IBM® Technical Support Appliance 配置助手指南

V2.7.0.0

2020 年 8 月

目录

简介

IBM Technical Support Appliance (TSA) 是一种易于使用的工具，让您能够从 IBM 支持合同中获得更多价值。TSA 可在 IT 基础架构中发现关键的信息技术元素及其关系，并将这些数据安全传输给 IBM 支持人员进行分析。IBM 支持人员可利用这些数据来深入了解数据中心内服务器与网络组件之间的复杂关系。

本文档旨在提供相应的信息和指导来帮助安装、规划和配置 TSA。

发现前网络注意事项

对 TSA 配置初始发现作业和传输作业之前，请确保已满足以下条件。假定已安装 TSA、可访问 Web 界面且 TSA 已更新至最新级别；否则请参阅《Technical Support Appliance 设置指南》（在本文档的其余部分中简称为《设置指南》）。

TSA 发现前网络注意事项	
网络	
	打开从 TSA 到 IBM 的防火墙访问。请参阅《设置指南》中的“**连接到 IBM 支持人员的配置需求**”部分。
	如果使用 SSL 代理来连接回 IBM，请确保已在 TSA 中配置了该代理。请参阅《设置指南》中的“**设置 IBM Connectivity**”部分。 - 不支持 SSL 检查。如果在代理上使用 SSL 检查，请针对这些流程禁用 SSL 检查。
	如果 TSA 与目标设备之间存在任何防火墙，请确保打开了必需的端口。有关更多信息，请参阅第 33 页上的“防火墙注意事项”部分。

文档

下面的链接会将您直接转至 Technical Support Appliance 信息 Web 站点。您可在此处找到开始使用 IBM Technical Support Appliance 所需的所有内容。您可以访问《设置指南》和安全文档，查看样本报告，以及从 ibm.com 下载 Technical Support Appliance 安装代码。

要了解有关 Technical Support Appliance 的更多信息，请访问：https://ibm.biz/TSAdemo

概述

TSA 可发现有关 IT 基础架构（包括已部署的操作系统组件、固件组件、物理服务器、网络设备、虚拟 LAN 等）的信息。为了优化所收集信息的广度和深度，必须在 TSA 内执行配置任务以识别发现设备。

TSA 将尝试最大程度地降低对客户网络环境的影响。因此，发现过程会使用一种可度量的迭代方式，这可能导致执行完整发现所需的时间多达 72 小时。可以通过查看**摘要**面板的**作业摘要**部分来监视发现作业的状态。

在发现过程中，TSA 最初尝试在不使用凭证的情况下检测已定义作用域内的设备。这包括使用 Nmap，通过低侵入性 IP 扫描、堆栈指纹识别和端口映射来发现设备并进行分类。通常，此活动的重要性不足以触发侵入检测系统 (IDS)，但如果存在严格的本地设置，那么可能会触发 IDS。

为了让 TSA 收集有关 IT 基础架构的信息，请提供以下信息：

- 作用域
- 访问凭证

定义作用域集

作用域集是单独作用域的逻辑分组。作用域使用 IP 地址来告知 TSA 从何处开始发现环境。作用域集由一个或多个作用域组成。有三种类型的作用域条目：

- 子网 - 由 IP 地址和子网掩码定义。子网仅限于 C 类子网。
- IP 范围 - 包括开始地址和结束地址之间的所有 IP 地址。
- IP 地址/主机 - 单个 IP 地址或主机名。

> 主机名是在输入时解析，而不是在发现时解析。请参阅第 5 页上的“创建作用域时需考虑的因素”部分，以获取详细信息。

如果需要，可以通过指定主机、范围或子网定义来为某个作用域定义作用域排除项。生成的 IP 地址将不被视为该作用域的一部分，也不会被扫描。

TSA 支持以下三种类型的作用域集：

1. **常规作用域集**：允许发现单个 IT 网络元素。作用域集包含一个或多个作用域，作用域使用 IP 地址、IP 地址范围或者网络或子网标识这些网络元素的位置。
2. **HMC 动态作用域集**：允许指定一个或多个 IBM POWER Systems HMC 的 IP 地址及其关联的凭证。此外，还可以收集有关 HMC 管理的所有 LPAR 的信息，而无需指出这些 LPAR 的 IP 地址。该动态作用域集可以使用所提供的凭证信息来成功访问这些 LPAR。

3. **VMware 动态作用域集**：允许指定一个或多个 VMware vCenter Server 或 ESXi 实例的 IP 地址及其关联的凭证。此外，还可以收集有关 VMware 管理的所有虚拟机的信息，而无需指出这些虚拟机的 IP 地址。该动态作用域集可以使用所提供的凭证信息来成功访问这些虚拟机。

对于 HMC 和 VMware vCenter Server/ESXi，建议使用动态作用域集。与为单个 LPAR/虚拟机创建和管理发现作用域相比，动态作用域集在 TSA 中所需的配置工作要少得多。另外，对于随时间推移添加和删除 LPAR 或虚拟机的环境，动态作用域集无需修改任何作用域集即可处理此需求。

有关如何在 TSA 上定义发现作用域的详细指示信息，请参阅《设置指南》中的“**设置发现作用域**”部分。

创建作用域时需考虑的因素

虽然尚未定义用于设置作用域的任何标准，但是有一些实际注意事项可帮助节省时间和工作量：

- 在可行的情况下，使用动态作用域集来定义对 HMC 及其管理的 LPAR 或者 VMware vCenter Server/ESXi 及其管理的虚拟机的发现。使用动态作用域集时，无需定义 LPAR 或虚拟机的作用域。
- 使用“IP 范围”或“子网”作用域可发现多个设备，而非使用单个 IP 地址或主机名。这会限制作用域定义的数量并简化管理工作。
- 如果使用子网作用域定义，那么每个作用域集仅包含一个子网作用域定义。确保子网作用域定义解析为 C 类网络（256 个 IP 地址）或更小的网络。
- 使用**“导入常规作用域集”**功能，可以根据指定的名称和输入文本文件中的 IP 地址列表来创建新的作用域集。有关更多信息，请参阅《设置指南》中的**“发现作用域”→“导入常规作用域集”**部分来获取指示信息。
- TSA 目前仅存储 IP 地址。这意味着主机名是在输入时解析，而不是在发现时解析。最佳实践建议您使用“IP 地址”或“IP 范围”（而不是主机名）作为作用域定义。
- 作用域集中的 IP 地址越多，发现所需的时间就越长。为了最大程度地缩短发现所需的时间，请将作用域的目标设置为仅限要发现的元素。

> 使用“常规作用域集”时，将解析作用域集（扩展任何范围或子网作用域定义后）所得到的 IP 地址的累计数量限制为不超过 400。如果为单个作用域集扫描了 400 个以上的 IP 地址，那么在发现过程中可能会遇到性能、服务器或网络问题。

- TSA 不会阻止在多个作用域集中定义 IP 地址。通常应避免这种做法，因为这会增加发现时间而又收集不到任何其他信息。
- 将作用域分组到作用域集（构成设备的逻辑分组）：

- 将相同的设备类型分组到同一个作用域集。例如，为 IBM FlashSystem 存储子系统创建一个作用域集。
- 将同一地理位置的设备分组在一起。
- 根据业务应用程序或服务对设备进行分组。

发现凭证

除少数例外，发现需要某种级别的访问权才能获取全面了解环境所需的详细信息。

通常应在发现设备上创建一些服务帐户，以供 TSA 使用。请参阅下面的部分，以了解每种平台类型所需的特定访问权。为简化这些服务帐户的管理过程，请针对给定产品系列的所有设备使用相同的用户名。

通过使用以下策略之一，可以简化用于维护服务帐户（供 TSA 用于连接到设备）的任务：

- 使用未过期的密码创建服务帐户
- 将 SSH 密钥用于支持使用这些密钥的设备产品系列

有关如何在设备上定义访问凭证的详细指示信息，请参阅《设置指南》中的“**设置发现凭证**”部分。

设置发现凭证时需考虑的因素

设备将尝试按照凭证在访问列表中出现的顺序使用这些凭证。为了加快发现速度，请确保按照最符合您的环境的凭证顺序使用这些凭证。下面是一些注意事项：

- 在适当的情况下将凭证限制于特定作用域集。这会限制不必要的登录尝试并提高发现性能。
- 可使用 SSH 密钥来发现以下设备：
  - AIX
  - Cisco
  - Linux
  - HMC
  - IBM i
  - IVM
  - Sun SPARC (Solaris)
  - SVC/V7000
  - VIOS
  - Fortinet
  - HP-UX
  - IBM FlashSystem
  - F5 Big IP
  - Check Point

一个作用域集只能链接一个 SSH 密钥凭证。

- 最佳实践是创建专供 TSA 使用且具有最低级别的必需权限的单独服务帐户。

入门

本部分介绍了有关配置 TSA 的一些最佳实践和建议。

TSA 的初始设置和配置

按照《设置指南》的以下部分中指定的指示信息进行操作：

- 安装 Technical Support Appliance
- 登录到 Technical Support Appliance
- 接受许可协议
- 使用设置向导设置 Technical Support Appliance

为发现做准备

建议使用迭代过程，最初仅配置网络的一小部分来执行发现操作，然后在每次迭代中添加更多的网络部分，直至覆盖所需的所有网络部分。

> 最佳实践是在对作用域和/或凭证执行重大添加/修改操作后保存 TSA 配置的备份。有关更多信息，请参阅《IBM Technical Support Appliance 设置指南》中的“备份与复原”部分。

发现作业步骤

对于每次发现迭代，请执行以下步骤：

1. 准备设备以执行发现操作。有关任何必需的设备和凭证配置需求，请参阅第 9 页上的“设备发现配置”部分。
2. 对于 HMC 动态作用域集，请执行以下步骤：
   a. 在“**HMC 动态作用域集**”页面中添加 HMC 的 IP 地址。
   b. 在“**HMC 动态作用域集**”页面中添加 HMC 的凭证。
   c. 选择要发现的 LPAR 类型。提供每种类型的凭证。

