V 2.7.0.0

Technical Support Appliance
设置指南

声明

在使用本资料及其支持的产品之前，请阅读第 131 页的『声明』中的信息。

第二十三版（2020 年 8 月）

本版本适用于 IBM® Technical Support Appliance V2.7.0 以及所有后续发行版和修订版，直到在新版本中另有声明为止。

目录

图

第 1 章 简介

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，然后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应用程序、中间件、服务器与网络组件之间的复杂关系。

TSA 包含基于 Web 的用户界面 (UI) 以设置和定制系统和访问的访问权。UI 还支持您修改数据发现和传输的计划安排。

在发现过程中，TSA 最初尝试在不使用发现凭证的情况下检测已定义作用域内的端点。这包括使用 Nmap，并尝试利用最少量的侵入性 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。

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。

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。

用户帐户和用户组

执行任何 TSA 功能都需要一定的权限级别。如果已认证的用户尝试在没有相应权限级别的情况下执行某个功能，那么将显示一条错误并且不会执行该功能。

在组织内，可以创建角色来执行多种作业功能。可向特定角色分配执行特定操作的权限。可向 TSA 用户分配特定角色，通过这些角色分配，TSA 用户便可以获得必需的权限来执行特定系统功能。这样，获得某种角色的任何用户就会具有与该角色关联的权限级别，并且可轻松地向角色添加用户、将用户从一种角色更改为另一种角色，或者从角色中移除用户。

在 TSA 中，可使用具有相关权限级别的用户组来管理角色。可使用用户帐户来管理用户。可以向用户帐户分配一个或多个用户组中的成员资格，通过这些成员资格，用户就会具有相应权限级别来执行特定功能。

此外，可以将用户组进一步限制于所选作用域集。作用域集是用于标识 TSA 可发现的 IT 元素的 IP 地址、地址范围或子网的集合。通过指定用户组的作用域集限制，可以进一步限制此用户组成员的访问权。例如，通过结合使用权限级别和与特定用户组相关联的作用域集限制，可以创建特定于平台的用户组，例如，负责维护 Linux® 系统的用户。

发现作用域和作用域集

发现作用域可标识您希望 TSA 发现的资源。 发现作用域可分组为不同的发现作用域集。

您可以指定发现作用域，方法是使用 IP 地址、IP 地址范围或网络/子网来定义在发现期间可访问的资源。发现作用域最小可为单个 IP 地址，最大可为一个 IP 地址范围或网络。

要简化作用域集的创建过程，可使用文件来导入 IP 地址列表。有关更多信息，请参阅第 61 页的『导入作用域集』部分。

发现作用域中的 IP 地址越多，发现所需的时间就越长。通过禁用或启用发现作用域集或从作用域集内的作用域中排除 IP 地址、IP 地址范围或网络/子网，可以修改发现规模。

注: 为获得更好的性能，请将作用域集中的 IP 地址（IP 地址、IP 地址范围、子网和排除项）的累计数量限制为 400 或更小值。

相关任务

添加用户帐户和组

您可以通过添加用户帐户和组来控制对 TSA 功能的访问。

发现凭证

发现凭证是用户名、密码或 SSH 密钥以及简单网络管理协议 (SNMP) 共用名字符串（供 TSA 用来在发现期间访问资源）的集合。

必须针对要发现的资源设置和维护发现凭证。提供的访问信息因凭证类型而异，但是通常至少包含用户名和密码或 SSH 密钥。

发现凭证可用于所有作用域集或仅用于单个作用域集。通过定义用于单个作用域集的凭证，可以提高性能并阻止可能会导致帐户被锁定的无效登录尝试。

在访问资源时，TSA 会继续按照“**发现凭证**”页面上列出的顺序使用与特定作用域相关联的各个凭证，直至允许 TSA 访问该资源。例如，在访问计算机系统时，TSA 将使用计算机系统凭证列表中指定且与所含作用域集相关联的第一组用户名和密码。如果该组用户名和密码不适用于特定计算机系统，那么 TSA 会自动使用计算机系统凭证列表中指定的下一组用户名和密码。

提示: 在保存凭证之前，可以测试是否指定了适用于系统类型的凭证，例如，**计算机系统**、**计算机系统 (Windows)**、**SNMP** 或 **SNMPV3**。通过此测试，可确保有效定义了凭证。

提示:

- 将服务帐户与特定类型（例如，AIX® 或 Windows）的所有设备的公共密码结合使用。然后，可以定义单个凭证来发现此设备类型的所有实例。
- 将帐户与未到期的密码结合使用。
- 使用 SSH 密钥（在需要时）。

发现计划安排

在计划安排的日期和时间运行发现，以确保发现的数据始终是最新的准确数据。TSA 具有缺省“完全发现”计划安排，此计划安排对所有已定义的作用域集执行发现。可根据需求修改此缺省计划安排。您还可以创建计划安排，允许作用域集发现分布在两个不同日期和时间之间。您还可以查看所运行的最后一个发现的详细信息、历史记录和状态。

在修改发现计划安排时，可指定发现的名称、作用域集、开始时间和频率。如果发现计划安排是缺省发现，那么只能修改发现的开始时间和频率。您还可以按需运行发现。

发现的持续时间取决于许多因素（也包括资源的数量和复杂性），完成发现最多可能需要 72 小时。

传输计划安排

按计划安排的日期和时间安全地将发现的数据打包并传输给 IBM 支持人员，以确保 IBM 具有最新的准确信息。TSA 具有缺省传输计划安排，您可根据需要来修改该传输计划安排。您还可以按需运行传输。您还可以查看运行的最后一个传输的状态。

传输的耗用时间会因发现的数据量而异。

第 2 章 先决条件

要设置并使用 TSA，需要确保满足先决条件，例如，发现环境的必需凭证以及用于连接到 IBM 支持人员的配置需求。

注: 以下部分中的所有先决条件对于 TSA 都是强制性的，但 第 3 页的『TSA 需求』 部分中指定的需求除外。

下载 TSA 映像

TSA 映像同时适用于 Microsoft Hyper-V [*TSA-HYPERV-<version>*] 和 VMware [*TSA-VMWARE-<version>*] 服务器。

您可以在以下位置获得下载指示信息：https://ibm.biz/TSAdemo

TSA 需求

在设置并使用 TSA 之前，请确保满足以下先决条件。

x86 64 位硬件
必须在 x86 64 位系统上装入 TSA。

虚拟机管理器
TSA 需要 VMware ESXi 或 Microsoft Hyper-V

注: 建议使用目前受支持的任何 ESXi 或 Hyper-V 版本。

处理器
TSA 至少需要 2.26 GHz 四核处理器。

CPU
TSA 需要 4 个 64 位 CPU。

内存
TSA 需要 16 GB 内存。

直接访问存储设备 (DASD)
TSA 需要 150 GB DASD。

网络
TSA 需要 1 Gb 以太网适配器。

必需的 Web 浏览器

基于 Web 的用户界面可用于设置和监视发现和传输。

TSA 支持以下因特网浏览器:

- Mozilla Firefox V68.9.0 Extended Support Release (ESR)
- 适用于 Windows 10 的 Microsoft Edge V83.0.478.54
- Google Chrome V83.0.4103.116（64 位）

您可以从以下站点下载这些浏览器:

- Mozilla Firefox (http://www.mozilla.org/products/firefox/)
- Microsoft Edge (https://www.microsoft.com/en-us/edge)
- Google Chrome (https://support.google.com/chrome/answer/95346?hl=en)

连接到 IBM 支持人员的配置需求

TSA 可通过直接连接或通过用户提供的代理（必须配置为允许与 IBM 通信）连接到 IBM 支持人员。如果使用代理，那么不支持 TLS/SSL 检查。必须允许通过代理的任何请求直接传递到 IBM，而不会发生 TLS/SSL 终止。

确保防火墙允许连接到 IBM 服务器主机名和 IP 地址（如网络连接表中所述）。如果网络不允许访问 IBM 服务器，TSA 与 IBM 支持人员之间的事务将失败。

表 *1.* 网络连接

DNS 名称	**IP 地址**	**端口**	**协议**
esupport.ibm.com	129.42.54.189	443	HTTPS（到 IBM）
	129.42.56.189		
	129.42.60.189		

IBM 服务器环境完全符合 NIST SP800-131A 标准，支持 TLS 1.2 协议、SHA-256 或更强大的散列功能以及至少 2048 位强度的 RSA 密钥。

注: 不支持 SSL 检查，如果在代理服务器上使用，请针对这些流禁用。

对于 Blue Coat 代理，禁用指向 IBM 服务器的“协议检测”。添加以下配置规则：

- url.domain=esupport.ibm.com detect_protocol (none)
- url.address=129.42.54.189 detect_protocol (none)
- url.address=129.42.56.189 detect_protocol (none)
- url.address=129.42.60.189 detect_protocol (none)

发现环境的凭证和软件需求

为发现您的环境中的端点或资源，TSA 必须有权访问这些资源。建议针对每个资源创建一个服务帐户，以专门供 TSA 访问此资源时使用。

针对资源创建服务帐户后，必须针对该服务帐户在 TSA 上定义和维护与资源上定义的凭证相匹配的凭证。TSA 将使用这些凭证来访问该资源。凭证需求因环境和要发现的资源类型而异，但是凭证通常包含用户名和密码或 SSH 密钥。某些资源还具有特定的软件需求。

凭证类型	**访问信息**
计算机系统	**用户名:** 要用于访问设备的用户名。 **密码/口令:** 用于访问设备的密码/口令。 **认证类型:** 设备的认证类型。 · **密码** - 使用所提供的密码。 · **PKI** - 使用与特定作用域集相关联的 SSH 密钥。
计算机系统 (Windows)	**用户名:** 用于访问 Windows 计算机系统的用户名。 **密码:** 用于访问 Windows 计算机系统的密码。

凭证类型	访问信息
网络元素 (SNMP)	**共用名字符串：** 设备的共用名字符串。
网络元素 (SNMPV3)	**用户名：** 用于访问设备的用户名。 **密码：** 用于访问设备的密码。 **私有密码：** 在针对 SNMP 设置数据加密时使用的密码。 **认证协议：** SNMP 使用的认证协议的类型。 · 无 · MD5 · SHA
其他（Cisco 设备）	**用户名：** 用于访问 Cisco 设备的用户名。 **密码：** Cisco 设备的密码。 **启用密码：** Cisco 设备的启用密码。
其他 (Cisco Works)	**用户名：** 用于访问 CiscoWorks 服务器的用户名。 **密码：** 用于访问 CiscoWorks 服务器的密码。

