录操作系统。

步骤2 打开操作系统本地用户文件夹（Windows 2003操作系统为“C:\Documents and Settings\administrator”，Windows 2008操作系统为“C:\Users\Administrator”），确认以下文件是否存在：“ddosCollectorInstalled.xml”。

如果文件不存在，请重新安装Anti-DDoS采集器。

步骤3 选择“开始 > 控制面板 > 管理工具 > 服务”。查看“Anti-DDoS Collector Service”、“Anti-DDoS Collector Monitor Service”、“mysqservice”服务是否存在，并且已经启动。

- 如果服务不存在，请重新安装Anti-DDoS采集器。
- 如果服务存在，但是没有启动，请右键单击该服务，在弹出的快捷菜单中选择“启动”。

如果无法启动，可能由于物理服务器可用内存不足所致。请尽量关闭不常用的且占用操作系统内存较大的应用程序，再次启动服务。

步骤4 登录ATIC管理中心，具体请参见[6.5 登录ATIC管理中心](#)。

步骤5 向ATIC管理中心中添加Anti-DDoS采集器,具体请参见联机帮助或《HUAWEI ATIC管理中心 操作指南》中的创建Anti-DDoS采集器。

- 如果添加成功，表示Anti-DDoS采集器安装成功。
- 如果添加失败，请确认ATIC管理中心服务器和采集器网络连通正常后，再次添加Anti-DDoS采集器。

如果执行以上步骤依然无法正常添加Anti-DDoS采集器，请联系技术支持工程师。

---结束

8 卸载 ATIC 管理中心

关于本章

介绍如何卸载ATIC管理中心及数据库。

8.1 卸载ATIC管理中心服务器

介绍如何卸载ATIC管理中心服务器。

8.2 卸载Anti-DDoS采集器

介绍如何卸载Anti-DDoS采集器。

8.3 卸载趋势防毒软件

介绍如何在服务器和客户端上卸载趋势防毒软件。

8.1 卸载 ATIC 管理中心服务器

介绍如何卸载ATIC管理中心服务器。

8.1.1 关闭 ATIC 管理中心

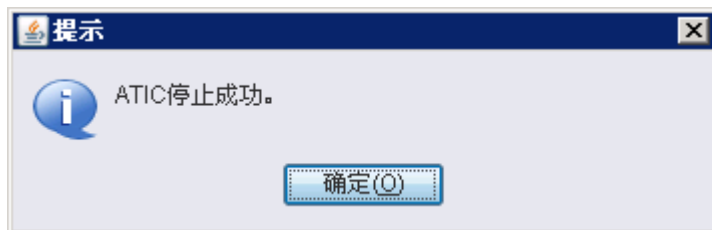
卸载ATIC管理中心前，需要先关闭ATIC管理中心软件及服务。本节介绍关闭ATIC管理中心的详细步骤。

操作步骤

步骤1 选择“开始 > 所有程序 > ATIC > Stop ATIC”。界面如下图所示。



步骤2 当界面如下图所示，表示已经正常关闭。单击“确定”，关闭窗口。



---结束

8.1.2 卸载 ATIC 管理中心服务器软件

介绍如何完全卸载ATIC管理中心服务器软件。

前提条件

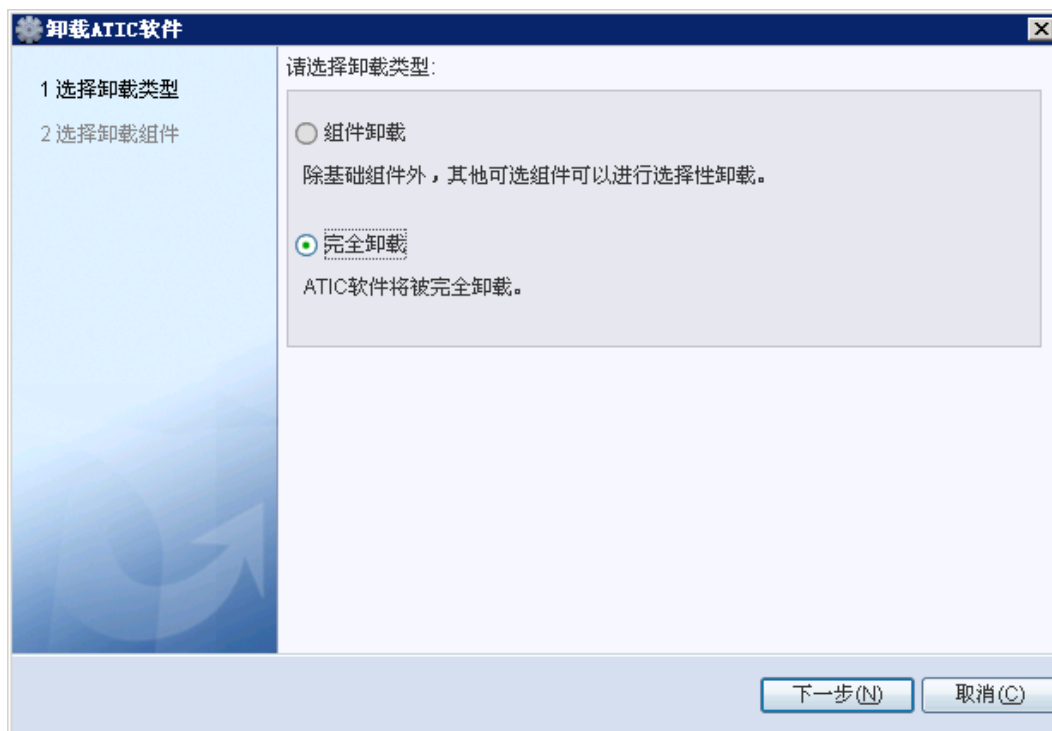
关闭ATIC管理中心，具体请参见[8.1.1 关闭ATIC管理中心](#)。

操作步骤

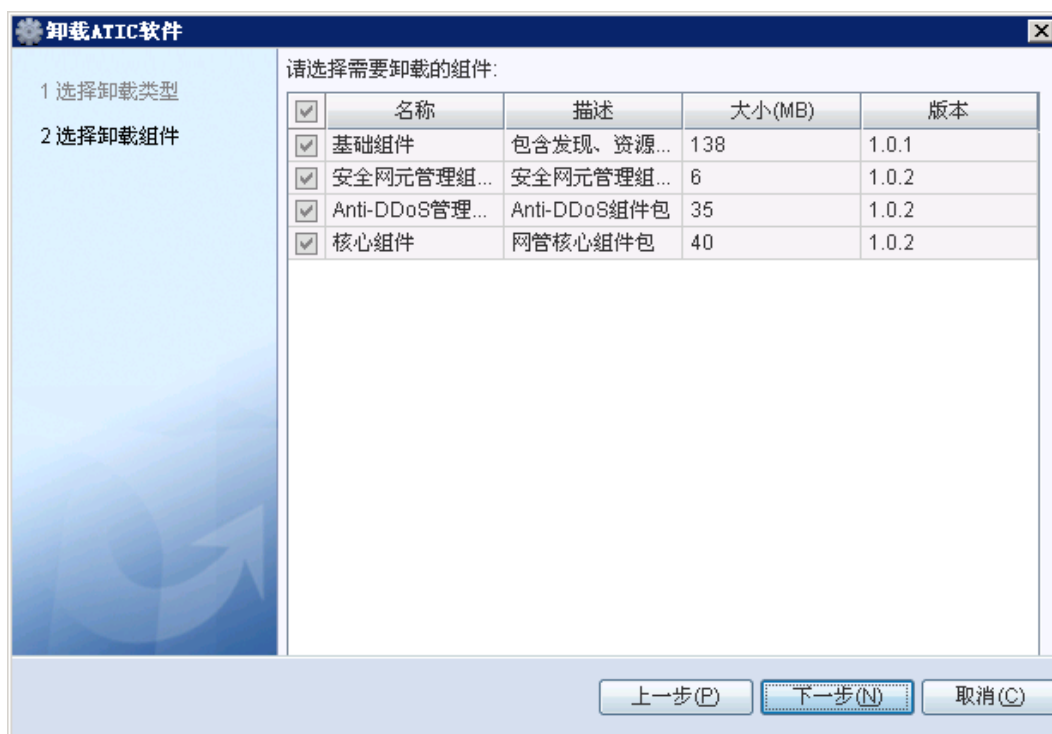
步骤1 以安装ATIC管理中心时的操作系统用户登录操作系统。

步骤2 选择“开始 > 所有程序 > ATIC > Uninstall ATIC”。或者双击打开安装路径下“D:\VSM\Runtime\bin\uninstall.vbe”文件。