      > 您可以选择要在创建动态作用域集时发现的 LPAR 类型，也可以通过编辑动态作用域集在后续迭代中添加 LPAR 类型。

   d. （可选）使用“**HMC 动态作用域集**”页面上的“测试”功能，验证是否正确定义了凭证并且可使用这些凭证来建立与 HMC 或其 LPAR 的连接。
3. 对于 VMWare 动态作用域集，请执行以下步骤：
   a. 添加 VMware vCenter Server 的 IP 地址。
   b. 添加不受 VMware vCenter Server 管理的任何 VMware ESXi 主机的 IP 地址。

c. 在“**VMware 动态作用域集**”页面中添加 VMware vCenter Server 和 ESXi 实例的凭证。

d. 选择要发现的虚拟机类型。提供每种类型的凭证。

> 您可以选择要在创建动态作用域集时发现的虚拟机类型，也可以通过编辑动态作用域集在后续迭代中添加虚拟机类型。

e. （可选）使用“**VMware 动态作用域集**”页面上的“测试”功能，验证是否正确定义了凭证并且可使用这些凭证来建立与 VMware vCenter Server 和 ESXi 实例及其虚拟机的连接。

4. 对于常规发现作用域，请执行以下步骤：

   a. 将所需的 IP 地址添加到相应的作用域集/作用域。如果 TSA 实例与发现设备之间存在防火墙，请确保在防火墙中打开了相应端口，以便成功执行发现操作。有关每种平台类型必须访问哪些端口的信息，请参阅第 33 页上的“防火墙注意事项”部分。

   b. 创建必要的凭证。使用“**新建发现凭证**”面板上的“测试”功能，验证是否正确定义了凭证并可使用这些凭证来建立与目标设备的连接。

5. 运行完整发现操作以扫描在此次迭代中添加的 IP 地址。

6. 运行传输操作以将数据上传到 IBM。

设备发现配置

除了提供凭证外，可能还需要满足特定的发现设备配置先决条件，以便 TSA 可以有效地发现和收集有用的组件信息。通过本部分，您可以识别环境中需要特定配置的发现设备。建议您创建具有最低必需权限的服务帐户；另请参阅“防火墙注意事项”部分，以获取端口和协议信息。

- 对于同时打开了 SSH 和 Telnet 端口的设备，出于安全考虑，TSA 将首先尝试使用 SSH 进行连接。如果此 SSH 连接失败，那么 TSA 将尝试使用 Telnet 进行连接。

操作系统和主机

平台
IBM Power Systems • 硬件管理控制台 (HMC) • Integrated Virtualization Manager (IVM) • 虚拟 I/O 服务器 (VIOS) 分区 • AIX • Linux on Power
IBM i
UNIX 系统 • Solaris • Solaris（通过 iLOM） • Linux • HP-UX
VMware vCenter Server 和 VMware ESXi
Windows
ATM 设备

管理模块
• Flex System Manager (FSM) • 机架管理模块 (CMM) • 高级管理模块 (AMM) • HP ProLiant 刀片服务器（通过 HP OnBoard Administrator） • 集成管理模块（IMM 和 IMM2） • HP Integrity 和 HP9000 服务器（通过 iLO）
单击以上每个链接以获取详细信息。

IBM Power Systems

对于通过 HMC 或 IVM 管理 LPAR 配置的 IBM Power Systems，请使用 HMC 动态作用域集。使用 HMC 动态作用域集，您可以为 HMC 创建作用域定义，并提供相关的 HMC 和 LPAR 凭证，但无需为每个受管 LPAR 创建作用域。发现 HMC 时，TSA 会确定该时间点存在哪些 LPAR，并自动扫描每个 LPAR。

对于通常采用静态 LPAR 配置的 IBM Power Systems，HMC 动态作用域集的替代方法是按以下顺序添加实体的作用域和凭证来进行迭代：

1. **HMC 或 IVM 实例**：HMC 将返回有关其管理的所有 Power Systems 及其逻辑分区的高级别信息。IVM 将返回其管理的单个系统的类似信息。
2. **VIOS 分区**：这将返回有关这些分区拥有的物理适配器和资源的信息。
3. **单个分区**：在某些情况下，非 VIOS 分区拥有物理适配器。

硬件管理控制台 (HMC)

要发现 HMC 实例，请完成以下步骤：

准备环境：

- 为了让 TSA 收集有关通过 HMC 管理 LPAR 的信息，HMC 必须能够使用 RMC 工具来与 LPAR 进行通信。确保将 HMC 和 LPAR 配置为允许此通信。有关用于 Linux 的 RMC 工具的更多信息，请参阅 https://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/yum.html
- 要启用安全数据收集，必须在 HMC 上启用远程命令执行。有关信息，请参阅位于以下地址的“启用和禁用 HMC 远程命令”：https://www.ibm.com/support/knowledgecenter/POWER7/p7ha1/enablinganddisablinghmcremotecommands.htm

访问凭证列表：

- 对于 HMC 动态作用域集 - HMC 服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 对于常规发现作用域集 - 计算机系统：HMC 服务帐户的用户名/密码或用户名/SSH 密钥认证。
- HMC 用户必须具有以下角色：
  - 资源角色：AllSystemResources
  - 任务角色（基于可执行命令行任务的 **hmcoperator**）：
    - 受管系统（lshwres、lssyscfg）
    - 逻辑分区（lshwres、lssyscfg、viosvrcmd）
    - HMC 配置 (lshmc)
- 如果有必要，可以使用具有 **hmcviewer** 权限的用户（服务帐户），但这会导致部分数据收集。

> 使用 **hmcviewer** 权限运行时，将无法获取有关 VIOS 分区拥有的适配器的信息。要获取此信息，请确保服务帐户至少具有 **hmcoperator** 权限。否则，请添加作用域和凭证以直接发现 VIOS 分区和 HMC。

Integrated Virtualization Manager (IVM)

要发现 IVM 实例，请完成以下步骤：

访问凭证列表：

- 计算机系统：IVM 服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 服务帐户必须具有“仅查看”权限。

虚拟 I/O 服务器 (VIOS) 分区

要发现 VIOS 实例，请完成以下步骤：

访问凭证列表：

- 对于 HMC 动态作用域集 - VIOS 分区服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 对于常规发现作用域集 - 计算机系统：VIOS 分区服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 服务帐户必须是管理员帐户（例如，**padmin**）。
- 服务帐户必须设置用户属性 **rlogin=true**。您可以使用 SMIT 或通过编辑 **/etc/security/user** 文件来设置此属性。
- **/etc/ssh/sshd_config** 文件中的参数 **PermitUserEnvironment** 必须设置为 **yes**。

AIX

要发现 AIX 实例，请完成以下步骤：

准备环境：

- 确保已安装 bos.perf.tools 和 openSSH/openSSL 程序包。
- 针对服务帐户禁用“无效登录，尝试失败”。

访问凭证列表：

- 对于 HMC 动态作用域集 - AIX 分区服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 对于常规发现作用域集 - 计算机系统：AIX 服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 服务帐户可以是 root 用户帐户或具有 sudo 权限的帐户。
- 服务帐户必须设置用户属性 **rlogin=true**。您可以使用 SMIT 或通过编辑 **/etc/security/user** 文件来设置此属性。
- 要在 AIX 中对非 root 用户服务帐户启用 sudo 权限：
  - 安装 sudo RPM (sudo-1.6.9p15-2noldap) 和 ssh 文件集（AIX 实例上的 openssh.base.server 和 openssh.base.client）。
  - 在目标 AIX 实例上创建可供 TSA 用于访问系统的非 root 用户标识。
  - 在每个 AIX 实例上修改 **/etc/sudoers**，以允许 TSA 使用 sudo 权限运行指定的命令。

```
# 命令别名规范
Cmnd_Alias TSA_CMDS = /usr/bin/lparstat, /usr/sbin/no, /usr/sbin/nfso,
/usr/bin/lslicense, /usr/sbin/vmo, /usr/sbin/ioo, /usr/sbin/lvmo,
/usr/sbin/schedo, /usr/bin/sysdumpdev, /usr/sbin/smtctl, /usr/sbin/emgr,
/usr/bin/sissasraidmgr, /usr/sbin/lswpar, /usr/sbin/cpuextintr_ctl,
/usr/sbin/lsnim, /usr/sbin/raso, /usr/sbin/bosdebug, /usr/sbin/chedition,
/usr/esa/bin/esacli, /usr/sbin/bootinfo, /usr/bin/mpio_get_config, /usr/bin/cat
/etc/objrepos/CuData,
/usr/bin/cat /etc/objrepos/CuData.vc, /usr/bin/cat /var/adm/ras/bootlog,
/usr/bin/cat /etc/lpp/diagnostics/data/diagrpt*.dat, /usr/bin/tapeutil,
/usr/lpp/OV/bin/opcagt, /usr/DynamicLinkManager/bin/dlnkmgr view,
/usr/sbin/powermt version, /usr/sbin/powermt display,
/usr/bin/pcmpath query, /usr/sbin/datapath query

# 用户权限规范
<User Name> ALL = NOPASSWD: TSA_CMDS
```

> <User Name> 是供 TSA 用于收集 AIX 信息的非 root 用户服务帐户。此 <User Name> 是每个 AIX 实例上的用户。每个 AIX 实例上的 **/etc/sudoers** 文件必须按照以上规范进行更新。

或

使用以下用户权限规范作为对 **/etc/sudoers** 上述修改的替代方法：

```
<User Name> ALL = NOPASSWD: ALL
```

> <User Name> 是供 TSA 用于收集 AIX 信息的非 root 用户服务帐户。该用户规范允许服务帐户对任何 AIX 命令使用 sudo 权限。

Linux on Power

要发现 Linux on Power 实例，请完成以下步骤：

准备环境：

- 针对服务帐户禁用“无效登录，尝试失败”

