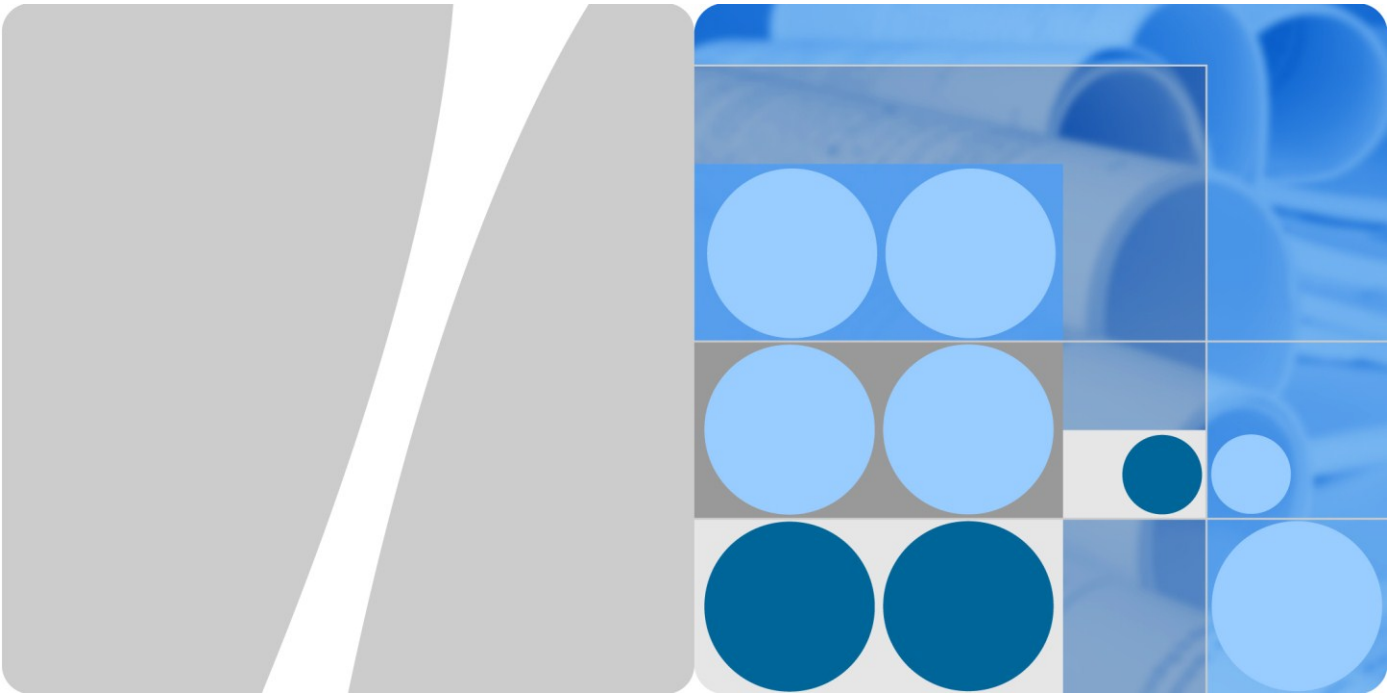


华为 TSM 终端安全管理系统
特性描述

华为技术有限公司

版权所有 © 华为技术有限公司 2012。 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


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

前　言

概述

本文档介绍 TSM 产品开发的背景、产品简介、产品特性、产品各个组成部件、软硬件配置要求、组网方案、功能特性及性能指标，方便一线工程师、网络规划工程师和系统管理员在购买、安装 TSM 产品之前充分了解 TSM。

产品版本

与本文档相对应的产品版本如下所示。

产品名称	产品版本
Secoway TSM	V100R002C07

读者对象

本文档主要适用于以下工程师：

- 数据配置工程师
- 网络规划工程师
- 系统维护工程师

约定

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

通用格式约定

格式	说明
宋体	正文采用宋体表示。
黑体	一级、二级、三级标题、Block Label 采用黑体。
楷体	警告、提示等内容用楷体表示。
“Terminal Display”格式	“Terminal Display”格式表示屏幕输出信息。此外，屏幕输出信息中夹杂的用户从终端输入的信息采用加粗字体表示。
“”	用双引号表示文件路径。如“C:\Program Files\Internet Explorer”。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多

格式	意义
	选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。

图形界面元素引用约定

格式	意义
“”	带双引号“”的格式表示各类界面控件名称和数据表，如单击“确定”。
>	多级菜单用“>”隔开。如选择“文件 > 新建 > 文件夹”，表示选择“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。

键盘操作约定

格式	意义
加“”的字符	表示键名。如“Enter”、“Tab”、“Backspace”、“a”等分别表示回车、制表、退格、小写字母 a。
“键 1+键 2”	表示在键盘上同时按下几个键。如“Ctrl+Alt+A”表示同时按下“Ctrl”、“Alt”、“A”这三个键。
“键 1，键 2”	表示先按第一键，释放，再按第二键。如“Alt，F”表示先按“Alt”键，释放后再按“F”键。

鼠标操作约定

格式	意义
单击	快速按下并释放鼠标的一个按钮。
双击	连续两次快速按下并释放鼠标的一个按钮。
拖动	按住鼠标的一个按钮不放，移动鼠标。

目 录

1 概述

关于本章

介绍开发 TSM 终端安全管理（Terminal Security Management）产品的背景、产品简介和产品特性。

1.1 背景

介绍企业在终端主机安全管理和终端用户的行为管理方面遇到的棘手问题。

1.2 产品简介

提升终端主机的安全防御能力，严格控制终端主机接入受控网络，从终端主机入手主动加强终端主机的安全管理，是企业保障内部网络安全的重要手段。

1.3 产品特性

介绍 TSM 的产品特性。

1.1 背景

介绍企业在终端主机安全管理和终端用户的行为管理方面遇到的棘手问题。

网络技术在企业信息化的过程中扮演着重要的角色。为了提升工作效率，员工通过传统以太网接入、无线接入、远程 VPN 接入多种方式接入内部网络协同办公，以便更好地共享现有的网络资源。

如何在企业中构建安全的网络，在办公便捷、网络资源合理共享的同时发现并隔离不合法和不安全的终端主机，确保只有被授权的和通过安全检查的终端主机才能访问网络资源，从而保护重要的网络资源，是困扰高层管理人员和 IT 部门的棘手问题。在企业中常见的网络安全问题有：

- 远程接入或移动办公会导致网络漏洞越来越多。

  分支机构的终端用户、远程办公的终端用户、合作伙伴、来访客户等多种终端用户接入公司总部网络，网络接入点和接入方式增多，导致网络漏洞成倍增加。
- 员工安全意识薄弱。

由于员工安全意识薄弱，设置弱口令、随意使用 USB 移动存储设备、私自接入互联网、不安装防病毒软件、不及时更新防病毒软件病毒库、随意下载并安装未经验证的软件、不及时安装操作系统补丁，可能会导致重要信息泄密、感染病毒等严重后果。

- 非法终端用户接入。

  外来人员在未经许可的情况下，能够轻易接入并访问公司的网络。

- 合法终端用户越权访问。

  因未对企业中的网络资源进行严格的访问权限控制，导致合法终端用户能够随意访问企业中的机密信息。

- 终端用户滥用资源。

  在未经许可的情况下，终端用户随意使用拨号上网设备连接 Internet。

- 移动存储设备管理混乱。

  未区分企业内部的移动存储设备和外来的移动存储设备。在使用企业内部的移动存储设备对外传输数据时，未对移动存储设备中的数据进行加密，在移动存储设备丢失后导致信息泄密。而外来的移动存储设备在企业内部随意使用，员工可能会将重要信息拷贝到外来的移动存储设备并带走。

- Microsoft Windows 操作系统发现越来越多的安全漏洞。

  因终端主机未及时安装补丁，可能招致黑客和恶意用户的攻击。

- 病毒泛滥。

  因未安装防病毒软件，终端用户在上网时容易感染病毒，并且容易在企业网中蔓延和传播。

- 黑客恶意破坏。

  黑客会利用 Microsoft Windows 的某些系统服务固有的缺陷或通过暴力破解长期未使用的账号入侵终端主机，再蓄意破坏企业中的 IT 系统。

- 随意共享目录导致安全隐患和信息泄密。

  因共享目录的权限设置不当导致机密文件泄密，并容易感染病毒。

- 安全策略不能及时落实。

  管理员缺乏监督手段，不能敦促未安装补丁的终端用户安装补丁或未更新病毒库的终端用户更新病毒库。

- 终端用户的违规行为得不到监控。

  管理员无法检查终端用户是否在上班时间访问与工作无关的网站，缺少取证手段。

1.2 产品简介

提升终端主机的安全防御能力，严格控制终端主机接入受控网络，从终端主机入手主动加强终端主机的安全管理，是企业保障内部网络安全的重要手段。

以下措施有助于企业保障内部网络安全：

- 加强网络接入控制管理，防止非授权、不安全的终端用户接入受控网络。
- 强制终端主机遵从安全策略，确保终端主机在接入受控网络之前是安全的。

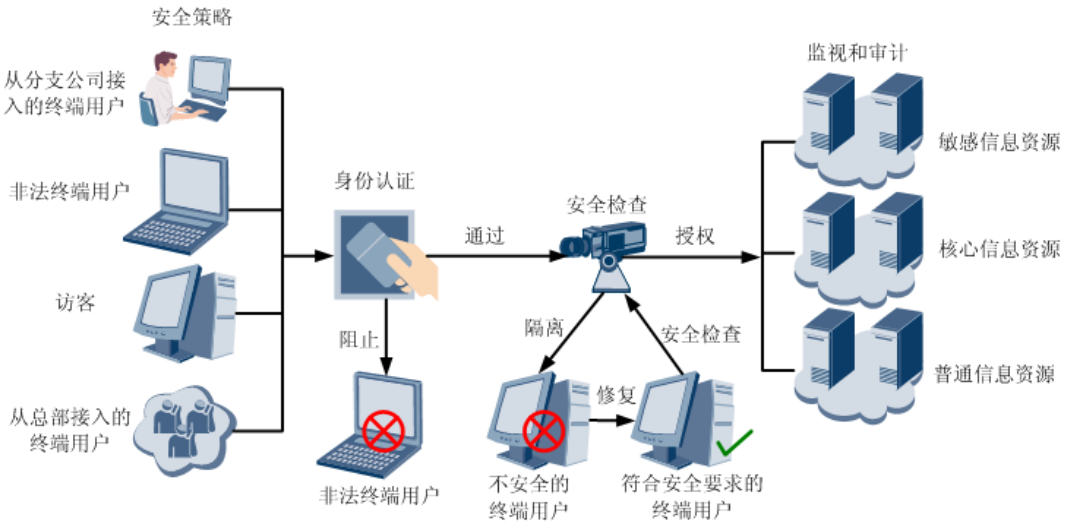
- 建立访问权限管理机制，根据终端用户的工作需要授予不同的访问权限，保护企业核心网络资源。
- 加强终端用户行为的管理力度，保障终端用户合理使用网络资源。
- 主动加固终端主机，修复已经发现的终端主机的安全漏洞，在终端主机上建立安全防范机制。

为了解决企业内部网络管理失控的问题，保障企业内部网络的畅通、终端主机的安全和公司信息数据的安全，实现企业网络安全建设的目标，华为技术有限公司推出 TSM 这款产品，该产品为企业提供整合的内部网络安全解决方案，实现从终端主机到业务系统的控制和管理功能。

TSM 基于 TSM 代理为企业提供安全接入控制、终端安全管理、补丁管理、终端用户的行为管理、软件分发和资产管理六大功能。其核心思想是建立网络准入控制机制，基本要素是安全检查、访问控制和安全修复。有效控制网络日渐增多的接入点，包括企业员工、外部访客、合作伙伴和临时雇员等对网络的访问，发现并隔离带有威胁的终端主机，提升网络防御安全威胁的能力。

TSM 的应用模型如图 1-1 所示。

图1-1 TSM 的应用模型



TSM 的主要功能特性包括：

- 终端接入控制。

  支持普通账号、MAC 地址、USB Key 和外部认证源 4 种身份认证方式，实现对企业员工、外部访客、合作伙伴和临时雇员等对网络访问的控制，保护业务系统安全。

  所谓外部认证源是指存放用户信息并能够完成用户身份鉴别功能的目录服务器。TSM 支持与 Novell eDirectory 认证服务器、Microsoft AD 域控制器、IBM Tivoli（International Business Machines Tivoli）认证服务器和 Sun One 认证服务器 4 种外部认证源联动来完成终端用户的身份认证。
- 终端安全管理。

全面评估终端主机的安全状态，强制隔离不安全终端主机，确保 IT 策略遵从，降低风险。

终端安全状态检查主要包括检查是否安装各种补丁，是否安装企业要求必须安装或禁止安装的软件，终端主机安装的防病毒软件是否符合要求，是否启用 ARP 防护功能等。

在检查结果的基础上，提供个性化的修复建议，协助安装各类补丁和必备的软件。

丰富而全面的安全策略，提供基于部门和用户角色灵活的安全策略控制，强制终端主机遵循管理员统一制定的安全策略，协助管理员评估终端主机的安全状态，消除终端存在的安全隐患，以便主动降低终端主机的安全威胁，保障终端用户合理使用网络资源。

强制隔离以下不安全终端：

- 存在重大安全隐患的终端主机。
- 未授权的外部终端主机。
- 未安装补丁的终端主机。
- 不符合安全策略要求的终端主机。

- 员工行为管理。

  全面控制各种移动存储介质的使用，规范员工合理使用网络资源，提高网络可用性和效率，防止网络滥用与恶意破坏。

  员工行为管理包括控制各种非法外连行为，控制网络流量，控制 IM、炒股、P2P 软件和网络游戏，控制 Web 访问和 IP 访问，ARP 防护，文件操作，移动存储设备管理，进程/服务黑白名单和外设接口管理。

- 补丁管理。

  支持与 WSUS（Windows Server Update Services）无缝集成，强制、及时、安全和准确的侦测系统漏洞，帮助终端主机及时更新补丁，避免由系统漏洞带来的安全威胁。

- 软件分发。

  支持将软件手工或按计划分发到终端主机，并支持按部门、按操作系统、按 IP 地址段进行分发。

- 资产管理。

  收集终端资产信息，跟踪资产变更状况，上报资产变更报表，关联人员与资产，查询资产信息。

1.3 产品特性

介绍 TSM 的产品特性。

TSM 充分考虑了大中小型企业网络的组网环境，具有如下特性：

- 多种网络接入控制方式，满足各种应用场景下的接入控制需求。
  - 电信级硬件安全接入控制网关，从网络层提供终端高可靠接入控制，部署和维护简单，性能卓越，最高支持 40000 并发用户数。

- 802.1x 网络接入控制方式，基于二层的访问控制，有效阻止局域网终端互访行为。
- 主机防火墙接入控制方式，基于身份认证等级灵活配置访问规则，部署、维护简单，可主动阻止或隔离未安装代理的不安全终端对其他终端的访问，减少威胁。

- 基于用户角色的最小授权访问控制，保障企业核心业务系统安全。

  基于用户角色提供最小授权访问控制，严格控制企业员工、外部访客、合作伙伴和临时雇员等对业务系统的访问范围，防止非授权终端访问，保障企业核心业务系统安全。

- 统一安全策略遵从和员工行为审计，全面保障终端安全、合规、受控。

  通过全面终端安全评估，强制实施统一安全策略，包括补丁检查、防病毒软件和注册表检查等二十多条安全策略，保障终端安全、受控和企业安全政策的落实。

- 持续的员工行为管理，保障更高的网络可用性和效率，防止网络滥用与恶意破坏。

  提供上网行为审计、全面的移动存储介质管理、系统进程监控等安全策略，对员工违规行为进行审计和取证，帮助提高员工安全意识，保障企业 IT 资源的合理使用。动态策略管理提供可定制、可扩展的安全策略，可分组织和角色灵活实施。

- 自动化补丁管理，并支持与 WSUS 联动，及时修复终端漏洞，主动消除安全缺口。

  依据自动化补丁检查结果，提供基于用户群组的补丁下发，支持分布式补丁分发，支持断点续传，保障下载的持续性；提供多种安装策略，并基于系统环境选择安装，及时、主动消除各种安全缺口。

- 多种身份认证方式，不同场景下灵活选择。

  可采用用户名/口令、MAC 地址、AD 域、LDAP 认证和 CA 认证，并支持 Web Agent 插件认证、Web 客户端认证，灵活满足访客和移动办公用户等临时接入认证需求。

- 自动收集信息资产状况，跟踪变更，保障资产可控可管。

  系统可自动收集终端软、硬件资产信息，统计输出企业资产状态报表；跟踪资产变更，输出变更报表，实现资产管理 IT 化，保障企业信息资产可控可管。

- 强大的集中管理能力，灵活的分权管理功能。

  系统具备强大的集中管理能力，同时又支持分权的管理功能，可实现不同地区管理员管理本地区终端，不同管理员权限不同。

- 部署灵活、方便，满足复杂网络环境下的部署需要。

  服务器可灵活部署，支持集中式或分布式部署；接入控制网关支持在路由设备上的直挂或旁挂，对企业现网改动小，并且支持集中式或分布式部署，可满足复杂网络环境下的部署需要。

- 高可靠性、逃生通道和负载均衡，保障企业业务连续性。

  系统自身具有高可靠性，服务器采用资源池方式，提供负载均衡和冗余备份；安全接入控制网关支持双机热备，提供系统安全逃生通道，灵活选择安全优先或业务优先，最大可能保障企业业务连续性。

