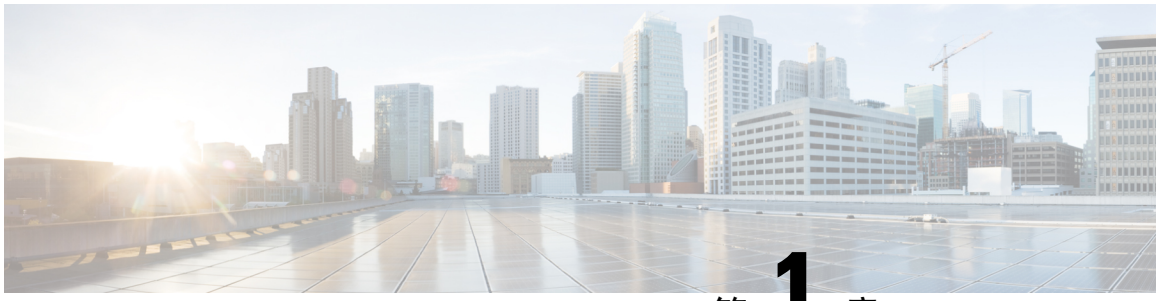
Cisco Secure Firewall Management Center 终端服务代理指南，版本 1.3

首次发布日期: 2021 年 3 月 2 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



第 1 章

管理中心终端服务代理简介

关于管理中心终端服务 (TS) 代理

Cisco Secure Firewall Management Center 终端服务代理允许Cisco Secure Firewall Management Center（以前称为 Firepower 管理中心） 唯一标识 Microsoft Windows 终端服务器监控的用户流量。如果没有 TS 代理，系统会将来自 Microsoft Windows 终端服务器的所有流量都识别为源自一个 IP 地址的一个用户会话。

注释 为避免潜在问题并确保您使用的最新软件，思科建议使用最新发布的 TS 代理版本。要查找最新版本，请访问思科支持站点。

在 Microsoft Windows 终端服务器上安装和配置时，TS 代理会为各个用户会话分配端口范围，并将该范围内的端口分配给用户会话中的 TCP 和 UDP 连接。系统会使用唯一端口来识别网络上用户的各个 TCP 和 UDP 连接。端口范围按最近最少使用时间来分配，这意味着在用户会话结束后，不会立即为新用户会话重新使用相同的端口范围。

注释 ICMP 消息会在没有端口映射的情况下传递。

在计算机的系统情景中运行的服务所生成的流量不会被 TS 代理跟踪。特别是，TS 代理不会识别服务器消息块 (SMB) 流量，因为 SMB 流量在系统环境中运行。

TS 代理支持每台 TS 代理 主机最多 199 个同步用户会话。如果单个用户同时运行多个用户会话，则 TS 代理会为每个单独的用户会话分配唯一的端口范围。当用户结束会话时，TS 代理可以将该端口范围用于另一个用户会话。

每个管理中心最多支持同时连接 50 个 TS 代理。

服务器上安装的 TS 代理有三个主要组件：

- 接口 - 用于配置 TS 代理和监控当前用户会话的应用
- 服务 - 监控用户登录和注销的程序
- 驱动程序 - 执行端口转换的程序

TS 代理可用于以下一项：

- 管理中心 上的TS代理 可用于用户感知和用户控制。有关使用系统中TS代理 数据的详细信息，请参阅《*Cisco Secure Firewall Management Center* 配置指南》。

注释 要将 TS 代理 用于用户感知和控制，必须将其配置为仅向 管理中心 发送数据。有关更多信息，请参阅配置 TS 代理。

服务器和系统环境要求

您必须满足以下要求才能在系统上安装和运行 TS 代理。

注释 为避免潜在问题并确保您使用的最新软件，思科建议使用最新发布的 TS 代理版本。要查找最新版本，请访问思科支持站点。

服务器要求

在以下 64 位 Microsoft Windows 终端服务器版本之一上安装 TS 代理：

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

注释 TS 代理安装需要服务器上有 653KB 的可用空间。

注释 如果 TS 代理服务器使用代理 Web 流量的防病毒软件，则用户流量通常会分配给系统用户，并且管理中心会将这些用户视为“未知”。要避免此问题，请禁用网络流量代理。

TS 代理是与您的服务器上安装的以下终端服务解决方案兼容：

- Citrix Provisioning
- Citrix XenDesktop
- Citrix XenApp
- Xen 项目虚拟机监控程序
- VMware vSphere 虚拟机监控程序/VMware ESXi 6.0
- Windows 终端服务/Windows 远程桌面服务 (RDS)

此版本的 TS 代理支持使用单个网络接口控制器 (NIC) 进行端口转换和服务器-系统通信。如果服务器上有两个或多个有效NIC，则TS代理只会对您在配置期间指定的地址执行端口转换。有效的NIC必须有一个 IPv4 或 IPv6 地址，或每种类型的一个地址；一个有效的 NIC 不能有多个相同类型的地址。