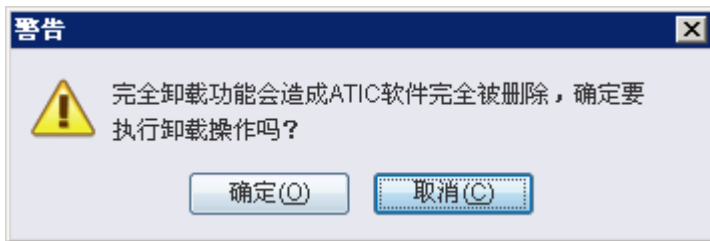
步骤3 选择“完全卸载”。



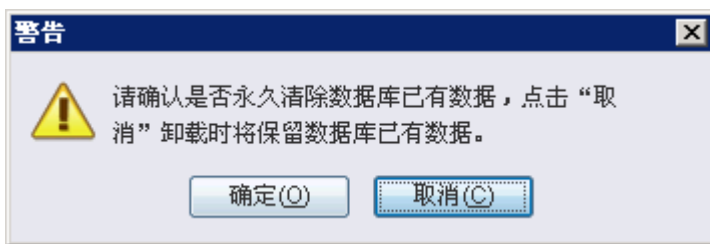
步骤4 单击“下一步”，显示“选择卸载组件”。



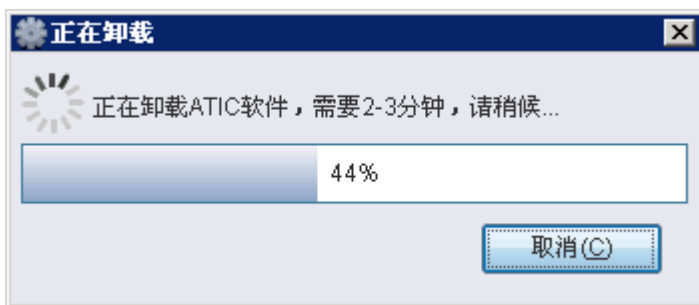
步骤5 单击“下一步”，弹出“警告”对话框。



步骤6 单击“确定”，弹出“警告”对话框。阅读提示信息，选择单击“取消”将保留历史数据，可供后续再次安装时使用。



步骤7 单击按钮进行选择后，弹出卸载进度条。
单击“取消”，将终止卸载操作。



步骤8 等待卸载完成后，弹出“提示”。



步骤9 单击“确定”，结束卸载。

步骤10 可选: 如果不保留历史数据，请手动删除安装目录“D:\VSM”。

----结束

后续处理

卸载过程因意外终止或卸载失败，后续处理请参见[8.1.3 卸载异常处理](#)。

8.1.3 卸载异常处理

如何处理由于ATIC管理中心服务器意外掉电、重新启动、系统崩溃或维护人员误操作等原因，导致正在运行的卸载程序异常关闭，卸载失败。

操作步骤

- 步骤1** 检查ATIC管理中心服务器是否已掉电。如果服务器电源指示灯灭，则表明已掉电，请重新打开电源开关。
- 步骤2** 选择“开始 > 控制面板 > 管理工具 > 服务”。
- 步骤3** 按表8-1顺序，停止服务。右键单击该服务，在弹出的快捷菜单中选择“停止”。

表 8-1 停止系统服务顺序

服务名称	使用对象
LEGOMonitor	ATIC管理中心服务器软件
LEGOWebSrv	ATIC管理中心服务器软件
LEGOService	ATIC管理中心服务器软件
mysqservice	ATIC管理中心服务器软件
Anti-DDoS Collector Monitor Service	Anti-DDoS采集器软件
Anti-DDoS Collector Service	Anti-DDoS采集器软件

- 步骤4** 选择“开始 > 运行”，输入cmd，打开命令行窗口。
- 步骤5** 按表8-1顺序，删除服务。输入命令`sc delete ServiceName`。其中ServiceName为服务名称。
- 步骤6** 手动删除“开始”菜单中的快捷方式。选择“开始 > 所有程序”，鼠标右键单击“ATIC”，在弹出的快捷菜单中选择“删除”。
- 步骤7** 打开操作系统本地用户文件夹（Windows 2003操作系统为“C:\Documents and Settings\administrator”，Windows 2008操作系统为“C:\Users\Administrator”），删除以下文件：
- “legoInstalled.xml”
 - “ddosCollectorInstalled.xml”
- 步骤8** 可选：如果不保留历史数据，请手动删除安装目录，如“D:\VSM”。