访问凭证列表：

- 对于 HMC 动态作用域集 - Linux 分区服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 对于常规发现作用域集 - 计算机系统：Linux 服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 要在 Linux 中对非 root 用户服务帐户启用 sudo 权限：
  - 在实际目标 Linux 实例上创建可供 TSA 用于访问系统的非 root 用户标识。
  - 在每个 Linux 实例上修改 **/etc/sudoers**，以允许 TSA 使用 sudo 权限运行指定的命令。

    # 命令别名规范
    Cmnd_Alias TSA_CMDS = /usr/sbin/lsvpd, /sbin/lsvpd, /usr/sbin/lscfg, /sbin/lscfg, /usr/sbin/lsmcode, /sbin/lsmcode, /usr/sbin/lvmdiskscan, /sbin/lvmdiskscan, /usr/sbin/dmidecode, /usr/bin/mtlib, /usr/bin/tapeutil, /usr/bin/crontab, /sbin/fdisk, /bin/ls -alR /boot/*, /bin/cat /proc/irq/*, /bin/cat /proc/net/vlan/config, /bin/cat /proc/ppc64/rtas/*, /bin/cat /proc/sys/kernel/cap-bound, /bin/cat /proc/sys/kernel/random/entropy_avail

    # 用户权限规范
    <User Name> ALL = NOPASSWD: TSA_CMDS

    > <User Name> 是供 TSA 用于收集 Linux 信息的非 root 用户服务帐户。此 <User Name> 是每个 Linux 实例上的用户。每个 Linux 实例上的 **/etc/sudoers** 文件必须按照以上规范进行更新。

    或

    使用以下用户权限规范作为对 **/etc/sudoers** 上述修改的替代方法：
    <User Name> ALL = NOPASSWD: ALL

    > <User Name> 是供 TSA 用于收集 Linux 信息的非 root 用户服务帐户。该用户规范允许服务帐户对任何 Linux 命令使用 sudo 权限。

- 如果对 AIX 使用 IBM Proweb 门户网站（这是 IBM 支持产品的一部分），那么建议使用 HMC 动态作用域集来配置 TSA。作为替代方法，您可以配置 TSA 以发现 Power Systems 上的 HMC 和逻辑分区（包括 VIOS）。
- 通过使用 HMC 动态作用域集进行扫描，获取每个 LPAR 的更详细的操作系统配置信息（可通过 ProWeb 进行检索和分析）。

> 有关针对 HMC 环境添加作用域和凭证的信息，请参阅《IBM Technical Support Appliance 设置指南》中的“**HMC 动态作用域**”部分。

- 通过扫描各种 Power Systems 实体来为报告收集的数据级别：
  - 通过仅扫描 HMC，您将获取 Identified、HMC Topology、Power Systems Firmware 、IBM i Recommendations 、Linux Recommendations、HMC/VIOS/AIX 和 Contract 选项卡上的所有基本信息以及部分适配器信息。
  - 通过直接扫描 VIOS 分区，您将获取有关适配器固件和所连接存储设备的其他信息。
  - 通过直接扫描 LPAR，您将获取有关 LPAR 的更多信息，包括特定软件（例如，PowerHA、GPFS 和 PowerSC）的操作系统详细信息和实例。

IBM i

使用 SSH 连接发现 IBM i 实例。如果 IBM i 实例未安装和配置 SSH，请完成以下步骤：

准备环境：

确保为 IBM i 7.2 安装并配置了以下产品/选项：

- IBM Portable Utilities for i，5733-SC1
- Qshell，5770-SS1，选项 30
- Portable App Solutions Environment，5770-SS1，选项 33
- IBM Developer Kit for Java，5770-JV1

确保为 IBM i 7.3 安装并配置了以下产品/选项：

- IBM Portable Utilities for i，5733-SC1
- Qshell，5770-SS1，选项 30
- Portable App Solutions Environment，5770-SS1，选项 33
- IBM Developer Kit for Java，5770-JV1，选项 16
- Java SE 8（32 位）

确保为 IBM i 7.4 安装并配置了以下产品/选项：

- IBM Portable Utilities for i，5733-SC1
- Qshell，5770-SS1，选项 30
- Portable App Solutions Environment，5770-SS1，选项 33
- IBM Developer Kit for Java，5770-JV1，选项 16
- Java SE 8（32 位）

要启动 SSH 守护进程，请执行以下命令：

SBMJOB CMD (CALL PGM (QP2SHELL) PARM('/QOpenSys/usr/sbin/sshd'))

要在 IBM i 上启动 SSHD 服务，请执行以下命令：
STRTCPSVR SERVER(*SSHD)

有关如何在 IBM i 上配置 SSH 的其他信息，请参阅以下红皮书中的第 21-23 章：
http://www.redbooks.ibm.com/redpapers/pdfs/redp4163.pdf

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 虽然需要满足其他对象权限要求才能收集 PTF 信息（使用 **DSPPTF** 命令完成此操作），但是服务帐户可以具有任何用户类（包括 ***USER**）。
- **DSPPTF** 附带了以下对象权限限制：
  - 此命令附带了 ***EXCLUDE** 公共权限
  - **QPGMR**、**QSYSOPR**、**QSRV** 和 **QSRVBAS** 用户概要文件附带了使用此命令的专用权限
  - 与往常一样，**QSECOFR** 用户概要文件或具有 ***SECOFR** 用户类的任何用户概要文件都可以运行此命令
- 对象类型为 ***CMD** 的 **QSYS/DSPPTF** 对象可以编辑其权限，以允许任何其他用户运行此命令。
- 如果为 TSA 创建了新的服务帐户，那么以下建议适用：
  - 使用 ***USER** 用户类创建用户概要文件
  - 使用 **GRTOBJAUT** 命令以允许此用户概要文件运行 **DSPPTF** 命令；对象是对象类型为 ***CMD** 的 **QSYS/DSPPTF**。

UNIX 系统

Solaris

要发现 Solaris 设备，请完成以下步骤：

准备环境：

- 在 Solaris 系统上，确保已安装 SUNWscpu（源代码兼容性）程序包。
- 在一些 Solaris 系统上，必须安装并配置 SNEEP 才能获取序列号。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 服务帐户可以是非 root 用户帐户。

Solaris（通过 Oracle iLOM）

要通过 Oracle iLOM 发现 Solaris 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。

- 服务帐户可具有“**操作员**”或“**管理员**”权限。

Linux

如果 Linux 实例正在 IBM Power System 上运行，请参阅第 13 页上 IBM Power Systems 下的 Linux on Power 部分以获取指示信息。

要发现 Linux on x86 设备，请完成以下步骤：

准备环境：

- 确保已安装 pciutils 程序包。其中包含的 lspci 命令用于收集有关适配器以及与外部存储设备的连接的信息。

访问凭证列表：

- 对于 VMware 动态作用域集 - Linux 虚拟机服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 对于常规发现作用域集 - 计算机系统：Linux 服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 将 /bin/sh 设置为此帐户的 shell。
- 对于 Linux (x86)，服务帐户可以是 root 用户帐户或具有 sudo 权限的帐户。
- 要使用非 root 用户服务帐户进行发现，请将以下内容添加到 Linux 系统上的 **/etc/sudoers** 文件中。

  # 命令别名规范
  Cmnd_Alias TSA_CMDS = /usr/sbin/dmidecode

  # 用户权限规范
  <User Name> ALL = NOPASSWD: TSA_CMDS

  > <User Name> 是供 TSA 用于收集 Linux 信息的非 root 用户服务帐户。此 <User Name> 是每个 Linux 实例上的用户。每个 Linux 实例上的 **/etc/sudoers** 文件必须按照以上规范进行更新。

  或
  使用以下用户权限规范作为对 **/etc/sudoers** 上述修改的替代方法：
  <User Name> ALL = NOPASSWD: ALL

  > <User Name> 是供 TSA 用于收集 Linux 信息的非 root 用户服务帐户。该用户规范允许服务帐户对任何 Linux 命令使用 sudo 权限。

HP-UX

要发现 HP-UX 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码或用户名/SSH 密钥认证。

- 要在 HP-UX 中对非 root 用户服务帐户启用 sudo 权限：
  - 在每个 HP-UX 设备上修改 **/usr/local/etc/sudoers**，以允许 TSA 使用 sudo 权限运行指定的命令。

    # 命令别名规范
    Cmnd_Alias TSA_CMDS =/usr/sbin/diskinfo,/opt/hpvm/bin/hpvmstatus

    # 用户权限规范
    <User Name> ALL=(ALL) NOPASSWD:TSA_CMDS

    <User Name> 是供 TSA 用于收集 HP-UX 信息的非 root 用户服务帐户。

VMware vCenter Server 和 VMware ESXi

对于 VMware 环境，使用 VMware 动态作用域集。使用 VMware 动态作用域集，您可以为 VMware vCenter Server/ESXi 创建作用域定义，并提供相关的 VMware 和虚拟机凭证，但无需为每个受管虚拟机创建作用域。发现 VMware vCenter Server/ESXi 时，TSA 会确定该时间点存在哪些虚拟机，并自动扫描每个虚拟机。

对于通常采用静态虚拟机配置的 VMware 环境，VMware 动态作用域集的替代方法是按以下顺序添加实体的作用域和凭证来进行迭代：

1. **vCenter Server 实例**：这将返回有关其管理的 ESXi 主机及其虚拟机访客的高级别信息。
2. **ESXi 主机**：添加不受 vCenter Server 管理的 ESXi 主机。
3. **单个虚拟机访客**：这允许收集有关操作系统的更多详细信息。

在针对 VMware 环境配置 TSA 时，建议执行以下操作：

1. 配置 TSA 以发现 VMware vCenter Server（如果可用）。发现 VMware vCenter Server 会自动使 TSA 收集 vCenter Server 所管理的所有 VMware ESXi 主机的相关信息。但不需要这些 ESXi 主机的配置信息。
2. 配置 TSA 以仅在 ESXi 主机不受 VMware vCenter Server 管理时发现 VMware ESXi 主机。
3. 在 ESXi 主机托管的每个虚拟机上安装 VMware Tools。如果未安装 VMware Tools，那么将无法访问某些库存数据，例如，IP 地址或已安装的操作系统。
4. 配置每个 VMware ESXi 主机以使 CIM 接口处于活动状态。CIM 接口允许 TSA 收集有关 ESXi 主机中适配器的详细信息。有关 CIM 提供程序的更多信息，请参阅 第 44 页上的“附录 C”。