注释 如果在连接到服务器的任何设备上启用了路由器通告，则这些设备可以将多个 IPv6 地址分配给服务器上的 NIC，并让用于 TS 代理的 NIC 失效。

系统要求

此版本的TS 代理支持连接到运行 6.4 或更高版本系统的独立或高可用性管理中心。

通过 TS 代理对管理中心问题进行故障排除

请参阅以下部分以了解通过 TS 代理对管理中心问题进行故障排除的信息。

有关此版本中已知问题和已修复问题的信息，请参阅已解决的问题，第 8 页。

管理中心不显示系统进程的用户信息

TS 代理不会跟踪在系统情景中运行的服务所生成的流量。特别是，请注意以下事项：

- TS 代理不会识别服务器消息块 (SMB) 流量，因为 SMB 流量在系统环境中运行。

- 一些防病毒应用会将 Web 流量代理到内部网关或云网关，以便在病毒到达客户端计算机之前将其捕获。但是，这意味着防病毒软件通常使用系统帐户；在这种情况下，管理中心会将用户视为“未知”。要解决此问题，请禁用网络流量代理。

未按预期发生 TS 代理用户超时

您必须将服务器上的时间与 管理中心上的时间进行同步。

TS 代理不转换用户会话端口

在以下情况下，TS 代理不会执行端口转换：

- 用户会话超过设置的**最大用户会话数**。例如，如果**最大用户会话数 (Max User Sessions)** 被设置为 29，则 TS 代理不会对第 30 个用户会话执行端口转换。
- 所有可用端口都在使用中。例如，如果**用户端口 范围**值为每个用户会话指定 1000 个端口，则 TS 代理不会对第 1001 个 TCP/UDP 连接执行端口转换，直到用户结束另一个 TCP/UDP 连接并释放端口。
- 用户会话没有关联的域。例如，如果服务器管理员的会话由本地系统而非外部 Active Directory 服务器进行身份验证，则服务器管理员登录到服务器但无法访问网络，并且TS代理不会为用户会话分配端口。

TS 代理未按预期执行端口转换

如果手动编辑服务器的 IP 地址，则必须编辑TS 代理上的**服务器 NIC (Server NIC)**。然后，保存 TS 代理配置并重新启动服务器。

TS 代理将用户报告为“未知”且规则不匹配

如果其他供应商的终端服务代理与思科终端服务 (TS) 代理在同一服务器上运行，则用户连接的端口号可能不在指定的用户端口范围内。因此，用户可能会被标识为“未知”用户，从而导致身份规则与用户不匹配。

要解决此问题，请禁用或卸载与思科 TS 代理在同一服务器上运行的其他终端服务代理。

未按预期向管理中心报告用户会话

如果更新TS代理配置以连接到不同的管理中心，则必须在保存新配置之前结束所有当前用户会话。有关详细信息，请参阅结束当前用户会话，第 23 页。

客户端应用流量作为用户流量报告给管理中心

如果服务器上安装了客户端应用，并且该应用配置为绑定到使用**系统端口**之外的端口的套接字，则必须使用**排除端口 (Exclude Port)** 字段从转换中排除该端口。如果未排除该端口且该端口属于您的**用户端口**，则 TS 代理可能会将该端口上的流量报告为不相关的用户流量。

为防止出现这种情况，请将客户端应用配置为绑定到使用**系统端口**范围内的端口的套接字。

服务器应用超时、浏览器超时或 TS 代理-管理中心连接失败

如果 TS 代理服务器上的应用结束 TCP/UDP 连接，但未完全关闭关联的端口，则 TS 代理无法使用该端口进行转换。如果 TS 代理在服务器完全关闭端口之前尝试使用该端口进行转换，则连接会失败。

注释　您可以使用 `netstat` 命令（用于摘要信息）或 `netstat -a -o -n -b` 命令（用于详细信息）来识别未完全关闭的端口；这些端口的状态为 `TIME_WAIT` 或 `CLOSE_WAIT`。

如果您遇到此问题，请扩大受此问题影响的 TS 代理端口范围：

- 如果错误关闭的端口在**用户端口**范围内，则会发生服务器应用或浏览器超时。
- 如果错误关闭的端口在**系统端口**范围内，则会发生 TS 代理-管理中心连接失败。

TS 代理-管理中心连接失败

如果在配置过程中点击**测试 (Test)** 按钮时 TS 代理无法与管理中心建立连接，请检查以下各项：

- 确保不超过 50 个 TS 代理客户端同时尝试连接到管理中心。
- 确认您提供的**用户名**和**密码**是具有 REST VDI 权限的 管理中心用户的正确凭证，如创建 REST VDI 角色，第 17 页中所述。

  您可以查看管理中心上的审核日志，以确认 TS 代理的用户身份验证是否成功。
- 如果在配置后立即连接到高可用性配置中的辅助管理中心失败，则这属于预期的行为。TS 代理始终与主用管理中心通信。