2 体系结构

关于本章

介绍 TSM 的系统组成及最低软硬件配置。

2.1 系统组成

TSM 包括 TSM 管理中心、TSM 管理器、TSM 控制器、扫描器、安全接入控制网关、802.1x 交换机和 TSM 代理几个部件。

2.1.1 组网图

通过组网图帮助读者了解 TSM 终端安全管理系统的组成结构。

TSM 的系统组成图如图 2-1 和图 2-2 所示。

图2-1 TSM 分级组网方案

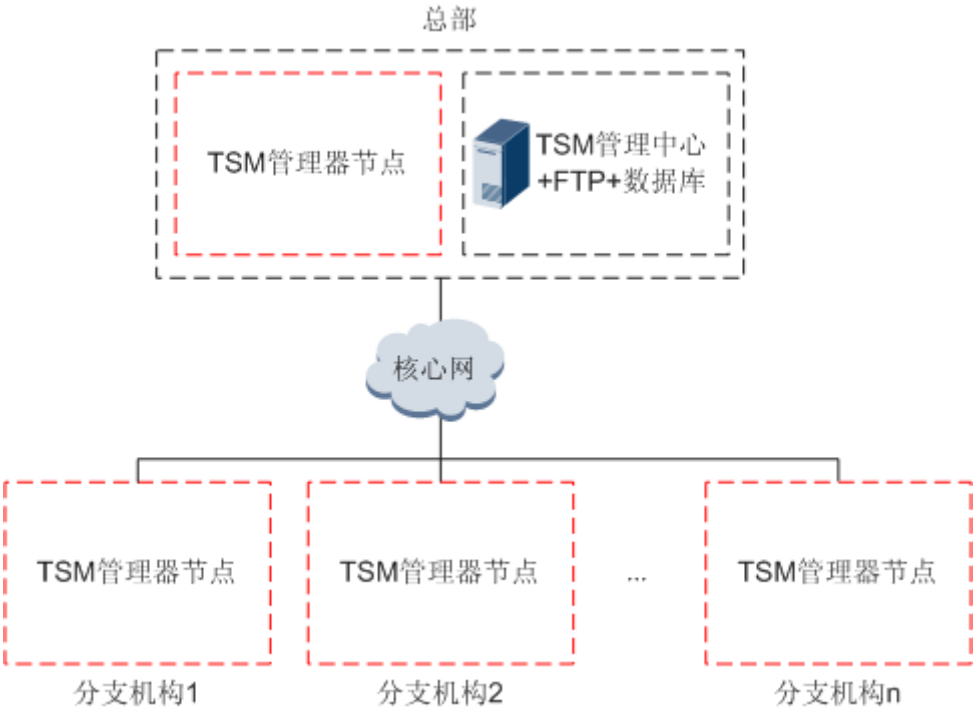
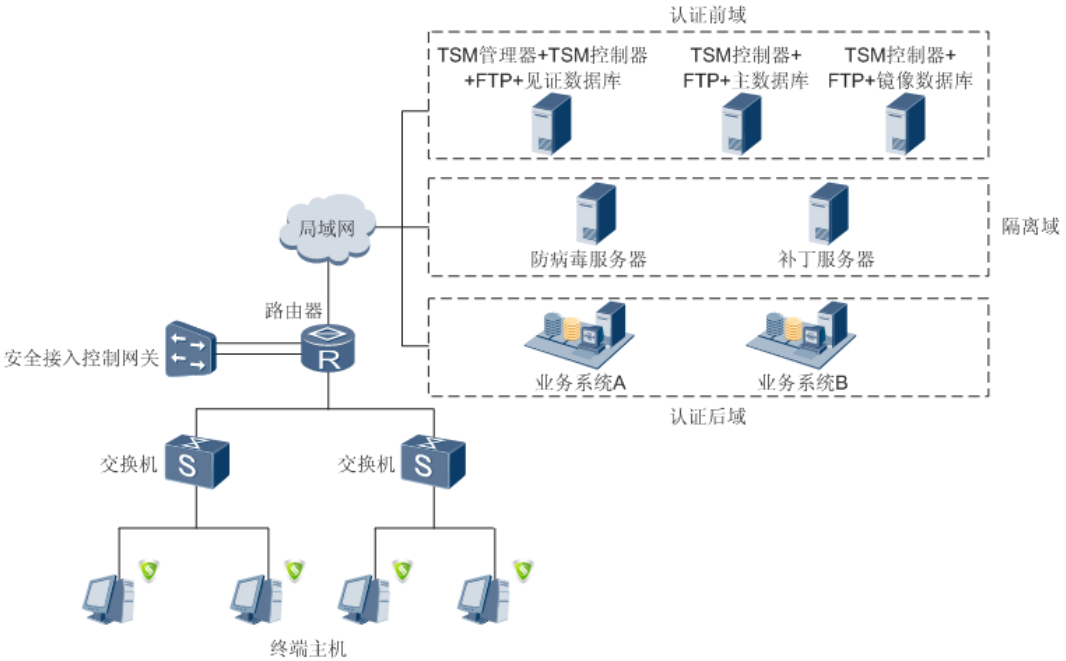


图2-2 TSM 管理器节点的组网图



2.1.2 TSM 管理中心

TSM 管理中心是为分级式组网专门设立的组件，主要负责为 TSM 管理器分配 License、分配 Microsoft Windows 操作系统补丁模板、分配策略模板、分配软件分发任务。

TSM 管理中心适用于上级组织对部署于下级组织的 TSM 管理器进行管理的场合。例如在电信运营商、银行、交通、能源行业，组织结构具有明显的分级特征，并且总部需要在省节点（或省中心对地市节点）推行推荐性的 Microsoft Windows 操作系统补丁部署规则和策略部署规则。只有在分组式组网环境中才需要部署 TSM 管理中心，并且 TSM 管理中心与 TSM 管理器无法安装在同一台硬件服务器。

TSM 管理中心的具体功能有：

- 管理 TSM 管理器。
  - 在接管 TSM 管理器之前，TSM 管理中心对 TSM 管理器的身份进行验证。
  - 以 TSM 管理中心作为上级节点，所有的 TSM 管理器作为下级节点，TSM 管理中心与 TSM 管理器之间组成分级式的组织结构，TSM 管理中心接管所有的 TSM 管理器。
  - 允许 TSM 管理中心的管理员远程登录 TSM 管理器进行查看或修改配置。
- 管理 TSM 管理器的 License。
  - 上传 License。
  - 为 TSM 管理器分配 License。
  - 将更新后的 License 同步下发至 TSM 管理器。
  - 从 TSM 管理器回收 License。
- 管理策略模板。
  - 上传和删除策略。
  - 为 TSM 管理器创建策略模板，并定制策略的运行参数。
  - 为不同的 TSM 管理器下发不同的策略模板，并把更新后的参数下发至 TSM 管理器。
  - 检查 TSM 管理器的策略与 TSM 管理中心的策略之间的兼容性，确保在 TSM 管理器与 TSM 管理中心之间的策略兼容的情况下，才会把策略模板下发至 TSM 管理器处执行。
  - 保护策略模板。禁止 TSM 管理器的管理员修改和删除从 TSM 管理中心获取的策略模板。
- 管理 Microsoft Windows 操作系统补丁。
  - 从微软官方网站获取 Microsoft Windows 操作系统补丁。
  - 从以前导出的 Microsoft Windows 操作系统补丁文件中导入补丁。
  - 允许 TSM 管理器从 TSM 管理中心获取 Microsoft Windows 操作系统补丁，或者 TSM 管理器自行从微软官方网站下载 Microsoft Windows 操作系统补丁。
  - 从语言、操作系统类型、补丁级别、知识库号几个方面配置需要下载的补丁。
  - 支持下载 Microsoft Windows 操作系统的 Hotfix 补丁和 SP 补丁。
  - 在不直接连接 Internet 的情况下，通过 Proxy 服务器下载补丁。

- 提供补丁特征库和补丁的下载日志，供管理员在处理补丁下载故障时参考。
- 将 TSM 管理中心已下载的 Microsoft Windows 操作系统补丁导出以达到备份补丁的目的，方便在升级或重新安装 TSM 管理中心时快速导入补丁。
- 提供自动匹配和手工设置需要安装的补丁两种工作模式。
- 为不同的 TSM 管理器下发不同的补丁模板，并把更新后的参数下发至 TSM 管理器。
- 保护策略模板。禁止 TSM 管理器的管理员修改和删除从 TSM 管理中心获取的补丁模板。

- 管理软件分发任务。
  - 通过内部数据源或外部数据源创建软件分发任务。
  - “.exe”、“.msi”、“.bat”、“.vbs”、“.js”五种格式的软件可实现下发完成后自动安装或运行。
  - 向管辖范围内的所有 TSM 管理器下发软件分发任务，从而解决在分支机构中统一推行安装某些软件难的问题。
  - 支持管理员自定义执行参数，以满足个性化的安装要求。例如，如果待分发的软件支持静默安装参数，设置静默安装参数后，可在不干扰终端用户工作的情况下实现自动安装。
  - 自定义软件安装时间，方便管理员将软件安装的时间安排在业务空闲期，例如午休时段，以减少软件安装对终端用户的干扰。

2.1.3 TSM 管理器

TSM 管理器是 TSM 的管理服务器。管理员通过 IE 浏览器登录 TSM 管理器进行日常维护操作。

TSM 管理器的主要功能包括：

- 系统配置
  - 支持上传 License 文件、代理软件和代理升级包。
  - 支持系统管理员、系统权限管理。
  - 支持代理升级管理。
  - 支持管理员登录日志、视频监控日志和系统日志管理。
  - 支持对接入控制、TSM 控制器、应用服务器、数据库、终端参数、Web 超链接、证书认证和服务器监控进行配置。
- 组织人员管理
  - 支持对部门和用户进行管理。
  - 部门结构支持多级方式，以树状结构进行管理。
  - 支持同步 Microsoft AD 域控制器，Novell eDirectory、IBM Tivoli 和 Sun One 认证服务器的部门和账号信息。
  - 支持添加、修改、查询、删除本地部门和用户。
- 安全策略管理
  - 包括检查类和监控类策略。
  - 支持根据企业总体信息安全要求配置安全策略模板，并下发给终端用户。

- 补丁管理
  - 支持与 WSUS（Windows Server Update Services）联动帮助终端主机自动下载和安装 Windows 操作系统补丁。
  - 支持配置补丁部署模板，并下发给终端用户。
- 软件分发

  软件分发功能适用于管理员需要批量主动向终端主机分发软件（例如防病毒软件）并自动运行的场合，提供创建、查看、复制、撤销、删除软件分发任务功能。
- 资产管理
  - 支持记录资产从开始使用到报废期间的生命历程。
  - 支持采集终端主机的信息。
  - 支持记录终端主机软硬件的变更情况。
  - 支持按操作系统类型、资产类型、资产使用状态统计资产信息。
- 公告管理

  公告管理功能支持通过发布公告的形式向终端用户发送通知，提供创建、查看和删除公告。在管理员创建公告后，TSM 管理器会在公告的有效期内向上线的终端主机分发公告。
- 报表管理

  TSM 提供多种报表供管理员查阅，以便管理员详细了解终端主机中的安全检查结果、终端用户的违规情况、终端用户的上下线记录、Windows 操作系统补丁的安装情况、TSM 代理版本升级的进度、软件下发任务的执行进度。

2.1.4 TSM 控制器

TSM 控制器是 TSM 的控制服务器。TSM 控制器主要负责验证终端用户的身份、对终端主机进行安全检查，以及与准入控制设备联动实现最小授权的访问控制等。

TSM 控制器的主要功能包括：

- 向 TSM 代理、Web Agent 插件和 Web 客户端提供服务。
  - 验证终端用户的身份。
  - 向 TSM 代理、Web Agent 下发策略参数。
  - 检查 TSM 代理的安全认证结果。
  - 向 TSM 管理器上报资产和终端用户的违规信息。
  - 向终端主机分发软件、补丁和公告。
- 与安全接入控制网关联动控制终端主机接入受控网络。
  - 对于尚未通过身份认证的终端用户，TSM 控制器将会通知安全接入控制网关终端用户具有访问认证前域的权限。
  - 对于已经通过身份认证，但未通过安全检查的终端用户，TSM 控制器通知安全接入控制网关开放隔离域的访问权限。
  - 对于同时通过身份认证和安全认证的终端用户，TSM 控制器通知安全接入控制网关开放隔离域和认证后域的访问权限。

所谓认证前域是指终端主机在通过身份认证之前能够访问的区域。不需要进行身份认证即可访问的公共网络资源（如 DNS 服务器、外部认证源、TSM 控制器等）部署在本区域。

所谓隔离域是指在终端用户通过了身份认证但未通过安全认证时允许终端主机访问的区域。能够帮助终端用户消除违规信息的相关资源（如补丁服务器、防病毒服务器等）部署在本区域。

所谓认证后域是指终端用户通过认证后能够访问的区域。需要受控访问的网络资源（如 ERP 系统、财务系统、数据库系统）部署在本区域。

- 与支持 802.1x 的交换机联动控制终端主机接入受控网络。
  - 为外部提供简单的 RADIUS 服务，确保外部系统能够使用 TSM 的账号信息进行身份认证。
  - 对于已经通过身份认证的终端用户，TSM 控制器将会通知支持 802.1x 交换机开放访问网络的权限。
  - 对于未通过身份认证的终端用户，TSM 控制器将会通知 802.1x 交换机关闭访问网络的权限。

TSM 控制器以资源池方式工作。TSM 支持多台 TSM 控制器，这些 TSM 控制器共同分担大量终端用户同时上线（如上班高峰期大量终端用户在集中时段上线）的瞬时负载。当某台 TSM 控制器发生故障时，确保 TSM 代理能够迅速切换至其他 TSM 控制器进行身份认证、安全认证，保证网络业务能够正常开展。

2.1.5 扫描器

扫描器的作用是发现和管理网络中现有的设备，尤其是已经安装 TSM 代理终端主机数量和未安装 TSM 代理的终端主机数量，在管理员制定或调整 TSM 代理的部署策略时作为参考的依据。

部署 TSM 代理是终端安全管理业务逐步推行的过程，按阶段分可分为试点和推广两个阶段，最终的目标是实现终端安全业务全覆盖。在终端安全管理业务逐步推行的过程中，管理员重点关注的是，如何确保所有的终端主机全部安装 TSM 代理，确保终端安全不会成为网络安全中最薄弱的环节。

扫描器是为了帮助管理员发现没有安装 TSM 代理的终端主机而开发的，主要功能有：

- 通过扫描任务发现网络中的设备，并将设备自动分为 PC 设备、服务器、交换路由设备、打印机、IP Phone 和未知设备六种。
- 对于 PC 设备而言，能够识别已经安装 TSM 代理的终端主机和尚未安装 TSM 代理的终端主机。
- 允许管理员标识需要安装 TSM 代理的终端主机和不需要安装 TSM 代理的终端主机。
- 支持实时启动和停止扫描任务。
- 支持周期性的扫描任务和一次性的扫描任务。
- 支持按 IP 地址段和按 ARP 表两种方式发现设备。
- 在发现新的设备接入受控网络和 TSM 代理被卸载时以告警邮件的方式提醒管理员。
- 支持对设备进行分组管理。

2.1.6 安全接入控制网关

安全接入控制网关用于控制终端访问受控网络的权限，向隶属不同角色的终端用户和不同安全状况的终端用户开放不同的权限。

安全接入控制网关的主要功能包括：

- 根据 TSM 控制器反馈的信息，开放终端用户访问受控网络的权限。
- 防止外部非授权的终端用户访问企业的受控网络。
- 防止内部合法但不安全的终端用户访问企业的受控网络。
- 隔离连接到受控网络但没有进行安全认证的终端用户。
- 逃生通道。

  当 TSM 控制器发生严重故障，存活的 TSM 控制器无法承担正常的身份认证和安全认证的时候，TSM 控制器与安全接入控制网关之间的心跳协议能够及时检测故障并打开逃生通道，开放网络的访问权限，保证业务正常开展。

  所谓心跳协议，是指安全接入控制网关定期向 TSM 控制器发送存活检测报文，如果没有收到 TSM 控制器的响应报文，在启用逃生通道的情况下，安全接入控制网关将会允许所有的终端用户接入受控网络。

  当心跳协议发现 TSM 控制器从故障中恢复后，安全接入控制网关将会自动关闭逃生通道，安全接入控制机制重新生效，终端用户必须通过身份认证和安全认证才能接入受控网络。

在启用控制接入功能的情况下，安全接入控制网关将执行如下操作：

- 尝试连接 TSM 控制器，并在连接 TSM 控制器成功后，向 TSM 控制器请求同步认证前域的规则和认证后域的规则，把规则转换为 ACL。其中认证前域对应 1 条 ACL，每个受控域对应 1 对 ACL。受控域对应的 1 对 ACL 由 permit 语句和 deny 语句组成，分别对应允许访问受控域和禁止访问受控域。
- 从交换机或路由器上接收数据流，并检查进入安全接入控制网关的报文。根据报文对应的 IP 地址的认证状态确定下一步如何处理。
  - 如果该 IP 地址未经过身份认证，安全接入控制网关将会使用认证前域对应的 ACL 对报文进行处理。该条 ACL 与管理员在 TSM 管理器上配置的认证前域相对应。
  - 如果该 IP 地址已经通过身份认证，安全接入控制网关将该报文从认证前域切换至认证后域，并根据认证后域对应的 ACL 对报文进行处理。

2.1.7 802.1x 交换机

802.1x 交换机的主要功能是对终端主机进行接入控制。通过端口控制技术，保证只有通过身份认证的终端主机才能接入受控网络，防止未经授权的终端主机接入受控网络。

TSM 服务器对应于 IEEE802.1x 的认证服务器系统，用户接入层设备则实现 IEEE802.1x 的接入控制单元，IEEE802.1x 的用户接入系统集成在 TSM 代理中。

接入控制单元的每个物理端口内部有受控端口和非受控端口等逻辑划分。非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证随时接收用户接入系统

发出的认证 EAPOL 报文。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。

802.1x 交换机对终端主机进行接入控制时：

- 若终端用户已经通过身份认证和安全认证，则终端用户能够访问认证后域。
- 若终端用户已经通过身份认证而未通过安全认证，则终端用户能够访问隔离域。

说明

认证后域和隔离域分别对应于管理员分配的一个 VLAN。

802.1x 交换机支持 GUEST VLAN，企业的访客将进入 GUEST VLAN，只能访问认证前域。

2.1.8 TSM 代理

TSM 代理是 TSM 中的一个组件，作为 TSM 的客户端安装在终端主机侧，负责与 TSM 管理器联动，实施管理员在 TSM 管理器定制的安全管理规则。

TSM 代理根据安装过程的不同可以分为需要依照安装向导在终端主机安装的 TSM 代理和通过插件注册方式实现的 Web Agent 插件。

TSM 代理的主要功能包括：

- 身份认证。

  通过输入用户名和口令、选择 MAC 地址或输入外部认证源账号和密码，完成终端用户的身份认证。
- 安全认证。

  从 TSM 管理器获取安全策略参数，根据下载的参数对终端主机进行安全检查，例如补丁检查、杀毒软件检查等，并且把检查结果作为安全认证的依据。
- 资产管理。
  - 终端用户通过输入管理员分配的资产编码能够完成本机资产注册。
  - 支持设置资产所在地和资产责任人账号，实现责任人和资产的绑定。
  - 支持查看资产注册状态和资产信息。
- 补丁管理。