要发现 vCenter Server 实例以及有关其管理的 ESXi 服务器的信息，请完成以下步骤：

准备环境

- 在 ESXi 主机托管的每个虚拟机上安装 VMware Tools。
- 配置每个 VMware ESXi 主机以使 CIM 接口处于活动状态。
- 必须能够从 TSA 访问 CIM 端口 (5989)（防火墙已解除阻止等），以便执行完全发现。

访问凭证列表：

- 对于 VMware 动态作用域集 - VMware vCenter Server 服务帐户的用户名/密码。
- 对于常规发现作用域集 - 计算机系统：VMware vCenter Server 服务帐户的用户名/密码。
- 服务帐户必须具有“**管理员**”角色权限，或者具有拥有以下附加权限的自定义只读角色的最低权限：
  - 全局 → 许可证
  - 全局 → 设置
  - 主机→ CIM
  - 主机 → 配置 → 变更设置
  - 主机→ CIM→ CIM 交互

要直接发现 ESXi 设备，请完成以下步骤：

准备环境

- 在 ESXi 主机托管的每个虚拟机上安装 VMware Tools。
- 配置每个 VMware ESXi 主机以使 CIM 接口处于活动状态。

访问凭证列表：

- 对于 VMware 动态作用域集 - VMware ESXi 服务帐户的用户名/密码。
- 对于常规发现作用域集 - 计算机系统：VMware ESXi 服务帐户的用户名/密码。
- 服务帐户必须具有“**管理员**”角色权限。

Windows

TSA 支持通过以下方法来发现 Windows 实例：

- WINRM
- SMB1

首选使用“Windows（通过 WINRM）”，因为这是一种更安全的接口。

Windows（通过 WINRM）

要通过 WINRM 发现 Windows 设备，请完成以下步骤：

准备环境：

准备环境的最常用方法是使用由目标 Windows 服务器上安装的认证中心生成的服务器证书。该证书必须满足以下条件：

- 来自认证中心的根证书和中级证书属于“受信任的根证书颁发机构”证书。
- 服务器证书安装在“个人”证书部分。
- 服务器证书必须显示其已发放给服务器的标准主机名。
- 服务器证书必须包含此服务器的私钥。

以下命令将配置 WINRM 以建立远程 HTTPS 连接：
winrm quickconfig -transport:https

此命令将执行以下操作：

- 启动 WINRM（如果当前未处于活动状态）
- 修改 WINRM 服务，以便 WINRM 在系统重新启动时自动启动
- 配置 WINRM HTTPS 侦听器
- 修改 Windows 防火墙规则以便允许远程 HTTPS 连接

此命令将生成以下输出。输入 **y** 以确认这些更改。

```
WinRM 服务已在此机器上运行。
WinRM 未设置为允许远程访问此机器以进行管理。
必须进行以下更改：

在 HTTPS://* 上创建 WinRM 侦听器，以接受对此机器上任何 IP 的 WS-Man 请求。
配置要用于 CredSSP 认证的服务的 CertificateThumbprint 设置。
配置 LocalAccountTokenFilterPolicy 以向本地用户远程授予管理权限。

执行这些更改 [y/n]？ y

已针对远程管理更新了 WinRM。

已在 HTTPS://* 上创建了 WinRM 侦听器，以接受对此机器上任何 IP 的 WS-Man 请求。
已配置该服务的必需设置。
已配置 LocalAccountTokenFilterPolicy 以向本地用户远程授予管理权限。
```

最后，为了能够通过 HTTPS 进行用户标识/密码认证，请运行以下命令：
winrm set winrm/config/service/auth @{Basic="true"}

替代方法是使用自签名证书。有关此配置的指示信息，请参阅第 44 页上的“附录 D：使用 WINRM 的 Windows”。

访问凭证列表：

- 对于 VMware 动态作用域集：服务帐户的用户名/密码。
- 对于常规发现作用域集：计算机系统 (Windows)：服务帐户的用户名/密码。
- 服务帐户必须是以下某个组的成员：
  - Administrators
  - WinRMRemoteWMIUsers__

要向 WinRMRemoteWMIUsers__ 组添加用户，请使用以下命令：
net localgroup WinRMRemoteWMIUsers__ [user_id] /add

Windows（通过 SMB1）

要发现 Windows 设备，请完成以下步骤：

准备环境：

- 确保在目标设备上启用了 Windows Scripting Host (WSH) 或 Windows Management Instrumentation (WMI) 服务以及 VBScript。
- 确保端口 445 未被防火墙或 IP 安全策略阻止，因为 TSA 需要基于 TCP/IP 的服务器消息块 (SMBv1) 协议。
- 要应用安全策略，请转至**开始 → 控制面板 → 管理工具**，然后根据您的策略是存储在本地还是存储在 Active Directory 中来选择以下导航：
  - 存储在本地的策略：**管理工具 → 本地安全策略 → 本地计算机上的 IP 安全策略**
  - 存储在 Active Directory 中的策略：**管理工具 → 缺省域安全设置 → Active Directory 上的 IP 安全策略，或者管理工具 → 缺省域控制器安全设置 → Active Directory 上的 IP 安全策略**
- TSA 需要访问隐藏的远程管理磁盘共享，才能访问系统 %TEMP% 和其他目录。TSA 还需要访问进程间通信共享 (IPC$)，才能访问远程注册表。确保启动了进程间通信共享服务器服务。要启动该服务器服务，请转至**控制面板 → 管理工具 → 服务 → 服务器**。
- 确保远程注册表服务处于活动状态。这是 TSA 与 Windows 设备建立会话的前提条件。

访问凭证列表：

Windows 2012 R2 及更高版本：

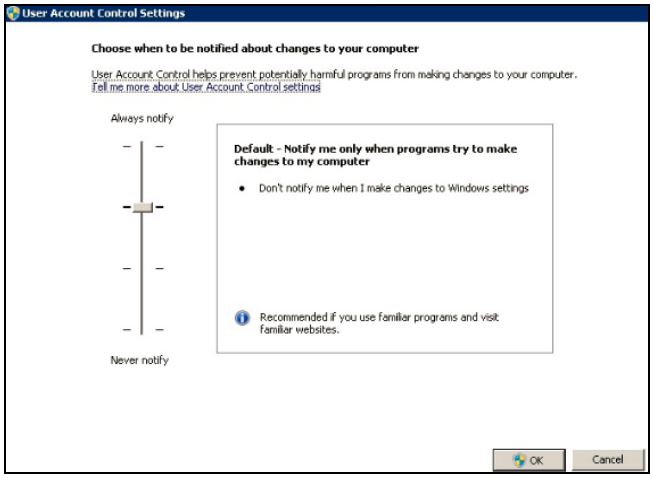
- 对于 VMware 动态作用域集 - 基本管理员帐户/密码。无论用户帐户控制 (UAC) 设置如何，都可以使用此帐户。
- 对于常规发现作用域集 - 计算机系统 (Windows)：基本管理员帐户/密码。无论用户帐户控制 (UAC) 设置如何，都可以使用此帐户。

- 如果满足某些条件，那么可以使用基本管理员帐户以外的其他帐户。该帐户必须是本地或域管理员帐户，并且用户帐户控制（UAC）设置必须满足某些要求。有关受支持的帐户类型和 UAC 设置的组合，请参考下表。有关 UAC 的其他详细信息，请参考 Microsoft Windows 文档。

	用户帐户控制设置			
	始终通知	**仅在程序尝试对计算机进行更改时通知我（缺省设置）**	**仅在程序尝试对计算机进行更改时通知我（请勿让桌面灰显）**	**从不通知**
基本管理员	**是**	**是**	**是**	**是**
域管理员组中的用户	**否**	**是**	**是**	**是**
本地管理员组中的用户	**否**	**是**	**是**	**是**
非管理员帐户（域或本地）	**否**	**否**	**否**	**否**

- 要访问 UAC 设置，请单击**开始**，然后单击**控制面板**。在搜索框中输入 **uac**，然后单击**更改用户帐户控制设置**。

以下是缺省设置：



ATM 设备

可以发现某些型号的 ATM 设备。要发现 ATM 设备（包括有关其组件的基本信息），请完成以下步骤：

准备环境：

- Wincor Nixdorf 型号 - 按照有关 Windows（通过 SMB） 的指示信息进行操作。

管理模块

对于 IBM Flex Systems，最好是按以下顺序添加实体的作用域和凭证来进行迭代：

1. **Flex System Manager (FSM)：**这将返回有关 Flex System Manager、其管理的机架以及相关计算节点的高级别信息。

   > 如果不存在 FSM，那么建议扫描 Flex 系统上的 CMM 和任何由 HMC 管理的 POWER 计算节点。

2. **机架管理模块 (CMM)：**对于不受 FSM 管理的机架，请转至每个 CMM 以检索有关每个机架及其相关节点的高级别信息。
3. **计算节点：**这将返回有关操作系统的详细信息。

Flex System Manager (FSM) 设备

要发现 FSM 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有 **SMAdmin** 权限。

机架管理模块 (CMM) 设备

要发现 CMM 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须至少具有“**操作员**”权限。

高级管理模块 (AMM) 设备

要发现 AMM 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须至少具有“**操作员**”权限。

HP Proliant 刀片服务器（通过 HP OnBoard Administrator）

对于 Hewlett Packard (HP) ProLiant 服务器，最好是为 HP OnBoard Administrator (HP OBA) 实体添加作用域和凭证。HP OBA 将返回有关 HP OnBoard Administrator、其管理的机柜以及机柜中包含的计算节点的高级别信息。