  如果辅助管理中心被激活，则与主要管理中心的连接将失败。

服务器上的系统进程或应用出现故障

如果服务器上的系统进程正在使用或侦听不在**系统端口**范围内的端口，则必须使用**排除端口 (Exclude Port)** 字段手动排除该端口。

如果服务器上的应用正在使用或侦听 Citrix MA 客户端 (2598) 或 Windows 终端服务器 (3389) 端口，请确认在**排除端口 (Exclude Port)** 字段中排除这些端口。

管理中心 显示 TS 代理中的“未知”用户

在以下情况下，管理中心会显示来自 TS 代理中的“未知”用户：

- 如果 TS 代理驱动程序组件意外失败，则在停机期间看到的用户会话将在管理中心上记录为未知用户。
- 一些防病毒应用会将 Web 流量代理到内部网关或云网关，以便在病毒到达客户端计算机之前将其捕获。但是，这意味着防病毒软件通常使用系统帐户；在这种情况下，管理中心会将用户视为“未知”。要解决此问题，请禁用网络流量代理。

- 如果高可用性配置中的主管理中心发生故障，则在故障转移期间的 10 分钟停机时间内由 TS 代理报告的登录将按如下方式进行处理：
  - 如果以前未在管理中心上看到过用户，并且TS代理报告了用户会话数据，则该数据在管理中心上记录为“未知”用户活动。
  - 如果之前在管理中心上看到过该用户，则会正常处理数据。

停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

NIC 未显示在服务器 NIC 列表中

您必须在任何连接到服务器的设备上禁用路由器通告消息。如果启用了路由器通告，则设备就会为服务器上的 NIC 分配多个 IPv6 地址，从而让 NIC 无法与 TS 代理一起使用。

有效的 NIC 必须有一个 IPv4 或 IPv6 地址，或每种类型的一个地址；一个有效的 NIC 不能有多个相同类型的地址。

排除 TS 代理的问题

管理中心测试连接失败

如果您以本地用户（而不是域用户）身份登录到 TS 代理服务器，则管理中心测试的 TS 代理测试连接将失败。发生这种情况是因为，默认情况下，TS 代理不允许系统进程在网络上通信。

要解决此问题，请执行以下任一操作：

- 选中**配置 (Configure)** 选项卡页面上的**未知流量通信 (Unknown Traffic Communication)** 以允许流量，如TS 代理配置字段，第 13 页中所述。
- 以域用户（而不是本地用户）身份登录 TS 代理计算机。

TS 代理将用户报告为“未知”且规则不匹配

如果其他供应商的终端服务代理与思科终端服务 (TS) 代理在同一服务器上运行，则用户连接的端口号可能不在指定的用户端口范围内。因此，用户可能会被标识为“未知”用户，从而导致身份规则与用户不匹配。