注： 有关凭证和软件需求的更多信息，请参阅《配置助手指南》。

第 3 章 安装 Technical Support Appliance

TSA 包含了一些预安装的软件。它将作为 VMware 安装映像或 Microsoft Hyper-V 安装 VHDX 映像进行打包和分发。对于 VMware，可使用 VMware vSphere Client 或 VMware Web 界面（针对 ESXi）来安装 TSA。对于 Hyper-V，可使用 Hyper-V Manager 来安装 TSA。本部分提供了使用其中任何方法安装 TSA 的步骤。

使用 VMware ESXi Web 界面进行安装

开始之前
TSA 需要装入 VMware ESXi 6.5 或更高版本来控制硬件。

关于此任务
请执行以下步骤以安装 TSA 映像。

过程

1. 通过 VMware ESXi Web 界面登录到 ESXi 系统。
2. 单击**创建/注册虚拟机**。这样会显示“**新建虚拟机**”向导。

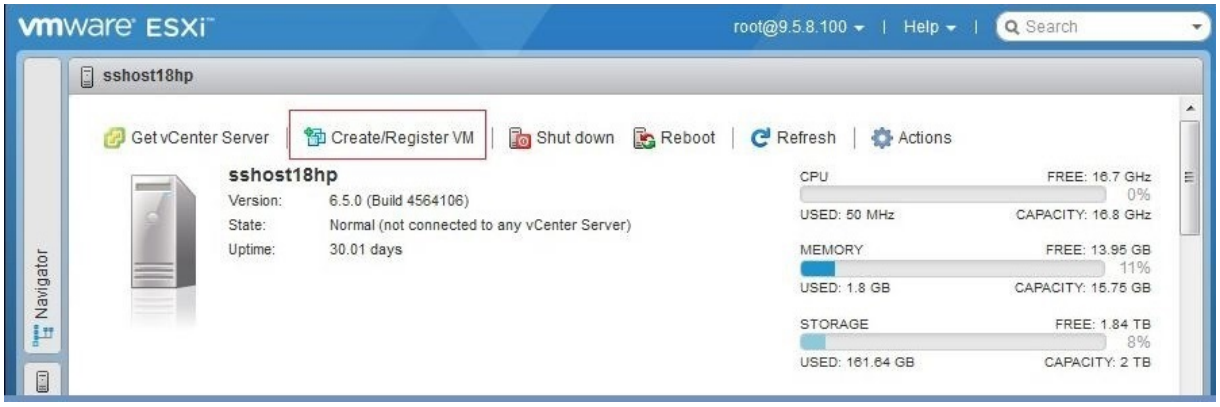

图 *1.* 创建/注册虚拟机

3. 在“**选择创建类型**”屏幕上，选择**从 OVF 或 OVA 文件部署虚拟机**选项，然后单击**下一步**。

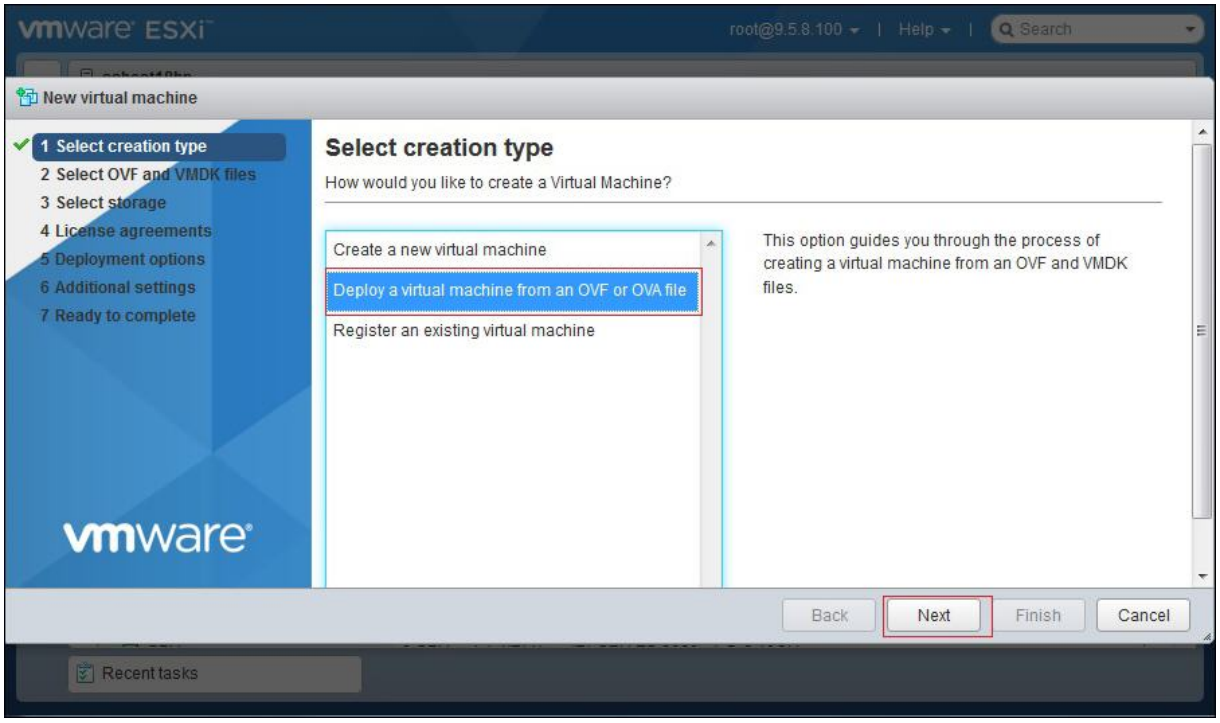

图 *2.* 选择创建类型

4. 在“**选择 OVF 和 VMDK 文件**”屏幕上，输入虚拟机的名称或使用缺省值。

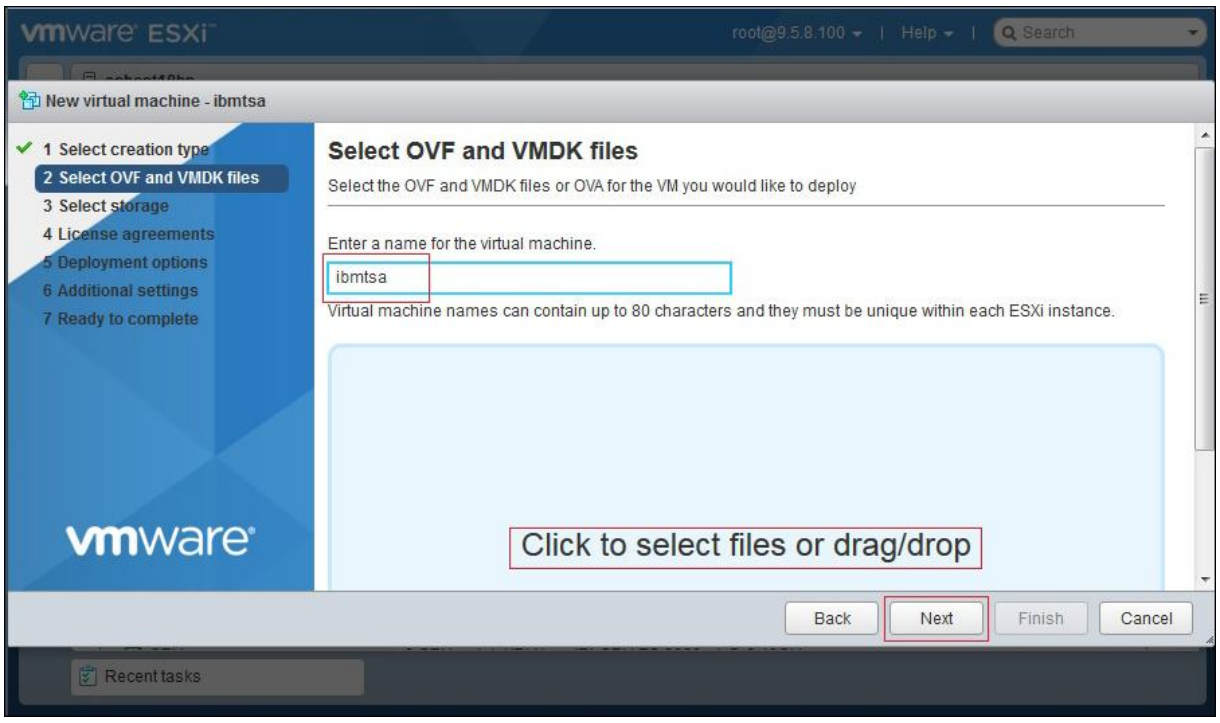

图 *3.* 选择 *OVF* 和 *VMDK* 文件

5. 在**单击以选择文件或拖放文件**框中单击鼠标，选择已从 Fix Central 下载的映像文件，然后单击**下一步**。
6. 在“**选择存储设备**”屏幕上，从显示的列表中选择用于存储配置和磁盘文件的数据存储设备。然后，单击**下一步**。