  协助终端用户下载、安装各种类型的补丁程序，以修补已经发现的操作系统、数据库、MS Office、IE 浏览器的漏洞。
- 软件分发。
  - 支持自动从 TSM 管理器下载管理员分发的软件。
  - 支持查看详细的软件分发任务。
- 公告管理。
  - 支持自动下载 TSM 管理器下发的公告。
  - 支持查看 TSM 管理器下发的公告。

2.2 配置要求

介绍 TSM 各个部件对软硬件配置的最低要求。

2.2.1 服务器的配置要求

介绍 TSM 管理中心、TSM 管理器、TSM 控制器、扫描器、FTP 服务器和数据库的配置要求。

TSM 管理中心、TSM 管理器、TSM 控制器、扫描器、FTP 服务器、数据库这六项的软硬件配置均相同，配置要求请参见表 2-1。

表2-1 服务器软硬件的配置要求

配置项	配置要求
CPU（Central Processing Unit）	Xeon 四核 5405 2.0GHz × 2 或以上（**最低配置**）
内存	4GB
网卡	2 块
操作系统	Microsoft Windows Server 2003 R2 标准简体中文版或英文版，32 位，带 SP2 补丁 Microsoft Windows Server 2008 R2 标准简体中文版或英文版，64 位，带 SP1 补丁（**推荐配置**）
数据库	Microsoft SQL Server 2005 标准简体中文版或英文版，32 位，带 SP3 补丁 Microsoft SQL Server 2008 标准简体中文版或英文版，32 位，带 SP3 补丁 Microsoft SQL Server 2008 标准简体中文版或英文版，64 位，带 SP3 补丁（**推荐配置**）
TSM 管理器支持的 Web 浏览器	• Microsoft Internet Explorer 6.0，不带 SP 补丁、带 SP1 补丁或带 SP2 补丁 • Microsoft Internet Explorer 6.5，不带 SP 补丁、带 SP1 补丁或带 SP2 补丁 • Microsoft Internet Explorer 7.0 • Microsoft Internet Explorer 8.0

扫描器的软硬件配置要求请参见表 2-2。

表2-2 扫描器的软硬件配置要求

配置项	最低配置
支持的操作系统	• Microsoft Windows Server 2003

配置项	最低配置
	• Microsoft Windows XP • Microsoft Windows 7
Microsoft Windows XP 标准配置	• CPU：800MHz • 内存：256MB
Microsoft Windows 7 标准配置	• CPU：1GHz • 内存：1GB • 图形处理器：支持 DirectX 9（开启 AERO 效果），显存容量 128MB

2.2.2 TSM 客户端的配置要求

介绍 TSM 客户端的软硬件配置的最低要求，包括 TSM 代理、TSM Web Agent 插件和 Web 客户端。

TSM 代理的软硬件配置的最低要求

TSM 代理的软硬件配置的最低要求请参见表 2-3。

表2-3 TSM 代理的软硬件配置的最低要求

配置项	最低配置
Microsoft Windows XP 标准配置	• CPU：800MHz • 内存：256MB
Microsoft Windows Vista Capable 标准配置	• CPU：800MHz • 内存：512MB • 图形处理器：支持 DirectX 9
Microsoft Windows Vista Premium Ready 标准配置	• CPU：1GHz • 内存：1GB • 图形处理器：支持 DirectX 9，Pixel Shader 2.0 和 32bit/pixel，显存容量 128MB • 硬盘：容量 40GB，15GB 的可用空间
Microsoft Windows 7 标准配置	• CPU：1GHz • 内存：1GB • 图形处理器：支持 DirectX 9（开启 AERO 效果），显存容量 128MB
软件预留安装空间	200MB
支持的操作系统（32	• Microsoft Windows 2000 专业版，带 SP4 补丁，支持简

配置项	最低配置
位）	体中文或英文 • Microsoft Windows 2000 服务器版，带 SP4 补丁，支持简体中文或英文 • Microsoft Windows 2000 高级服务器版，带 SP4 补丁，支持简体中文或英文 • Microsoft Windows XP 家庭版，不带 SP 补丁、带 SP1 补丁、带 SP2 补丁或带 SP3 补丁，支持简体中文或英文 • Microsoft Windows XP 专业版，不带 SP 补丁、带 SP1 补丁、带 SP2 补丁或带 SP3 补丁，支持简体中文或英文 • Microsoft Windows XP 专业版，带 SP2 补丁，支持法语 • Microsoft Windows Server 2003 标准版，不带 SP 补丁、带 SP1 补丁或带 SP2 补丁，支持简体中文或英文 • Microsoft Windows Server 2003 企业版，不带 SP 补丁、带 SP1 补丁或带 SP2 补丁，支持简体中文或英文 • Microsoft Windows Vista 家庭普通版，带 SP1 补丁，支持简体中文或英文 • Microsoft Windows Vista 家庭高级版，带 SP1 补丁，支持简体中文或英文 • Microsoft Windows Vista 商业版，带 SP1 补丁，支持简体中文或英文 • Microsoft Windows Vista 企业版，带 SP1 补丁，支持简体中文或英文 • Microsoft Windows Vista 旗舰版，带 SP1 补丁，支持简体中文或英文 • Microsoft Windows 7 RTM 专业版，支持简体中文或英文 • Microsoft Windows 7 RTM 旗舰版，支持简体中文或英文
支持的操作系统（64 位）	• Microsoft Windows XP，支持英文 • Microsoft Windows 7 RTM 专业版，支持简体中文或英文 • Microsoft Windows 7 RTM 旗舰版，支持简体中文或英文

说明

与 TSM 代理兼容的其他安全类软件请参见“与 TSM 代理兼容的其他安全类软件”。

TSM Web Agent 插件支持的 IE 浏览器

TSM Web Agent 插件支持的操作系统及 IE 浏览器请参见表 2-4。

表2-4 TSM Web Agent 插件支持的 IE 浏览器

配置项	最低配置
支持的 Microsoft Windows 操作系统（32 位）	• Microsoft Windows 2000 专业版，带 SP4 补丁，支持简体中文或英文 • Microsoft Windows 2000 服务器版，带 SP4 补丁，支持简体中文或英文 • Microsoft Windows 2000 高级服务器版，带 SP4 补丁，支持简体中文或英文 • Microsoft Windows XP 家庭版，不带 SP 补丁、带 SP1 补丁、带 SP2 补丁或带 SP3 补丁，支持简体中文或英文 • Microsoft Windows XP 专业版，不带 SP 补丁、带 SP1 补丁、带 SP2 补丁或带 SP3 补丁，支持简体中文或英文 • Microsoft Windows XP 家庭版，带 SP2 补丁，支持法语 • Microsoft Windows XP 专业版，带 SP2 补丁，支持法语 • Microsoft Windows Server 2003 标准版，不带 SP 补丁、带 SP1 补丁或带 SP2 补丁，支持简体中文或英文 • Microsoft Windows Server 2003 企业版，不带 SP 补丁、带 SP1 补丁或带 SP2 补丁，支持简体中文或英文 • Microsoft Windows Vista 家庭普通版，不带 SP 补丁或带 SP1 补丁，支持简体中文或英文 • Microsoft Windows Vista 家庭高级版，不带 SP 补丁或带 SP1 补丁，支持简体中文或英文 • Microsoft Windows Vista 商业版，不带 SP 补丁或带 SP1 补丁，支持简体中文或英文 • Microsoft Windows Vista 企业版，不带 SP 补丁或带 SP1 补丁，支持简体中文或英文 • Microsoft Windows Vista 旗舰版，不带 SP 补丁或带 SP1 补丁，支持简体中文或英文 • Microsoft Windows 7 RTM 专业版，支持简体中文或英文 • Microsoft Windows 7 RTM 旗舰版，支持简体中文或英文
支持的 Microsoft Windows 操作系统（64 位）	• Microsoft Windows XP，支持英文 • Microsoft Windows 7 RTM 专业版，支持简体中文或英文 • Microsoft Windows 7 RTM 旗舰版，支持简体中文或英

配置项	最低配置
	文
支持的 Microsoft Windows 平台的 IE 浏览器（32 位）	• Microsoft Internet Explorer 6.0，不带 SP 补丁、带 SP1 补丁或带 SP2 补丁 • Microsoft Internet Explorer 6.5，不带 SP 补丁、带 SP1 补丁或带 SP2 补丁 • Microsoft Internet Explorer 7.0 • Microsoft Internet Explorer 8.0

说明

TSM Web Agent 插件不支持在 64 位的 IE 浏览器下运行。

Web 客户端支持的操作系统及 Web 浏览器

Web 客户端支持的操作系统及 Web 浏览器请参见表 2-5。

表2-5 Web 客户端支持的操作系统及 Web 浏览器

配置项	最低配置
支持的 Microsoft Windows 操作系统	• Microsoft Windows 98，支持简体中文或英文 • Microsoft Windows 2000 专业版，支持简体中文或英文 • Microsoft Windows 2000 服务器版，支持简体中文或英文 • Microsoft Windows 2000 高级服务器版，支持简体中文或英文 • Microsoft Windows XP 家庭版，支持简体中文或英文 • Microsoft Windows XP 专业版，支持简体中文或英文 • Microsoft Windows Server 2003 标准版，支持简体中文或英文 • Microsoft Windows Server 2003 企业版，支持简体中文或英文 • Microsoft Windows Vista 家庭普通版，支持简体中文或英文 • Microsoft Windows Vista 家庭高级版，支持简体中文或英文 • Microsoft Windows Vista 商业版，支持简体中文或英文 • Microsoft Windows Vista 企业版，支持简体中文或英文 • Microsoft Windows Vista 旗舰版，支持简体中文或英文 • Microsoft Windows 7 RTM 专业版 • Microsoft Windows 7 RTM 旗舰版

配置项	最低配置
支持的 Microsoft Windows 平台的 Web 浏览器	• Microsoft Internet Explorer 6.0（32 位和 64 位） • Microsoft Internet Explorer 6.5（32 位和 64 位） • Microsoft Internet Explorer 7.0（32 位和 64 位） • Microsoft Internet Explorer 8.0（32 位和 64 位） • Firefox 2.0 • Mozilla 5.0
支持的非 Microsoft Windows 操作系统	Linux 的所有版本
支持的非 Microsoft Windows 平台的 Web 浏览器	• Firefox 2.0 • Mozilla 5.0

2.2.3 与 TSM 配套的防火墙型号及软件版本

列出能够作为硬件安全接入控制网关的防火墙型号及软件版本，方便管理员在 TSM 项目实施阶段检查所配套的硬件安全接入控制网关是否符合要求。

支持接入控制功能的防火墙型号及软件版本请参见表 2-6。

表2-6 与 TSM 配套的防火墙型号及软件版本

防火墙型号	软件版本
USG21xx/USG22xx/USG51xx	V100R005C00 或以上版本
	V100R003 或以下版本
USG53xx	• V100R003 • V200R001
	V100R002
USG55xx	V200R001

3 组网应用

关于本章

TSM 支持集中式组网、分布式组网和分级式三种组网方案。

3.1 组网概述

介绍认证前域、隔离域和认证后域应该部署的网络资源，三种接入控制方式和对应的组网规划。

TSM 将企业内部的网络资源分别部署于认证前域、隔离域和认证后域。

- 认证前域部署终端用户在通过认证之前需要访问的网络资源，包括 TSM 管理器、TSM 控制器、DNS（Domain Name Service）服务器、外部认证源（如 Microsoft AD 域控制器、Novell eDirectory 等目录服务器）。认证前域只部署终端用户不需要身份认证就能够访问的网络资源，属于不需要 TSM 管理器保护的公共网络资源。
- 当终端用户通过了身份认证，但未能够通过安全认证时，终端用户进入隔离域。隔离域部署能够帮助终端用户消除违规信息的网络资源（如防病毒服务器、补丁

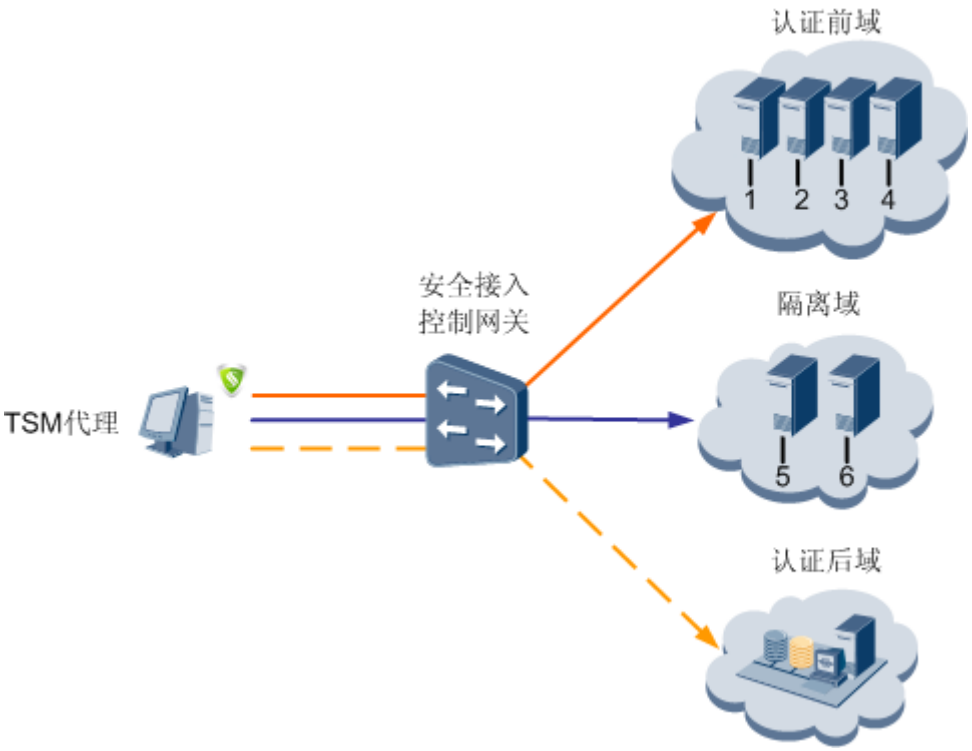
服务器）。未通过身份认证的终端用户无法访问隔离域，故 TSM 管理器能够保护隔离域中的网络资源。

- 当终端用户通过了身份认证和安全认证时，终端用户进入认证后域。认证后域部署企业内部需要保护的网络资源。按照最小授权原则，根据需要保护的业务资源，划分为若干认证后域。

当终端用户接入受控网络时，TSM 支持安全接入控制网关、802.1x 交换机和软件安全接入控制网关三种方式实现安全接入控制。

- 安全接入控制网关支持以直路方式部署在受控网络与终端用户之间，或以旁路方式部署在需要保护的网络资源与终端用户所在的网络之间的路由器旁边。安全接入控制网关方式如图 3-1 所示。