要通过 HP OnBoard Administrator (OBA) 发现 HP Proliant 刀片服务器，请完成以下步骤：

准备环境：

- HP OBA 必须处于活动模式。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有 HP Onboard Administrator 的“**OA 管理员**”、“**OA 操作员**”或“**OA 用户**”**权限**。建议使用“**OA 用户权限**”角色。

TSA 仅从处于活动状态的 HP OnBoard Administrator 中收集信息。它不会从处于待机状态的 HP OnBoard Administrator 中收集任何信息。

集成管理模块 (IMM) 和集成管理模块 II (IMM2) 设备

要发现 IMM 和 IMM2 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户可以具有任何有效权限。

HP Integrity 和 HP9000 服务器（通过 iLO）

iLO 是 HP Integrity 和 HP9000 服务器中的独立处理器卡，用于提供有关服务器的基本硬件信息。插入该服务器后，即使该服务器本身尚未打开电源，iLO 也会立即进入活动状态。

要通过 HP Integrity 和 HP9000 服务器的 iLO 来发现摘要级别的库存信息，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户可以使用任何有效的权限级别。建议使用“**用户**”权限。

网络设备

本部分提供了有关以下类型的网络设备的详细信息：

平台
BNT 交换机
Brocade 交换机
Check Point
Cisco 交换机
F5 Big-IP (TMOS)
Fortinet (FortiOS)
IBM B 型存储区域网络 (SAN) 交换机
Juniper 交换机
Palo Alto Networks (PAN-OS)
QLogic 交换机
单击以上每个链接以获取详细信息。

BNT 交换机

要发现 BNT 交换机，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有“**管理员**”权限。

Brocade

要发现 Brocade 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 禁用虚拟 Fabric 模式：服务帐户可以使用任何有效权限。建议使用“**用户**”权限。
- 启用虚拟 Fabric 模式：服务帐户需要 Fabric OS 的“**管理员**”权限。

Check Point

要发现 Check Point 系统，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码或用户名/SSH 密钥认证。

- 服务帐户必须具有“管理员”权限 (**adminRole**)。
- 服务帐户必须具有 SSH 访问权才能运行 CLI 命令。

Cisco

要发现 Cisco 设备，您可以使用以下计算机系统凭证或 SNMP 凭证：

访问凭证列表：

- 计算机系统或其他（Cisco 设备）或其他 (Cisco Works)：服务帐户的用户名/密码或用户名/SSH 密钥。
- 服务帐户需要“**网络管理员**”角色权限。
- SNMP：输入共用名字符串（针对 SNMPv1 和 SNMPv2）。
- SNMP (SNMPv3)：
  - 输入：
    - 用户名
    - 密码
    - 专有密码（可选）
  - 选择认证协议：无、MD5、SHA

> 请务必为 TSA 提供一个共用名字符串，此字符串具有作用域网络中所有设备的只读访问权。

F5 Big-IP (TMOS)

要发现运行 TMOS 的 F5 Big-IP 系统，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 服务帐户必须具有 F5 的“管理员”权限。
- 服务帐户必须具有 SSH 访问权才能运行 TMSH CLI 命令。

Fortinet (FortiOS)

要发现运行 FortiOS 的 Fortinet 设备，请完成以下步骤：

准备环境

- 确保将系统控制台配置为显示完整命令输出：

```
config system console
set output standard
end
```

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 服务帐户必须至少具有只读权限。

IBM B 型存储区域网络 (SAN) 交换机

要发现 IBM B 型 SAN 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 禁用虚拟 Fabric 模式：服务帐户可以使用任何有效权限。建议使用“**用户**”权限。
- 启用虚拟 Fabric 模式：服务帐户需要 Fabric OS 的“**管理员**”权限。

Juniper

要发现 Juniper 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码
- 服务帐户必须具有“管理员”权限。

> **注**：必须在设备上安装 Junos® V12.1 或更高版本，才能发现内存大小信息。

Palo Alto Networks (PAN-OS)

要发现运行 PAN-OS 的 Palo Alto Networks 系统，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有“超级用户”或“超级用户（只读）”权限
- 服务帐户必须具有 REST API 访问权（端口 443）。

QLogic 交换机

要发现 QLogic 交换机，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有“管理员”权限。

存储设备

本部分提供了有关以下类型的存储设备和磁带设备的详细信息：

平台
EMC Corporation Storage
HP StorageWorks P2000 Modular Smart Array
IBM DS3xxx、DS4xxx 或 DS5xxx
IBM DS6xxx 或 DS8xxx
IBM FlashSystem V9000

平台
IBM ProtecTier
IBM SVC 或 V7000/V3700
IBM TS3100 磁带库
IBM TS3200 磁带库
IBM TS3310 磁带库
IBM TS3494 或 TS3953 磁带库
IBM TS3500 或 TS3584 磁带库
IBM TS4500 磁带库
IBM TS7700 磁带库
IBM V7000 Unified
IBM XIV
nSeries 或 NetApp

单击以上每个链接以获取详细信息。

EMC Corporation Storage

EMC CLARiiON/VNX/VMAX

要发现 EMC CLARiiON/VNX/VMAX 设备，请完成以下步骤：

准备环境：

- 确保在 Windows 或 Linux 系统上安装了 EMC SMI-S Provider 产品的实例。缺省情况下，TSA 会遵循 EMC SMI-S 建议，使用 SLP 发现提供程序的位置。如果您的网络安全策略阻止了 SLP 网络流量，那么可以将 TSA 配置为在不使用 SLP 的情况下直接访问 EMC SMI-S Provider。
- 如果您的网络安全策略不允许 SLP 网络流量，请使用“**发现设置 → 连接设置**”页面，以提供有关 EMC SMI-S Provider 侦听查询请求时所用的端口的信息。
- 确保 SMI-S Provider 正在使用的 IP 地址中至少有一个 IP 地址是在作用域集中定义的。TSA 将连接到 SMI-S Provider，以检索有关其管理的 EMC 设

备的信息。无需将单个 EMC 设备的 IP 地址放在作用域集中。TSA 将尝试使用 HTTPS（如果可用）来连接到 SMI-S Provider，否则将使用 HTTP 进行连接。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户可以使用任何有效角色。建议使用“**监控者**”角色。

只需在 TSA 中输入 SMI-S Provider 的凭证。无需输入 EMC 设备的凭证。

EMC Data Domain

要发现 EMC Data Domain 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户可以具有最低必需权限。

HP StorageWorks P2000 Modular Smart Array

要发现 HP Storage 系统，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户可以具有最低必需权限。

IBM DS3xxx、DS4xxx 或 DS5xxx 存储设备

要发现 IBM DS3xxx、DS4xxx 或 DS5xxx 设备，请完成以下步骤：

准备环境：

- 确保存储管理器允许使用远程 **smcli** 命令。

访问凭证列表：

- 对于不受保护的存储设备，不需要任何凭证。
- 对于受保护的存储设备，请完成以下步骤：
  - 计算机系统：服务帐户的用户名/密码。
  - 服务帐户可以具有“**管理员**”或“**监控者**”角色。建议使用“**监控者**”角色。

IBM DS6xxx/DS8xxx 存储设备

要发现 IBM DS6xxx/DS8xxx 设备，请完成以下步骤：

准备环境：

- 确保存储管理器允许使用远程 **dscli** 命令。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。

- 服务帐户必须具有“**监控者**”角色。

IBM FlashSystem V9000

要发现 IBM FlashSystems，请完成以下步骤：

准备环境：

- 对于旧型号，MCP（管理控制端口）必须处于活动状态才能成功发现系统。
  - 要检查系统是否处于活动状态，请运行以下命令：system status。
  - 在这两个 IP 地址中，如果有一个 IP 发生故障，那么系统将进入被动状态。要使其他以太网端口变为活动状态，请运行以下命令：sync activate。
  - 已发现的系统必须是管理 IP 地址和/或配置节点。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码或用户名/SSH 密钥认证。
- 服务帐户可以使用任何有效角色。建议使用“**监控者**”角色。

IBM ProtecTIER

要发现 ProtecTIER 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有“管理员”权限。

IBM SVC 或 V7000/V3700 存储设备

要发现 SVC 和 V7000/V3700 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：用于认证的用户名/密码或用户名/SSH 密钥。
- 服务帐户可以使用任何有效角色。建议使用“**监控者**”角色。

IBM TS3100 磁带库

要发现 TS3100 磁带库设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有“管理员”权限。

IBM TS3200 磁带库

要发现 TS3200 磁带库设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有“管理员”权限。

IBM TS3310 磁带库

要发现 TS3310 磁带库设备，请完成以下步骤：

准备环境：

- 始终在安全模式下配置 Web 服务。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有“管理员”权限。

IBM TS3494 或 TS3953 磁带库

要发现 TS3494 或 TS3953 磁带库设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户可以具有最低必需权限。

IBM TS3500 或 TS3584 磁带库

必须满足以下先决条件：

- TS3500 磁带库的固件级别必须为 8xxx（或更高）。
- 必须已安装并启用 Advanced Library Management System (ALMS)。

支持 SSL 连接和非 SSL 连接。

要发现 TS35xx 磁带库设备，请完成以下步骤：

准备环境：

- 可将 TS3500 Web 界面配置为“**无密码保护**”或“**密码保护**”
  - 如果激活了“**密码保护**”，请按下面的“**访问凭证列表**”中所述来创建凭证。
  - 如果禁用了“**密码保护**”，那么不需要任何凭证。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有“管理员”权限。

IBM TS4500 磁带库

必须满足以下先决条件：

- TS4500 磁带库的固件级别必须为 1.4.1.2 或更高级别（最高级别为 1.7.0.0）。
- 必须已安装并启用 Advanced Library Management System (ALMS)。

支持 SSL 连接和非 SSL 连接。

要发现 TS4500 磁带库设备，请完成以下步骤：

准备环境：

- 可将 TS4500 Web 界面配置为仅限“**密码保护**”。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须映射到“**服务**”角色。

IBM TS7700 磁带库

要发现 TS7700 磁带库设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户只需“**只读**”权限。