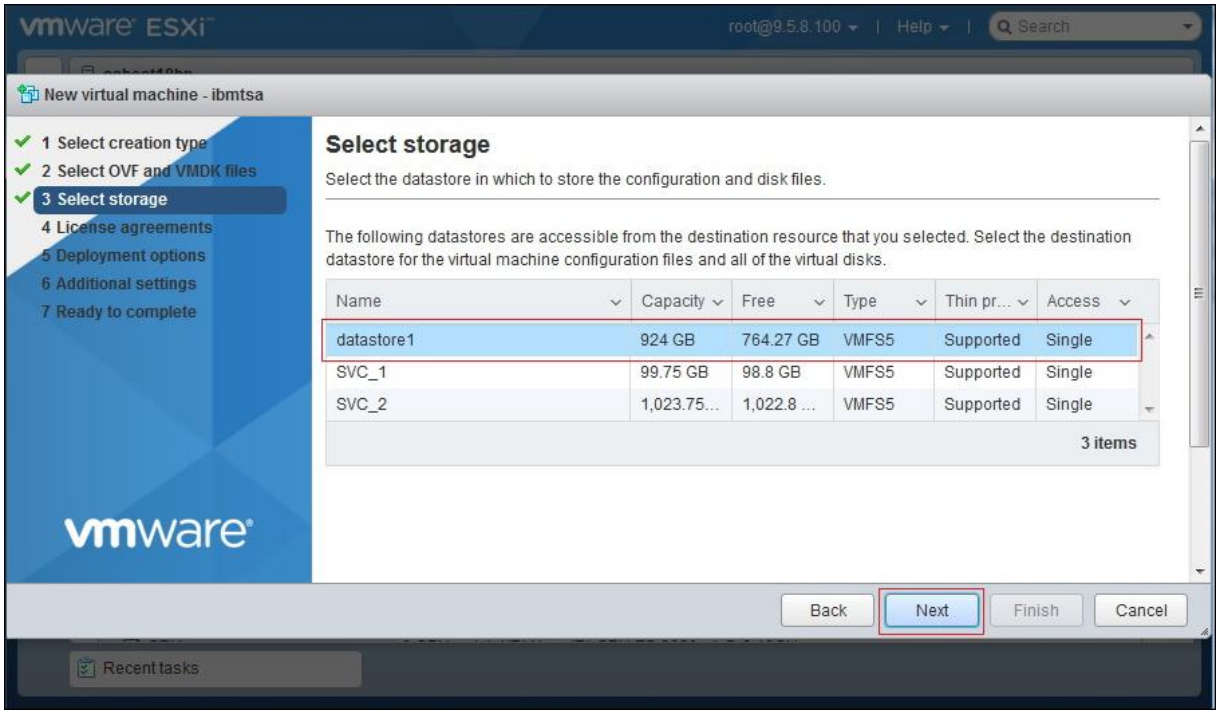

图 *4.* 选择存储设备

7. 在“**部署选项**”屏幕上，从**虚拟机网络**下拉列表中选择网络映射。

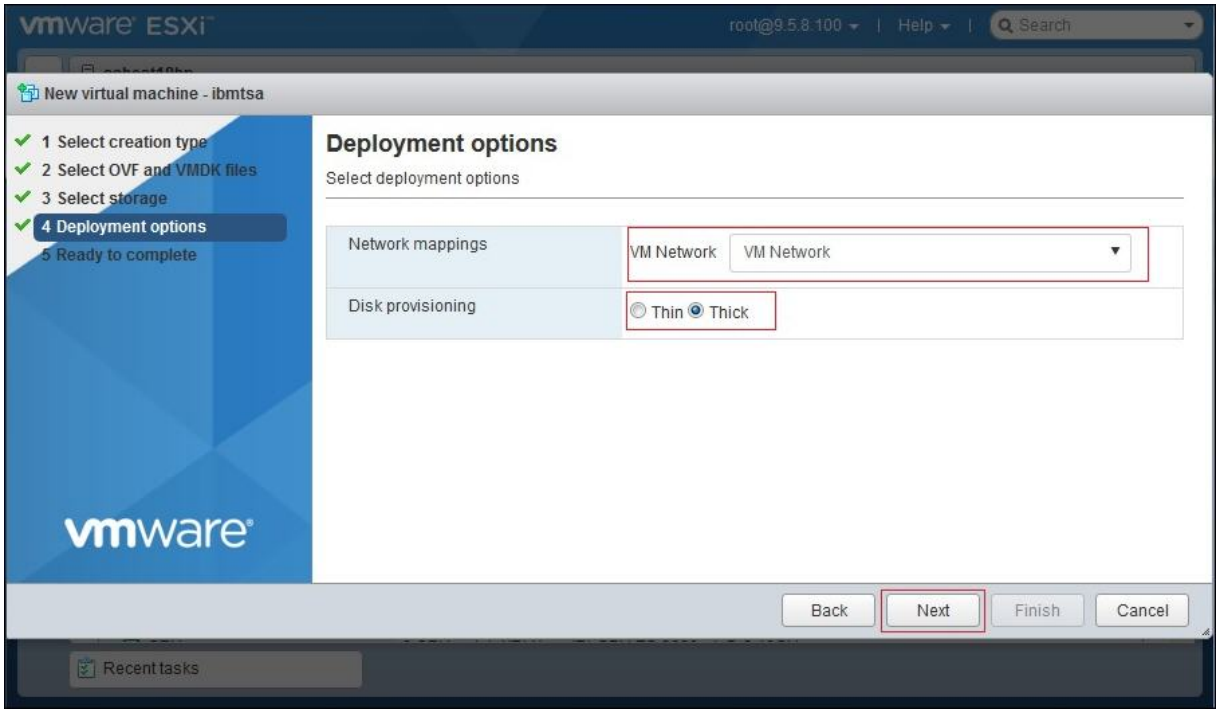

图 *5.* 部署选项

8. 对于磁盘供应，选择**密集**选项，然后单击**下一步**。
9. 在“**准备完成**”屏幕上，复查已指定的所有设置。如果想要进行任何更改，请单击**后退**并对相关选项执行更改。如果对这些更改感到满意，请单击**完成**。

要点: 在部署虚拟机时，将不会刷新浏览器。

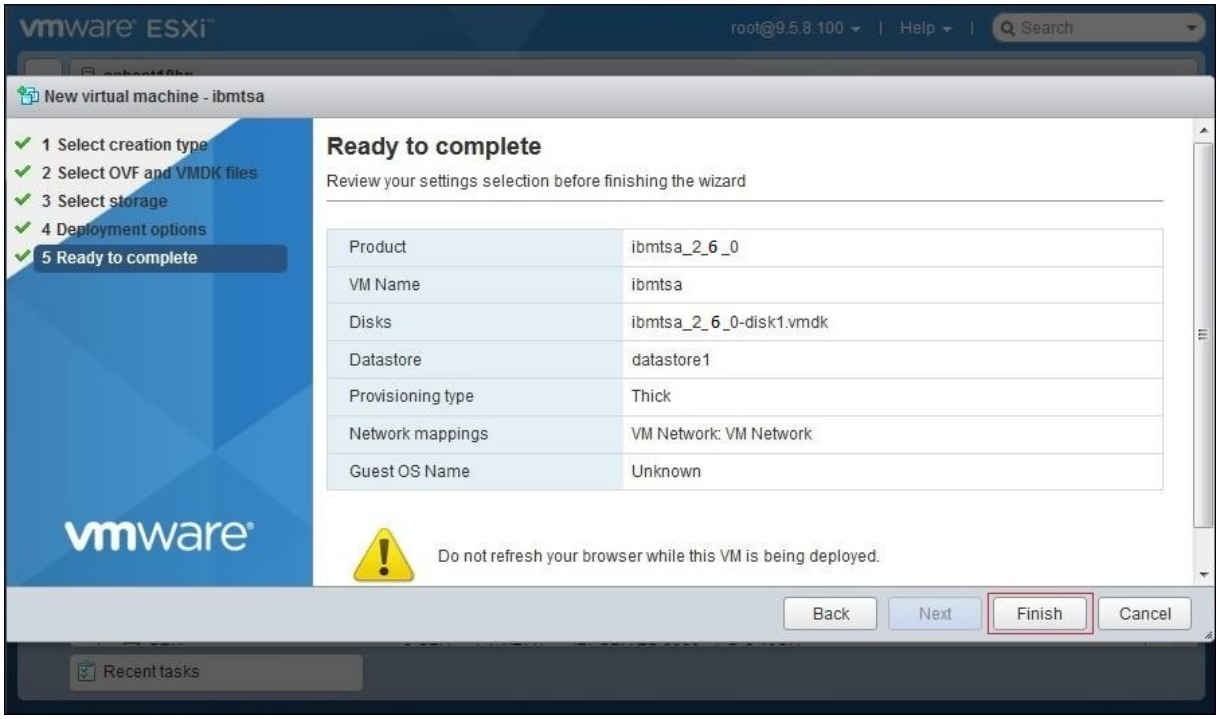

图 6. 复查所选设置

在系统上安装 TSA 虚拟机。

10. 在 TSA 控制台中，对于 **ibmtsa 登录**，输入 **tsausr**；对于**密码**，输入 **configTsa**。
11. 必需： 要更改登录密码，请继续执行第 17 页的『更改 tsausr 密码（必需）』部分中列出的步骤。
12. 要完成安装，请继续执行第 17 页的『配置网络详细信息』部分中列出的步骤。

在 Microsoft Hyper-V 上安装 TSA

开始之前

在 Hyper-V 上设置并使用 TSA 之前，请确保满足以下先决条件：

- Hyper-V Server 2012、2016 或 2019
- Hyper-V Manager
- 已通过 Hyper-V Manager 创建虚拟网络交换机

关于此任务

请执行以下步骤以在 Hyper-V 上安装 TSA。

过程

要在 Hyper-V 上安装 TSA，请执行以下步骤：

1. 下载 TSA 映像后，从 *ibmtsa_2700.zip* 解压缩 *ibmtsa_2700.vhdx* 文件，并将其移动到 Hyper-V 服务器上的某个目录。
2. 启动 Hyper-V Manager 并从客户机系统连接到 Hyper-V 服务器。
3. 单击**浏览**并选择在系统上保存的映像。

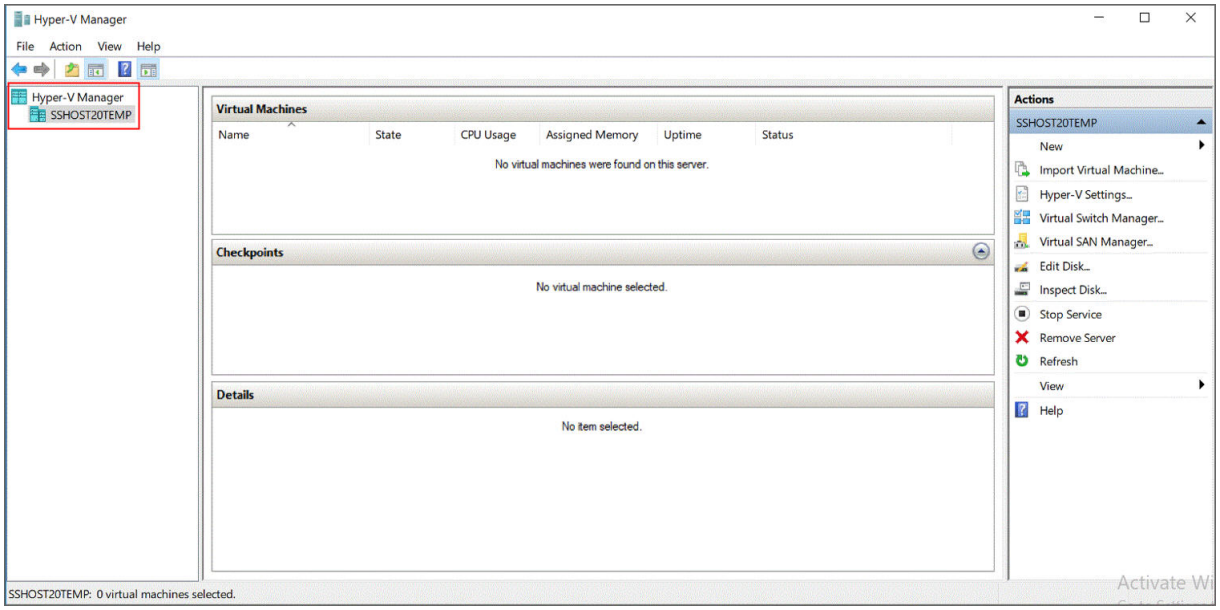

图 *7. Hyper-V Manager*

4. 从**操作**菜单中，选择**新建** → **虚拟机**。这样会显示“**新建虚拟机**”向导。
5. 输入新虚拟机的**名称**，然后单击**下一步**。