----结束

8.2 卸载 Anti-DDoS 采集器

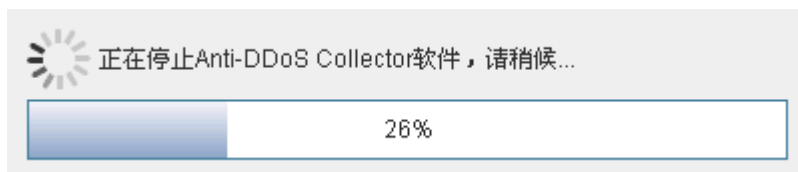
介绍如何卸载Anti-DDoS采集器。

8.2.1 关闭 Anti-DDoS 采集器

卸载Anti-DDoS采集器前，需要先关闭Anti-DDoS采集器的软件和服务。本节介绍关闭Anti-DDoS采集器的详细步骤。

操作步骤

步骤1 选择“开始 > 所有程序 > Anti-DDoS Collector > Stop Collector”。界面如下图所示。



步骤2 当界面如下图所示，表示已经正常关闭。单击“确定”，关闭窗口。



---结束

8.2.2 卸载 Anti-DDoS 采集器软件

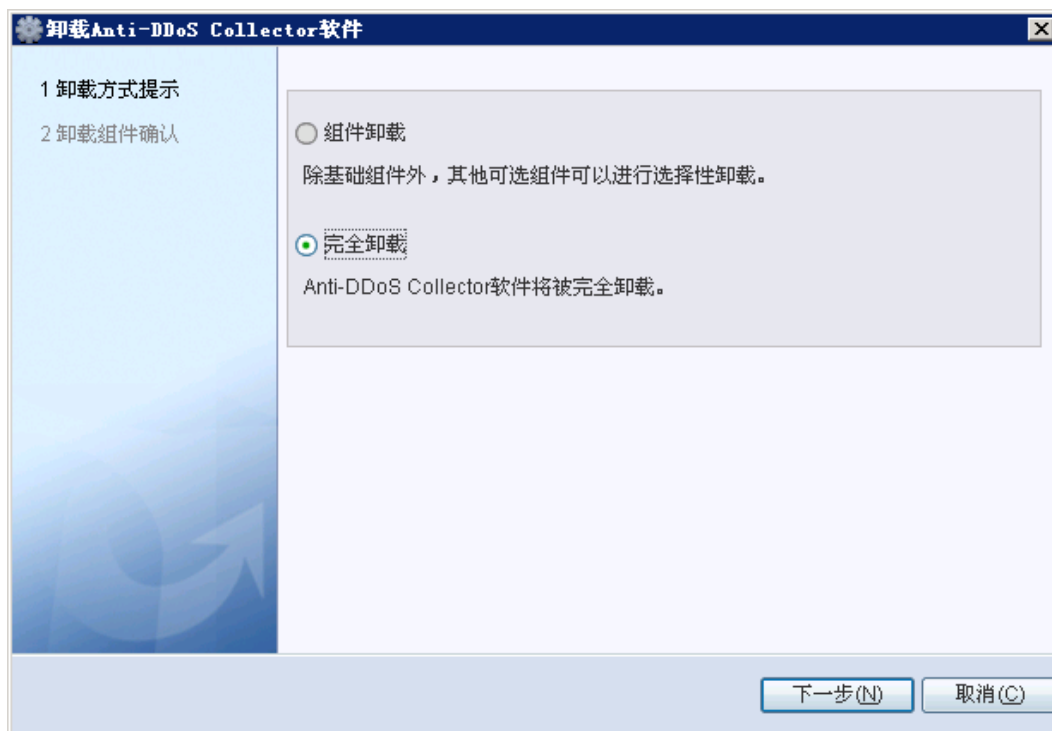
介绍卸载Anti-DDoS采集器软件的操作步骤。

操作步骤

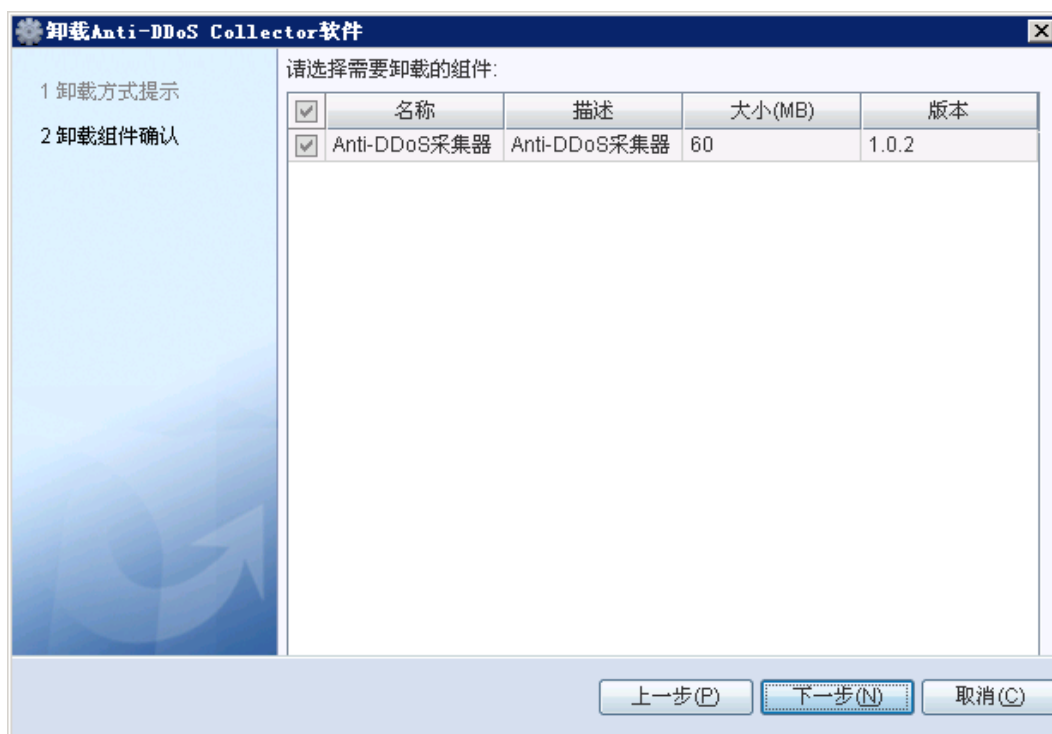
步骤1 以安装Anti-DDoS采集器时的操作系统用户登录操作系统。

步骤2 选择“开始 > 所有程序 > Anti-DDoS Collector > Uninstall Collector”。

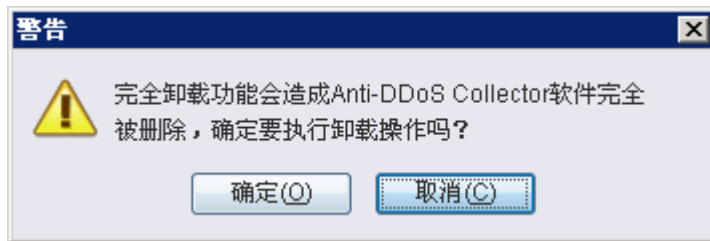
步骤3 在“卸载方式提示”对话框中，选择“完全卸载”。



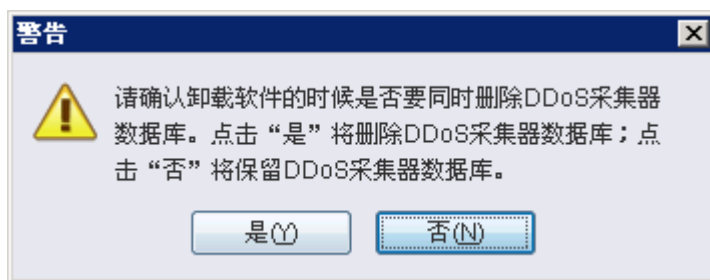
步骤4 单击“下一步”，弹出“卸载组件确认”对话框。



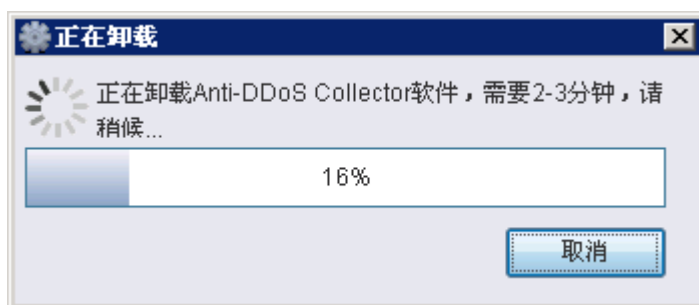
步骤5 单击“下一步”，弹出“警告”对话框。确认删除采集器。



步骤6 弹出“警告”对话框。单击“确定”，删除Anti-DDoS采集器的数据库。
选择单击“取消”将保留历史数据，可供后续再次安装时使用。



步骤7 弹出卸载进度条，开始卸载。单击“取消”，终止卸载操作。



步骤8 弹出“提示”，说明Anti-DDoS采集器卸载成功。



步骤9 单击“确定”，结束卸载。

步骤10 可选: 如果不保留历史数据，请手动删除Anti-DDoS采集器安装目录，如“D:\VSM\antiddos_collector”。

----结束

8.2.3 卸载异常处理

如何处理由于Anti-DDoS采集器意外掉电、重新启动、系统崩溃或维护人员误操作等原因，导致正在运行的卸载程序异常关闭，卸载失败。

操作步骤

- 步骤1** 检查Anti-DDoS采集器是否已掉电。如果服务器电源指示灯灭，则表明已掉电，请重新打开电源开关。
- 步骤2** 选择“开始 > 控制面板 > 管理工具 > 服务”。
- 步骤3** 按表8-2顺序，停止服务。右键单击该服务，在弹出的快捷菜单中选择“停止”。

表 8-2 停止系统服务顺序

服务名称	使用对象
mysqservice	ATIC管理中心服务器软件
Anti-DDoS Collector Monitor Service	Anti-DDoS采集器软件
Anti-DDoS Collector Service	Anti-DDoS采集器软件

- 步骤4** 选择“开始 > 运行”，输入cmd，打开命令行窗口。
- 步骤5** 按表8-2顺序，删除服务。输入命令`sc delete service name`。其中`service name`为服务名称。
- 步骤6** 可选: 如果不保留历史数据，请手动删除安装目录，如“D:\VSM\antiddos_collector”。
- 步骤7** 手动删除“开始”菜单中的快捷方式。选择“开始 > 所有程序”，鼠标右键单击“Anti-DDoS Collector”，在弹出的快捷菜单中选择“删除”。
- 步骤8** 打开操作系统本地用户文件夹（Windows 2003操作系统为“C:\Documents and Settings\administrator”，Windows 2008操作系统为“C:\Users\Administrator”），删除以下文件：“ddosCollectorInstalled.xml”。

----结束

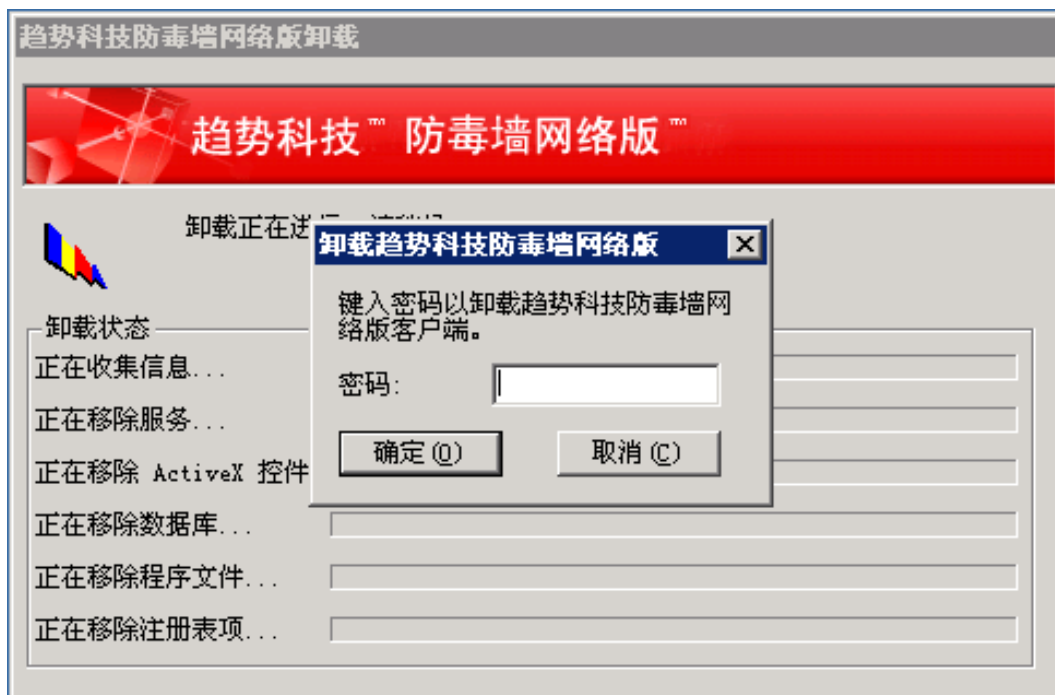
8.3 卸载趋势防毒软件

介绍如何在服务器和客户端上卸载趋势防毒软件。

8.3.1 卸载防毒软件客户端

操作步骤

- 步骤1** 登录客户机，选择“开始 > 所有程序 > 趋势科技防毒墙网络版客户端 > 卸载防毒墙网络版客户端”，卸载趋势科技防毒墙网络版客户端。
- 也可以选择从“控制面板 > 添加或删除程序”中删除趋势科技防毒墙网络版客户端。
- 步骤2** 输入客户端卸载密码。
- 单击“确定”。