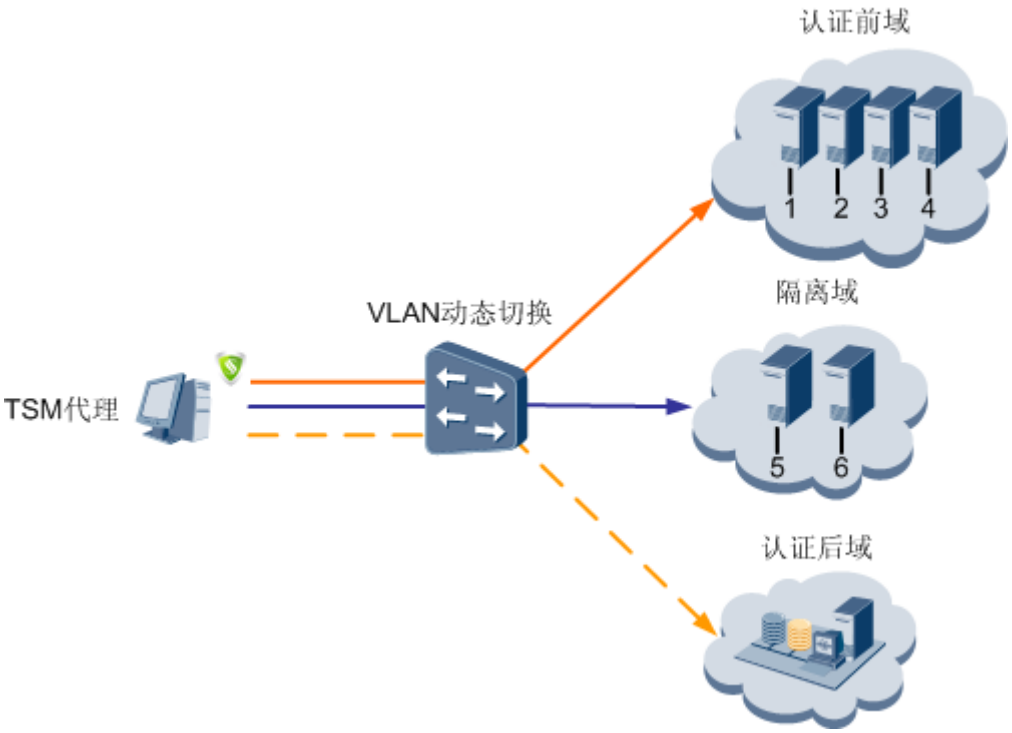
图3-1 安全接入控制网关方式



1	TSM 管理器
2	TSM 控制器
3	外部认证源
4	DNS 服务器
5	防病毒服务器
6	补丁服务器

- 802.1x 接入控制方式支持 VLAN 动态切换，实现终端用户有无权限访问认证前域、隔离域或认证后域的控制。802.1x 接入控制方式如图 3-2 所示。

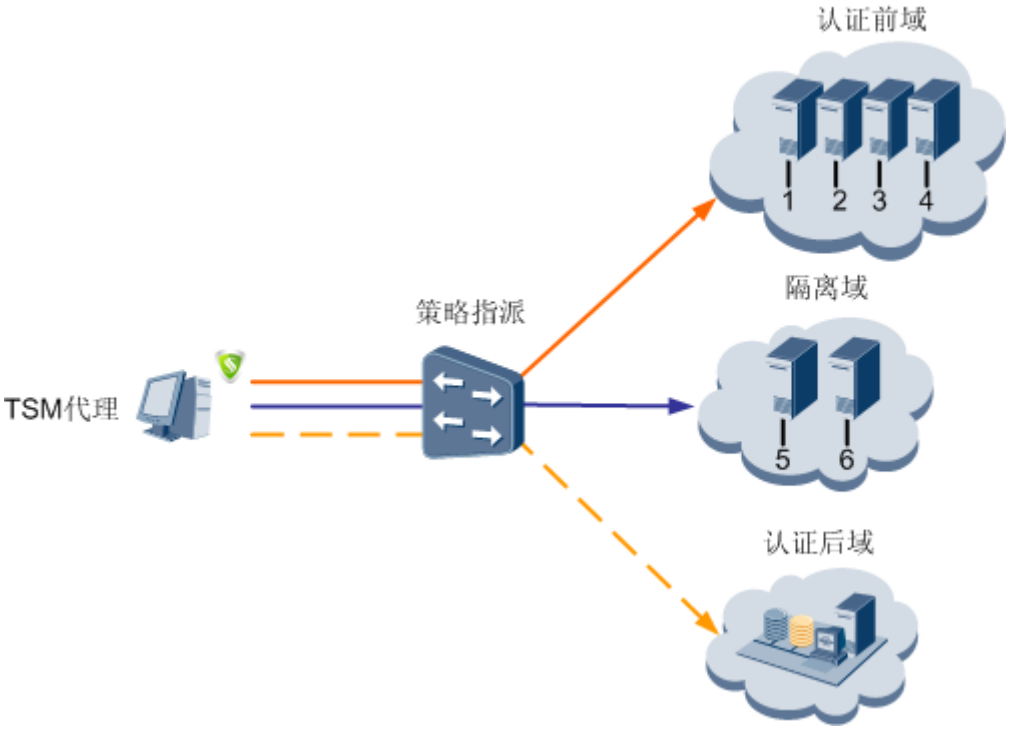
图3-2 802.1x 接入控制方式



1	TSM 管理器
2	TSM 控制器
3	外部认证源
4	DNS 服务器
5	防病毒服务器
6	补丁服务器

- 软件安全接入控制网关通过 TSM 控制器向 TSM 代理指派策略实现终端用户接入控制。软件安全接入控制网关方式如图 3-3 所示。

图3-3 软件安全接入控制网关方式



1	TSM 管理器
2	TSM 控制器
3	外部认证源
4	DNS 服务器
5	防病毒服务器
6	补丁服务器

为了提高 TSM 的可靠性，在组建网络时，依据终端数量采取不同的分配方案，终端数与分配方案对应关系请参见表 3-1。

表3-1 终端数与分配方案对应关系

终端数及可靠性要求	分配方案	硬件服务器数量
1～2000，无备份	硬件服务器 1：TSM 管理器+TSM 控制器+配置数据库+日志数据库	1 台硬件服务器
2000～10000，带 TSM 控制器备份	硬件服务器 1：TSM 管理器+TSM 控制器+日志数据库 硬件服务器 2：TSM 控制器+配置数据库	2 台硬件服务器

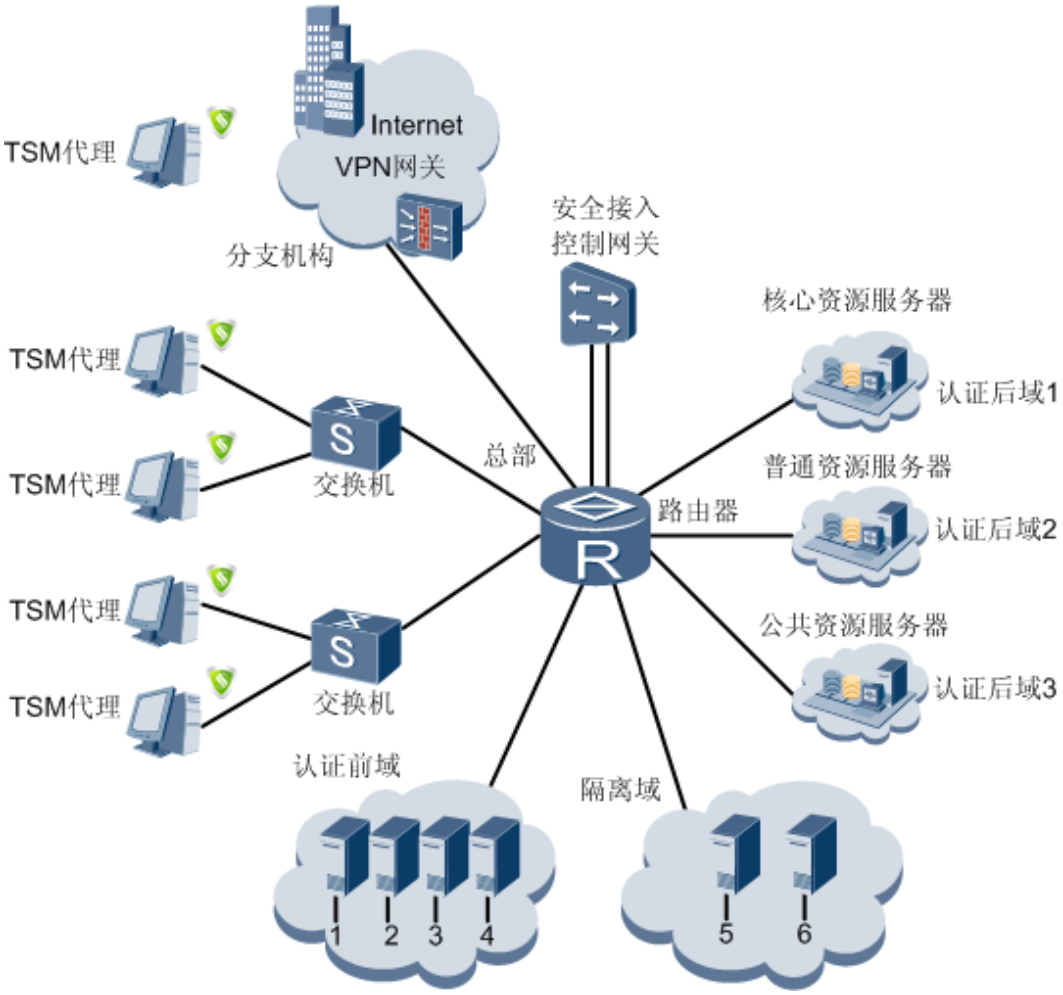
终端数及可靠性要求	分配方案	硬件服务器数量
1～10000，带 TSM 控制器、数据库备份	硬件服务器 1：TSM 管理器+配置数据库 硬件服务器 2：TSM 控制器+镜像配置数据库+备份日志数据库 硬件服务器 3：TSM 控制器+见证服务数据库+日志数据库	3 台硬件服务器
10000～20000，带 TSM 控制器、数据库备份	硬件服务器 1：TSM 管理器+日志数据库+见证服务数据库 硬件服务器 2：TSM 控制器 硬件服务器 3：TSM 控制器+配置数据库+备份日志数据库 硬件服务器 4：TSM 控制器+镜像配置数据库	4 台硬件服务器

3.2 集中式组网

集中式组网方式的特点是将 TSM 管理器、TSM 控制器和数据库服务器集中部署在一个地区。

TSM 的集中式组网显示如图 3-4 所示。

图3-4 TSM 的集中式组网



1	TSM 管理器+TSM 控制器+FTP 服务器
2	TSM 控制器+数据库+FTP 服务器
3	外部认证源
4	DNS 服务器
5	防病毒服务器
6	补丁服务器

无论是本地终端用户还是通过 VPN（Virtual Private Network）网关接入总部的远程终端用户，均需要到总部 TSM 控制器完成身份认证，下载最新的策略及运行参数，获取软件分发任务中需要下载的软件。通过认证后根据终端用户所属的角色分配认证后域的访问权限，访问认证后域中的网络资源。

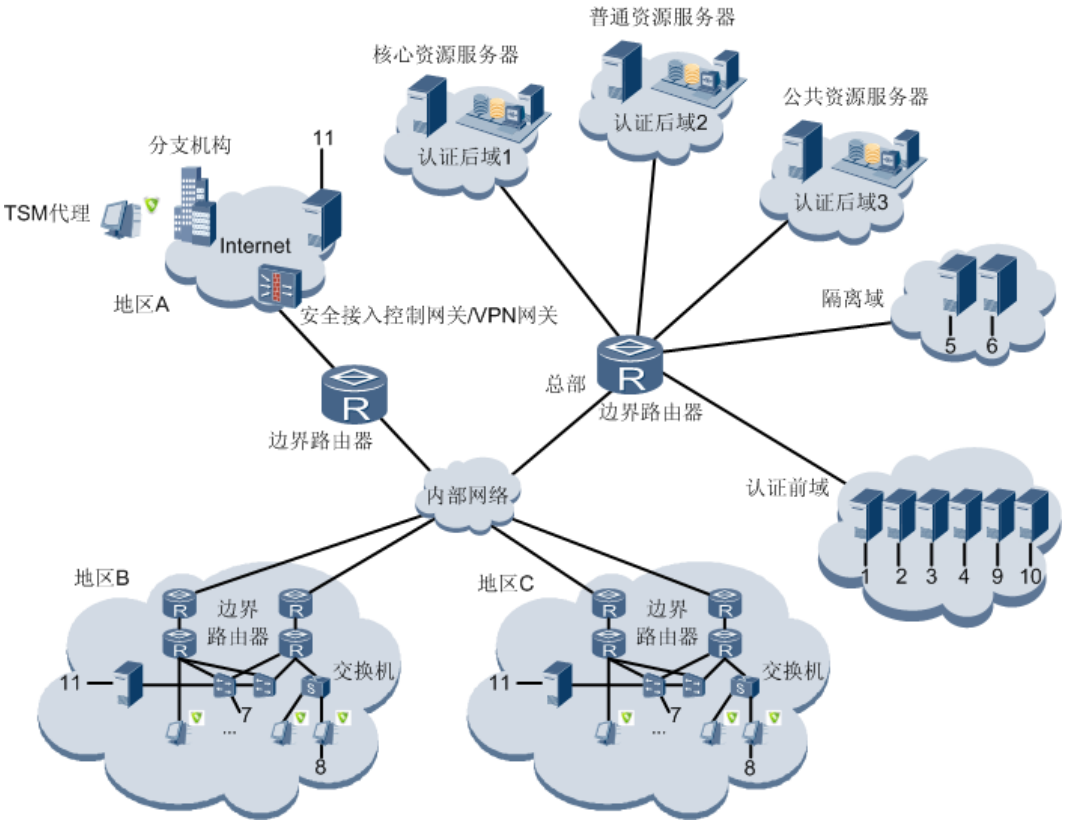
该组网方式适用于大部分终端用户分布集中在一个地区办公，少数终端用户在分支机构办公的场合。

3.3 分布式组网

分布式组网方式的主要特点是将 TSM 管理器和数据库服务器部署在总部，而 TSM 控制器部署在分支机构。

TSM 的分布式组网显示如图 3-5 所示。

图3-5 TSM 的分布式组网



1 TSM 管理器+TSM 控制器+FTP 服务器+见证数据库

2 TSM 控制器+FTP 服务器+主数据库

3 外部认证源

4 DNS 服务器

5 补丁服务器

6 防病毒服务器

7 安全接入控制网关

8 TSM 代理

9 TSM 控制器+FTP 服务器+镜像数据库

10 TSM 控制器+FTP 服务器+违规信息扩展数据库

11 TSM 控制器+FTP 服务器

各个地区的终端用户在所属地区的 TSM 控制器完成身份认证，下载最新的策略及运行参数，获取软件分发任务中需要下载的软件。通过认证后根据终端用户所属的角色分配认证后域的访问权限，访问认证后域中的网络资源。

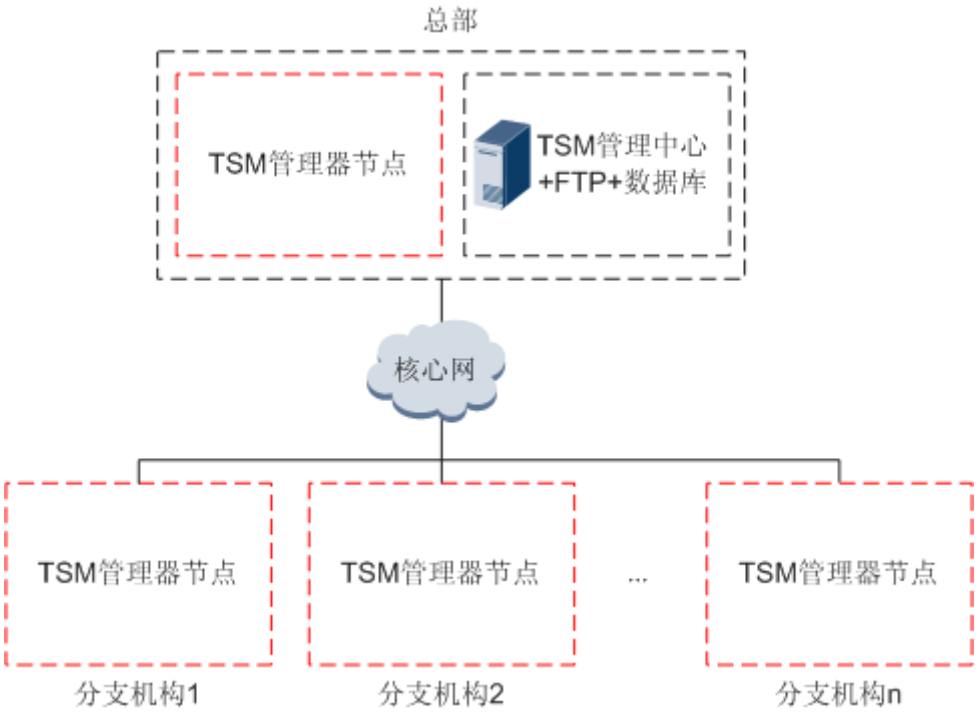
该组网方式适用于终端用户分布在若干个地区办公，分支机构的终端用户通过 VPN 网关接入总部，并且总部需要对分支机构进行统一管理的场合。

3.4 分级式组网

分级式组网方式的主要特点是将 TSM 管理中心部署在总部，而 TSM 管理器部署在分支机构。

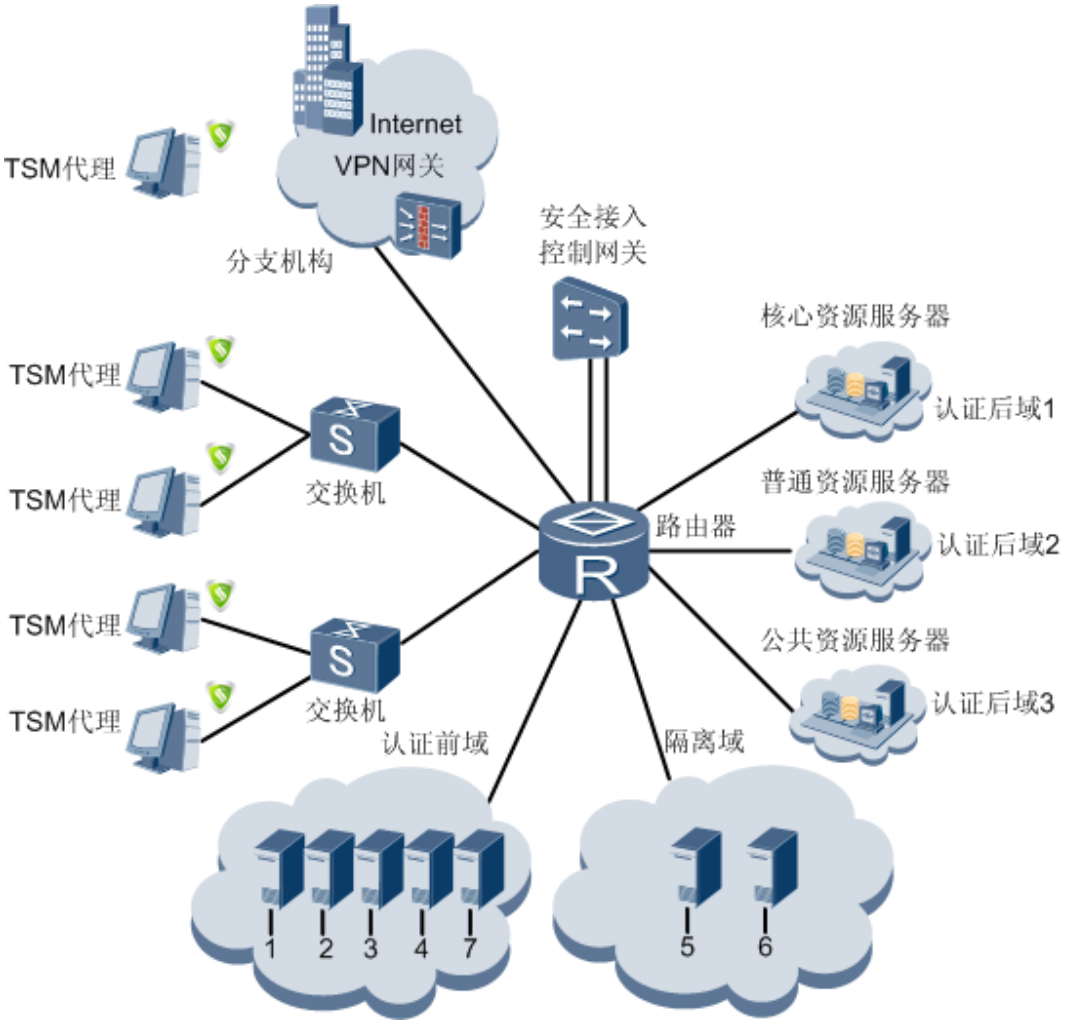
TSM 的分级式组网显示如图 3-6 所示。

图3-6 TSM 分级组网方案



TSM 管理器节点的组网图显示如图 3-7 所示。

图3-7 TSM 管理器节点的组网图



1 TSM 管理器+TSM 控制器+FTP 服务器+见证数据库

2 TSM 控制器+FTP 服务器+主数据库

3 外部认证源

4 DNS 服务器

5 防病毒服务器

6 补丁服务器

7 TSM 控制器+FTP 服务器+镜像数据库

在分级组网环境中，分支机构需要部署一套完整的 TSM 管理器节点。而总部需要部署一套 TSM 管理器节点和 TSM 管理中心节点，TSM 管理器节点用于提供总部的接入控制功能，而 TSM 管理中心提供分级 License 管理、分级补丁管理和分级策略管理功能。在总部，TSM 管理器和 TSM 管理中心必须安装在不同的硬件服务器上。