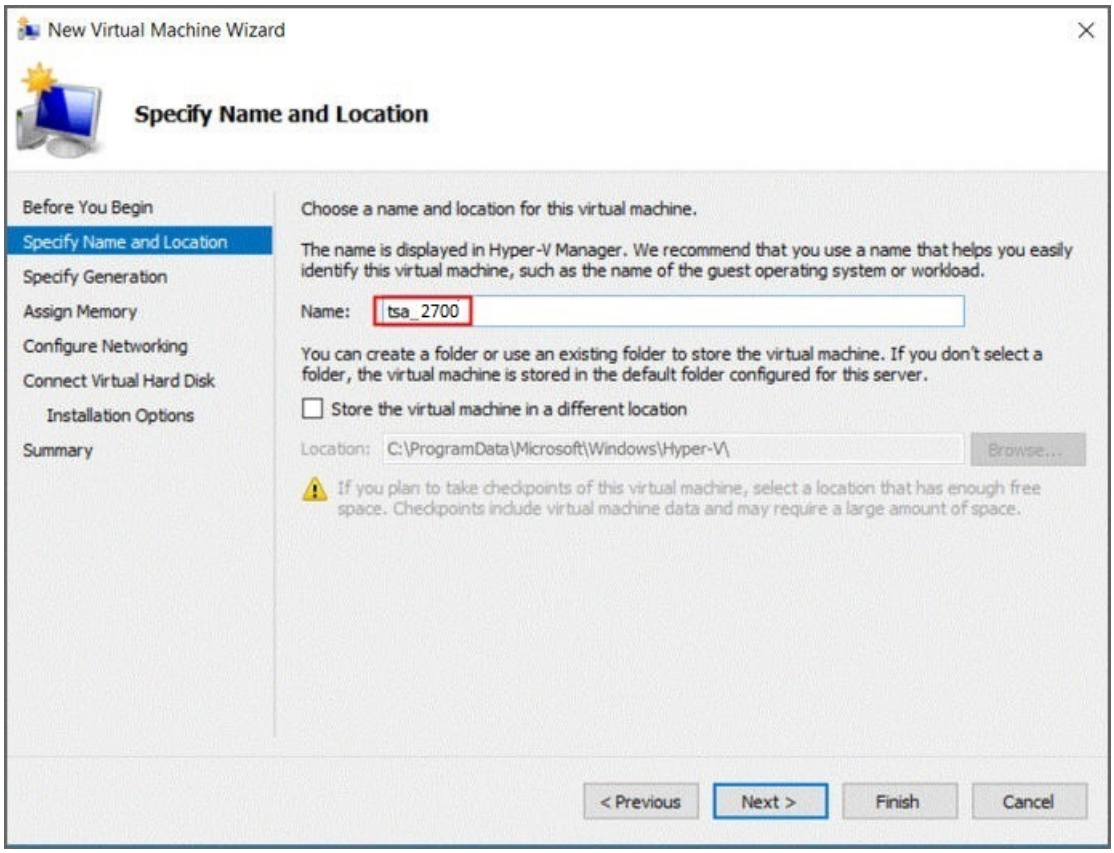

图 *8.* 虚拟机名称

6. 选择**第 1 世代**作为虚拟机的世代，然后单击**下一步**。

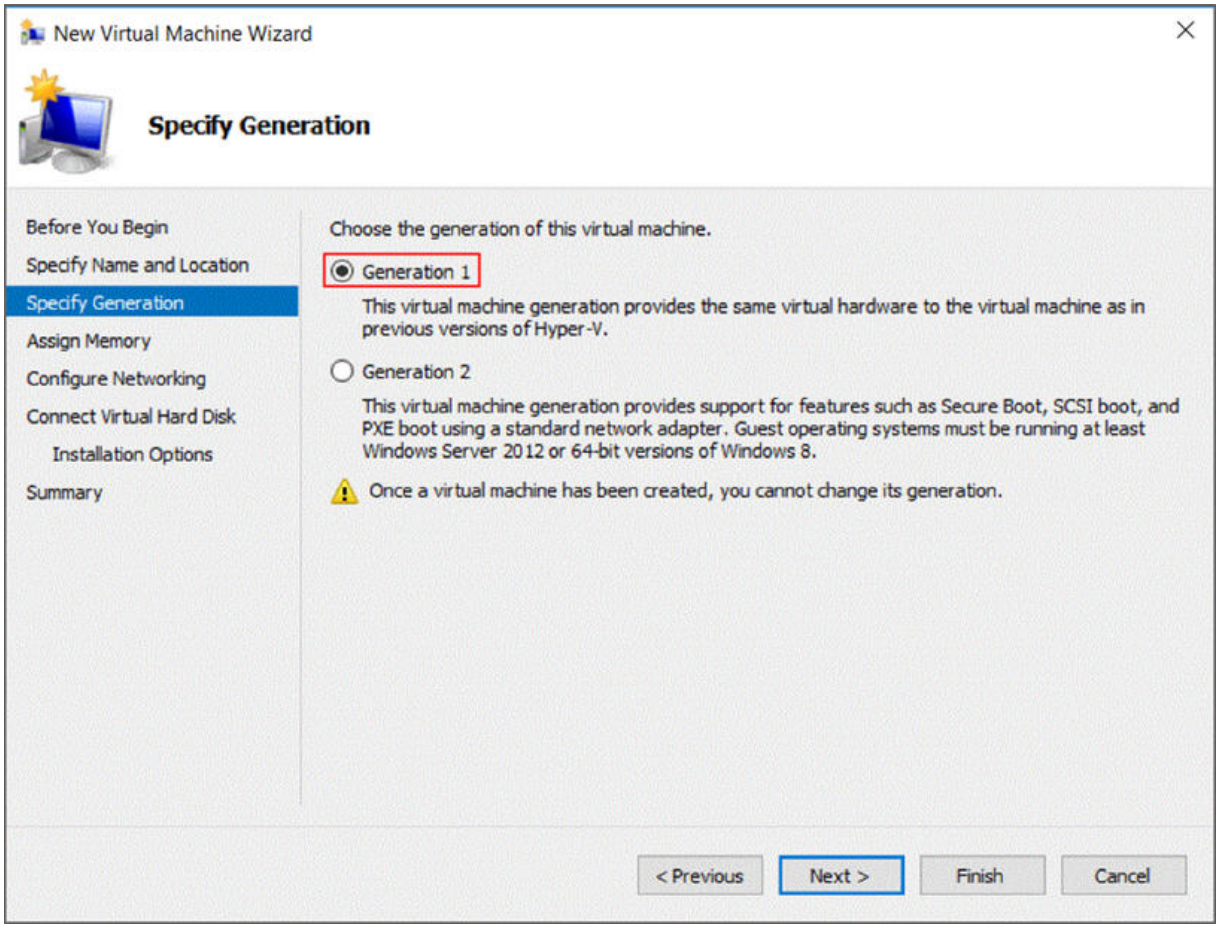

图 *9.* 指定世代

7. 对于**启动内存**，输入 *16384* MB，然后单击**下一步**。

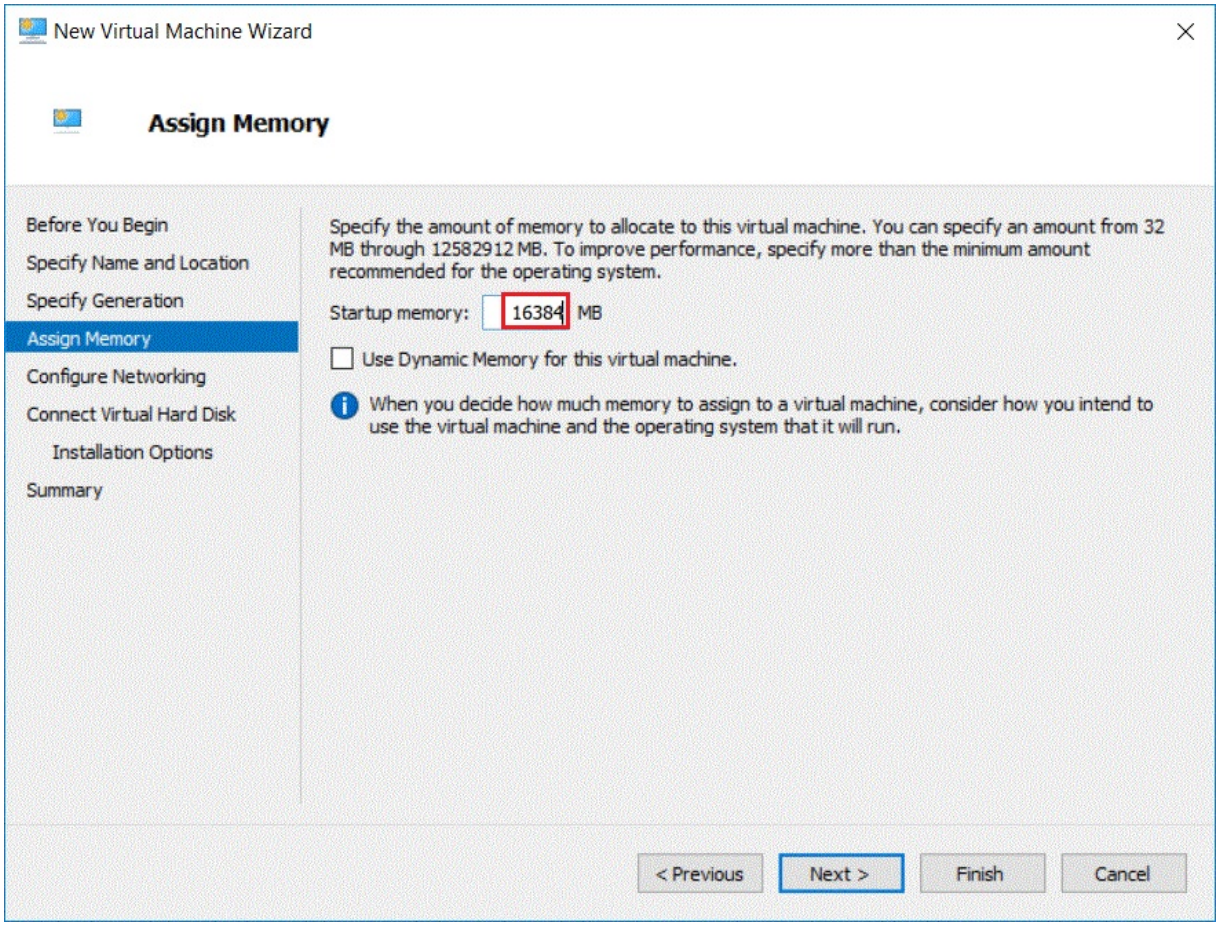

图 *10.* 启动内存

8. 选择预配置的虚拟交换机，然后单击**下一步**。

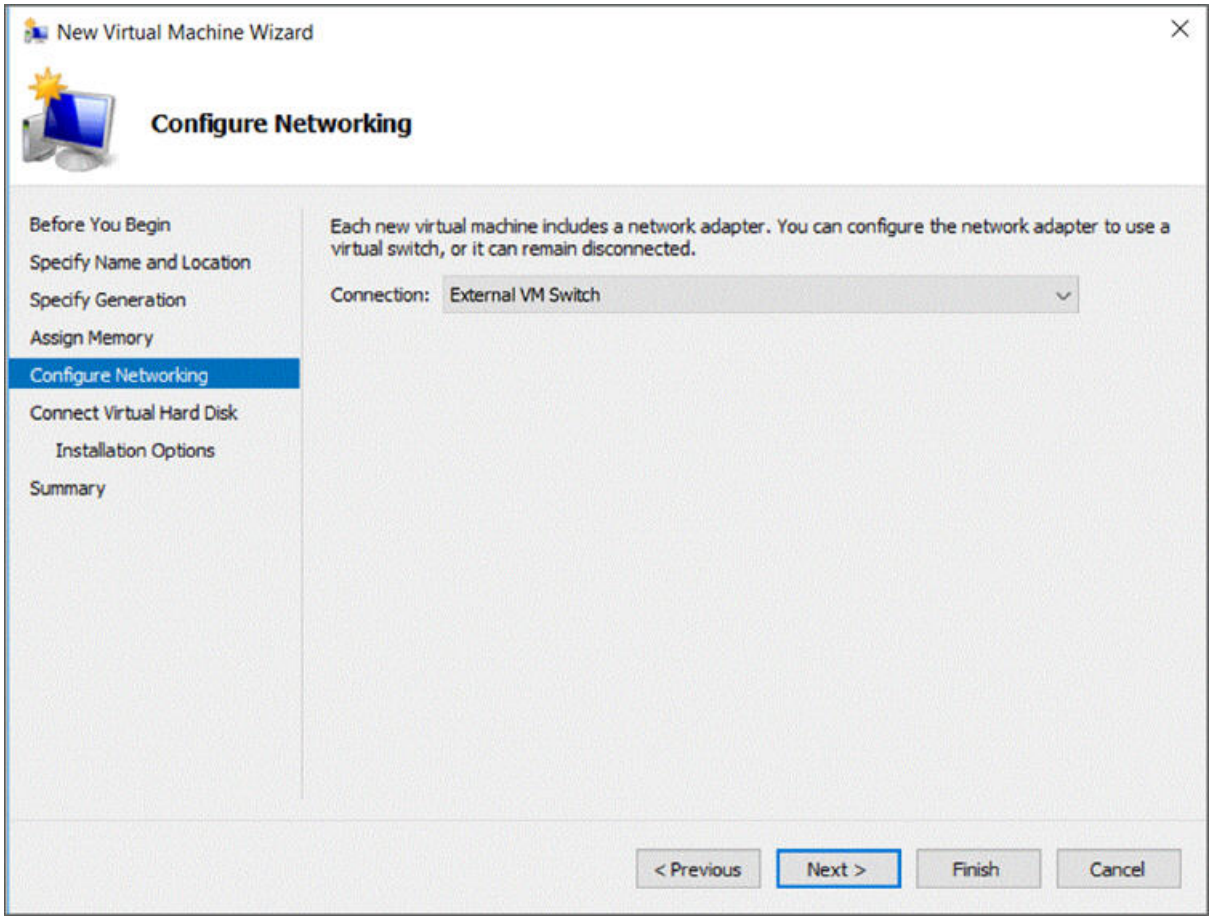

图 *11.* 配置网络

9. 选择**使用现有虚拟硬盘**选项，并浏览在步骤 2 中复制到 Hyper-V 服务器的 *ibmtsa_2700.vhdx* 文件，然后单击**下一步**。