IBM V7000 Unified 存储设备

要发现 V7000 Unified 设备，请完成以下步骤：

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户可以使用任何有效角色。建议使用“**监控者**”角色。

IBM XIV 存储设备

要发现 XIV 设备，请完成以下步骤：

准备环境：

- 确保存储管理器允许使用远程 **xcli** 命令。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户必须具有“**只读**”用户角色。
- 请注意，XIV 系统可能针对生成警报前的无效登录尝试次数设置了较低的阈值。如果使用大型凭证集，那么可能会超出此限制，并导致报告不必要的问题。请尝试将 XIV 设备分组在一个作用域集中，并将其服务帐户凭证限制在该作用域集内。

nSeries 或 NetApp 存储设备

要发现 nSeries 或 NetApp 设备，请完成以下步骤：

准备环境：

- 使用 Data ONTAP CLI、RLM CLI 和 SP CLI 配置的系统均支持数据收集。但是不支持 BMC CLI。
- 必须开启 **telnet.distinct.enable** 选项。

访问凭证列表：

- 计算机系统：服务帐户的用户名/密码。
- 服务帐户可以具有最低必需权限。

防火墙注意事项

设备与发现设备之间的防火墙可能会阻止进行成功的完全发现。

在必须穿过防火墙的情况下，可能需要在防火墙中打开某些端口，具体取决于用户要发现的设备类型。通常应打开端口 22 (SSH) 和 161 (SNMP)，然后根据受支持的设备来打开下表中的相应端口。

发现端点	**端口**	**接口/协议**
多个	161	SNMP
存储设备		
DS6000/DS8000	1750 (HTTP) 或 1751 (HTTPS)	DSCLI
DS3000/DS4000/DS5000	2463	SMCLI
XIV	7778	XCLI
nSeries 或 NetApp	22/23	SSH 或 Telnet
SVC 或 V7000/V3700	22	SSH
V7000 Unified	22	SSH
IBM TS3500	443/80	HTTPS 或 HTTP
IBM TS4500	443/80	HTTPS 或 HTTP
IBM TS7700	443/80	HTTPS 或 HTTP
IBM TS3100/TS3200/TS3310	80	HTTP
IBM TS3494 或 TS3953	23	Telnet
IBM ProtecTier	22	SSH
HP Storage	22/23	SSH 或 Telnet
IBM Flash System V9000	22	SSH

发现端点	端口	接口/协议
EMC Corporation Storage - CLARiion/VNX/VMAX	427 -（缺省值）在允许 SLP 发现时使用；如果禁用了 SLP 发现，那么将不使用此端口。 由 EMC SMI-S Provider 配置的 HTTPS/HTTP 端口；缺省值为 5989/5988	SLP 或 HTTPS/HTTP
	您可以启用或禁用 SLP 发现选项（用于通过 EMC SMI-S Provider 发现 EMC 存储设备）。	
EMC Corporation Storage – EMC Data Domain	22	SSH*
操作系统和主机		
FSM	22/23	SSH 或 Telnet
CMM	22/23	SSH 或 Telnet
AMM	22/23	SSH 或 Telnet
HP Proliant 刀片服务器（通过 HP OnBoard Administrator）	22/23	SSH 或 Telnet
IMM 和 IMM2	22/23	SSH 或 Telnet
HP Integrity/HP 9000 服务器的 HP iLO	22/23	SSH* 或 Telnet
网络设备		
Brocade	161/22 /23	SNMP 、 SSH 或 Telnet
IBM B 型存储区域网络 (SAN) 交换机	22 /23	SSH 或 Telnet

发现端点	端口	接口/协议
Cisco	161/22/23	SNMP、SSH 或 Telnet
BNT	22/23	SSH 或 Telnet
Juniper	22/23	SSH 或 Telnet
QLogic	22/23	SSH* 或 Telnet
Fortinet (FortiOS)	22/23	SSH 或 Telnet
Palo Alto Networks (PAN-OS)	443	HTTPS
F5 Big-IP (TMOS)	22/23	SSH 或 Telnet
Check Point	22/23	SSH 或 Telnet
操作系统/服务器平台		
HMC	22	SSH
VIOS	22	SSH
AIX	22	SSH
Linux	22	SSH
Windows	445	SMBv1
VMware vCenter	443	HTTPS
VMware ESXi	443 或 5989	HTTPS
IVM	22/23	SSH 或 Telnet
IBM i	22	SSH
SUN	22	SSH

- 对于由 SSH 标记的设备，TSA 仅支持 SSH v1*。

发现作业问题

大多数发现作业问题是由于访问或权限问题引起的。

最常见的访问问题是由于防火墙阻止访问设备上的必要端口引起的。需要打开且可访问的端口因设备类型而异。请参阅第 33 页上的“防火墙注意事项”部分来确定哪些端口适用。

最常见的权限问题包括：

- **未定义凭证**。确保在 TSA 中定义了设备的凭证，并在设备上创建了相应的服务帐户。
- **凭证的用户名或密码不正确**。在创建或编辑凭证时，可使用“**测试**”功能来验证凭证是否有效。
- **凭证的密码已到期**。
- **凭证缺少设备的必需权限**。要确定目标设备的凭证要求，请参阅第 9 页上的“设备发现配置”部分。
- **使用有效凭证类型**。对于 Windows 设备，请创建“计算机系统 (Windows)”凭证，而不是“计算机系统”凭证。

检查**“认证状态”**页面（**工具 → 认证状态**），以查看是否有任何服务帐户凭证的密码已过期或失效。

后续注意事项

在 TSA 中定义所需的网络部分并成功进行扫描后，可以让 TSA 按照期望的计划安排来运行定期发现和传输。

下面是一些期望的后续活动：

- 定期与您的 IBM 代表一起复查 TSA 生成的报告。
- 定期通过 TSA 用户界面执行备份，以保存 TSA 配置的副本。

此操作不会保存 TSA 收集的数据。它仅保存配置信息。

- 定期检查**“认证状态”**页面（**工具 → 认证状态**），以查看是否有任何服务帐户凭证的密码已过期或失效。
- 更新设备上服务帐户的密码时，请务必在 TSA 中也更新这些密码，以便使 TSA 中的凭证定义与目标设备上的凭证保持同步。
- 如果您的安全策略允许这样做，请考虑使用未过期的密码来设置服务帐户或者使用 SSH 密钥。这样就无需在 TSA 用户界面中和在设备上定期更新密码。

故障诊断

用于 AMM 发现的活动会话

AMM 设备有一项设置可限制并发活动会话的数量（最多 20 个）。如果此设置的值不足以允许 TSA 创建会话，那么将无法发现 AMM 设备。

要更改 AMM 设备的活动会话数限制，请执行以下步骤：

1. 通过在 Web 浏览器中输入 AMM 设备的 IP 地址来登录到 AMM Web 界面。
2. 转至 **MM 控制 → 登录概要信息**。
3. 单击供 TSA 用于发现设备的登录标识。
4. 增加**最大并发活动会话数**设置值。
5. 单击页面右下方的**保存**。

附录 A：术语和定义

假定读者已深入了解了因特网协议 (IP) 网络和协议。

术语	定义
发现设备	这指的是可被 TSA 发现的已部署的 IT 基础架构组件。典型设备包括：服务器、计算机系统（例如，IBM、Dell 和 HP）、存储元素和网络元素（例如，交换机、网桥、路由器）。

附录 B：杂项

用户界面下载功能

在某些情况下，使用 Web 浏览器时，无法成功完成“下载所有日志”操作（来自**活动日志**页面）、“下载文件”操作（来自**发现历史记录**页面）或“下载文档”操作（来自**文档**页面）。要解决此问题，请尝试按《IBM Technical Support Appliance 设置指南》中所述来切换到其他受支持的 Web 浏览器。如果没有这样的选项，请尝试将浏览器的属性重置为缺省设置。

附录 C：针对 VMware ESXi 的 CIM 提供程序

CIM 提供程序是一组 VMware ESXi 插件，可用于收集有关运行 VMware ESXi 的服务器的其他硬件和固件信息。TSA 和 VMware vCenter 都可以从这些附加信息中获益。

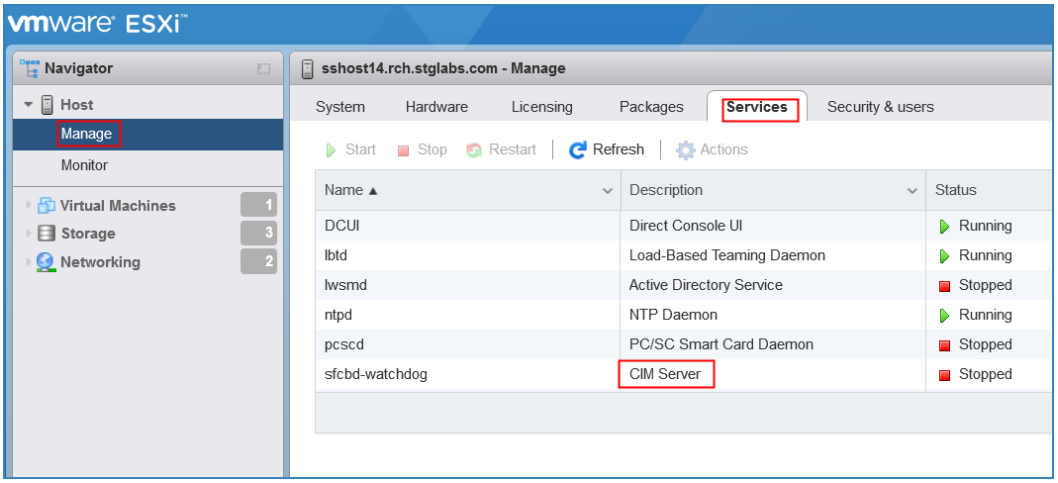
CIM 提供程序插件是由服务器和组件制造商开发的。为确保 ESXi 中包含 CIM 提供程序插件，请使用包含 CIM 提供程序插件的自定义安装映像。对于未安装 CIM 提供程序的现有 VMware ESXi 实例，请从服务器和组件制造商处获取必要的插件，然后将这些插件安装到 ESXi 中。VMware 提供了制造商所提供的各种插件的列表。