步骤3 密码确认无误后，开始卸载趋势防毒软件客户端程序。



步骤4 卸载完毕后，卸载程序会自动关闭。

---结束

8.3.2 卸载防毒软件服务器

操作步骤

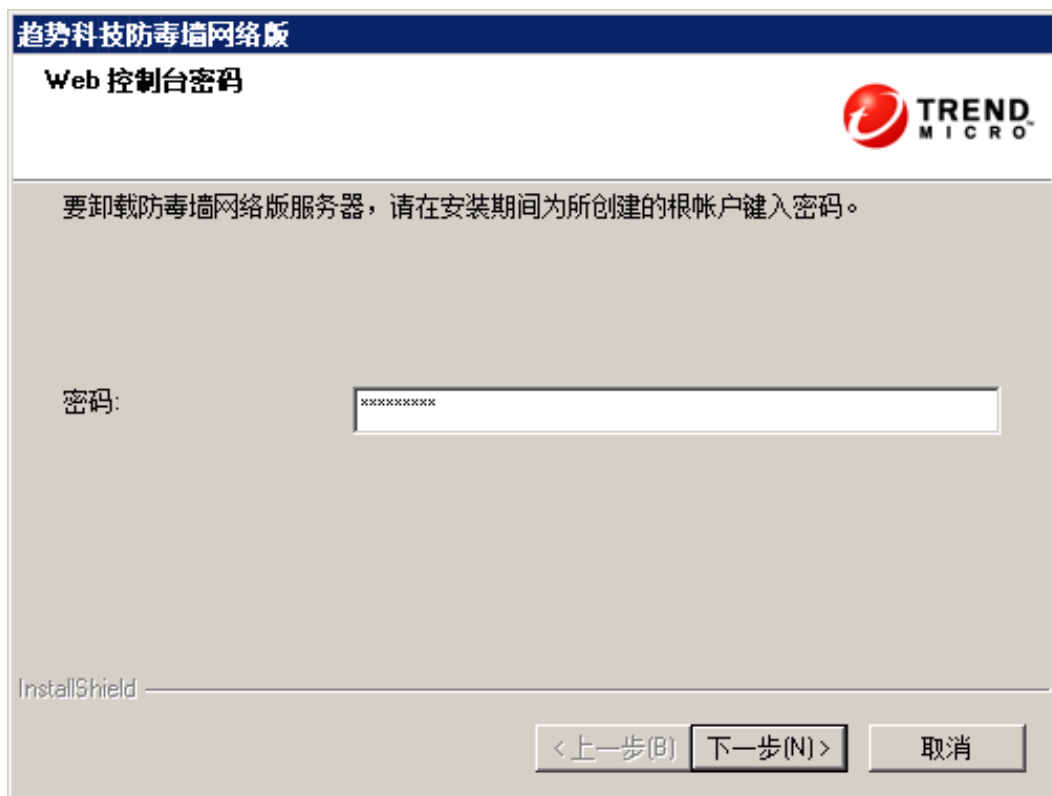
步骤1 登录服务器端，选择“开始>所有程序>趋势科技防毒墙网络版服务器>卸载防毒墙网络版”，卸载趋势科技防毒墙网络版服务器。

也可以选择从“控制面板>添加或删除程序”中卸载趋势科技防毒墙网络版服务器。

步骤2 系统弹出卸载对话框，单击“下一步”继续执行卸载程序。



步骤3 输入Web控制台密码，单击“下一步”继续执行卸装程序。



步骤4 密码确认无误后，单击“下一步”，开始卸载OfficeScan服务器程序。



步骤5 卸装完成后，弹出“卸装完成”对话框，单击“完成”，结束防毒墙网络版卸装。



---结束

9 附录

关于本章

- 9.1 如何查看Windows操作系统中某端口的占用情况及释放端口
- 9.2 ping程序被禁用导致安装服务器至33%时进程自动结束
- 9.3 使用HTTPS协议登录ATIC管理中心时，如何安装安全证书
- 9.4 修改ATIC管理中心服务器或采集器软件中IP地址的配置信息
- 9.5 修改ATIC管理中心服务器软件中WEB端口的配置信息
- 9.6 修改ATIC管理中心服务器和采集器软件中MySQL数据库的配置信息

9.1 如何查看 Windows 操作系统中某端口的占用情况及释放端口

背景信息

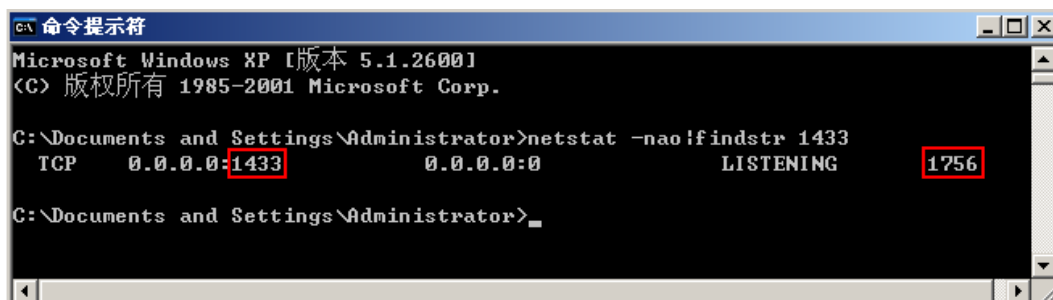
安装ATIC管理中心前，需要检查使用的端口是否被操作系统其他程序占用。如果端口已被占用，必须释放才能进行安装操作。

ATIC管理中心相关的端口请参见[1.3 端口列表](#)。这里以1433端口为例进行说明。

操作步骤

步骤1 选择“开始 > 所有程序 > 附件 > 命令提示符”。

步骤2 输入如下命令：`netstat -nao|findstr 1433`。



```
C:\> 命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -nao|findstr 1433
TCP 0.0.0.0:1433 0.0.0.0:0 LISTENING 1756

C:\Documents and Settings\Administrator>
```

说明

其中“1756”即占用端口“1433”的应用程序的进程号。

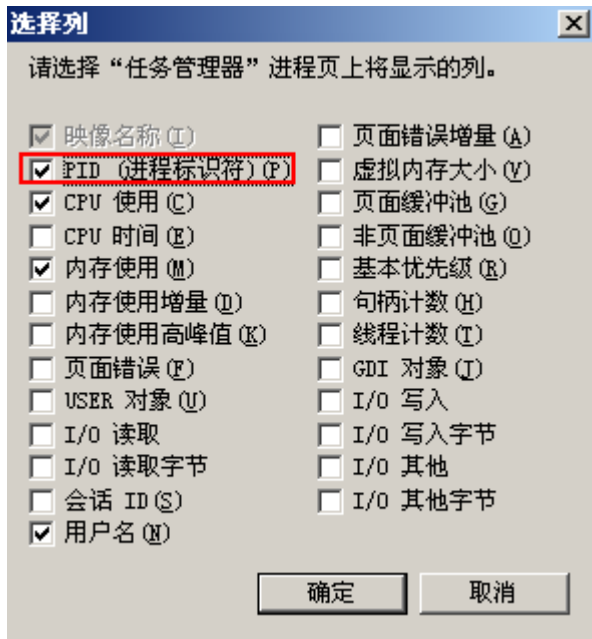
如果没有第三方软件占用此端口，则输入此命令后无返回信息。

步骤3 右键单击任务栏空白处，选择“任务管理器”。

步骤4 单击“进程”页签。

步骤5 选择“查看 > 选择列”。

步骤6 选中“PID（进程标识符）”复选框。



步骤7 单击“确定”。

步骤8 根据占用“1433”端口的PID“1756”在“Windows任务管理器”找到对应的进程。



步骤9 当此进程是网管进程之外的第三方软件时，结束该进程。

- 如果要避免该程序丢失数据，请以正常的方式停止该程序。不同的程序提供的停止方式不同，请参见该程序提供的文档，此处不再赘述。

- 如果需要强制结束进程并且确认丢失的是不重要的数据，选中目标进程，单击“结束进程”，在弹出的警告页面中，单击“是”。

---结束

9.2 ping 程序被禁用导致安装服务器至 33%时进程自动结束

现象描述

安装ATIC管理中心服务器至33%时，安装进程自动结束。

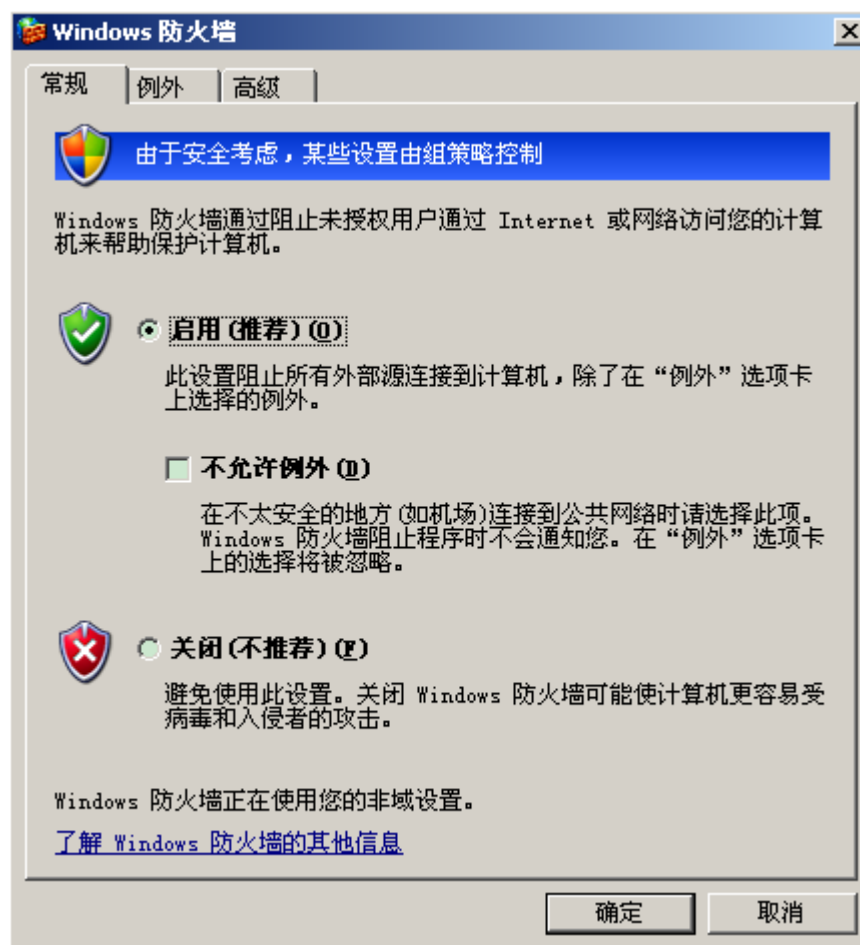
可能原因

服务器上开启了防火墙，但未将ping程序加入到例外程序，导致服务器无法ping通数据库（数据库的默认安装地址是127.0.0.1），安装失败。

处理步骤

- 步骤1** 以具有administrator权限的操作系统用户登录操作系统。
以操作系统Windows Server 2003 R2 Standard with SP2为例。
- 步骤2** 选择“开始 > 设置 > 控制面板”。
- 步骤3** 双击“Windows 防火墙”。
界面如[图9-1](#)所示。