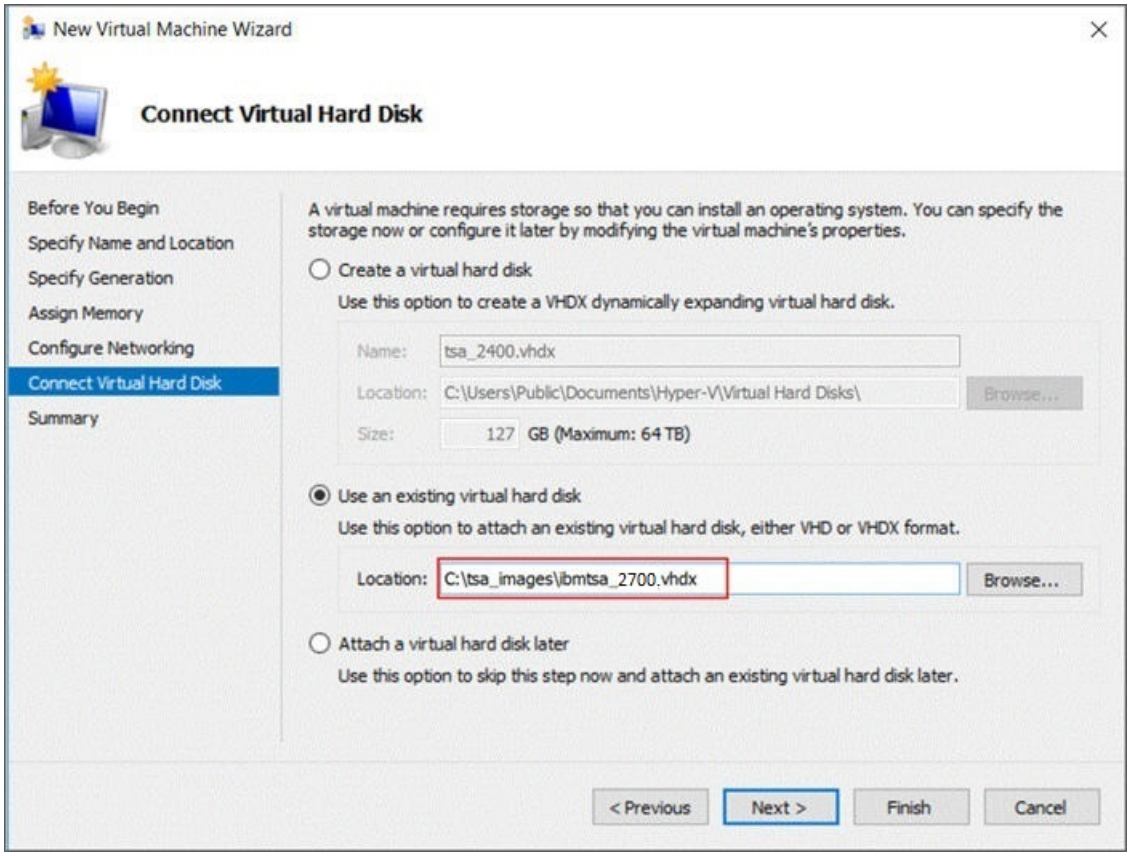

图 *12.* 连接虚拟硬盘

10. 在“**摘要**”页面中，复查设置并单击**完成**。

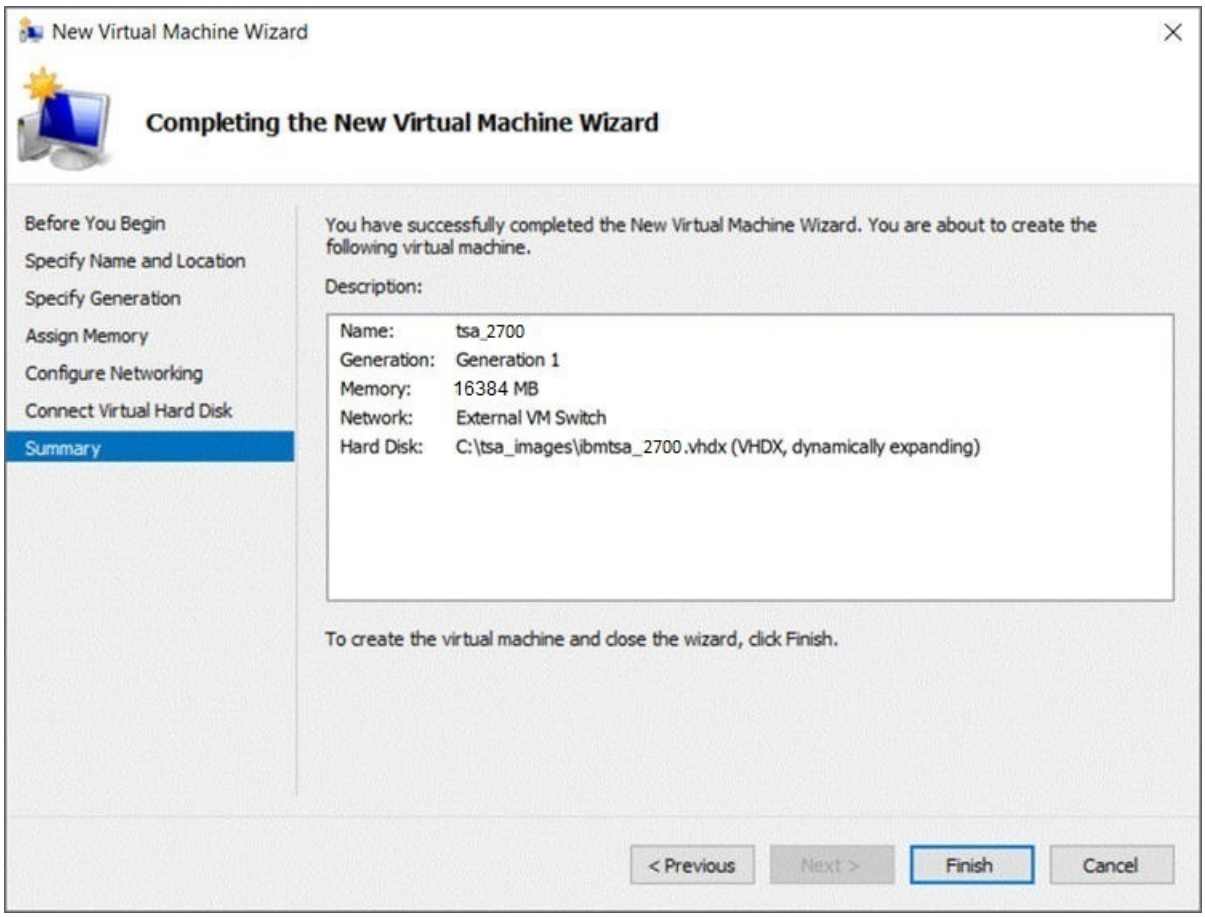

图 *13.* 摘要

11. 这样会在 Hyper-V Manager 下添加新虚拟机。选择虚拟机，转至**操作**菜单，然后单击**启动**。

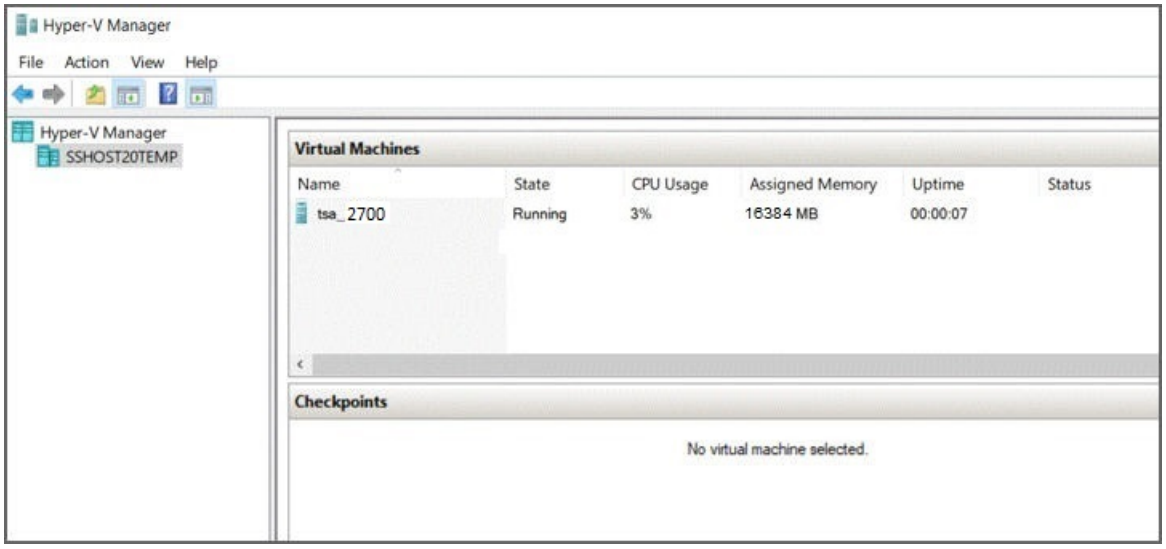

图 *14. Hyper-V Manager*

12. 从**操作**菜单，选择**连接**以启动控制台会话。在 TSA 控制台中，对于 **ibmtsa 登录**，输入 **tsausr**；对于**密码**，输入 **configTsa**。
13. 必需： 要更改登录密码，请继续执行第 17 页的『更改 tsausr 密码（必需）』部分中列出的步骤。
14. 要完成安装，请继续执行第 17 页的『配置网络详细信息』部分中列出的步骤。

更改 *tsausr* 密码（必需）

出于安全考虑，建议更改 *tsausr* 密码的初始值。请执行以下步骤以更改 *tsausr* 密码。

过程

1. 从“**TSA 配置菜单**”中选择选项 **2) 更改 tsausr 密码**。

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsausr password
3) Set Appliance certificate to default
4) Exit

Choose an option: 2
```

图 *15.* 更改密码

2. 在**新密码**提示处输入新密码。在**重新输入新密码**提示处输入相同的密码。新密码的长度必须至少为 7 个字符。

```
Changing password for user tsausr.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Returning to menu in 5 seconds...
```

图 *16.* 新密码

配置网络详细信息

过程

1. 从“**TSA 配置菜单**”中选择选项 **1) 设置网络配置**。

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsausr password
3) Set Appliance certificate to default
4) Exit

Choose an option: _
```

图 *17.* 设置网络配置

2. 输入以下网络配置详细信息。

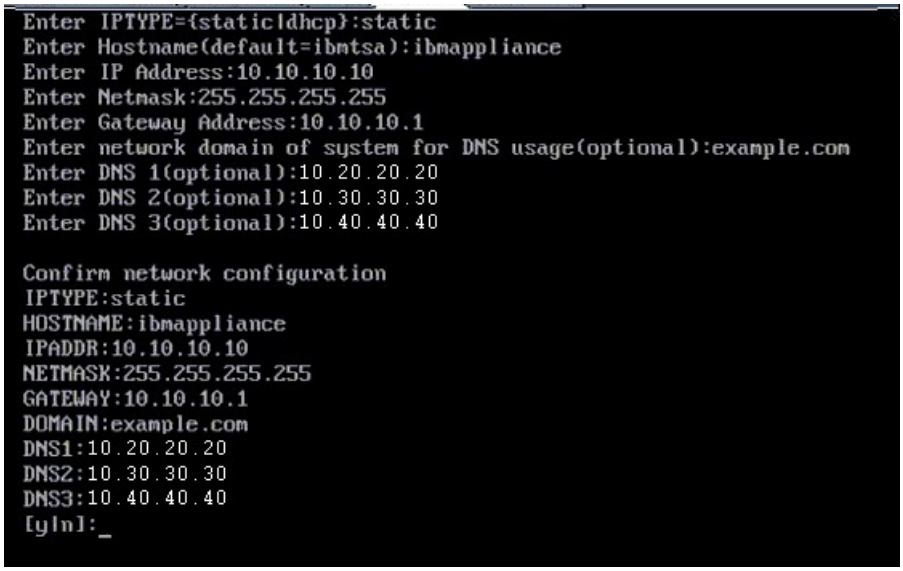

图 *18.* 网络配置

a) **输入 IPTYPE = {static|dhcp}**。输入 `static` 或 `dhcp`。如果输入了 `static`，请执行以下步骤，否则执行第 119 页的『附录 C 配置 DHCP 网络详细信息』部分中的 `dhcp` 配置步骤