该组网方式适用于终端用户分布在若干个地区办公，分支机构与总部之间的终端安全管理业务相对独立（与分布式组网而言），并且总部对分支机构终端安全管理业务提供监督和建议的场合。

4 功能特性

关于本章

介绍 TSM 的功能特性，包括终端主机安全管理、终端用户行为管理、终端主机安全接入控制、软件分发、Windows 操作系统补丁管理、资产管理六大业务。

4.1 终端主机安全管理

TSM 提供基于 Microsoft Windows 操作系统的终端安全检查功能，发现终端主机的安全漏洞并引导终端用户进行修复。

4.2 终端用户行为管理

TSM 提供基于终端的员工行为管理功能，目的在于提醒终端用户在使用终端主机时遵守企业制定的行为规范，通过规范员工的行为来提高内网安全管理的能力。

4.3 终端主机安全接入控制

安全接入控制用于控制终端访问网络的权限，对不同安全状况的终端用户开放不同的权限。

4.4 USB 移动存储设备管理

介绍对终端主机的 USB 接口缺乏严格管理给保障企业信息安全带来的挑战，以及 TSM 如何应对这种挑战。

4.5 软件分发

TSM 提供软件分发功能，将软件手工或按计划自动分发到相应的终端主机上，并支持按部门、按操作系统进行分发。

4.6 补丁管理

TSM 提供补丁管理功能，帮助终端用户解决系统漏洞修复工作，提高企业终端主机的安全水平，降低 IT（Information Technology）系统维护成本。

4.7 资产管理

TSM 提供资产管理功能，统一管理企业资产，提高效率，降低维护成本，避免员工私自更改企业终端主机的配置，降低资产遗失的风险。

4.1 终端主机安全管理

TSM 提供基于 Microsoft Windows 操作系统的终端安全检查功能，发现终端主机的安全漏洞并引导终端用户进行修复。

TSM 提供基于 Microsoft Windows 操作系统的终端主机的安全策略检查功能，对终端主机的系统配置状况、安装的软件信息、屏保配置、本地冗余账号等进行检查，并支持对操作系统补丁、Office 补丁、IE 补丁、SQL Server 数据库补丁的更新情况进行检查并自动下载补丁，检查病毒库更新状态。

TSM 代理支持在如下两个阶段执行安全策略：

- 在 TSM 代理启动后执行安全策略。
- 在终端用户通过身份认证后执行安全策略。

4.1.1 检查防病毒软件

该策略支持防病毒软件配置文件和与 Microsoft Windows 安全中心联动两种方式，检查终端主机是否安装指定的防病毒软件、防病毒软件的版本及病毒库的更新周期是否符合要求。

该策略能够实现如下功能：

- 检查终端主机是否安装了指定的防病毒软件，以及防病毒软件是否正在运行。如果防病毒软件没有安装或者防病毒软件没有运行，允许配置其违规等级。
- 检查防病毒软件的版本是否正确，以及防病毒软件病毒库是否更新，允许配置防病毒软件的更新周期。如果防病毒软件在指定的更新周期内未更新病毒库，允许配置其违规等级。

检查防病毒软件策略支持的防病毒软件有：

- Symantec AntiVirus 10.0 企业版
- Symantec Endpoint Protection 11.0
- 金山毒霸 2006
- 金山毒霸 2007
- 金山毒霸 2009
- 江民杀毒软件 2006
- 江民杀毒软件 KV2006
- 江民杀毒软件 KV2008
- 江民杀毒软件 KV2009
- 江民杀毒软件 KV2010
- 江民杀毒软件 KVNET2008
- 江民杀毒软件 KVNET2009
- 江民杀毒软件 KVNET2010
- Rising AntiVirus Software 2006
- Rising AntiVirus Software 2007
- Rising AntiVirus Software 2008

- Rising AntiVirus Software 2009
- Rising Internet Security 2009
- 卡巴斯基反病毒软件 6.0
- 卡巴斯基反病毒软件 7.0
- 卡巴斯基反病毒软件 2009
- 卡巴斯基反病毒软件工作站 5.0
- Mcafee VirusScan Enterprise 7.1
- Mcafee VirusScan Enterprise 8.5
- Mcafee SecurityCenter 8.0
- 熊猫 Panda 7.0
- Trend Micro OfficeScan 5.0
- Trend Micro OfficeScan Clinet/Server Version V7.3
- CA Anti-Virus Ez 7.1.8.0
- CA Anti-Virus V8.1.634.0
- Nod32 3.0
- Microsoft Forefront Client Security

如果终端主机出现如下情况之一则属于违规行为：

- 未安装上述的防病毒软件。
- 防病毒软件未处于运行状态。
- 防病毒软件版本或病毒库版本达不到指定的版本要求。
- 防病毒软件的病毒库尚未设置为周期性更新。

TSM 代理支持与金山毒霸网络版 5.0、金山毒霸网络版 5.5、江民杀毒软件 KV2008、江民杀毒软件 KV2009、江民杀毒软件 KV2010、江民杀毒软件 KVNET2008、江民杀毒软件 KVNET2009、江民杀毒软件 KVNET2010 进行联动，允许管理员设置：

- 上述 8 款软件的病毒库更新周期。
- 当防病毒软件的版本过低时是否强制升级防病毒软件的版本。
- 通过认证后是否调用防病毒软件进行查杀病毒。

检查防病毒软件策略能够提醒或强制终端用户安装上述的防病毒软件、周期性升级病毒库，以便降低病毒入侵的风险。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行防病毒软件检查。

4.1.2 检查操作系统补丁

检查终端主机已安装的 Microsoft Windows 操作系统补丁并记录未安装的补丁。在终端用户未安装指定的补丁时，TSM 代理和 TSM Web Agent 插件提供自动和手动两种方式安装补丁。

检查 Microsoft Windows 操作系统补丁支持的功能有：

- 在部署 WSUS（Windows Server Update Services），或部署 TSM 自身的补丁管理功能的情况下，按 Microsoft Windows 操作系统的补丁级别周期检查终端主机是否安装指定级别的补丁，支持自动下载补丁、自动安装补丁功能。
- 根据指定的补丁列表检查终端主机是否安装了列表中的所有补丁。

如果存在未安装的操作系统补丁则属于违规行为。

对于没有安装 Microsoft Windows 操作系统补丁的终端主机，修复说明请参见表 4-1。

表4-1 未安装 Microsoft Windows 操作系统补丁的修复说明

条件	修复说明
如果采用补丁列表检查方式检查终端主机是否安装某个 Microsoft Windows 操作系统补丁。	管理员需要配置 Microsoft Windows 操作系统补丁的安装路径和违规描述。 当未安装需要安装的 Microsoft Windows 操作系统补丁时，终端用户需要手动安装该补丁，然后重新执行身份认证才能消除违规。
如果采用 TSM 与 WSUS 联动的方式检查 Microsoft Windows 操作系统补丁。	当终端主机未安装指定的 Microsoft Windows 操作系统补丁时，当终端用户单击“自动修复”后，TSM 代理将会自动下载、自动安装 Microsoft Windows 操作系统补丁，完成自动修复。
如果仅仅使用 TSM 的补丁管理模块检查终端主机是否安装 Microsoft Windows 操作系统补丁。	

说明
在安装某些 Microsoft Windows 操作系统补丁后可能会要求重新启动终端主机，为了确保业务的连贯性，在终端用户在单击“自动修复”后，Microsoft Windows 操作系统补丁完成安装之前允许 TSM 控制器为该终端主机开放网络的访问权限。

检查操作系统补丁策略支持的 Microsoft Windows 操作系统有：

- Microsoft Windows 2000（仅 32-bit 版本）
- Microsoft Windows XP （32-bit 版本和 64-bit 版本）
- Microsoft Windows Vista（仅 32-bit 版本）
- Microsoft Windows Server 2003 （仅 32-bit 版本）
- Microsoft Windows 7 （32-bit 版本和 64-bit 版本）

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行 Microsoft Windows 操作系统补丁检查。

4.1.3 检查注册表配置

检查指定的注册表子键和键值是否存在。

注册表是指 Microsoft Windows 操作系统用来存储计算机软硬件信息及 Microsoft Windows 自身的配置信息的数据库。

键是指注册表编辑器左边窗口的文件夹。

子键是指注册表编辑器中隶属于键的子文件夹。

键值是指注册表编辑器中右边窗口的字符串，包括：

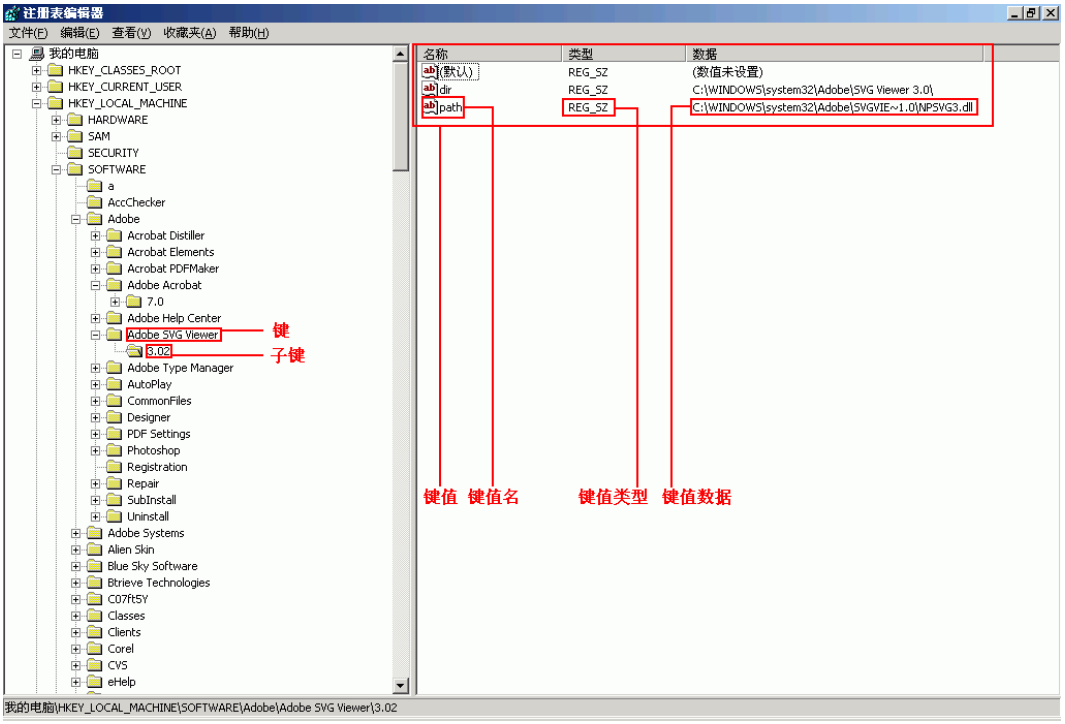
- 名称
- 数据类型
- 数值

说明

要打开注册表，登录 Microsoft Windows 操作系统后，选择“开始 > 运行”，在“打开”文本框输入“regedit”，然后单击“确定”。

键、子键、键值名称、键值类型、键值数据的界面显示如图 4-1 所示。

图4-1 键、子键、键值名称、键值类型、键值数据举例



违规说明及自动修复说明请参见表 4-2。

表4-2 检查注册表子键策略的违规说明

规则	违规	自动修复
注册表中必须存在键值 A。	终端主机的注册表不存在键值 A。	TSM 代理将会自动在终端主机的注册表创建对应的键值，使键值名称、键值数据和管理员设置的键值名称、键值数据保持一致。

规则	违规	自动修复
	终端主机的注册表存在子键 A，但数值与规则设置的数据类型、数值不匹配。	TSM 代理将会自动在终端主机的注册表修改同名子键的键值数据，使同名子键的键值数据和管理员设置的键值数据保持一致。
注册表中不能存在子键 A。	终端主机的注册表存在子键 A。	TSM 代理将会自动在终端主机的注册表删除子键 A。

检查注册表子键策略能够检查对 Microsoft Windows 安全影响较大的注册表子键及键值（如光盘自动运行）是否符合管理员预先设置的要求，降低因注册表键值设置不合理导致 Microsoft Windows 安全性下降的风险。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行注册表子键检查。

4.1.4 检查屏保设置

检查终端主机的屏幕保护参数设置是否满足安全策略的要求，包括是否启用屏幕保护功能、是否启用密码保护功能以及屏幕保护启动时间。

如果在“显示属性”对话框中出现如下情况之一则属于违规行为：

- “屏幕保护程序”被设置成“(无)”。
- 等待时间超过管理员预先设置的时间。
- 未启用“在恢复时使用密码保护”功能。

检查屏保设置策略支持自动修复功能。当 TSM 代理发现终端主机的屏保参数设置不符合该策略预设的要求时，终端用户只需选中“自动修复”，并单击“修复”，按该策略预设的参数设置终端主机的屏保参数。自动修复完成后，注销操作系统后新的屏保参数设置生效。

检查屏保设置策略能够提醒终端用户设置屏幕保护程序及密码，并将启动屏幕保护程序之前的等待时间设为合理值，降低终端用户在离开终端主机而未执行锁定操作的情况下，终端主机被非授权用户使用的风险。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行屏保设置检查。

4.1.5 检查文件共享

检查终端主机共享目录的设置情况，并根据配置的违规用户（如 Everyone、Users）检查共享目录的合法性。如果终端主机的共享目录权限包含违规用户则属于违规行为。

在 Microsoft Windows Vista 操作系统中使用角色表示操作权限：

- 读者拥有只读权限。
- 参与者拥有写入权限。
- 共有者拥有完全控制权限。

检查文件共享策略支持自动修复功能。当 TSM 代理或 TSM Web Agent 插件发现终端主机的共享目录权限设置不符合该策略预设的要求时，终端用户只需选中“自动修复”，并单击“修复”，TSM 代理或 TSM Web Agent 插件将会停止不符合安全要求的目录共享。

检查文件共享策略能够降低无序共享导致信息泄密或恶意攻击的风险。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行共享目录检查。

4.1.6 检查系统冗余账号

系统冗余账号是指在 Microsoft Windows 操作系统中最后一次登录的时间超出预先设置的时间范围的账号。

如果终端主机存在系统冗余账号则属于违规行为。

检查系统冗余账号策略仅支持手工修复功能。当发现终端主机存在系统冗余账号时，终端用户需要手工删除系统冗余账号，然后重新执行身份认证才能消除违规。

系统冗余账号往往容易被管理员忽略，成为黑客攻击的目标。检查系统冗余账号策略能够提醒终端用户及时删除系统冗余账号，降低因系统冗余账号带来的安全风险。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行系统冗余账号检查。

4.1.7 检查打印机共享

检查终端主机是否开启打印机共享，以及打印机共享权限设置是否违规。

如果 TSM 代理发现终端主机存在其中一种情况则属于违规行为：

- 不允许共享打印机，如果发现共享打印机则属于违规行为。
- 允许用户或用户组（包含 Everyone）通过特定权限共享打印机，超出共享权限设置则属于违规。

其中，共享打印机的权限包括：

- 打印文档
- 管理打印机（包括打印文档）
- 管理文档

检查打印机共享策略能够提醒用户不要非法共享打印机，以便限制终端用户通过打印并带走机密文档导致信息泄密。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行打印机共享检查。

4.1.8 检查端口

检查终端主机是否开启了不必要并且有可能导致安全风险的服务。

根据管理员预先设置的端口或者端口范围检查终端主机开启的 TCP（Transfer Control Protocol）或者 UDP（User Datagram Protocol）端口。

如果终端主机开启的服务端口在管理员设置的禁止开启的服务端口范围内，则属于违规。终端用户必须关闭该端口对应的服务才能消除违规。

检查端口策略能够提醒终端用户关闭不必要并且可能招致安全风险的服务，以便提高终端主机防御攻击的能力。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行端口检查。

4.1.9 检查软件黑白名单

在终端主机上检查已经安装的软件是否合法，或者需要强制安装的软件是否尚未安装。

检查软件黑白名单策略仅支持手工修复违规功能，其中软件黑白名单的含义及违规修复说明请参见表 4-3。

表4-3 软件黑白名单的含义

名称	定义	修复说明
只能安装的软件白名单	只能安装的软件白名单是指终端用户只能安装白名单中的软件，安装其他软件则属于违规行为。	如果已经安装了软件白名单以外的软件，终端用户需要卸载该软件，并重新进行安全检查才能消除违规。
必须安装的软件白名单	必须安装的软件白名单是指终端用户必须安装白名单中的所有软件，存在白名单中的任意一款软件未安装则属于违规行为。	管理员需要在 TSM 修复服务器配置软件的安装路径和违规描述。 当未安装需要强制安装的软件时，终端用户需要从手工下载和安装该软件，然后重新执行身份认证才能消除违规。
软件黑名单	软件黑名单是指管理员禁止终端用户在终端主机上安装的软件清单。 如果终端用户在终端主机上安装软件黑名单中的任意一款软件则属于违规行为。	如果已经安装了软件黑名单列出的软件，终端用户需要卸载该软件，然后重新执行身份认证才能消除违规。