图 9-1 打开“Windows 防火墙”

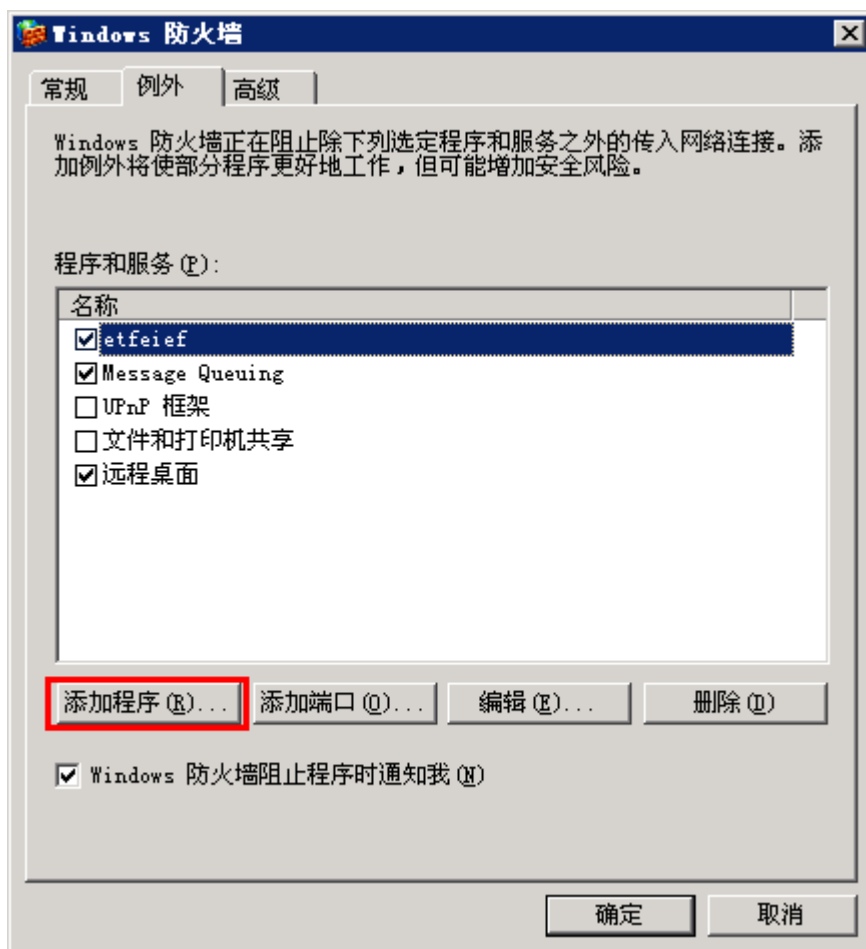


 说明

请确保未选中“不允许例外”。

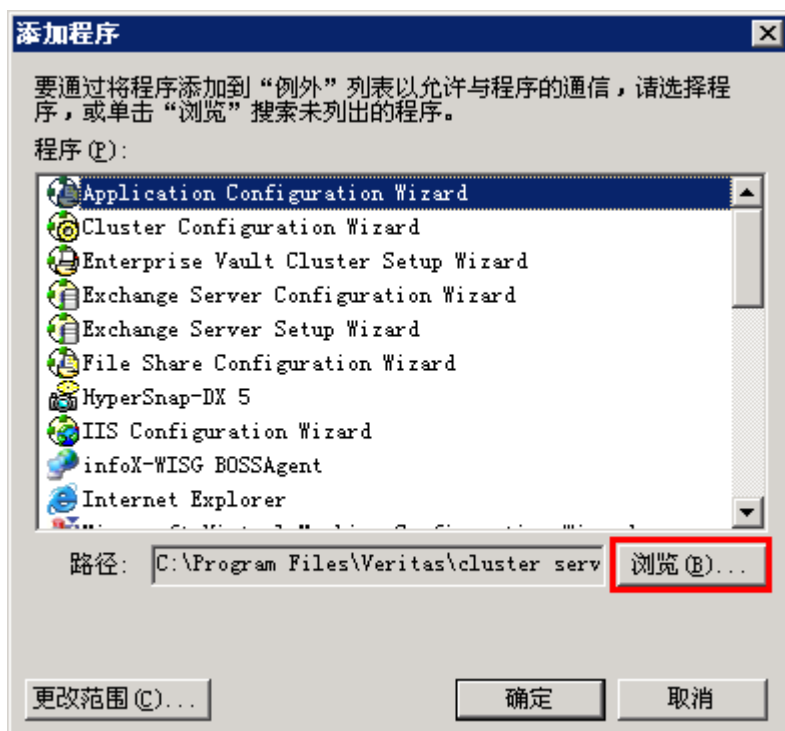
- 步骤4** 单击“例外”页签。
界面如图9-2所示。

图 9-2 添加例外程序



步骤5 单击“添加程序”。
界面如[图9-3](#)所示。

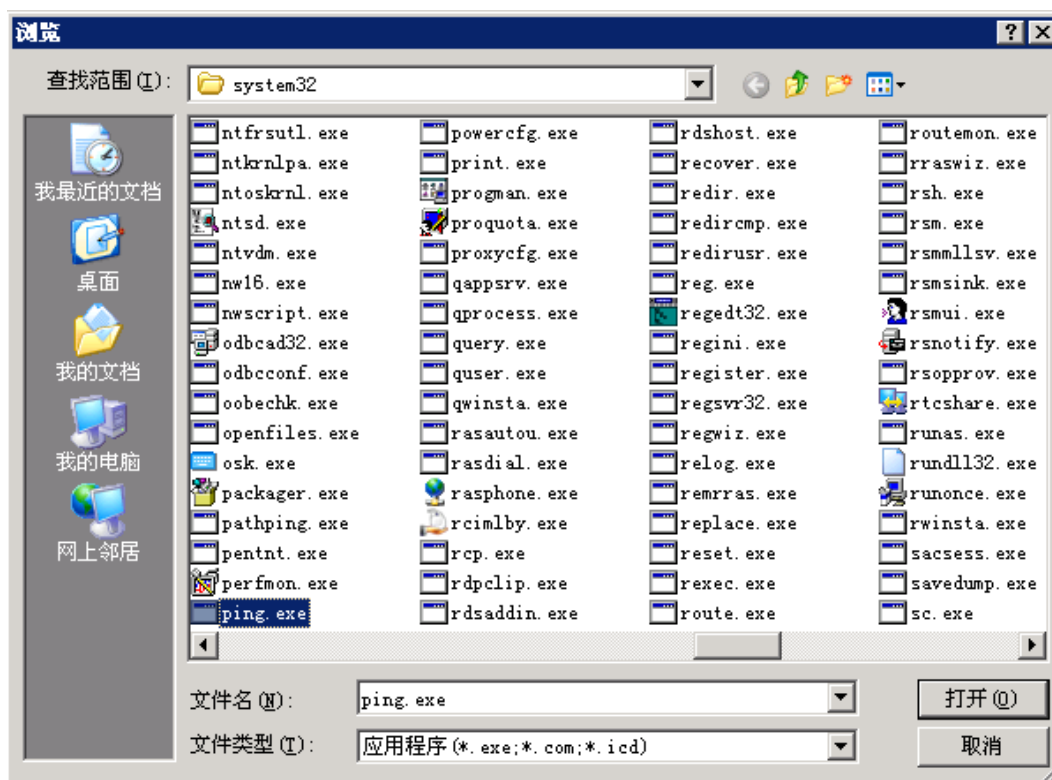
图 9-3 添加程序



步骤6 单击“浏览”。

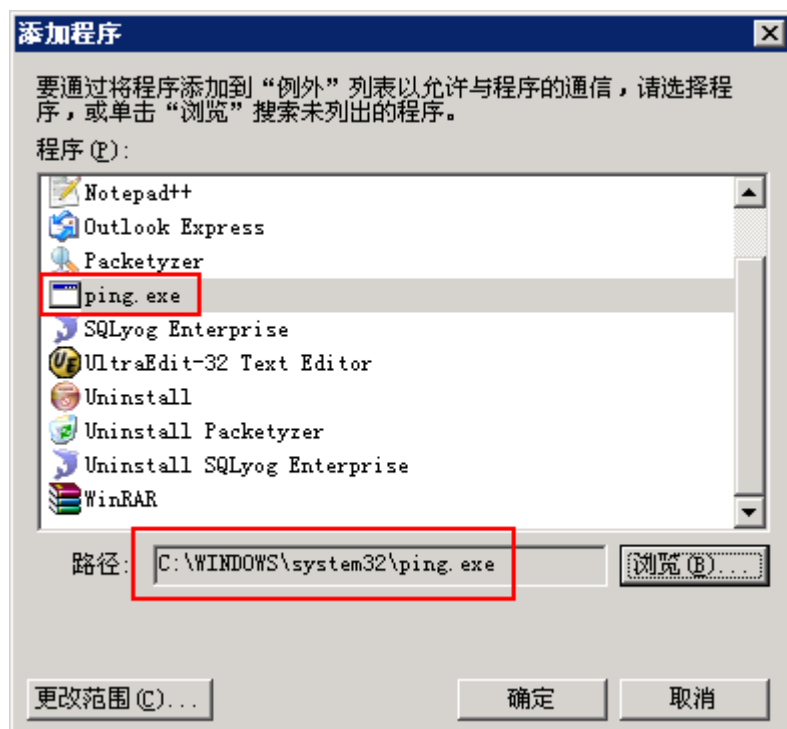
步骤7 在“C:\Windows\System32”目录下，选中“ping.exe”。
界面如图9-4所示。