要解决此问题，请禁用或卸载与思科 TS 代理在同一服务器上运行的其他终端服务代理。

升级时 TS 代理提示重启

有时，即使计算机的 IP 地址未发生变化，升级后 TS 代理也会报告 IP 地址更改，并提示您重新启动服务器。出现这种情况是因为 TS 代理检测到 IP 地址与以下注册表键值之间存在差异：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TSAgent\{IPv4 | IPv6}
```

如果键值与配置的主适配器 IP 地址不同，TS 代理会报告这一变化，并指示您保存配置和重启计算机。

例如，如果计算机被重新镜像或从备份中恢复，而 DHCP 分配了一个新的 IP 地址，就会出现这种情况。

您可以忽略该错误，但升级后无论如何都必须重启计算机。

Citrix Provisioning 客户端无法启动

您必须将 TS 代理配置为忽略为 Citrix Provisioning 服务器配置的 UDP 端口。

在TS 代理**保留端口 (Reserve Port)**字段中指定的值必须与 Citrix 调配**第一个和最后一个 UDP 端口号 (First and Last UDP port numbers)** 端口中的一个相匹配。

⚠

注意 如果未指定正确的端口，客户端将无法启动。

保存 TS 代理 IP 地址时的例外情况

当您尝试使用无效 IP 地址保存 TS 代理配置时，在极少数情况下会显示例外情况。无效 IP 地址可以是以下任何一种：

- 与网络上其他设备的 IP 地址相同。
- 在 TS 代理应用打开时更改 Windows 中的静态 IP 地址。

例外情况包括：

- `System.ArgumentException`：已经添加了具有相同密钥的项目。
- `System.NullReferenceException`：对象引用未设置为对象实例。

解决方法：将 TS 代理服务器的 IP 地址设置为有效的 IP 地址，保存 TS 代理配置，然后重新启动服务器。

通过用户代理进行问题故障排除

如果使用 TS 代理 和用户代理，则可以从用户代理排除 TS 代理 IP 地址，以免日志中出现非关键性错误。如果 TS 代理和用户代理检测到同一用户，则非关键性错误会写入日志。

为防止出现此情况，请排除 TS 代理的 IP 地址，以免用户代理进行记录。有关详细信息，请参阅《*Firepower* 用户代理配置指南》。

已解决的问题

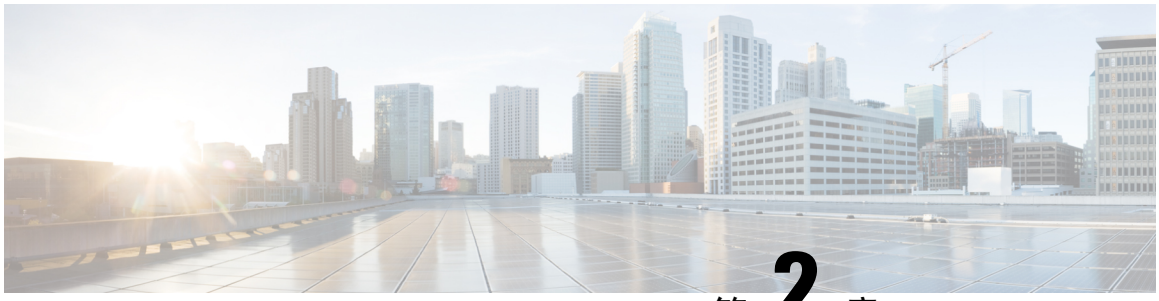
已解决的问题

Caveat ID 号码	说明
CSCvp10012	如果安装了 TS 代理，Windows 服务器将不再无响应。
CSCvn28482	执行 TAC 转储时，TS 代理不再无响应。此外，还会向转储中添加一个带有驱动程序过滤器的 XML 文件。

TS 代理的历史记录

特性	版本
• 新增了对 Citrix Provisioning 的支持 • 在TS 代理**保留端口 (Reserve Port)**字段中指定的值必须与 Citrix 调配**第一个和最后一个 UDP 端口号 (First and Last UDP port numbers)** 端口中的一个相匹配。 注意 如果未指定正确的端口，客户端将无法启动。	1.3

特性	版本
• 检测服务器上的 IP 地址变化，提示您保存配置并重新启动。请参阅 TS 代理配置字段，第 13 页。 • 使您能够升级到此版本，而无需卸载以前的版本。请参阅 安装或升级 TS 代理，第 11 页。 • 已将**排除端口 (Exclude Port)** 配置字段重命名为**保留端口 (Reserve Port)**. 请参阅 TS 代理配置字段，第 13 页。 • 对临时端口的支持。请参阅 TS 代理配置字段，第 13 页。 • 当超过 50% 的 TCP 或 UDP 端口用于特定会话时，**监控 (Monitor)** 选项卡页面会向您发出警告。请参阅 查看关于 TS 代理 的信息，第 19 页。 • 按最近使用最少的方式分配的用户会话端口范围。请参阅 关于管理中心终端服务 (TS) 代理，第 1 页。 • 让您能将故障排除信息导出到 XML 文件。请参阅 查看关于 TS 代理 的信息，第 19 页。 • 让您能够将用户会话重新传输到 管理中心。请参阅 查看关于 TS 代理 的信息，第 19 页。 • 尝试在卸载 TS 代理时结束所有用户会话。请参阅 卸载 TS 代理，第 24 页。	1.2
• 默认最大用户会话数从 200 更改为 30。 • 端口范围从 200 或更多更改为 5000 或更多 这些更改都将在TS 代理配置字段，第 13 页中讨论。	1.1
TS 代理 引入的功能。TS 代理让管理员能够使用端口映射来跟踪用户活动。安装在终端服务器上时，TS 代理会为各个用户会话分配端口范围，并将该范围内的端口分配给用户会话中的 TCP 和 UDP 连接。系统会使用唯一端口来识别网络上用户的各个 TCP 和 UDP 连接。	1.0



第 2 章

安装和配置 TS 代理

安装或升级 TS 代理

开始之前

- 确认您的环境支持 TS 代理，如服务器和系统环境要求， 第 2 页中所述。