该策略在应用时只能选择其中的一种组合方式：

- 必须安装软件白名单+软件黑名单。
- 只能安装软件白名单+必须安装软件白名单。

该策略能够提醒终端用户安装必备的软件，并提醒用户卸载不合法的软件，确保终端用户必须安装安全防护软件，卸载不合法的软件降低引入潜在的安全风险和侵犯软件版权的风险。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行软件黑白名单检查。

4.1.10 检查磁盘分区信息

检查终端主机的磁盘分区数量、分区大小、分区类型和隐藏分区是否符合安全设置。

当终端主机的磁盘包含磁盘分区（物理分区、逻辑分区或 U 盘分区）参数指定为非法的分区，或磁盘分区隐藏参数不符，则属于违规行为。

该策略能够提醒终端用户删除不合法的分区，避免磁盘非法分区导致终端主机存在安全漏洞。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行磁盘分区信息检查。

4.1.11 检查 IE 补丁

检查 IE 补丁策略检查 IE 浏览器的 SP 补丁是否满足要求。

如果终端主机安装 IE 浏览器的 SP 补丁版本不能满足要求则属于违规行为。

管理员需要配置 IE 浏览器 SP 补丁的安装路径和违规描述。当终端主机未安装 IE 浏览器指定版本的 SP 补丁时，终端用户需要手工下载和安装该补丁，然后重新执行身份认证才能消除违规。

检查 IE 补丁策略提醒终端用户安装指定 IE 浏览器版本的 SP 补丁，以便提高 IE 浏览器的安全性。

检查 IE 补丁的策略支持的 IE 浏览器版本有：

- IE 5.0
- IE 5.5
- IE 6.0
- IE 7.0
- IE 8.0

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行 IE 浏览器 SP 补丁检查。

4.1.12 检查 Office 补丁

如果在终端主机安装了 Microsoft Office 办公软件，检查 Office 补丁策略检查 Microsoft Office 的 SP 补丁是否满足要求。

如果在终端主机安装了 Microsoft Office 办公软件，但 SP 补丁版本不能满足要求则属于违规行为。

管理员需要配置 Microsoft Office 的 SP 补丁的安装路径和违规描述。当终端主机未安装 Microsoft Office 指定版本的 SP 补丁时，终端用户需要手工下载和安装该补丁，然后重新执行身份认证才能消除违规。

检查 Office 补丁策略提醒终端用户在安装 Microsoft Office 办公软件的同时安装指定版本的 SP 补丁，以便提高 Microsoft Office 办公软件的安全性。

检查 Office 补丁的策略支持的 Microsoft Office 版本有：

- Microsoft Office 2000
- Microsoft Office 2003
- Microsoft Office 2007

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行 Microsoft Office SP 补丁检查。

4.1.13 检查数据库补丁

检查数据库补丁策略检查 Microsoft SQL Server 的 SP 补丁是否满足要求。

如果终端主机安装的 Microsoft SQL Server 数据库是以下版本之一：

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005

但 Microsoft SQL Server 数据库的 SP 补丁版本不能满足要求则属于违规行为。

检查数据库补丁策略仅支持手工修复功能。管理员需要配置 Microsoft SQL Server 数据库对应的 SP 补丁的下载路径和违规描述。当发现终端主机已经安装了 Microsoft SQL Server 数据库，但尚未安装对应版本的 SP 补丁时，终端用户需要手工从指定的路径下载并安装 Microsoft SQL Server 的 SP 补丁，然后重新执行安全认证才能消除违规。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行数据库 SP 补丁检查。

4.1.14 检查账户安全

检查 Microsoft Windows 操作系统账户的密码是否身体符合要求。

现代企业的信息化程度越来越高，终端用户使用的账户也越来越多。有些安全意识薄弱的终端用户过于追求容易记忆而使用不安全的 Microsoft Windows 操作系统密码。例如，密码与账户名设置相同，密码设置为 123456。黑客能够轻易破解这些简单的密码，进而入侵终端主机，达到盗取机密信息、篡改数据或删除数据的目的。简单密码为网络安全留下潜在的安全隐患。

检查账户安全策略能够实现如下功能：

- 检查 Microsoft Windows 操作系统账户是否设置弱口令。

  弱口令的模式由管理员自行定义。如果发现密码匹配指定的弱口令模式，则属于违规行为。
- 启用 Microsoft Windows 操作系统账户的密码策略。如果密码的复杂度达不到要求，则属于违规行为。
  - 密码必须符合预设的复杂度要求。
  - 在终端主机的密码策略设置不符合管理员设置的密码复杂度设置时，修复终端主机的密码策略。
  - 设置密码的最小长度。
  - 设置密码的最长存留期和最短存留期。
  - 确保最新的密码不能与最近用过的密码相同。

  - 在连续尝试登录失败的情况下自动锁定账户。
  - 在连续尝试登录失败导致账户被锁定的情况下，设置自动解锁账户的时间间隔。
  - 设置连续尝试登录失败次数自动清零至少需要等待的时间。
- 检查用户组是否包括可能不安全的成员。

  例如，在终端主机加入 Microsoft AD 域的情况下，如果 users 用户组或 administrators 用户组包括 Domain users 成员，表明只要拥有 Microsoft AD 域账户的终端用户，都能登录 Microsoft Windows 操作系统。这种情况容易导致信息泄密或越权访问的问题。如果 Microsoft Windows 操作系统的用户组包括指定可能导致不安全的成员（如 Domain users），则属于违规行为。

该策略支持对通过 TSM 代理接入的终端主机检查本地账户，或曾经在本机登录过的 Microsoft AD 账户的密码设置是否符合要求。

4.1.15 自定义策略

自定义策略适用于在若干条策略的简单组合无法满足终端主机安全检查的要求，TSM 允许管理员对策略的检查项进行自定义设置，通过组合若干个检查项和执行脚本来设置违规后的处理措施，以便扩展策略的功能来满足自身的要求。

在自定义策略中提供的判断是否执行响应动作的条件有：

- 注册表项是否已经存在
- 注册表项值是否已经存在
- 注册表项值比较
- 文件已经存在
- 比较文件的 MD5 值
- 比较文件的版本
- 比较文件的创建、修改、访问时间
- 比较文件的大小
- 比较终端操作系统的类型
- 比较终端操作系统的语言
- 比较终端操作系统的 SP 补丁
- 判断系统正在运行某个服务
- 判断系统正在运行某个进程
- 判断系统已经安装了某个补丁

多个条件之间允许使用“或”（只需满足条件之一即可执行响应动作）或“和”（所有条件必须同时满足才能可执行响应动作），以便管理员对终端主机安全检查定义复杂的判断条件。

除了判断条件，管理员还需要定义响应动作，以便在满足条件的情况下采取一定的违规处罚措施。响应动作包括：

- 设置注册表键值
- 递增注册表键值

- 设置策略在执行之前休眠的时间，以便等待动作的执行结果返回。
- 从 Web 站点、FTP 文件服务器或 Microsoft Windows 的文件共享服务器下载并运行一个 Microsoft Windows 操作系统自身的文件（修复 Microsoft Windows 操作系统文件丢失的问题）
- 执行自定义的 VBS 格式、JS 格式、BAT 格式的脚本，而不仅仅局限于 TSM 默认提供的响应动作。
- 显示消息框，提供终端用户对自定义策略执行过程中需要了解的信息。
- 向 TSM 控制器上报违规信息。
- 向终端用户提供管理员自定义修复建议，以便帮助终端用户修复违规。
- 在出现严重违规的情况下隔离终端主机。

该策略支持对通过 TSM 代理或 TSM Web Agent 插件两种方式接入的终端主机进行 Microsoft Office SP 补丁检查。

4.2 终端用户行为管理

TSM 提供基于终端的员工行为管理功能，目的在于提醒终端用户在使用终端主机时遵守企业制定的行为规范，通过规范员工的行为来提高内网安全管理的能力。

4.2.1 ARP 防护

ARP（Address Resolution Protocol）防护策略提供对终端主机的 ARP 静态绑定功能，并能防止终端主机对网络发起 ARP 欺骗攻击和 ARP 泛洪攻击。

安装 TSM 代理并且启用 ARP 防护功能之后能够：

- 阻止从本终端主机发出 ARP 欺骗报文。

  从本终端主机发出的 ARP 报文中，如果 IP 地址和 MAC 地址与本终端主机的实际地址不匹配，则认为是欺骗报文。TSM 代理将会识别拦截 ARP 欺骗报文，以便阻止终端主机发起 ARP 欺骗攻击成为攻击源。
- 阻止从本终端主机发出 ARP 泛洪报文。

  从本终端主机发出的 ARP 报文中，如果频率大于阈值（缺省 25 个/s），则认为 ARP 报文异常。TSM 代理将会识别并拦截 ARP 泛洪报文，以便阻止终端主机发起 ARP 泛洪攻击成为攻击源。
- 提供 ARP 地址静态绑定功能。

  通过静态绑定功能，TSM 代理能够阻止来自外部的网关 ARP 地址欺骗。

该策略支持对通过 TSM 代理接入的终端主机进行 ARP 防护。

4.2.2 监控 USB 存储设备

以管理员预设的 USB 存储设备的访问控制策略开放终端用户对 USB 存储设备的访问权限，并记录终端用户访问 USB 存储设备的日志。

USB 存储设备正逐渐成为企业泄密的主要渠道之一。如何规范终端用户使用 USB 存储设备是管理员急需解决的问题之一。监控 USB 存储设备策略通过规范终端用户访问

USB 存储设备的行为，以及对 USB 存储设备中的文件进行加密，能够降低通过 USB 接口泄密的风险。在发生泄密时 TSM 管理器提供 USB 存储设备的插拔记录和文件拷贝的日志便于取证。

TSM 代理区分注册 USB 存储设备和非注册 USB 存储设备控制访问权限。在安装了 TSM 代理的情况下，除非终端用户通过身份认证和安全检查，并且管理员已经为该终端用户分配了 USB 存储设备的访问权限，否则监控 USB 存储设备被禁用。

监控 USB 存储设备提供的 USB 存储设备的访问控制策略请参见表 4-4。

表4-4 监控 USB 存储设备提供的 USB 存储设备的访问控制策略

USB 存储设备的访问控制策略	说明
禁用 USB 存储设备	• 提供禁用 USB 存储设备功能，包括 U 盘、USB 硬盘、USB 光驱。 • 在禁用 USB 存储设备的情况下，允许终端用户使用 USB 鼠标和 USB 键盘之类的非存储设备。
USB 存储设备只读控制	允许使用 USB 非存储设备和 USB 存储设备。对于 USB 存储设备，只允许读取文件，禁止往 USB 存储设备写入文件。
USB 存储设备文件操作监控功能	• 提供 USB 存储设备文件操作的监控能力，能够识别并且记录如下的文件操作：创建文件、拷入 U 盘、拷出 U 盘、内部复制、删除文件、编辑文件、重命名文件。 • 在禁用 USB 存储设备，或者 USB 存储设备只读控制生效的情况下，监控文件操作功能不生效。
USB 写加密功能	初次启用写加密功能时，通过随机生成方式或导入原来备份的密钥文件，TSM 能够生成密钥，保证终端用户拷贝到 USB 存储设备的文件能够被加密，并且只有具有权限的企业员工才能在终端主机的本地磁盘打开加密后的文件。 不同的 TSM 系统使用不同的密钥。通过导出密钥并设置口令，能够对 TSM 的密钥进行备份。在恢复密钥时，只有输入合法的口令才能导入原来备份的密钥，保证了密钥文件的安全性。

该策略支持对通过 TSM 代理接入的终端主机进行 USB 存储设备监控。

4.2.3 监控 DHCP 设置

监控终端主机是否采用 DHCP（Dynamic Host Configuration Protocol）方式获取 IP 地址。

在 IP 地址使用日益紧张的今天，管理员期待终端主机的 IP 地址统一由企业中的 DHCP 服务器统一自动分配来提高 IP 地址的使用效率。而终端用户私自手工设置静态 IP 地

址，很容易干扰 DHCP 服务器的正常工作并且造成 IP 地址冲突，造成 IP 地址管理上出现混乱。

例如，如果某台 Web 服务器的 IP 地址被设为静态 IP 地址 10.1.1.1，而终端用户将自己的终端主机的 IP 地址设为 10.1.1.1。其他终端用户将无法通过 10.1.1.1 这个 IP 地址访问 We 服务器，导致 Web 服务不可用，干扰其他终端用户的正常工作。

在 TSM 代理检查终端主机的 IP 设置的过程中，如果发现终端主机设置不是以 DHCP 方式获取 IP 地址，则属于违规行为。

TSM 控制器与安全接入控制网关联动，实现如下功能：

- 检查终端主机的网卡是否采用 DHCP 方式获取 IP 地址。
- 仅检查终端主机连接 TSM 控制器的网卡是否采用 DHCP 方式获取 IP 地址。
- 仅检查终端主机与 TSM 控制器连接之外的网卡是否采用 DHCP 方式获取 IP 地址。

如果管理员要强制终端主机使用 DHCP 方式获取 IP 地址，而不允许终端用户更改网卡获取 IP 地址的方式，则无法通过 TSM 控制器与安全接入控制网关联动检查部分网卡是否通过 DHCP 方式获取 IP 地址。

监控 DHCP 设置策略支持自动修复功能，当终端用户出现手工设置网卡的 IP 地址时，TSM 代理将会将网卡获取 IP 地址的方式自动修改为“自动获得 IP 地址”。

该策略支持对通过 TSM 代理接入的终端主机的获取 IP 地址方式进行监控。

4.2.4 监控非法外连

监控终端用户是否非法连入 Internet。

终端用户私自接入 Internet 可能会使终端主机无意之间感染病毒或木马，给企业内部网络安全带来较大的威胁。

监控非法外连策略支持以下两种模式：

- 允许通过合法路径连接外网

  当发现终端用户使用的代理服务器 IP 地址、路由 IP 地址或目的 IP 地址不在公司限定的范围之内时，TSM 代理将会向 TSM 控制器上报违规信息，由管理人员进行跟踪和确认。
- 禁止访问互联网

  当发现终端主机能够连通管理员在 TSM 管理器上设置的目标地址或域名上的指定端口时，TSM 代理将会向 TSM 控制器上报违规信息，由管理人员进行跟踪和确认。

该策略支持对通过 TSM 代理接入的终端主机实施非法外连进行监控。

4.2.5 监控本地服务

监视 Microsoft Windows 服务的运行状况，通过配置策略参数强制启动或禁用某些 Microsoft Windows 服务。

监控本地服务策略能够强制启动或禁用某些 Microsoft Windows 服务。

如果终端主机运行的 Microsoft Windows 服务不满足预先设置的要求，则属于违规行为：

- 管理员将指定 Microsoft Windows 服务的类型设为禁止运行，而 TSM 代理发现该服务正在启动或正在运行。
- 管理员将指定 Microsoft Windows 服务的类型设为要求运行，而 TSM 代理发现该进程尚未启动。

当发现策略参数预设为禁止的 Microsoft Windows 服务正在运行时，TSM 代理将会尝试停止该服务。

当发现策略参数预设为运行的 Microsoft Windows 服务尚未运行时，TSM 代理将会尝试启动该服务。

该策略支持对通过 TSM 代理接入的终端主机进行进程监控。

4.2.6 监控网络应用程序

监控终端主机网络应用程序的运行状态。

当发现网络应用程序启动时，TSM 代理将会根据管理员配置的规则和终端用户配置的规则进行检查：

- 如果管理员配置的规则或终端用户配置的规则禁止网络应用程序，则 TSM 代理将会阻止该网络应用程序启动。
- 如果管理员配置的规则和终端用户配置的规则相冲突，则 TSM 代理将会根据管理员配置的规则确定是否允许网络应用程序启动。
- 如果应用程序的名称与所有的规则设置的名称都不匹配，则 TSM 代理会根据管理员配置的 Default 规则确定是否允许网络应用程序启动。

监控网络应用程序策略能够拦截并禁止网络应用程序的启动，例如 IM（Instant Messaging）软件、炒股软件、P2P（Point to Point）软件、网络游戏，使终端用户在聚焦工作的同时提升企业内网安全管理水平。

该策略支持对通过 TSM 代理接入的终端主机进行网络应用程序监控。

4.2.7 监控屏幕拷贝

监控屏幕拷贝策略能够确保机密电子文档（例如 DWG 图片、AI 图片或 DOC 文档）不会被终端用户通过“PrintScreen”键截取屏幕非法保留或传播。

监控屏幕拷贝策略在执行时能够防止终端用户通过“PrintScreen”键截取屏幕，但不会产生报表。

该策略支持对通过 TSM 代理接入的终端主机进行屏幕拷贝监控。

4.2.8 监控网络连接

监控网络连接策略监视常见网络设备的运行状态。

终端用户私自接入 Internet 可能会使终端主机无意之间感染病毒或木马，给企业内部网络安全带来较大的威胁。

监控网络连接策略能够监控的网络设备有：

- MODEM（MOdulator-DEModulator）
- ISDN（Integrated Services Digital Network）
- PPPoE（PPP over Ethernet）拨号连接（仅限采用 Microsoft Windows 创建的拨号连接）
- VPN（Virtual Private Network）连接（仅限采用 Microsoft Windows 创建的 VPN 连接）

在管理员禁用上述一种或几种网络连接后，如果发现上述网络连接处于激活状态则属于违规行为，TSM 代理将会记录上述网络连接的开始和结束的时间，并自动断开连接，防止终端用户非法连接 Internet。