图 9-4 找到 ping.exe 文件



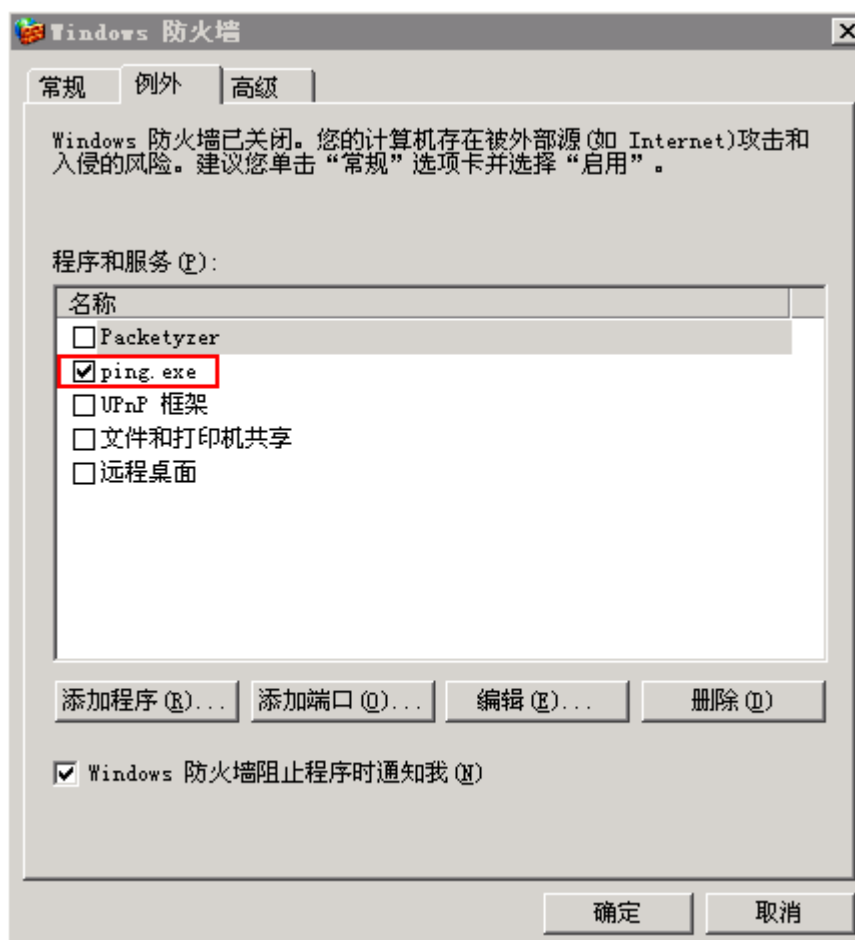
步骤8 单击“打开”。
界面如图9-5所示。

图 9-5 将“ping.exe”程序加入例外程序中



步骤9 单击“确定”。
界面如[图9-6](#)所示。

图 9-6 “ping.exe” 程序已加入例外程序中



步骤10 单击“确定”。

步骤11 如果以上操作完成后，在服务器上仍然无法ping通数据库（数据库的默认安装地址是127.0.0.1），则重启防火墙。

在“Windows防火墙”界面的“常规”页签中，先关闭防火墙，单击“确定”，再启用防火墙，单击“确定”。

步骤12 如果通过以上步骤，问题仍无法解决，请联系技术支持工程师。

---结束

9.3 使用 HTTPS 协议登录 ATIC 管理中心时，如何安装安全证书

背景信息

使用HTTPS协议登录ATIC管理中心时，会显示安全证书有问题。需要先创建安全证书并将其导入到浏览器中，才能确保安全登录。

操作步骤

步骤1 创建安全证书。

1. 进入“D:\VSM\Runtime\bin”目录，双击该目录下的**certificate.bat**文件，生成证书。
系统提示您先选择通过HTTPS协议访问ATIC管理中心的ATIC管理中心服务器IP地址，然后生成安全证书。如果ATIC管理中心服务器配置了多个IP地址，系统将列出所有的IP地址供您选择。

Please select the IP address which you will use to access System by https protocol. Enter "exit" to exit.

1. 129.29.61.110
2. 129.29.61.112
3. 129.29.61.111

Please enter your option:[1]

2. 请根据网络规划情况选择ATIC管理中心服务器的IP地址，系统默认选择第一个IP地址。按“Enter”键。

Generating certificate. Please wait...

Generating certificate for IP address 129.29.61.110 succeeded.

Please enter any key to exit...

3. 证书生成完毕后，请按任意键退出界面。

步骤2 安装安全证书。

- IE浏览器下，请执行以下操作步骤导入安全证书。

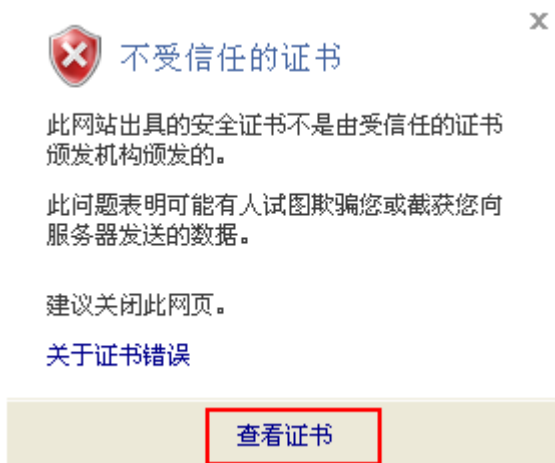
说明

本节以IE 8.0为例，介绍如何导入安全证书的操作步骤。其他版本的IE浏览器导入方法类似。

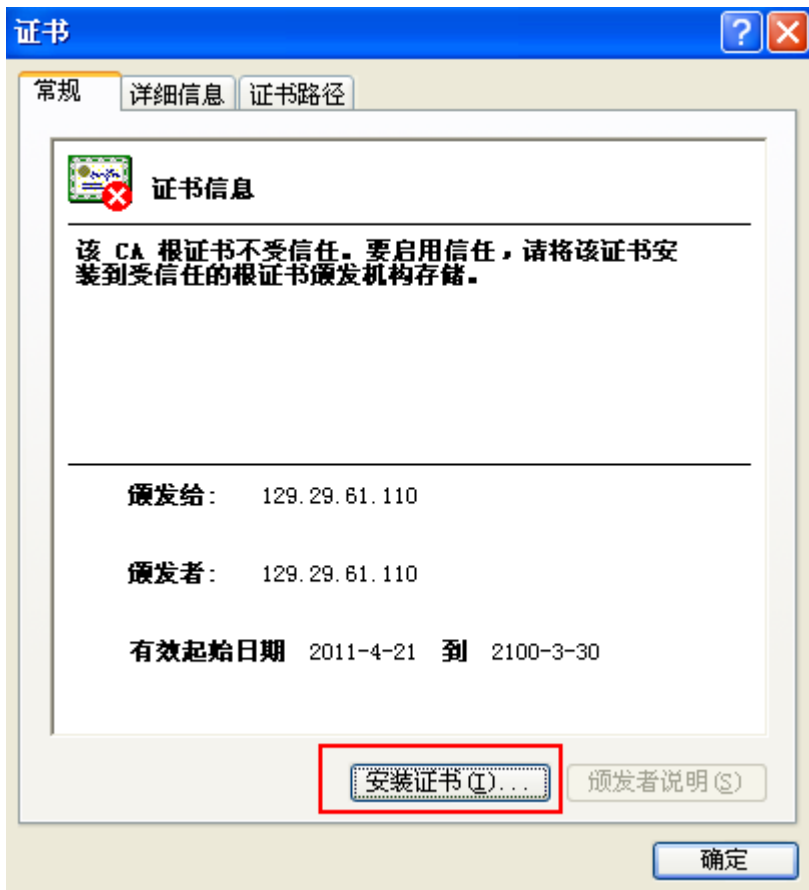
1. 打开IE浏览器，并在浏览器中输入“**https://IP:httpsport**”，登录ATIC管理中心。其中**IP**指启动ATIC管理中心时选择的ATIC管理中心服务器IP地址，**httpsport**指HTTPS服务端口。安装ATIC管理中心时，默认的HTTPS端口是443。如果安装时修改为其他端口，请输入端口号。