有关更多信息，请参阅 https://www.vmware.com/resources/compatibility/pdf/vi_cim_guide.pdf。

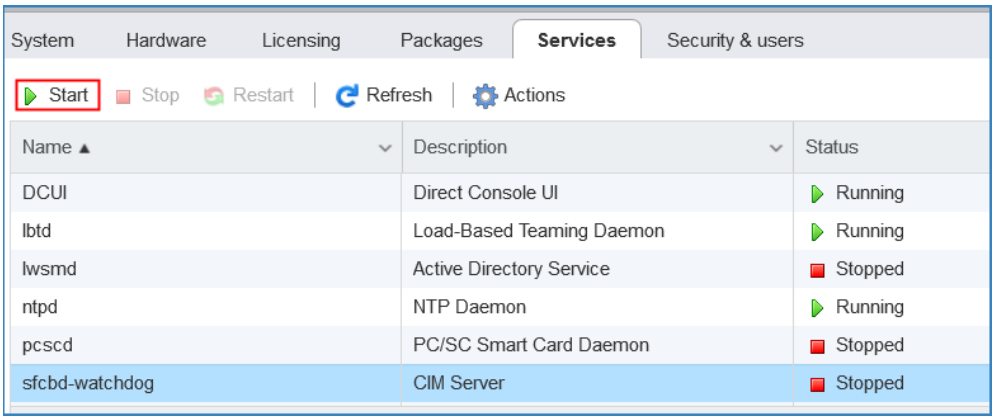
要确定 CIM 提供程序是否处于活动状态并在 CIM 提供程序处于不活动状态时将其开启，请执行以下步骤。

在 VMware vSphere Web Client 上

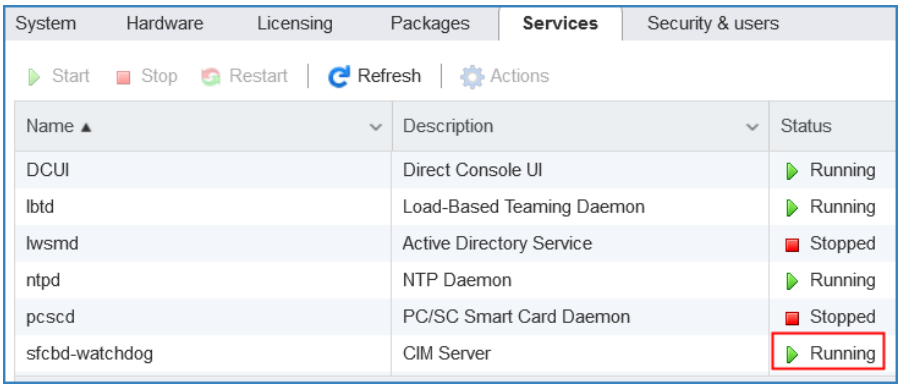
- 登录到 VMware vSphere Web Client。
- 在左侧导航窗口中单击**主机 → 管理**，并在右侧窗格中选择**服务**选项卡。
- 这样会显示包括 **CIM Server** 在内的一组服务。



- 如果 **CIM Server** 处于**停止**状态，请将其选中并单击“**启动**”。

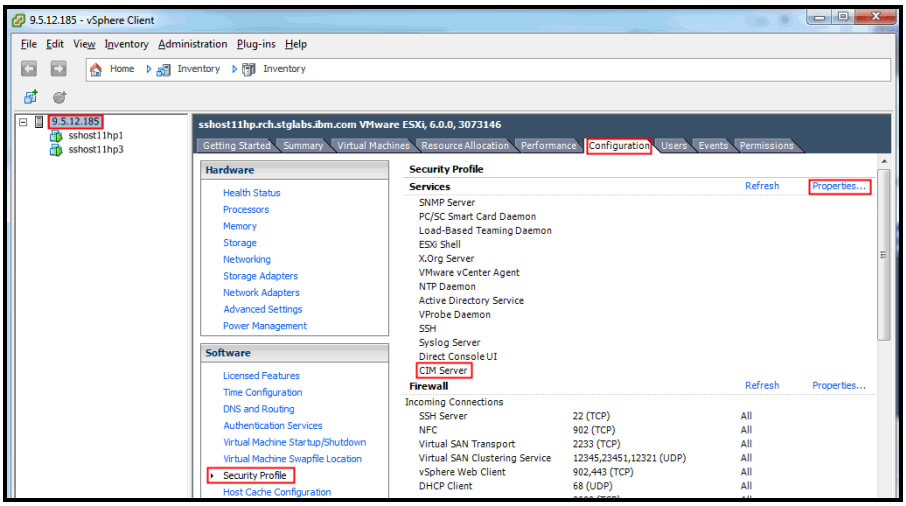


- CIM Server 服务将启动并处于“**正在运行**”状态。

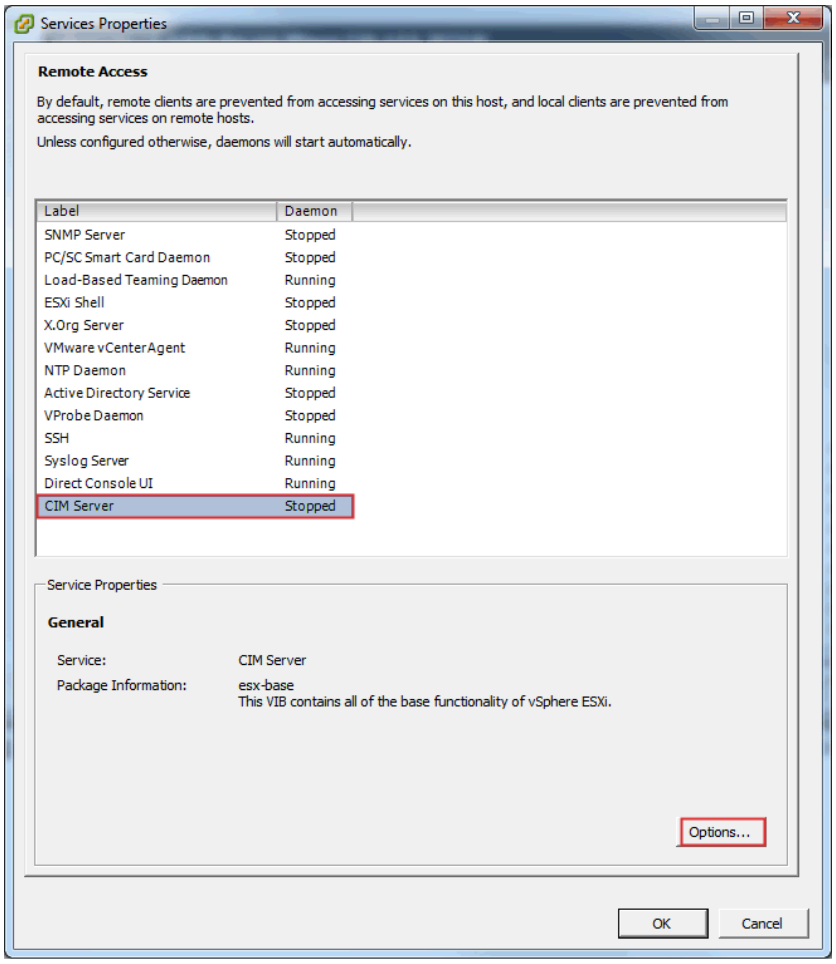


在 VMware vSphere Client 上

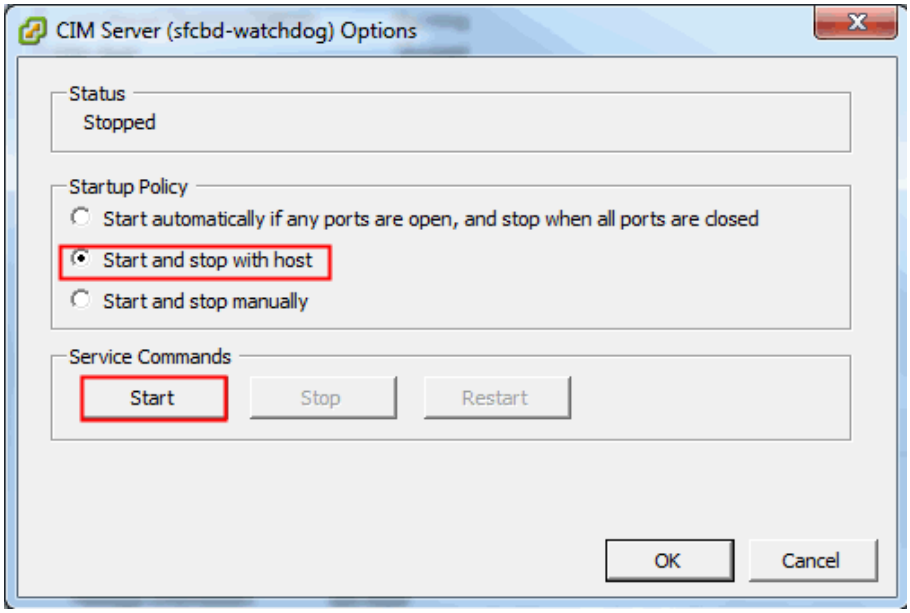
- 启动 VMware vSphere Client。
- 在左侧导航窗口中单击 ESXi 服务器 IP，并在右侧窗格中选择**配置**选项卡。
- 从右侧窗格的**软件**选择菜单中选择**安全概要文件**。这样会在**服务**部分中显示包括 **CIM Server** 在内的一组服务。