该策略支持对通过 TSM 代理接入的终端主机进行网络连接监控。

4.2.9 监控访问站点

通过配置网站的 URL（Uniform Resource Locator）地址禁止终端用户访问某些网站，或允许终端用户访问某些网站。

监控访问站点策略能够禁止终端用户访问某些网站，使终端用户在上班时间聚焦工作。另外，禁止访问某些可能带有恶意脚本的网站能够避免因浏览网页引入潜在的安全风险。

如果终端用户访问禁止网站列表中的网址则属于违规行为。

该策略支持对通过 TSM 代理接入的终端主机进行访问站点监控。

4.2.10 监控 IP 访问

监控终端主机访问网络是否符合管理员预设的规则。

监控 IP 访问策略能够监视、控制终端主机之间的互访，屏蔽终端主机自身某些重要的端口，提高终端主机的安全性。

监控 IP 访问策略支持以下两种工作模式：

- 禁止访问模式

  在未设置网络访问规则的情况下，终端主机访问网络的请求将会全部被拒绝，除非管理员允许终端主机访问指定的网段或指定的端口。
- 允许访问模式

  在未设置网络访问规则的情况下，终端主机访问网络的请求将会全部被放行，除非管理员禁止终端主机访问指定网段或指定的端口。

该策略支持对通过 TSM 代理接入的终端主机进行 IP 访问控制。

4.2.11 监控进程

监控 Microsoft Windows 操作系统正在运行的进程列表。根据管理员配置的参数获取 Microsoft Windows 操作系统的进程信息，并根据进程名拦截进程，阻止进程启动、或者关闭进程。

监控进程策略能够强制禁止终端主机运行某些进程（如 IM 软件、炒股软件、P2P 软件、网络游戏），强制终端主机运行其他一些进程（如防病毒软件、防火墙软件、计算机端口通信监视软件），使终端用户在聚焦工作的同时强化内网安全管理水平。

如果终端主机运行的进程不满足预先设置的要求，则属于违规行为：

- 管理员将指定进程的类型设为禁止运行，而 TSM 代理发现该进程正在启动或正在运行。
- 管理员将指定进程的类型设为要求运行，而 TSM 代理发现该进程尚未启动。

对于类型设为要求运行的进程而终端主机未运行该进程，TSM 代理与 TSM 控制器联动拒绝该终端主机访问认证后域。当终端用户单击修复链接时，TSM 代理将会尝试启动该进程以消除违规记录。

对于已经被拦截或者监视过的进程，TSM 管理器会记录这些进程的 MD5（Message Digest 5）。如果后续终端用户修改进程名，TSM 代理能够识别并且自动按照策略进行处理。

该策略支持对通过 TSM 代理接入的终端主机进行进程监控。

4.2.12 监控系统设备

监控系统设备策略具有监控终端主机使用外部设备的功能。

在信息安全控制较为严格的场合，要防止终端主机通过软驱、打印机、串行接口、并行接口、红外接口、1394 接口、Modem、PCMCIA、蓝牙接口、SD 卡、MMC 卡泄露机密信息，公司需要严格控制终端主机各种接口的使用。

监控系统设备策略支持的功能包括：支持启用或禁用软驱、打印机、串行接口、并行接口、红外接口、1394 接口、Modem、PCMCIA、蓝牙接口、SD 卡、MMC 卡。

该策略支持对通过 TSM 代理接入的终端主机进行系统设备监控。

4.2.13 监控网络流量

监控网络流量策略提供周期性的网络流量统计和控制功能。

网络流量监控策略能够有效避免终端主机（如运行 P2P 软件进行下载）占用过多的带宽导致网络拥塞，确保正常网络服务能够顺畅运行。

为了方便管理员灵活统计终端主机的网络流量，监控网络流量策略支持统计指定协议或指定协议+端口范围内的网络数据的流量进行流量监控。其中，“统计指定协议+端口范围”支持以下两种模式：

- 统计定义范围内的流量。
- 统计除定义范围内的所有其他流量。

管理员在 TSM 管理器设置严重违规的网络流量阈值。如果 TSM 代理发现终端主机的流量超过严重违规的网络流量阈值，TSM 代理将会断开终端主机与网络的连接，并且在指定的时间范围内终端主机无法访问网络。

该策略支持对通过 TSM 代理接入的终端主机进行网络流量监控。

4.2.14 监控多网卡

监控终端主机的网卡连接状态和无线网卡，并提供禁用无线网卡功能。

为了降低安全威胁从一个网络传播到另一个网络的风险，某些企业不允许一台终端主机通过多块以太网卡同时连接不同的网络，例如电信运营商的 BOSS（Business & Operation Support System）网和 OA（Office Automation）网。在终端主机已经接入一个网络时，必须与当前的网络断开连接。

监控多网卡提供检查终端主机的网卡连接状态、禁用无线网卡、监视无线网卡功能。

如果终端主机的网卡连接状态，或无线网卡的使用情况不符合管理员下发的策略要求，则属于违规行为，TSM 代理与 TSM 控制器联动拒绝该终端主机访问认证后域，并提醒终端用户修复违规信息后重新认证。

该策略支持对通过 TSM 代理接入的终端主机进行多网卡监控。

4.2.15 监视文件操作

监视终端用户在终端主机的本地硬盘（不包括映射网络驱动器中的文件和远程共享的文件）进行的文件操作。

监视文件操作策略能够帮助管理员跟踪终端用户更改指定文件或指定类型的文件的操作。该策略能够监视的文件操作包括：

- 创建文件
- 复制文件
- 编辑文件
- 重命名文件
- 删除文件

当发现终端用户操作的文件名与监视规则相匹配时，TSM 代理将会把终端用户名称、操作名称、操作时间和文件在终端主机本地上的路径上报 TSM 管理器供管理员查阅。

例如，为了统一产品宣传幻灯片的风格，不建议终端用户随意修改公司统一分发的幻灯片模板“blank.pot”。

在监控文件操作策略下发至 TSM 代理后，如果终端用户私自修改“blank.pot”，TSM 代理将会记录终端用户名称、操作名称、操作时间和文件在终端主机本地上的路径上报至数据库供管理员查阅。

该策略支持对通过 TSM 代理接入的终端主机进行文件操作监控。

4.2.16 监控光驱

监控光驱策略具有监控终端主机使用光驱设备的功能。

在信息安全控制较为严格的场合，要防止终端主机通过光驱设备泄露机密信息，公司需要严格控制终端主机使用光驱设备。

监控光驱策略支持禁用所有光驱和禁用刻录光驱的写功能。

该策略支持对通过 TSM 代理接入的终端主机进行光驱监控。

4.3 终端主机安全接入控制

安全接入控制用于控制终端访问网络的权限，对不同安全状况的终端用户开放不同的权限。

安全接入控制主要功能包括：

- 支持基于 TSM 代理的多种认证方式。

  支持普通账号、Microsoft AD 域账号、MAC（Media Access Control）账号、第三方 LDAP 账号多种认证方式。支持身份认证、执行终端主机安全管理策略和终端用户行为管理策略。其中第三方 LDAP 包括 Novell eDirectory、IBM Tivoli、Sun One，第三方 LDAP 认证说明请参见表 4-5。

表4-5 第三方 LDAP 认证支持的特性

特性	说明
LDAP 服务器故障身份认证自动通过	终端用户使用第三方 LDAP 账号认证，如果 TSM 控制器发现第三方的 LDAP 服务器出现故障，则 TSM 控制器允许终端用户身份认证自动通过，确保业务不会因第三方 LDAP 服务器故障而被中断。
支持受 SSL 保护的 Novell eDirectory	如果 Novell eDirectory 受 SSL 保护，以下的两种情况均支持通过 SSL 加密保护与 Novell eDirectory 之间的通信： • TSM 管理器从 Novell eDirectory 同步部门和账号 • 终端用户使用 Novell eDirectory 账号进行身份认证

Microsoft AD 域认证说明请参见表 4-6。

表4-6 Microsoft AD 域认证支持的认证方式

认证方式	说明
Kerberos 认证	Kerberos 属于一种网络认证协议，通过密钥系统在客户端与服务器之间提供强大的认证服务。Kerberos 的优点在于不依赖操作系统的身份认证，无需地址信任要求，无需物理安全要求，认证数据包可能被读取、插入、修改的情况下提供安全的身份认证服务。在身份认证安全性要求较高的情况下推荐使用 Kerberos 认证。 在使用 Kerberos 认证的情况下，要求终端主机与 Microsoft AD 域控制器和、TSM 管理器三者的时间保持同步。 为了减少非法终端用户伪造、篡改认证报文冒充合法终端用户情况发生，在进行身份认证时 TSM 代理支持强制进行 Kerberos 认证。如果 Microsoft AD 域认证采用 Kerberos 认证方式的情况下： • 如果终端主机已经加入 Microsoft AD 域，并且终端用户使用 Microsoft AD 域账号登录 Microsoft Windows 操作系统，则无须终端用户输入密码，TSM 代理将会完成自动登录。 • 如果终端用户并未使用 Microsoft AD 域账号登录 Microsoft Windows 操作系统，允许终端用户在 TSM 代理输入 Microsoft

认证方式	说明
	AD 域账号和密码方式进行 Microsoft AD 域认证。
非 Kerberos 认证	不采用 Kerberos 协议进行身份认证，而是通过校验 Microsoft AD 域控制器中的 objectguid 是否正确，验证 Microsoft AD 域认证是带合法。 因认证限制的条件较比 Kerberos 认证少，在 TSM 代理进行非 Kerberos 认证时，认证成功率会比 Kerberos 认证方式的认证成功率高，但认证安全性比不上 Kerberos，只适用于受信任的网络环境。 在使用非 Kerberos 认证方式时，如果 Microsoft AD 域控制器出现故障，则 TSM 控制器允许终端用户直接通过身份认证，确保在 Microsoft AD 域控制器失效时终端用户依然允许访问认证后域中受保护的网络资源，业务不会被中断。
支持受 SSL 保护的 Microsoft AD 域控制器	如果 Microsoft AD 域控制器受 SSL 保护，以下的两种情况均支持通过 SSL 加密保护与 Microsoft AD 域控制器之间的通信： • TSM 管理器从 Microsoft AD 域控制器同步部门和账号 • 终端用户使用 Microsoft AD 域账号进行身份认证

- 支持基于 TSM Web Agent 插件的多种认证方式。

  支持普通账号、Microsoft AD 域账号、第三方 LDAP 账号认证方式。支持身份认证、执行终端主机安全管理策略。
- 支持基于 Web 的无代理认证方式。

  提供基于 Web 的认证方式，只要用户登录 Web 客户端认证界面，身份认证通过后，即可访问正常的网络资源。支持身份认证功能。
- 支持终端用户进行匿名认证。

  名认证是指终端用户不需要认证账号和密码，在指定的网络区域通过支持匿名认证的登录类型即可完成认证的一种认证方式。

  匿名认证方式适用于组织不采用账号管理，内部员工没有账号和密码，或者外部访客不申请账号和密码，通过匿名方式进行认证的场合。采用匿名认证，能够监控在指定网络区域接入受控网络的终端主机，并对匿名用户进行安全检查、接入控制等业务的管理。

  匿名认证方式不需要终端用户输入认证账号和密码，通过 TSM 管理器内置的“~anonymous”账号和密码完成认证，能够降低管理员维护部门和账号信息的成本。对于终端用户，特别是访客，不需要申请特定的账号和密码，使得终端用户能够更容易、方便地通过认证，并接入到受控网络。
- 支持访客自助服务。

  当外来人员需要使用公司的网络时，负责接待的员工提出访客账号申请而不是管理员直接为外来人员申请账号，管理员只负责审批，从而减轻管理员的维护工作量，并由 TSM 管理器自动记录在案。审核通过后负责接待的员工把账号信息告诉被接待的外来人员，外来人员使用该账号进行身份认证后即可接入受控网络。
- 支持账号绑定 IP 地址和 MAC 地址。

账号绑定 IP 地址和 MAC 地址提供一种更为严格的验证方式，主要解决账号被盗用的问题。在账号绑定 IP 地址和 MAC 地址后，如果终端用户在认证时 IP 地址或 MAC 地址不匹配，则终端用户无法通过身份认证。

- 支持终端主机绑定 IP 地址。

  在使用静态 IP 地址的网络环境中，因终端用户私自修改主机的 IP 地址，导致 IP 地址与其他终端主机的 IP 地址或者服务器的 IP 地址冲突，进而干扰网络的正常运行。TSM 提供基于终端主机的 MAC 地址绑定 IP 地址的功能。绑定 IP 地址后，如果终端用户私自修改终端主机的 IP 地址，则该终端用户无法通过身份认证，进而无法接入受控网络，达到被隔离的效果，降低 IP 地址冲突造成对网络的干扰。

- 支持多种接入控制方式。
  - 支持 Eudemon 防火墙或 USG（Unified Security Gateway）统一安全网关作为安全接入控制网关对终端主机进行接入控制。

    安全接入控制网关的使用场景和方案特点请参见表 4-7。

表4-7 安全接入控制网关的使用场景和方案特点

使用场景	方案特点
• 适应大、中、小三种网络，终端主机相对集中或者集中分散若干个不同地区的场合。 • 适用于内部员工、临时雇员、访客、合作伙伴和远程用户 VPN 接入等权限不同的场合。 • 适用于操作和维护工作投入有限的场合。	• 基于用户角色访问权限控制机制。 • 在安装时不改变现网拓扑结构，维护简单。 • 能够实现电信级安全标准。 • 支持逃生通道和自动恢复故障功能。

在终端用户未通过身份认证的情况下，如果终端用户通过 Web 浏览器访问认证后域中的 Web 服务器时，Eudemon 防火墙或 USG（Unified Security Gateway）统一安全网关支持向终端用户推送 TSM 控制器的认证页面，方便未安装 TSM 代理的终端用户通过 Web 客户端方式进行身份认证。

在使用 Eudemon 防火墙或 USG（Unified Security Gateway）统一安全网关作为安全接入控制网关的情况下，TSM 允许管理员在不同的时段对相同的终端用户实施不同的接入控制规则。时段只支持两个，分别是指定时段和其余时段（又称默认时段）。区分上下班时段为终端用户分配两个不同的认证后域。

例如某些重要的服务器在上班时段必须有人全程值守，确保在重要服务器出现故障时立即着手处理。下班后由于无人值班，通过安全接入控制网关临时关闭重要服务器的访问权限，到第二天管理员上班时安全接入控制再自动开启重要服务器的访问权限。

- 支持 802.1x 交换机对终端主机进行接入控制。

  802.1x 交换机的使用场景和方案特点请参见表 4-8。

表4-8 802.1x 交换机的使用场景和方案特点

使用场景	方案特点
• 适用于网络规模较小、终端主机的物理位置集中的场合。 • 适用于接入层设备支持 802.1x 的场合。 • 适用于内部员工、临时雇员、合作伙伴等通过有线或无线网络接入的场合。 • 适用于网络管理员的技术水平高的场合。	• 支持二层网络协议，对设备的整体性能要求不高，可有效降低建网成本。 • 基于动态 VLAN、动态 ACL 下发的用户角色访问权限控制。 • 认证与业务分离，安全性高，抗攻击力强。 • 在通过认证前无法访问网络。 • 配置和维护 802.1x 交换机过于复杂，在出现故障时必须手动关闭 802.1x。 • 当使用公共认证协议的时候，终端主机通过 Windows 自带的 802.1x 认证客户端进行身份认证。 • 当使用私有协议认证的时候，终端主机必须运行 TSM 代理进行 802.1x 身份认证。

- 支持通过 NAC（Network Access Control）交换机对终端主机进行 Portal 接入控制。

  NAC 交换机的使用场景和方案特点请参见表 4-9。

表4-9 NAC 交换机的使用场景和方案特点

使用场景	方案特点
• 适用于网络规模较小、终端主机的物理位置集中的场合。 • 适用于内部员工、临时雇员、合作伙伴等通过有线或无线网络接入的场合。 • 适用于网络管理员的技术水平高的场合。	• 支持二层网络协议，对设备的整体性能要求不高，可有效降低建网成本。 • 基于动态 VLAN、动态 ACL 下发的用户角色访问权限控制。 • 认证与业务分离，安全性高，抗攻击力强。 • 在通过认证前只能访问管理员放行的网络资源。 • 部署位置灵活，NAC 交换机部署在接入层或数据中心的出口处。 • 终端主机无须安装客户端，降低部署成本，不支持终端主机隔离。 • 终端主机安装 Web Agent 插件或者 TSM 代理，支持终端主机隔离。

- 支持通过 NAC 交换机对例外设备进行 MAC 旁路接入控制。

  在采用 802.1x 交换机作为安全接入控制网关的情况下，对于无法安装 TSM 代理（作为 RADIUS 认证的客户端）的 IP 设备，如打印机和 IP Phone，因无法通过 802.1x 认证，无法使用网络导致这些设备无法被终端用户使用。

  MAC 旁路认证是为解决此问题而设计的认证方式。当 IP 设备进行 802.1x 认证失败后，把 IP 设备的 MAC 地址作为账号和密码发送至 RADIUS 服务器（TSM 控制器）进行认证。通过设置 IP 设备的 MAC 地址、接入的交换机、端口来达到放行的目的。只有 MAC 地址和管理员设置的 IP 设备的 MAC 地址相匹配，并且接入的交换机及端口正确才允许通过认证。认证通过后，NAC 交换机允许 IP 设备访问网络，供终端用户使用。
- 支持通过 IPSec 对终端主机进行接入控制。

  IPSec 接入控制方式的使用场景和方案特点请参见表 4-10。

表4-10 IPSec 接入控制方式的使用场景和方案特点

使用场景	方案特点
• 适应大、中、小三种网络，终端主机相对集中或者集中分散若干个不同地区的场合。 • 适用于内部员工、临时雇员、访客、合作伙伴和远程用户 VPN 接入等权限不同的场合。 • 适用于操作和维护工作投入有限的场合。	• 有效控制局域网内终端主机互相访问的行为。 • 提供隔离域，供未通过安全策略检查的终端主机进行安全漏洞修复。 • IPSec 属于纯软件控制方式，能够有效降低成本。 • 安装、配置和维护简单。 • 支持逃生通道，自动恢复故障。

- 支持混合使用上述接入控制手段实现有效的接入控制。

- 支持实体级接入控制。

  利用 Eudemon 防火墙或 USG 安全统一网关设备的联动和控制优势，能够控制终端用户访问指定资源的权限。
- 支持基于角色的接入控制。

  通过定义角色，将相关的资源访问权限授予角色，并将角色授予账号的方式来控制账号的访问权限。
- 支持对终端主机之间的互访控制。

  通过 802.1x，提供对终端互访的控制，防止未授权终端对网络资源的访问。
- 支持规则联动。

  在 TSM 管理器上配置认证前域、隔离域、认证后域的规则。
- 支持场所管理。

  在终端主机（尤其是便携式计算机）处于不同的网络环境下，可能需要应用不同的策略模板。例如，在办公室办公时使用策略模板 A。出差在外并且没有使用 VPN 接入时，使用策略模板 B。出差在外并且使用 VPN 接入公司内部网络时，使用安全策略 C。不同的场所对应不同的策略模板。TSM 代理能够支持由网络环境