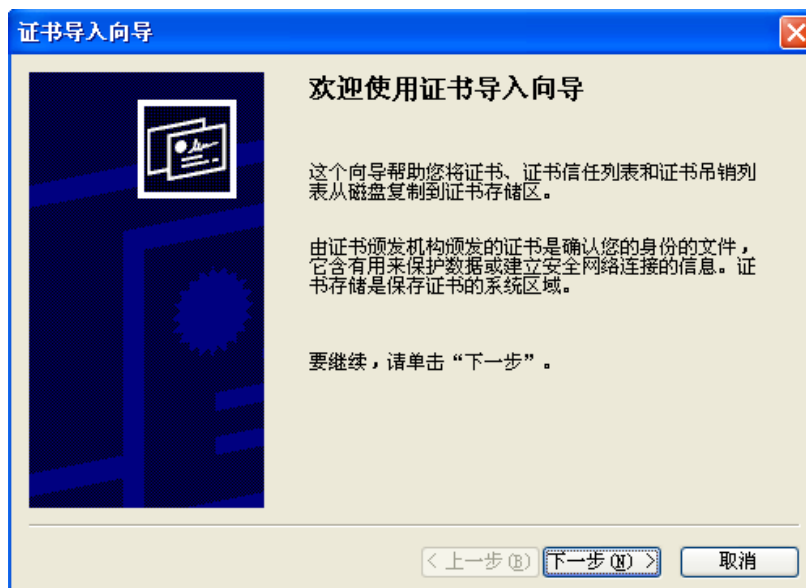
2. 系统提示“此网站的安全证书有问题”，需要您导入证书，单击“继续浏览此网站（不推荐）”。



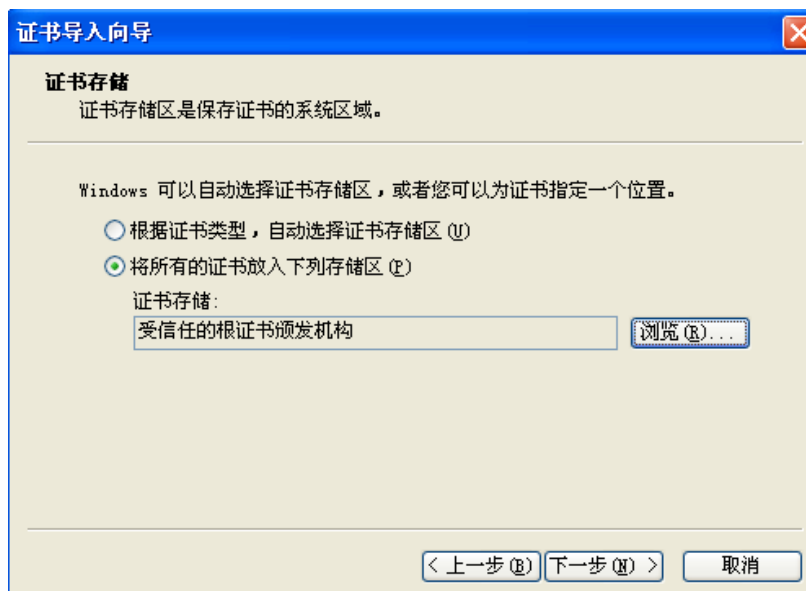
3. 单击浏览器地址栏右侧的“证书错误”，并在弹出窗口中单击“查看证书”。



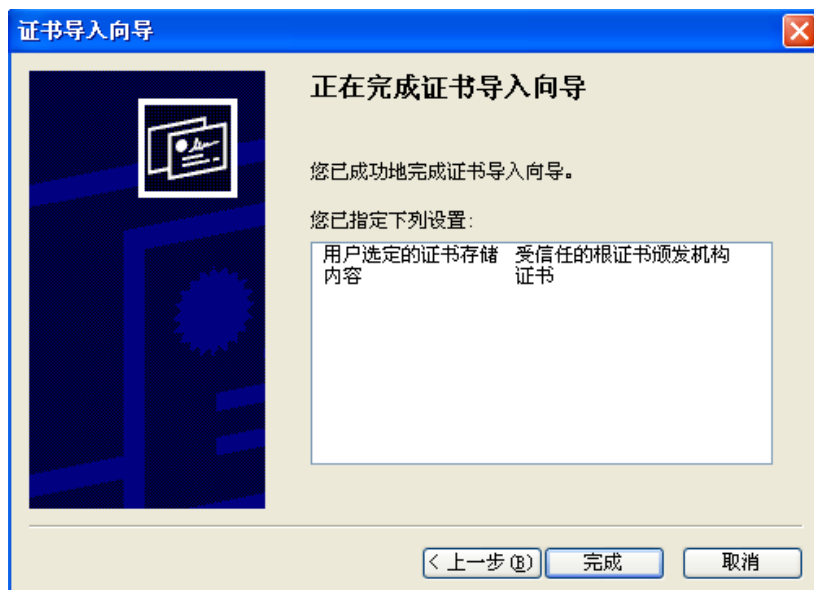
4. 在弹出的“证书”对话框中单击“安装证书”。



5. 在“证书导入向导”中，根据提示安装安全证书。单击“下一步”。



6. 选择证书的存储区，本节以自动选择证书存储区为例。选择“根据证书类型，自动选择证书存储区”，并单击“下一步”。



7. 完成证书导入后，单击“完成”。



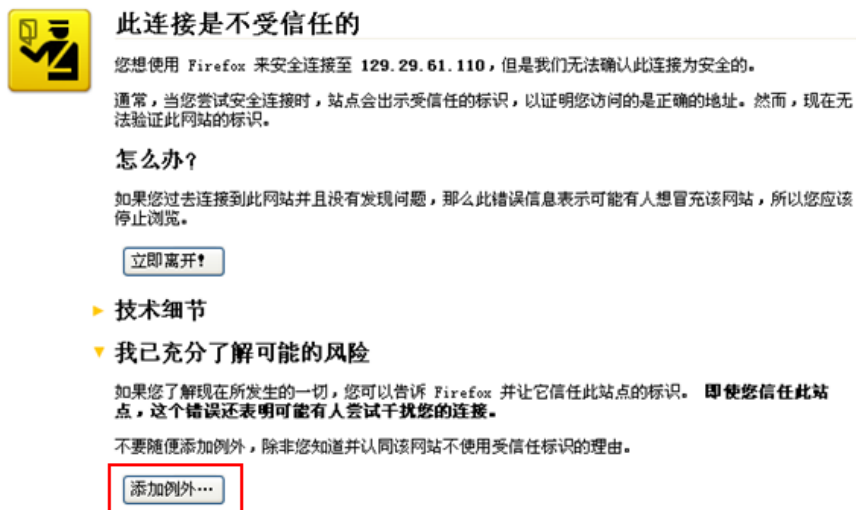
8. 在弹出的“安全警告”对话框中，单击“是”，确认安全证书的来源IP地址。
 9. 单击“确定”，导入证书成功。
- Firefox浏览器下，请执行以下操作步骤导入安全证书。

说明

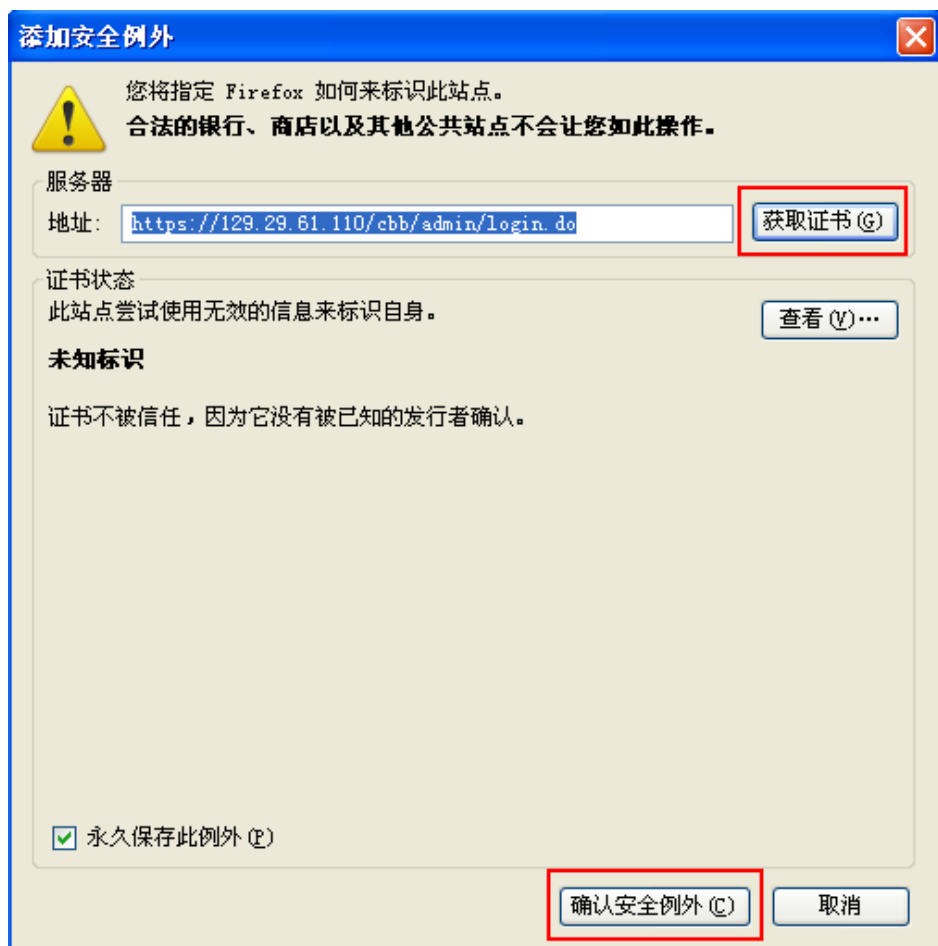
本节以Firefox 3.6.8为例，介绍如何导入安全证书的操作步骤。其他版本的Firefox浏览器导入方法类似。