IPTYPE: static

输入主机名（缺省值=ibmtsa）。您可以更改缺省主机名。 确保您使用的主机名是唯一的。

输入 IP 地址。

输入网络掩码和**输入网关**。

输入系统的网络域以供 DNS 使用（可选）。

输入 DNS 1（可选）、**输入 DNS 2（可选）**和**输入 DNS 3（可选）**。

此时会显示指定的网络配置详细信息以供确认。

b) 输入 **[y|n]** 以确认或丢弃网络配置。输入 **y** 将保存网络配置并自动重新启动系统。

注: 对于任何不正确的配置，您可以更改详细信息。输入 **n** 将忽略当前设置并从步骤第 18 页的『2.a』重新启动配置

c) 系统将在 15 秒内重新启动，以使新的网络配置生效。

d) 在使用安全 HTTP 的浏览器中，使用上面输入的主机名或 IP 地址来访问 TSA。
例如，`https://<hostname | IP address>`。

注: 在第一个连接上，浏览器可能显示安全异常。您必须接受安全证书并继续登录到 TSA。

注: 要通过用户界面修改 TSA 的基本网络设置，请执行第 30 页的『配置基本网络设置』中的步骤。要配置高级网络设置，请执行第 32 页的『配置高级网络设置』中的步骤。

3. 使用第 19 页的『第 4 章 设置 Technical Support Appliance』中列出的步骤设置 Technical Support Appliance

结果

成功设置 TSA 后，请参阅第 43 页的『第 5 章 设置到 IBM 的发现和传输』

第 4 章 设置 Technical Support Appliance

关于此任务
请执行以下步骤以快速开始使用 TSA。如果尚未执行此类操作，请查看第 3 页的『第 2 章 先决条件』。

过程

1. 第 19 页的『登录到 Technical Support Appliance』
2. 第 22 页的『接受许可协议』
3. 第 23 页的『使用“设置向导”进行初始配置』
   a) 第 24 页的『设置 IBM Connectivity』
   b) 第 25 页的『注册 Technical Support Appliance 』
   c) 第 27 页的『设置时钟』
   d) 第 28 页的『设置传输计划安排』
   e) 第 29 页的『更新 Technical Support Appliance』
4. 第 30 页的『配置网络设置』
5. 第 38 页的『设置证书』.
6. 可选： 第 121 页的『附录 D 用户帐户和用户组』

下一步做什么
在完成设置 TSA 后，请参阅第 43 页的『第 5 章 设置到 IBM 的发现和传输』以获取有关如何执行其他任务的信息。

登录到 Technical Support Appliance

过程

1. 从具有 TSA 网络访问权的系统打开因特网浏览器。
   有关更多信息，请参阅第 3 页的『必需的 Web 浏览器』。
2. 在浏览器地址栏中输入以下 URL：