- 在“服务”部分中选择**“属性...”**项。



- 如果 **CIM Server** 处于**停止**状态，请将其选中，并单击**“选项...”**。这样会显示以下对话框窗口。



- 选择**“启动策略”（通过主机**选项启动和停止），然后单击**“启动”**以激活 CIM Server。

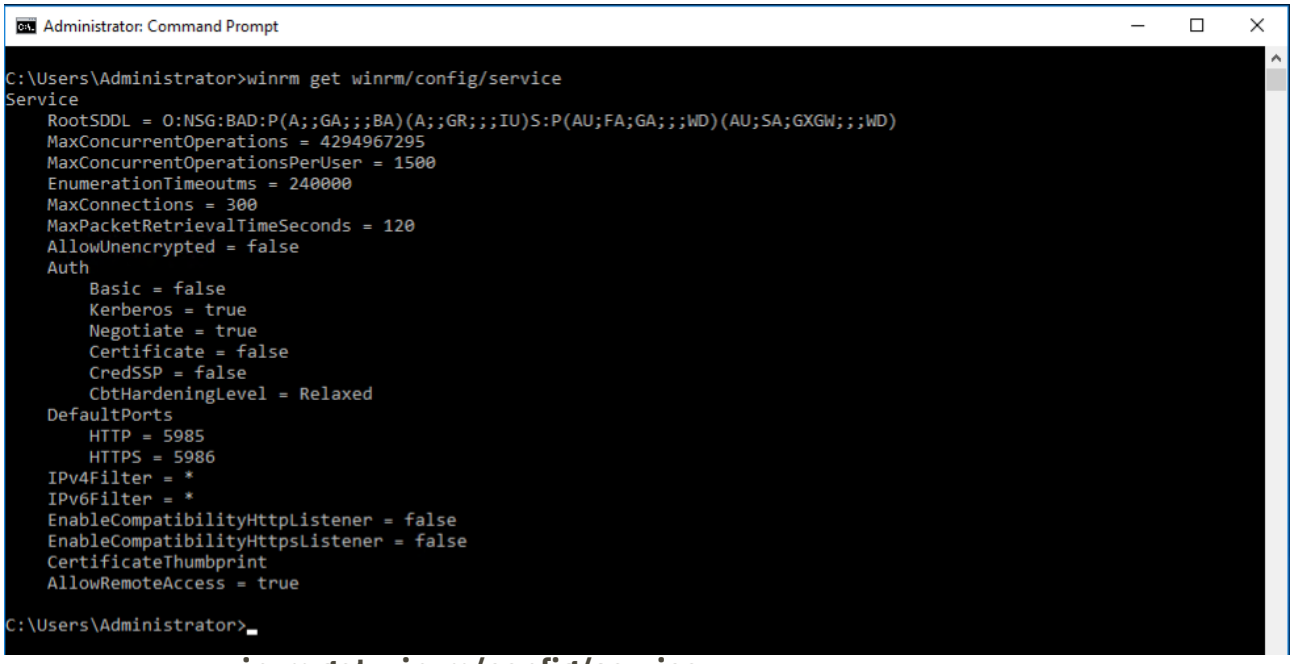
附录 D：使用 WINRM 的 Windows

对于 Windows 2012 和 2016 Server，WINRM 服务会自动启动。但是，在缺省情况下未启用远程管理。下面简要概括了在启用 WINRM 以允许使用自签名证书进行远程连接时需要执行的操作：

- 启用 WINRM 以接受使用用户标识/密码进行认证的 HTTPS 连接
- 将自签名证书与已启用的 WINRM 的 HTTPS 侦听器相关联
- 修改 Windows 防火墙以允许通过端口 5986（缺省 WINRM HTTPS 端口）进行入站连接

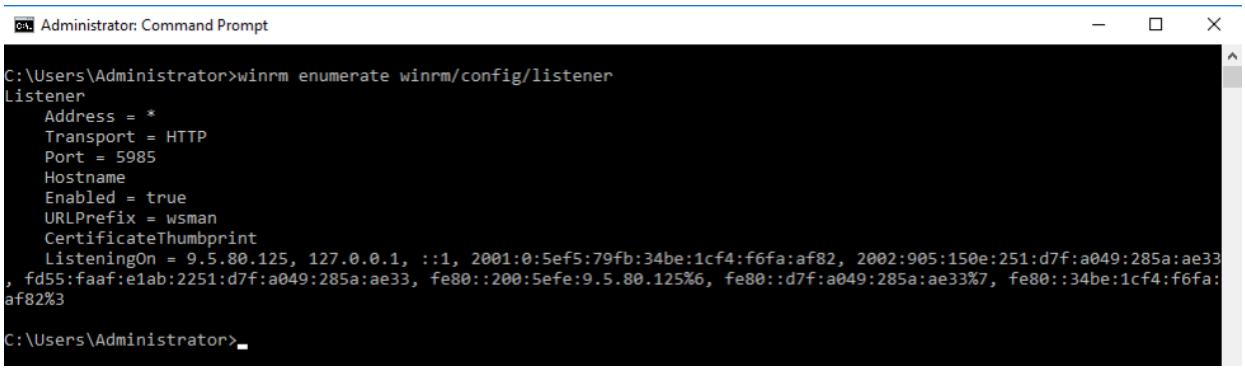
以下命令将准备 WINRM 以允许通过 HTTPS 进行远程连接：

- 使用以下命令来确定 WINRM 服务的当前状态：



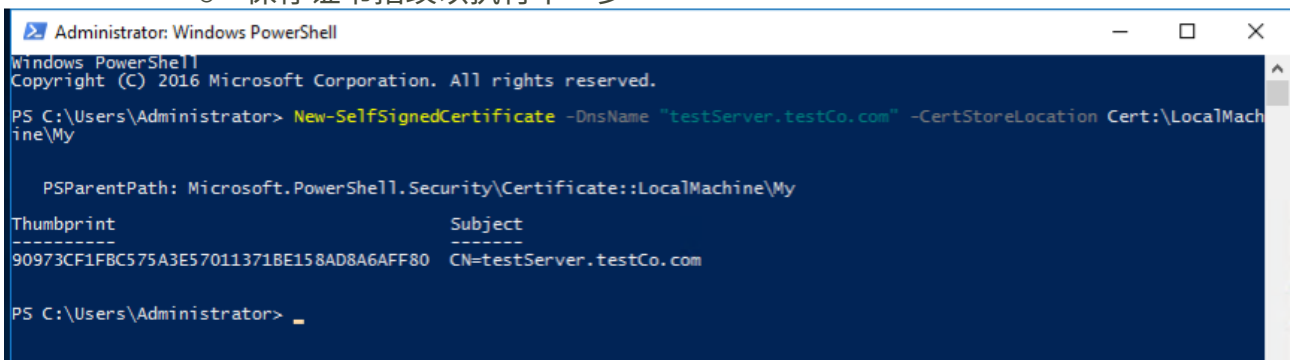
winrm get winrm/config/service

- **AllowUnencrypted** 的值必须为 *false*。如果该值为 *true*，请使用以下命令来将其更改为 *false*：
  winrm set winrm/config/service @{AllowUnencrypted="false"}
- **Basic** 的值必须为 *true*。如果该值为 *false*，请使用以下命令来将其更改为 *true*：
  winrm set winrm/config/service/auth @{Basic="true"}
- 使用以下命令来确定 WINRM 是否有 HTTPS 侦听器：
  winrm enumerate winrm/config/listener



- 在上面的命令示例中，只存在一个 HTTP 侦听器，因此需要配置一个 HTTPS 侦听器。要启用 HTTPS 侦听器（如果未配置）：
  - 使用 PowerShell 创建自签名证书：
    New-SelfSignedCertificate -DnsName "myHost@myBusiness.com" -CertStoreLocation Cert:\LocalMachine\My

    将以上示例中的 DnsName **(myHost@myBusiness.com)** 替换为 Windows 服务器的 Windows 标准域名。
  - 保存证书指纹以执行下一步



- 创建 HTTPS 侦听器：
  winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="myHost@myBusiness.com"; CertificateThumbprint="[COPIED_CERTIFICATE_THUMBPRINT]"}
- 检查以确保现在已配置 HTTPS：
  winrm enumerate winrm/config/listener
- 修改 Windows 防火墙以允许到 WINRM 的入站远程连接：
  - 转至“**控制面板 → 系统和安全 → Windows 防火墙**”
  - 单击**“高级设置”**。这样会显示**“具有高级安全的 Windows 防火墙”**窗口。
  - 单击**入站规则**。
  - 选择**操作**菜单并单击**新建规则**。这样会显示**新建入站规则向导**。
  - 选择**端口**并单击**下一步**。
  - 选择 **TCP → 特定本地端口**并指定 5986。单击**下一步**。
  - 选择**允许连接**选项并单击**下一步**。
  - 选中**域**、**私有**和**公共**复选框（如果尚未选中），然后单击**下一步**。
  - 为新规则命名（例如，Windows 远程管理 (HTTPS-In)）并单击**完成**。

声明

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
美国出版

2020 年 8 月。

本文档是为在美国国内供应的产品和/或服务而编写的。IBM 可能在其他国家或地区不提供本文档中讨论的产品、功能特性或服务。

本信息可随时更改而不另行通知。有关您所在区域可获取的产品、功能特性和服务的信息，请向您当地的 IBM 业务联系人咨询。

所有关于 IBM 未来方向和意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

IBM、IBM 徽标、POWER、System I、System p 和 i5/OS 是 International Business Machines Corporation 在美国和/或其他国家或地区的商标或注册商标。可在 http://www.ibm.com/legal/copytrade.shtml 中找到 IBM 拥有的美国商标的完整列表。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

IBM 硬件产品可能使用新部件制造而成，也可能同时使用了新部件和二手部件。无论属于何种情况，我们的保修条款均适用。

此设备遵守 FCC 规则。在最终交付给买方前，此设备将遵守相应的 FCC 规则。

涉及非 IBM 产品的信息是从这些产品的供应商处获取的。

有关非 IBM 产品功能的问题应与这些供应商联系。

IBM 因特网主页为 http://www.ibm.com。

可以在 http://www.ibm.com/systems/p 上找到因特网上的 IBM System p 主页。

可以在 http://www.ibm.com/systems/i 上找到因特网上的 IBM System i 主页。

PSW03007-CNZH-00