- 结束所有当前用户会话，如结束当前用户会话， 第 23 页中所述。

步骤 1 以具有管理员权限的用户身份登录到服务器。

步骤 2 从支持站点下载 TS 代理软件包：`TSAgent-1.3.0.exe`。

注释 直接从站点下载更新。如果通过邮件传输文件，文件可能会损坏。

步骤 3 右键点击`TSAgent-1.3.0.exe`，然后选择**以管理员身份运行 (Run as Administrator)**。

步骤 4 点击**安装 (Install)**，然后按照提示安装或升级 TS 代理。
您需要重新启动计算机才能使用 TS 代理。

下一步做什么

- 确认 TS 代理正在运行，如查看 TS 代理服务组件的状态， 第 23 页中所述。
- 启动 TS 代理，如启动和停止 TS 代理进程， 第 24 页中所述。
- 按照配置 TS 代理， 第 12 页中所述配置 TS 代理。

如果是从较早的 TS 代理版本升级，并且使用的是 Citrix Provisioning，则升级后必须在**保留端口 (Reserve Port)** 字段中输入 `6910`。

注释 如果 TS 代理安装程序报告 .NET Framework 失败，请运行 Windows 更新并尝试重新安装 TS 代理。

启动TS 代理配置界面

引用

如果桌面上有 TS 代理快捷方式，请双击该快捷方式。否则，请使用以下程序启动 TS 代理配置界面。

步骤 1 以具有管理员权限的用户身份登录到服务器。

步骤 2 打开 `C:\Program Files (x86)\Cisco\Terminal Services Agent`。

步骤 3 查看 TS 代理的程序文件。

注释 程序文件仅供查看。请勿删除、移动或修改这些文件。

步骤 4 双击 `TSAgentApp` 文件以启动 TS 代理。

配置 TS 代理

使用 TS 代理接口来配置 TS 代理。您必须保存更改并重新引导服务器，更改才会生效。

开始之前

- 如果要连接到系统，请按照《*Cisco Secure Firewall Management Center* 配置指南》中的说明，针对服务器要监控的用户配置并启用一个或多个 Active Directory 领域。
- 如果要连接到系统，请配置具有 REST VDI 权限的用户帐户。

  您必须在管理中心中创建 REST VDI 角色，如创建 REST VDI 角色，第 17 页中所述。
- 如果您已经连接到系统，并且正在更新 TS 代理配置以连接到不同的管理中心，则必须在保存新配置之前结束当前的所有用户会话。有关详细信息，请参阅结束当前用户会话，第 23 页。
- 将 TS 代理服务器上的时间与系统上的时间同步。
- 查看并了解配置字段，如 TS 代理配置字段，第 13 页中所述。

步骤 1 在安装了 TS 代理的服务器上，启动 TS 代理，如启动TS 代理配置界面，第 12 页中所述。

步骤 2 点击**配置 (Configure)**。

步骤 3 导航到选项卡页面的常规设置部分。

步骤 4 在**最大用户会话数 (Max User Sessions)** 中输入值。

步骤 5 选择要用于端口转换和通信的**服务器 NIC**。

如果服务器的 IP 地址稍后发生变化，则系统会提示您保存配置并重新启动服务器以便让变化生效。

步骤 6 在**系统端口 (System Ports)** 和**用户端口 (User Ports)** 中输入值。在有效配置中，系统和用户端口范围不重叠。

步骤 7 在 **保留端口 (Reserve Port)** 中输入值（以逗号分隔）。

预留端口 (Reserve Port) 会自动填充 Citrix MA 客户端 (2598)、Citrix Provisioning (6910) 和 Windows 终端服务器端口的预期值。您必须排除 Citrix MA 客户端和 Windows 终端服务器端口。

如果您使用的是 Citrix Provisioning，并且是从较早的 TS 代理版本升级，则必须在此字段中输入 **6910**。

步骤 8 导航到选项卡的 REST API 连接 (REST API Connection) 设置部分。

步骤 9 在**主机名/IP 地址 (Hostname/IP Address)** 和**端口 (Port)** 中输入值。

管理中心 需要使用**端口** 443。

步骤 10 输入**用户名**和**密码**。

步骤 11 或者，在第二行字段中重复步骤 9 和 10，以配置备用（故障转移）连接。

步骤 12 点击**测试 (Test)** 以测试 TS 代理与系统之间的 REST API 连接。

如果配置了主和辅助管理中心，则与辅助管理中心的测试连接会失败。这是预期行为。TS 代理始终与主用管理中心通信。如果主管理中心进行故障转移并变为非活动管理中心，则 TS 代理会与辅助（现在处于活动状态）管理中心通信。

步骤 13 点击**保存 (Save)** 并确认要重新启动服务器。

TS 代理配置字段

以下字段用于配置 TS 代理上的设置。

常规设置

表 *1:*“常规设置”字段

字段	说明