   ```
   https://<hostname or IP address>
   ```

   注: 如果 `<hostname>` 无效，那么尝试指定的 TSA 的 IP 地址。
3. 出现提示时，输入以下信息：

   用户标识：
   输入 `admin`

   密码：
   输入 TSA 管理员密码。

   初始密码为 `passw0rd`。在登录到 TSA 后，必须更改此初始密码。

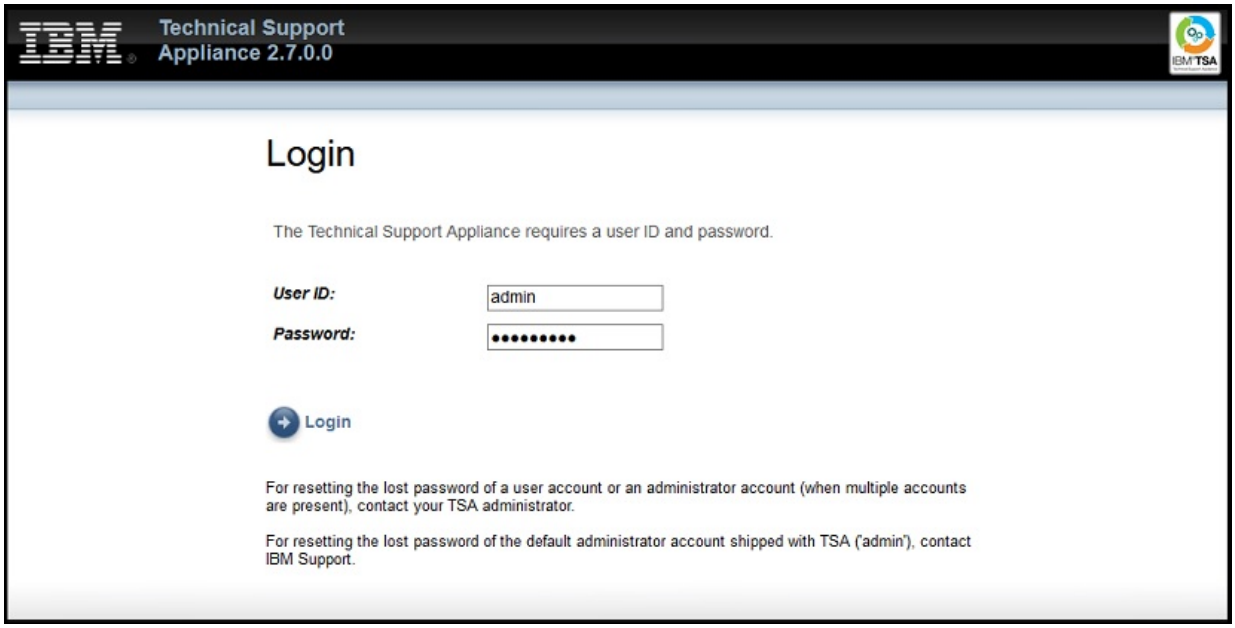

图 *19.* 登录

首次登录时将显示“**更改密码**”页面。

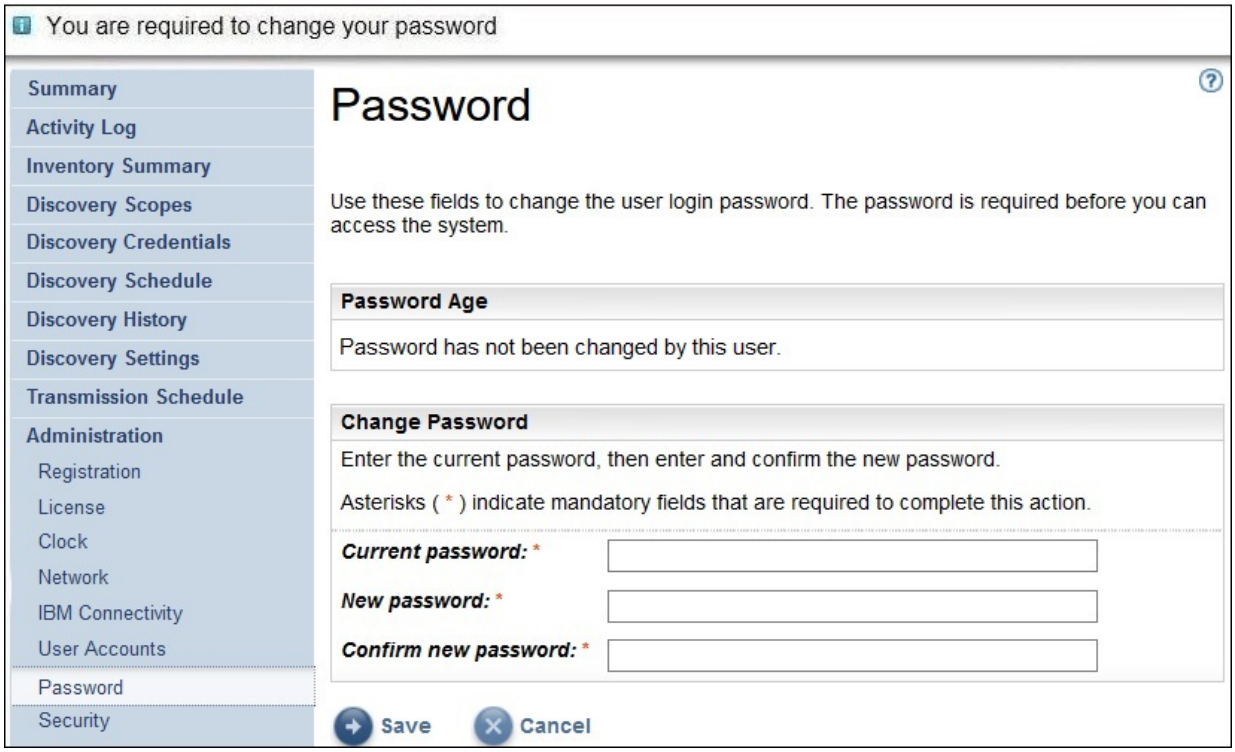

图 *20.* 更改密码

要更改初始密码，请执行以下步骤：

a) 输入新密码。

密码必须遵守以下规则：

· 必须至少包含 8 个字符

· 必须至少包含 1 个字母字符和 1 个非字母字符

· 不得包含用户名

· 不得与之前的 8 个密码相同

· 必须每 90 天至少更改一次，但每天不能更改多次。

b) 在**确认新密码**字段中重新输入新密码。

比较您输入的两个密码以确认它们相互匹配，然后再保存密码。

c) 记录新密码，以备将来参考。

要点: 无法恢复密码，因此，如果密码丢失或被遗忘，您将无法登录到 TSA 来更改凭证。如果丢失或忘记用户帐户或者管理员帐户（如果有多个帐户）的密码，请与 TSA 管理员联系。如果丢失或者遗忘缺省管理员帐户（TSA 随附）的密码，请与 IBM 支持人员联系。

d) 单击**保存**。对于首次登录，将显示“**许可协议**”页面。

接受许可协议

阅读并接受许可协议以继续。

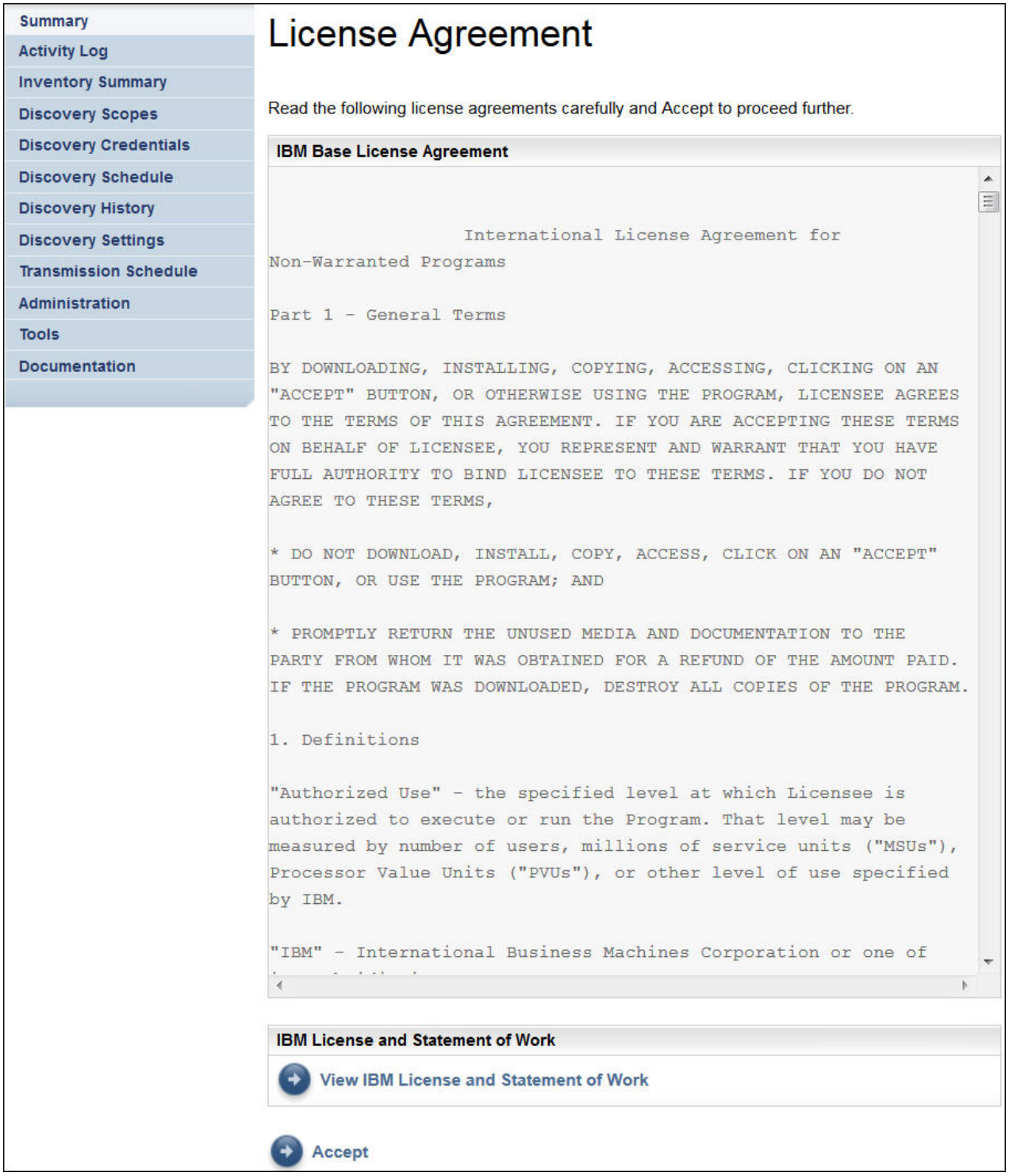

图 *21.* 许可协议

“许可协议”包含以下项:

- **IBM 基本许可协议**：显示 IBM 基本许可协议。
- **IBM 许可证和工作说明书**：单击**查看 IBM 许可证和工作说明书**以查看 IBM 许可证和工作说明书。

注: TSA 符合 GDPR [EU/2016/679]。您可以在“**IBM 许可证和工作说明书**”部分中查看 GDPR 合规信息。

- **IBM 声明和信息**：单击**查看 IBM 声明和信息**以查看 IBM 声明和信息。
- **单独许可代码的条款和条件**：单击**查看单独许可代码的条款和条件**以查看单独许可代码的条款和条件。

单击**接受**以接受协议。接受许可后，会显示“**设置向导**”以配置 TSA。您可以通过“**设置向导**”配置 TSA，也可以退出向导并按照需求配置 TSA 设置。

注: 在导航窗格中，单击**管理 > 许可证**以查看已接受的最新许可协议。

相关概念

第 23 页的『使用“设置向导”进行初始配置』
使用“**设置向导**”设置 TSA 以进行初始配置。

第 109 页的『配置 Technical Support Appliance 』
如果退出或跳过在“**设置向导**”中配置任何设置，那么可以从 TSA 的左侧导航菜单中手动配置。