1. 打开Firefox浏览器，并在浏览器中输入“https://IP:httpsport”，登录ATIC管理中心。

其中IP指启动ATIC管理中心时选择的ATIC管理中心服务器IP地址，httpsport指HTTPS服务端口。安装ATIC管理中心时，默认的HTTPS端口是443。如果安装时修改为其他端口，请输入端口号。



2. 系统提示“此连接是不受信任的”。单击“我已充分了解可能的风险 > 添加例外”。



3. 单击“获取证书”后，单击“确认安全例外”，导入证书。

步骤3 证书导入成功后，请关闭浏览器后再重新打开浏览器，并在浏览器地址栏中输入“https://IP:httpsport”，登录ATIC管理中心。

- 如果浏览器不再弹出证书错误的提示信息，且能够正常登录ATIC管理中心，表示安全证书已导入成功。
- 如果浏览器仍然弹出证书错误的提示信息，请检查ATIC管理中心服务器的IP地址选择是否正确。

---结束

9.4 修改 ATIC 管理中心服务器或采集器软件中 IP 地址的配置信息

当ATIC管理中心服务器或采集器的IP地址发生变化时，都会导致ATIC管理中心无法正常运行，必须修改ATIC管理中心软件中服务器或采集器IP地址的配置信息。

- 当ATIC管理中心服务器与采集器集中式部署时，修改IP地址配置信息，请参见[当ATIC管理中心服务器与采集器集中式部署时，修改IP地址配置信息的解决方法](#)。
- 当ATIC管理中心服务器与采集器分布式部署时，修改服务器IP地址配置信息，请参见[当ATIC管理中心服务器与采集器分布式部署时，修改服务器IP地址配置信息的解决方法](#)。
- 当ATIC管理中心服务器与Anti-DDoS采集器分布式部署时，修改Anti-DDoS采集器IP地址配置信息，请参见[当ATIC管理中心服务器与Anti-DDoS采集器分布式部署时，修改Anti-DDoS采集器IP地址配置信息的解决方法](#)。

当 ATIC 管理中心服务器与采集器集中式部署时，修改 IP 地址配置信息的解决方法

1. 以安装ATIC管理中心的管理员登录操作系统。
2. 修改ATIC管理中心软件服务器IP地址。
 - a. 选择“开始 > 所有程序 > ATIC > Configuration Tool”。
 - b. 单击“服务器IP配置”页签，设置新的IP地址。



- c. 单击“确定”。

当ATIC管理中心服务和采集器服务正在运行时，系统弹出提示框提示将停止服务，单击“确定”。

- d. 系统开始修改IP地址，直到界面弹出修改IP成功的提示框。

 说明

如果界面弹出提示框提示同步修改数据库中采集器IP地址失败时，请检查ATIC管理中心与数据库的连通性。

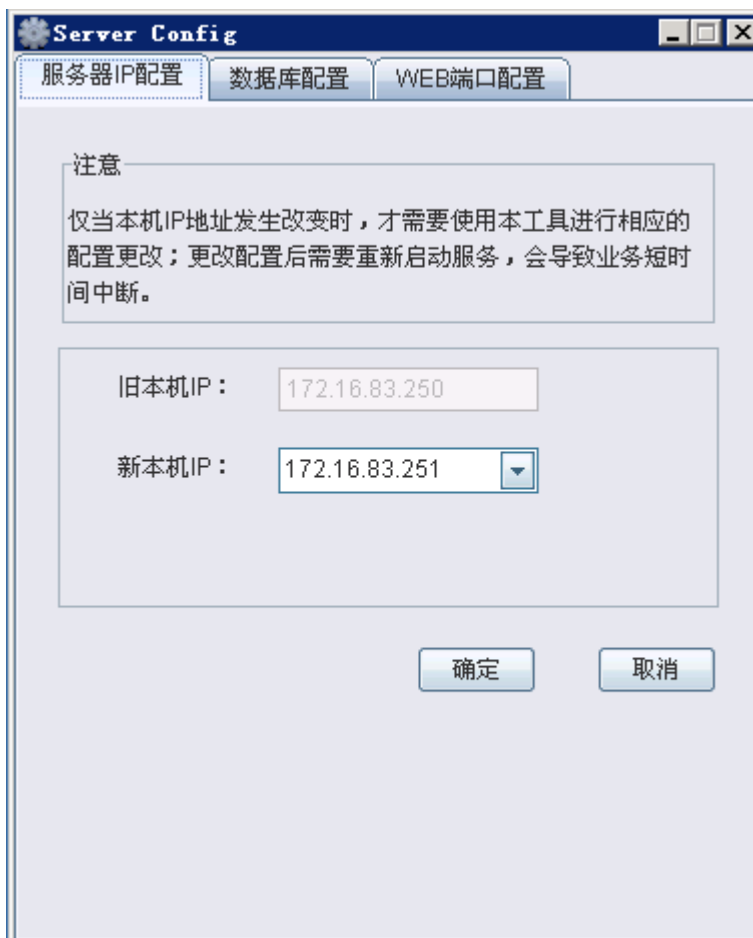
- e. 单击“确定”，重新启动服务。

3. 使用新的IP地址登录ATIC管理中心。

能够正常登录，并且如果ATIC管理中心中已添加采集器，那么采集器IP地址已修改且正常连接，说明修改服务器和采集器IP地址成功。

当 ATIC 管理中心服务器与采集器分布式部署时，修改服务器 IP 地址配置信息的解决方法

1. 修改ATIC管理中心软件服务IP地址。
 - a. 在服务器所在的机器上，以安装ATIC管理中心的管理员登录操作系统。
 - b. 选择“开始 > 所有程序 > ATIC > Configuration Tool”。
 - c. 单击“服务器IP配置”页签，设置新的IP地址。



- d. 单击“确定”。
当ATIC管理中心服务正在运行时，系统弹出提示框提示将停止服务，单击“确定”。
 - e. 系统开始修改IP地址，直到界面弹出修改IP成功的提示框。
 - f. 单击“确定”，重新启动服务。
2. 用新的IP地址登录ATIC管理中心。
能够正常登录，如果ATIC管理中心中已添加采集器，那么采集器连接正常，说明修改服务器IP地址成功。

当 ATIC 管理中心服务器与 Anti-DDoS 采集器分布式部署时，修改 Anti-DDoS 采集器 IP 地址配置信息的解决方法

1. 在安装Anti-DDoS采集器的机器上，以安装采集器时的管理员登录操作系统。
2. 选择“开始 > 所有程序 > Anti-DDoS Collector > Configuration Tool”。
3. 在“服务器IP配置”界面，设置修改后的采集器IP地址。



4. 单击“确定”，系统开始修改配置文件中的采集器IP地址，直到界面弹出修改IP成功的提示框。
5. 单击“确定”，重新启动服务。
6. 在ATIC管理中心中添加修改后的采集器IP地址，能够添加成功且连接正常，说明修改Anti-DDoS采集器IP地址成功。

9.5 修改 ATIC 管理中心服务器软件中 WEB 端口的配置信息

背景信息

当需要修改登录ATIC管理中心时使用的WEB端口或者修改通过HTTPS协议访问ATIC管理中心的IP地址时，请按照本节内容操作。

操作步骤

- 步骤1** 以安装ATIC管理中心的管理员登录操作系统。
- 步骤2** 选择“开始 > 所有程序 > ATIC > Stop ATIC”，停止ATIC管理中心服务。
- 步骤3** 选择“开始 > 所有程序 > ATIC > Configuration Tool”。
- 步骤4** 单击“WEB端口配置”页签。

HTTP端口默认为8080，HTTPS端口默认为443。



- 步骤5** 输入WEB端口修改后的信息：HTTP端口、HTTPS端口、通过HTTPS协议访问系统的IP地址。单击“测试”，弹出“检测完毕，所有端口均可用”提示框，表明修改后的这些端口可用，单击“确定”，退出提示页面。
- 步骤6** 单击“确定”。
- 步骤7** 系统开始修改WEB端口，直到弹出修改WEB端口成功的提示框。
- 步骤8** 单击“确定”，重新启用服务。
- 步骤9** 使用修改后的端口号能够登录ATIC管理中心，说明修改WEB端口成功。

---结束

9.6 修改 ATIC 管理中心服务器和采集器软件中 MySQL 数据库的配置信息

背景信息

当ATIC管理中心服务器使用的MySQL数据库的信息，如IP地址、TCP端口、用户名和密码等，发生变更后，需要立即手动修改ATIC管理中心服务器软件中的配置信息。否则ATIC管理中心将不能够正常运行。

操作步骤

步骤1 在安装服务器软件的操作系统中，选择“开始 > 所有程序 > ATIC > Configuration Tool”；在安装采集器软件的操作系统中，选择“开始 > 所有程序 > Anti-DDoS Collector > Configuration Tool”。

步骤2 单击“数据库配置”页签。

ATIC管理中心服务器和采集器安装时将在物理服务器上静默安装MySQL数据库。MySQL数据库使用的TCP端口：3306，用户名：ddosatic，密码：Admin_123。

以服务器软件界面为例。



步骤3 输入数据库修改后的信息：IP地址、TCP端口、用户名和密码等。单击“连接测试”，弹出“连接成功”提示框，表明修改内容正确，单击“确定”，退出提示页面。

步骤4 单击“确定”。

当ATIC管理中心服务或采集器服务正在运行时，系统弹出提示框提示将停止服务，单击“确定”。

步骤5 系统开始修改数据库的配置信息，直到界面弹出修改数据库成功的提示框。

步骤6 单击“确定”，重新启动服务。

---结束