保留端口 (Reserve Port)	要让 TS 代理忽略的端口。以逗号分隔列表的形式输入要排除的端口。 TS 代理会使用 Citrix MA 客户端 (2598)、Citrix Provisioning (6910) 和 Wind 务器 (3389) 的默认端口值来自动填充**保留端口 (Reserve Port)**。如果未排除 口，需要使用这些端口的应用可能会失败。 在TS 代理**保留端口 (Reserve Port)**字段中指定的值必须与 Citrix 调配**第一个 UDP 端口号 (First and Last UDP port numbers)** 端口中的一个相匹配。 **注意** 如果未指定正确的端口，客户端将无法启动。 **注释** 如果服务器上的进程正在使用或侦听不在**系统端口**范围内的端 使用**保留端口 (Reserve Port)** 字段手动排除该端口。 **注释** 如果服务器上安装了客户端应用，并且该应用配置为使用特定 到套接字，则必须使用**保留端口 (Reserve Port)** 字段从转换中排
最大用户会话数	您希望 TS 代理监控的最大用户会话数。一个用户一次可以运行多个用户会 默认情况下，此版本的 TS 代理支持 29 个用户会话，最多 199 个用户会话
服务器 NIC	此版本的 TS 代理支持使用单个网络接口控制器 (NIC) 进行端口转换和服务 信。如果服务器上有两个或多个有效NIC，则TS代理只会对您在配置期间 执行端口转换。 TS 代理会使用安装TS 代理的服务器上的每个 NIC 的 IPv4 地址和/或 IPv6 充此字段。有效的 NIC 必须有一个 IPv4 或 IPv6 地址，或每种类型的一个 有效的 NIC 不能有多个相同类型的地址。 **注释** 如果服务器的IP地址发生变化，则系统会提示您保存配置并重 器以便让变化生效。 **注释** 您必须在任何连接到服务器的设备上禁用路由器通告消息。如 由器通告，则设备就可以为服务器上的 NIC 分配多个 IPv6 地址 NIC 无法与 TS 代理一起使用。

字段	说明
系统端口	用于系统进程的端口范围。TS代理将忽略此活动。配置**开始**端口以指示 位置。配置**范围**值以指示要为每个单独的系统进程指定的端口数。 思科建议的**范围**值为5000或更大。如果您发现TS代理经常用完系统进程 大**范围**值。 **注释** 如果系统进程需要指定的**系统端口**之外的端口，请将该端口 **口 (Exclude Port)** 字段中。如果未在**系统端口 (System Ports** 或排除系统进程使用的端口，则系统进程可能会失败。 TS 代理使用以下公式自动填充**结束**值： `( [Start value] + [Range value] ) - 1` 如果您的输入导致**结束**值超出了**用户端口**的**开始**值，则必须调整**开始**和
用户端口	要为用户指定的端口范围。配置**开始**端口以指示要开始范围的位置。配 示要在每个用户会话中为 TCP 或 UDP 连接指定的端口数。 **注释** ICMP 流量无需端口映射即可进行传递。 思科建议的**范围**值为1000或更大。如果您发现TS代理经常用完用户流量 大**范围**值。 **注释** 当使用的端口数超过**范围**值时，系统将阻止用户流量。 TS 代理使用以下公式自动填充**结束**值： `[Start value] + ( [Range value] * [Max User Sessions value] ) -` 如果您的输入导致**结束**值超过 65535，则必须调整**开始**和**范围**值。
临时端口	输入允许TS 代理监控的临时端口（也称为动态端口）范围。

字段	说明
未知流量通信	选中**允许 (Permit)** 以便让 TS 代理允许流量通过系统端口；但是，TS 代理口使用情况。系统端口供本地系统帐户或其他本地用户帐户使用。（本地存在于 TS 代理服务器上；它没有相应的 Active Directory 帐户。）您可以以允许以下类型的流量： • 允许本地系统帐户运行的流量（例如服务器消息块 (SMB)），而不是管理中心会将此流量识别为来自“未知”用户，因为该用户并不存在 Directory 中。 如果您使用本地系统帐户登录到TS代理服务器，启用此选项还使您能与管理中心的连接。 • 当用户或系统会话用完其范围内的所有可用端口时，TS代理将允许流端口。此选项会启用流量；管理中心会将流量识别为来自未知用户。 当系统端口需要用于保持系统健康时，如域控制器更新、身份验证、理接口 (WMI) 查询等，这尤其有用。 取消选中可阻止系统端口上的流量。

REST API 连接设置

您可以配置主连接和备用（故障转移）系统设备：

- 如果您的系统设备是独立的，请将 REST API 连接字段的第二行留空。
- 如果系统设备部署有备用（故障转移）设备，请使用第一行配置与主设备的连接，使用第二行配置与备用（故障转移）设备的连接。

表 *2*: “*REST API* 连接设置”字段

字段	说明
主机名/IP 地址 (Hostname/IP Address)	系统设备的主机名或 IP 地址。
端口 (Port)	系统用于 REST API 通信的端口。（管理中心通常使用端口 443。）