变化自动切换场所，或者由终端用户手工切换场所，以便在不同的策略模板中进行切换，在不同的场所实施不同的安全策略。

- 支持通过防火墙配置助手简化终端主机接入控制的分批部署，并且在 TSM 控制器出现异常时由防火墙配置助手放行网络，确保管理员在处理故障时终端用户访问网络业务不会被中断。

4.4 USB 移动存储设备管理

介绍对终端主机的 USB 接口缺乏严格管理给保障企业信息安全带来的挑战，以及 TSM 如何应对这种挑战。

背景

近年来，移动存储设备种类越来越丰富，如 USB 移动硬盘、各类 Flash Disk（U 盘）、各种存储卡（SD/MMC、CF/XD/MS、TF、M2）、USB MP3/MP4、智能手机、数码相机等。相关缩略语的全称请参见表 4-11。

表4-11 缩略语及全称

缩略语	全称
USB	Universal Serial Bus
SD	Secure Digital Card
MMC	MultiMedia Card
CF	Compact Flash
XD	Extreme Digital Card
MS	Memory Stick
TF	Trans Flash Card
MP3	MPEG Layer-3
MP4	MPEG Layer-4

上述品种繁杂的移动存储设备在带来便利和更高效率的同时，也给企业信息安全带来了如下严峻的挑战。缺乏对 USB 接口及移动存储设备进行有效管理给企业信息安全带来的挑战请参见表 4-12。

表4-12 缺乏对 USB 接口及移动存储设备进行有效管理给企业信息安全带来的挑战

挑战	说明
无法控制外来移动存储设备的随意接入。	外来移动存储设备随意通过终端主机接入企业网络，带走机密数据，而且移动存储设备携带的病毒容易感染终端主机。

挑战	说明
无法保证内部移动存储设备丢失后导致的信息外泄。	移动存储设备未进行任何安全保护，企业保存重要信息的存储设备外出丢失后导致重要信息外泄。 因无法对存储设备使用进行授权控制，企业普通存储设备内部丢失后无法保证不被随意访问而导致信息外泄。
无法保证数据的安全交换。	移动存储设备不做任何控制，无法解决移动存储设备在内外网间、安全等级不同的网络交换时容易导致数据外泄的问题。
病毒快速蔓延。	未进行移动存储设备免疫处理，容易导致 U 盘病毒在企业网中传播。

在面对上述信息安全威胁时，企业通常通过如下手段来应对移动存储设备的安全威胁：

- 直接剪断 USB 接口与主板之间连接的数据线。
- 要求终端主机供应商从 BIOS（Basic Input Output System）中清除读写 USB 的功能。
- 在终端主机外加安全机箱，防止员工私自拆卸机箱，并交由独立的信息安全部门来管理。
- 在终端主机安装远程监视软件。
- 在办公区安装摄像头监视终端用户是否违规使用移动存储设备。
- 落实信息安全制度，通过制定信息安全规范及其相应惩罚措施来确保企业数据安全。
- 购买专用的移动存储介质管理系统，禁止移动存储设备在连接 Internet 的机器上使用。
- 管理敏感信息的部门设立一台专用的终端主机，用 U 盘将数据拷入专用的终端主机，然后通过终端主机刻录光盘，最后通过光盘拷入敏感信息管理系统。

这些传统的保护措施具有如下缺点：

- 操作方式过于僵化。
- 成本过高。
- 容易给员工不信任感。
- 难以取证。
- 无法实现终端用户与互联网之间数据交换的需求。
- 效率低且存在安全隐患。
- 无法从根本上确保企业数据安全。

TSM 支持的移动存储设备类型

TSM 能够支持 TSM 代理对表 4-13 中列出的移动存储设备的访问权限进行控制。

表4-13 支持的移动存储设备类型

移动存储设备类型		举例
标准 USB 存储设备	以存储作为其唯一功能的 USB 存储设备	USB 移动硬盘、Flash Disk（U 盘）、存储卡（SD/MMC、CF/XD/MS、TF、M2）。
	以存储作为其辅助功能的 USB 存储设备	带 USB 接口的 MP3/MP4、多合一设备（杀毒 U 盘、U3、无线数据卡内接存储、数字证书 USBKey 自带存储）、有盘符智能手机、数码相机。

说明

表 4-14 中列出的设备类型不在 TSM 的管理和控制范围之内。TSM 会自动识别这些设备并允许终端用户正常使用。

表4-14 非控制设备类型

设备类型	举例
USB 智能卡类	USB 证书、USB 加密狗等。
USB 人机接口类	USB 键盘、USB 鼠标、USB 手写板等。
USB 打印机类	USB 接口的打印机。

注册移动存储设备

注册移动存储设备的目的在于方便管理员对移动存储设备进行分类和登记，并区分对待未注册设备。

注册移动存储设备有利于强制终端用户遵守公司制定的移动存储设备管理规范，确保企业重要数据不会通过移动存储设备外泄。

注册移动存储设备的主要功能请参见表 4-15。

表4-15 注册移动存储设备的主要功能

功能	说明
标识移动存储设备	TSM 根据移动存储设备标识来进行授权和控制，移动存储设备标识要求全局唯一。TSM 支持如下两种方式标识移动存储设备： • 读取移动存储设备的序列号作为自身的唯一标识符。仅

功能	说明
	适用于移动存储设备的序列号不重复的场合。可支持的移动存储设备包括 U 盘、USB 光驱和 USB 刻录机。 • 向移动存储设备写入 ID 作为自身的唯一标识符（UUID 方式）。适用于移动存储设备不存在序列号、序列号重复或者使用读卡器接入存储卡的场合。
存储设备注册方式	所有移动存储设备由终端用户在安装 TSM 代理的终端主机进行，移动存储设备在注册后会被全盘加密。 • 在终端用户无感知的情况下由 TSM 代理自动完成存取加密数据。 • 全盘加密注册后的移动存储设备在未安装 TSM 代理的终端主机上必须格式化后才能正常使用。该种注册方式确保移动存储设备丢失后不能打开文件，无须担心敏感信息外泄。 说明 多合一设备支持按照设备类型分别进行注册和控制。例如：自带光驱功能的移动存储设备能够对存储设备进行注册和控制，而对光驱则不进行控制。 TSM 不会在物理上破坏移动存储设备。所有已注册移动存储设备在未安装 TSM 代理的终端主机上格式化后恢复成普通设备。但是在企业内网中，在已安装 TSM 代理的终端主机格式化移动存储设备时，该移动存储设备又会被 TSM 代理自动全盘加密，整个过程对终端用户是无感知的。
注销移动存储设备	适用于移动存储设备不需要在企业中使用的场合。 1. 管理员在 TSM 管理器删除移动储存设备的注册信息。 2. 终端用户在没有安装 TSM 代理的终端主机格式化移动储存设备。
移动存储设备挂失和解除挂失	挂失适用于移动存储设备遗失，管理员需要阻止已遗失的移动存储设备在企业中继续使用的场合。将移动存储设备修改为挂失状态后，该移动存储设备将无法在企业中继续使用。 如果移动存储设备重新找到，管理员需要为挂失状态的移动存储设备解除挂失，以便移动存储设备在企业内部继续使用。

管理维度

TSM 提供按账号、按网络区域和部门三种维度来管理移动储存设备，以此作为移动存储设备实施授权和审计策略的对象。

管理维度的主要功能请参见表 4-16。

表4-16 管理维度

类型	说明
账号	为单个账号授予移动存储设备的访问权限。授权的优先级最高。
网络区域	为若干个 IP 地址段中认证的所有账号授予移动存储设备的访问权限。授权的优先级仅将于账号的授权优先级。
部门	组织创建方法包括： • 手工创建：管理员通过手工创建部门来创建企业组织信息。 • 从 Excel 文件导入：管理员通过从 Excel 格式文件导入部门的方式来创建企业组织信息。 • 从外部数据源同步：支持手工或自动从外部数据源同步组织信息。TSM 支持定义同步映射规则，如定义将目录服务器的 A、B 部门同步到 TSM 的 F 部门下。

控制方式和审计策略

移动存储设备的授权级别说明请参见表 4-17。

表4-17 移动存储设备的授权级别说明

访问权限	说明
禁用	TSM 将禁止终端用户在安装了 TSM 代理的终端主机上使用 USB 移动存储设备，允许使用 USB 非存储设备（如 USB 鼠标）。
只读	TSM 代理禁止终端主机向移动存储设备写入数据，但允许打开存放在移动存储设备中的文件，从移动存储设备拷出文件，以便实现单向转移数据的功能。
文件监控	不限制终端用户在移动储存设备进行读写文件，但 TSM 代理会记录终端用户在移动储存设备中的文件操作，供管理员查阅。
写入加密	当拷贝文件至移动存储设备中的加密文件夹时，TSM 将加密该文件，只有下发了“只读”、“文件监控”或“写入加密”参数的终端用户才具有权限在终端主机的本地磁盘打开加密后的文件。 此种方式在不慎遗失移动储存设备时立即向管理员申请挂失，则无需担心文件泄密问题。

审计策略包括：

- USB 拔插日志

  记录终端用户在终端主机插入或拔出移动存储设备的时间、账号、姓名、IP 地址、MAC 地址、操作类型（插入或拔出）。

- 文件操作日志

  记录终端用户在终端主机插入或拔出移动存储设备的时间、账号、姓名、IP 地址、MAC 地址、操作类型（新建、复制、修改、重命名、删除）、文件路径。

基于终端主机和终端用户的授权和审计策略

TSM 支持从上级部门继承授权和审计策略，也支持为终端主机/计算机组、终端用户/部门单独设置授权和审计策略，以实现细颗粒的管理。管理员分别为终端主机和终端用户授予移动存储设备的访问权限，便于理解和使用。

例如，对涉及信息安全的财务部定制如下策略：

1. 禁止使用未注册的移动存储设备，部门内部已注册的移动存储设备允许正常读写，禁止使用其他部门的移动存储设备。
2. 为了满足财务部与上级部门日常沟通交流，允许财务部内部的某些移动存储设备以只读方式接入上级部门，授权上级部门的某些移动存储设备允许接入财务部以读写方式使用。
3. 财务部数据非常敏感，需要启用写入加密功能防止信息外泄。
4. 对财务部接入的移动存储设备实施 USB 插拔和文件操作审计。

无需专用设备实现安全数据交换

凭借只读功能单向转移数据以及终端用户身份认证，移动存储设备能够实现不同安全等级的网络之间、终端主机之间的安全数据交换功能。

分级权限管理

TSM 提供多级管理模式。管理员为下级管理员授权，下级管理员允许在授权范围内继续为下级管理员授权，依此类推。

不同分组的管理员只能对授权范围内的移动存储设备进行管理，不允许越权使用，也不允许给下级管理员授予更大的权限。

多重保护

TSM 代理提供多重保护功能，防止人为绕过控制和暴力破解，构建信息安全的坚实壁垒。TSM 代理的防护措施请参见表 4-18。

表4-18 TSM 代理的防护措施

防护措施	说明
TSM 代理防卸载	终端用户想要卸载 TSM 代理之前必须输入密码，卸载密码可由管理员在 TSM 服务器设置。
防止 TSM 代理非法终	TSM 代理进程受到保护，终端用户无法终止该进程。即使

防护措施	说明
止的双重保护	该进程被异常终止，所有移动存储设备均不能在该终端主机使用。
TSM 代理文件防暴力破解	终端用户无法通过修改、删除文件或拷入其他终端主机的 TSM 代理文件来绕过权限控制。
VMware 虚拟机保护	终端用户无法通过 VMware 虚拟机来绕过物理机器上的移动存储设备权限控制。
安全模式保护	如果 Microsoft Windows 操作系统在安全模式下运行，TSM 代理自动禁用移动存储设备。

特殊场景控制

TSM 支持离线控制和离线审计两种特殊场景。特殊场景及说明请参见表 4-19。

表4-19 TSM 支持的特殊场景及说明

特殊场景	说明
离线控制	• 终端主机在第一次认证或上线前离线，系统将阻止使用所有的存储设备。 • 终端主机在认证后或上线后离线，系统根据最近一次在线的控制或审计方式授权。
离线审计	对于离线操作，TSM 根据客户端审计方式授权进行自动审计。网络恢复后自动将审计数据上传至 TSM 服务器，将审计日志标记为离线日志。

4.5 软件分发

TSM 提供软件分发功能，将软件手工或按计划自动分发到相应的终端主机上，并支持按部门、按操作系统进行分发。

TSM 软件分发功能提供对多种软件、补丁、文件等分发的支持。

软件分发的主要功能如下：

- 分发软件到终端主机。

  TSM 提供软件分发功能，支持对 exe 或 msi 文件的分发和自动执行。
- 支持软件分发任务的增加、修改、查询、删除。
- 支持软件完整性校验。

  支持软件完整性校验，对文件进行采用，然后计算 MD5。

- 支持软件提示安装和静默安装。

  支持把分发下去的软件自动安装。管理员配置了 exe 或 msi 的执行参数以便实现通过静默方式安装软件。
- 支持按部门、操作类型、终端用户、IP 地址段分发软件。
- 支持断点续传。
- 支持 FTP 传输协议。
- 支持子网快速下载方式分发软件。
- 支持分布式软件分发。

  允许配置多台 FTP 服务器，设置其中一台为主 FTP 服务器，其他的为镜像 FTP 服务器。多台 FTP 服务器之间自动实现同步。
- 支持分级式软件分发。

  管理员在 TSM 管理中心给指定的 TSM 管理器节点下发一个软件，TSM 管理器的管理员收到 TSM 管理中心下发的软件分发任务后，再自行分发给指定的目标（账号、网络区域或部门）。

4.6 补丁管理

TSM 提供补丁管理功能，帮助终端用户解决系统漏洞修复工作，提高企业终端主机的安全水平，降低 IT（Information Technology）系统维护成本。

补丁管理的主要功能如下：

- 支持 Microsoft Windows 操作系统补丁、Microsoft SQL Server 数据库补丁、Microsoft Internet Explorer 补丁、Microsoft Office 补丁。
- 支持自动下载补丁。

  TSM 管理器能够自动从微软网站下载补丁（允许服务器通过代理连接互联网），支持从上级 TSM 管理器同步补丁。
- 支持补丁集的导入、导出。

  支持补丁集的导入、导出功能，实现补丁的备份和恢复。
- 提供补丁信息列表。

  给出从微软同步的补丁信息列表，包括补丁名称、补丁严重程度、补丁是否部署、补丁发布时间。对于某些补丁提供补丁的漏洞描述等信息。
- 补丁部署情况列表。

  对于要求部署的每一个补丁，查看补丁的部署情况，包括发现未部署该补丁的终端主机数和已经部署了该补丁的终端主机数。对于未部署该补丁的终端主机，查看终端主机列表，便于管理员查找未部署补丁的终端主机和实施管理。
- 提供补丁下载历史记录。

  提供补丁下载的历史记录，便于管理员查看以往的补丁下载情况。
- 分布式补丁分发。

  允许配置多台 FTP 服务器，设置其中一台为主 FTP 服务器，其他的为镜像 FTP 服务器。多台 FTP 服务器之间自动实现同步，允许管理员配置同步周期。

4.7 资产管理

TSM 提供资产管理功能，统一管理企业资产，提高效率，降低维护成本，避免员工私自更改企业终端主机的配置，降低资产遗失的风险。

TSM 通过安装在终端主机上的 TSM 代理采集软硬件资产信息，并能跟踪资产信息变化，支持资产信息的自动发现，资产管理还包括对资产基本信息的录入、查询，硬件信息的获取和资产责任人的管理。

资产管理主要功能包括：

- 自动采集资产的信息。

  提供资产的自动采集功能，包括操作系统、软件清单、硬件清单、硬盘序列号和 BIOS 信息。在报修终端主机时，如果需要硬盘序列号和 BIOS 信息，管理员可以从 TSM 管理器查询资产信息时获取，无须到终端主机处查询。通过采集和统计，能够防止员工不实施资产绑定引入的其他问题。
- 维护资产的归属地。

  支持资产和责任人绑定，资产和部门绑定，一个资产只能有一个责任人。支持资产的转移与删除。
- 导入和导出资产信息。

  提供资产的导入和导出功能，生成 Excel 文件。
- 资产的统计和报表。

  生成资产报表，提供资产的统计和变更分析。
- 资产变更上报。

  上报资产变更信息，定时跟踪软、硬件资产变更情况。
- 资产告警。

  当资产发生变更时产生告警，便于管理员持续跟踪资产信息。

5 安全策略

系统安全性

TSM 通过以下机制确保系统的安全性：

- 操作系统安全加固

  提供操作系统安全加固功能，确保安装服务器的操作系统安装最新的补丁，增强操作系统的安全性。
- 密码＋验证码认证机制

  管理员登录必须输入账号、密码和验证码。密码需要满足复杂度要求，连续输入错误的密码账号将会被锁定，防止暴力破解密码。
- 会话过期机制

  管理员登录后如果超过规定时间没有进行操作，管理员将会被强制下线。
- 安全的访问通道控制

  管理员只能通过 HTTPS 方式访问 TSM 管理器；TSM 控制器与 TSM 代理采用 HTTPS 协议通信。

数据安全性

TSM 通过以下机制确保数据的安全性：

- 数据安全策略

  存储数据的磁盘采用 RAID，具有冗余机制，单块磁盘的损坏不会导致数据丢失。
- 数据转储策略

  提供数据转储功能，将操作日志、违规信息等数据保存到指定的转储目录。
- 数据库镜像策略

  提供数据库镜像功能，确保当数据库出现故障时业务处理不会中断、数据不会丢失。

操作安全性

TSM 通过以下机制确保操作维护的安全性：

- 权限控制

实现分权分级的权限控制，管理员登录后根据权限使用相应的功能，并在权限范围内管理用户。

- 系统操作日志

  提供 TSM 管理器和工具的操作日志，以便后续安全审计使用。