用户名 (Username) 和密码 (Password)	用于连接的凭证。 • 系统需要在管理中心上具有 REST VDI 权限的用户的用户名和密码。用户的详细信息，请参阅《*Cisco Secure Firewall Management Center S* 指南》。

创建 REST VDI 角色

要将TS 代理连接到管理中心，您的用户必须具有 REST VDI 角色。默认情况下未定义 REST VDI。您必须创建角色并将其分配给 TS 代理配置中使用的任何用户。

有关用户和角色的详细信息，请参阅《*Cisco Secure Firewall Management Center Snort 3* 配置指南》。

步骤 1 以有权创建角色的用户身份登录管理中心。

步骤 2 点击**系统 (System)** > **用户 (Users)**。

步骤 3 点击**用户角色 (User Roles)** 选项卡。

步骤 4 在“用户角色”(User Roles) 选项卡页面上，点击**创建用户角色 (Create User Role)**。

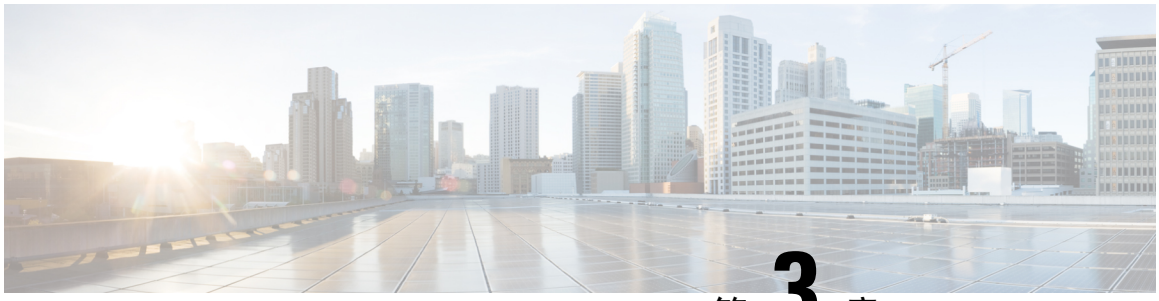
步骤 5 在“名称”(Name) 字段中输入 `REST VDI`。

角色名称不区分大小写。

步骤 6 在基于菜单的权限部分，选中 **REST VDI** 并确保同时选中**修改 REST VDI (Modify REST VDI)**。

步骤 7 点击**保存 (Save)**。

步骤 8 将角色分配给 TS 代理配置中使用的用户。



第 3 章

查看 TS 代理 数据

查看关于 TS 代理 的信息

使用以下程序查看网络上的当前用户会话，以及分配给每个会话的端口范围。数据为只读。

步骤 1 在安装了 TS 代理 的服务器上，按启动TS 代理配置界面， 第 12 页中所述启动 TS 代理接口。

步骤 2 点击**监控 (Monitor)** 选项卡。将显示以下列：

- **REST 服务器 ID (REST Server ID)**：报告信息的 管理中心 的主机名或 IP 地址。如果您使用的高可用性配置，那么这些信息将非常有用。
- **源 IP (Source IP)**：以 IPv4 和/或 IPv6 格式显示用户的 IP 地址值。如果同时配置了 IPv4 和 IPv6 地址，并且刚创建了新会话，则 IPv4 和 IPv6 地址将在不同的行中显示。
- **状态 (Status)**：显示为用户分配端口的状态。有关详细信息，请参阅查看连接状态， 第 20 页。
- **会话 ID (Session ID)**：标识用户会话的编号。一个用户一次可以有多个会话。
- **用户名 (Username)**：与此会话关联的用户名。
- **域 (Domain)**：用户登录的 Active Directory 域。
- **端口范围 (Port Range)**：分配给用户的端口范围。（值 0 表示分配端口时出现问题；有关详细信息，请参阅查看连接状态， 第 20 页）。
- **TCP 端口使用情况 (TCP Ports Usage)** 和 **UDP 端口使用情况 (UDP Ports Usage)**：显示每个用户的已分配端口百分比。当百分比超过 50% 时，字段背景为黄色。当百分比超过 80% 时，字段背景为红色。
- **登录日期 (Login Date)**：用户登录的日期。

步骤 3 下表显示可执行的操作：

项目	说明
点击列标题	按该列对表中的数据进行排序。

项目	说明
	在**按用户名过滤 (Filter by Username)** 搜索字段中输入用户名的一部分或完整用户名。
	点击可刷新此选项卡页面上显示的会话。
	将以下有关 TS 代理的故障排除信息导出为文本文件： • 包含 TS 代理配置数据的 XML 文件 • **netstat -a -n -o** 命令的输出 • Windows 任务列表 • 正在运行的驱动程序列表
	选中一个或多个会话旁边的框，以将这些会话重新传输到管理中心。您可以在管理中心的用户服务发生故障时使用此功能。 例如，假设用户在管理中心上的用户服务失败后登录到TS代理服务器。您可以使用此选项在用户服务恢复后再次发送用户会话。这应该会导致在“状态”(Status)列中为该用户显示**成功 (Success)**。

查看连接状态

当用户登录安装了TS代理的终端服务时，会创建一个新的系统会话，为该会话分配一个端口范围，并将结果发送到管理中心，以便传播到托管设备。

通过“监控”(Monitor) 选项卡页面，您可以确认端口范围是否已成功发送到管理中心。该进程可能失败的原因包括：

- 网络连接问题

  无效的 VDI 凭证
- 令牌到期
- 为该领域配置的域名不正确

步骤 1 在安装了 TS 代理 的服务器上，按启动TS 代理配置界面 ， 第 12 页中所述启动 TS 代理接口。

步骤 2 点击**监控 (Monitor)** 选项卡。

步骤 3 “状态”(Status) 列包含以下值之一：

- **待处理 (Pending)**：操作处于待处理状态，但尚未完成。

- **失败 (Failed)**：操作失败。点击**失败 (Failed)** 字样可查看错误消息。 如果错误指示与 管理中心的通信失败，请尝试重新传输该会话的流量，如查看关于 TS 代理 的信息中所述。
- **成功 (Success)**：操作已成功完成。

查看管理中心上的 TS 代理用户、用户会话和 TCP/UDP 连接数据

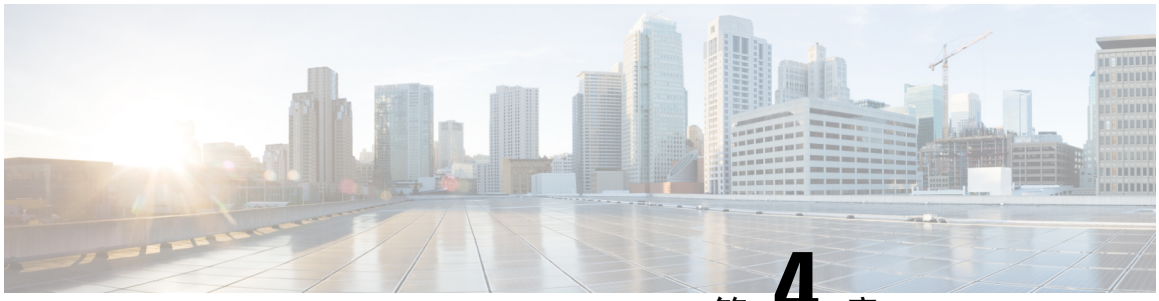
使用以下程序查看 TS 代理报告的数据。有关管理中心表的详细信息，请参阅《*Cisco Secure Firewall Management Center Snort 3* 配置指南》。

步骤 1 登录到您为服务器监控的用户配置了领域的管理中心。

步骤 2 要查看用户表中的用户，请选择**分析 (Analysis)** > **用户 (Users)** > **用户 (Users)**。如果 TS 代理用户的会话当前处于活动状态，管理中心将填充**当前 IP (Current IP)**、**结束端口 (End Port)** 和**开始端口 (Start Port)**列。

步骤 3 要查看用户活动表中的用户会话，请选择**分析 (Analysis)** > **用户 (Users)** > **用户活动 (User Activity)**。如果 TS 代理报告了用户会话，管理中心将填充**当前 IP (Current IP)**、**结束端口 (End Port)** 和**开始端口 (Start Port)**列。

步骤 4 要查看连接事件表中的 TCP/UDP 连接，请选择**分析 (Analysis)** > **连接 (Connections)** > **事件 (Events)**。管理中心会用报告连接的 TS 代理的 IP 地址填充**发起方/响应方 IP (Initiator/Responder IP)** 字段，并用 TS 代理分配给连接的端口填充**源端口/ICMP 类型 (Source Port/ICMP Type)** 字段。



第 4 章

管理TS 代理

结束当前用户会话

使用以下步骤从网络中注销用户并结束其会话。

步骤 1 以具有管理员权限的用户身份登录到 TS 代理服务器。

步骤 2 打开**开始 (Start)** > > **所有程序 [All Programs]** > **任务管理器 (Task Manager)**.

步骤 3 点击**更多详细信息 (More Details)** 展开窗口。

步骤 4 点击**用户 (Users)** 选项卡。

步骤 5 （可选）要通知用户您将结束其会话，请右键点击用户会话，然后选择**发送消息 (Send message)**。

步骤 6 右键点击用户会话，然后选择**结束 (Sign off)**。

步骤 7 点击**注销用户 (Sign out user)** 以确认操作。

查看 TS 代理服务组件的状态

使用以下程序确认TS代理服务组件正在运行。有关服务组件的详细信息，请参阅关于管理中心终端服务 (TS) 代理， 第 1 页。

步骤 1 以具有管理员权限的用户身份登录到服务器。

步骤 2 打开**开始 (Start)** > **工具 (Tools)** > **服务 (Services)**。

步骤 3 找到 `CiscoTSAgent` 并查看**状态 (Status)**。

步骤 4 （可选）如果 TS 代理服务组件已停止，请按照启动和停止 TS 代理进程，第 24 页中所述启动 TS 代理服务。

启动和停止 TS 代理进程

使用以下程序启动或停止 TS 代理服务组件。

步骤 1 以具有管理员权限的用户身份登录到服务器。

步骤 2 打开**开始 (Start)** > **管理工具 (Administrative Tools)** > **服务 (Services)**。

步骤 3 导航到 `CiscoTSAgent` 并右键点击以打开上下文菜单。

步骤 4 选择**启动 (Start)** 或**停止 (Stop)** 以启动或停止 TS 代理服务。

查看服务器上的 TS 代理活动日志

如果支持人员提示，请使用以下程序来查看服务组件的活动日志。

打开**工具 (Tools)** > **事件查看器 (Event Viewer)** > **应用和服务日志 (Applications and Services Log)** > **终端服务代理日志 (Terminal Services Agent Log)**。

卸载TS 代理

使用以下程序从服务器卸载 TS 代理。卸载 TS 代理会从服务器中删除接口、服务和驱动程序。卸载 TS 代理还会终止报告给管理中心的活动用户会话。强加密修改不会被删除。

步骤 1 以具有管理员权限的用户身份登录到服务器。

步骤 2 打开**开始 (Start)** > **控制面板 (Control Panel)**。

步骤 3 点击**所有控制面板项目 (All Control Panel Items)** > **程序和功能 (Programs and Features)**。

步骤 4 右键点击**终端服务代理 (Terminal Services Agent)** 并选择**卸载 (Uninstall)**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。