使用“设置向导”进行初始配置

使用“**设置向导**”设置 TSA 以进行初始配置。

接受许可协议后，会自动显示“**设置向导**”。

注: 要手动启动“**设置向导**”，请在导航窗格中单击**工具 > 设置向导 > 启动设置向导**。

图 *22.* 设置向导

“**设置向导**”将指导您完成以下步骤:

- 第 24 页的『设置 IBM Connectivity』
- 第 25 页的『注册 Technical Support Appliance 』
- 第 27 页的『设置时钟』
- 第 28 页的『设置传输计划安排』
- 第 29 页的『更新 Technical Support Appliance』

注: 如果退出或跳过在“**设置向导**”中配置任何设置，那么可以从 TSA 的导航窗格中手动配置。有关配置这些设置的更多信息，请参阅第 109 页的『附录 B 配置 Technical Support Appliance 』。

设置 IBM Connectivity

过程

您可以查看、更改和测试 TSA 用于连接到 IBM 的配置。

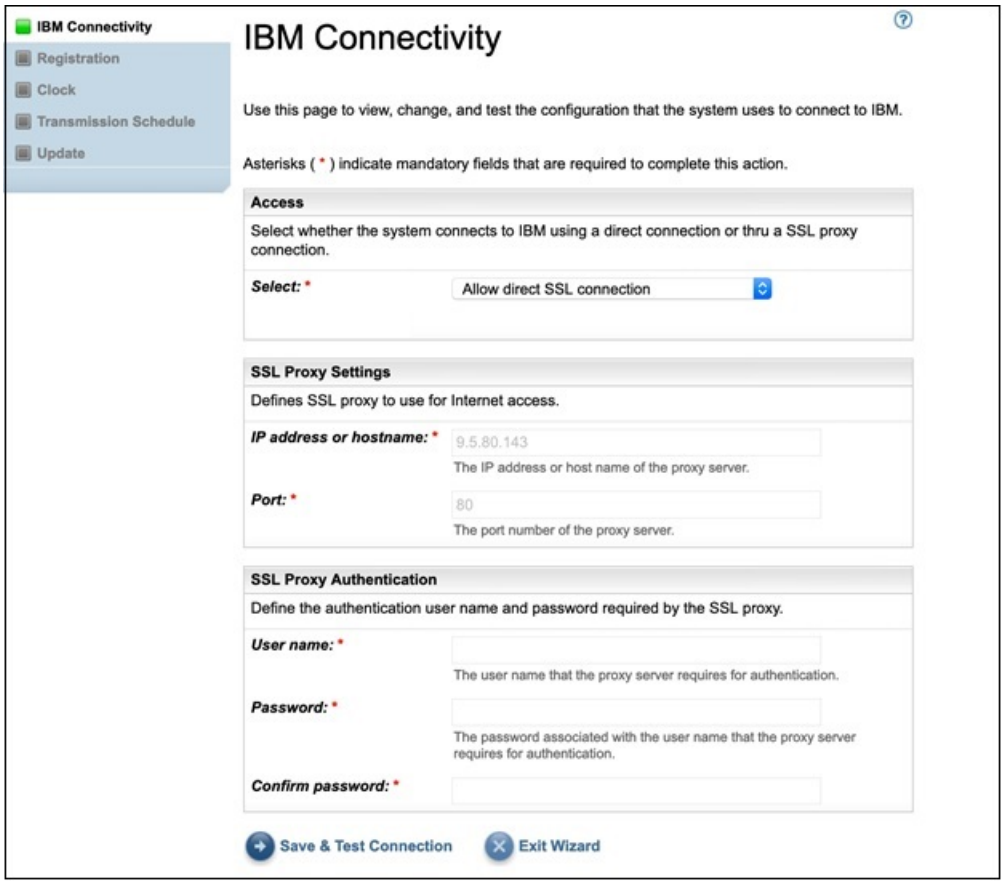

图 *23. IBM Connectivity*

1. 在“**访问**”窗格中，从以下因特网访问类型中进行选择：

   允许直接 SSL 连接
   TSA 使用直接连接来连接到 IBM。

   使用 SSL 代理连接
   TSA 使用 SSL 代理连接来连接到 IBM。

   使用认证 SSL 代理连接
   TSA 使用认证 SSL 代理连接来连接到 IBM。

2. 如果已选择**使用 SSL 代理连接**或**使用认证 SSL 代理连接**，请为代理服务器指定以下信息。

   IP 地址或主机名
   代理服务器的 IP 地址或主机名。

   注: 输入的主机名不得包含下划线 (“_”)。

   端口
   代理服务器的端口号。

3. 如果已选择**使用认证 SSL 代理连接**，请为代理服务器指定以下信息：

   用户名
   代理服务器进行认证所需的用户名。

   密码
   代理服务器进行认证所需的、与用户名关联的密码。

确认密码

再次输入密码。比较您输入的两个密码以确认它们相互匹配，然后再保存密码。

下一步做什么

· 单击**保存和测试连接**以保存和测试指定的连接。如果连接成功，那么会显示**继续**按钮。

· 单击**继续**以转至“**注册**”页面。

-或者-

· 单击**退出向导**以退出“**设置向导**”并转至“**摘要**”页面。

注册 Technical Support Appliance

您可以查看和更改系统服务联系人和实际位置。

过程

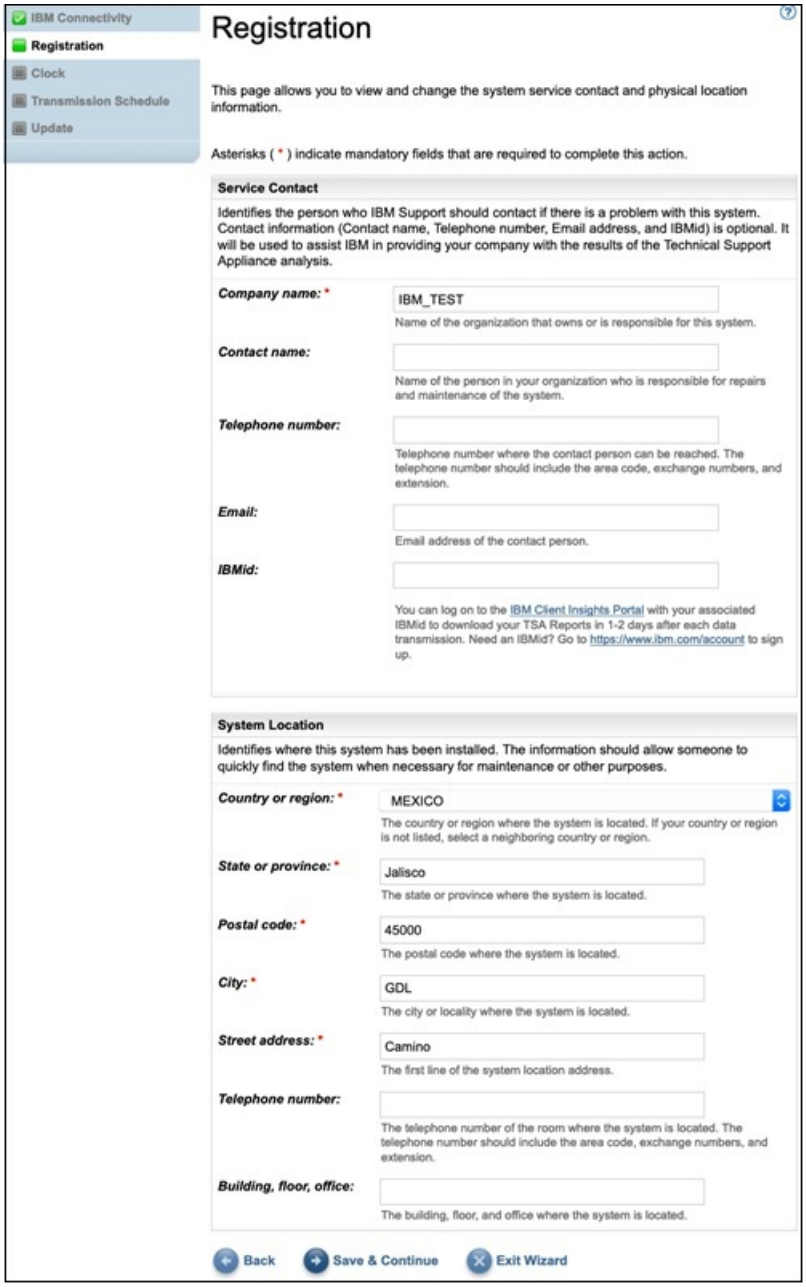

图 *24.* 注册

1. 在以下字段中指定服务联系人信息：

   公司名称
   使用 TSA 的组织的名称。

   联系人姓名
   （可选）组织中负责 TSA 的人员的姓名。

   电话号码
   （可选）可与联系人联系的电话号码。电话号码应包含区号、交换号和分机号。请勿在电话号码中使用括号。

   电子邮件
   （可选）联系人的电子邮件地址。

   IBMid
   （可选）您想要授权其在 IBM Client Insights 门户网站上查看报告的人员的 IBMid。

   注: 在每次数据传输后 1-2 天内，您可以使用关联的 IBMid 登录到 https://clientinsightsportal.ibm.com/ 来下载 TSA 报告。要注册 IBMid，请转至 https://www.ibm.com/account。

   注: 服务联系人标识当系统出现问题时 IBM 支持人员应联系的人员。联系人信息可帮助 IBM 向贵公司提供 Technical Support Appliance 分析的结果。
2. 在以下字段中指定 TSA 位置信息：

   国家或地区
   TSA 所在位置的国家或地区。

   州或省/自治区/直辖市
   TSA 所在位置的州或省/自治区/直辖市。如果您不确定州或省/自治区/直辖市，请输入未知

   邮政编码
   TSA 所在位置的邮政编码。

   城市
   TSA 所在位置的城市或地区。

   街道地址
   TSA 位置地址。

   电话号码
   （可选）TSA 所在房间的电话号码。电话号码应包含区号、交换号和分机号。请勿在电话号码中使用括号。

   大厦、楼层和办公室
   （可选）TSA 所在的大厦、楼层和办公室。

下一步做什么

· 单击**保存并继续**，以保存注册信息，并继续完成“**时钟**”页面。

· 单击**后退**以返回到 **IBM Connectivity** 页面。

-或者-

· 单击**退出向导**以退出“**设置向导**”并转至**摘要**页面。

设置时钟

在设置期间，可以设置 TSA 系统时间、日期和本地时区。

过程

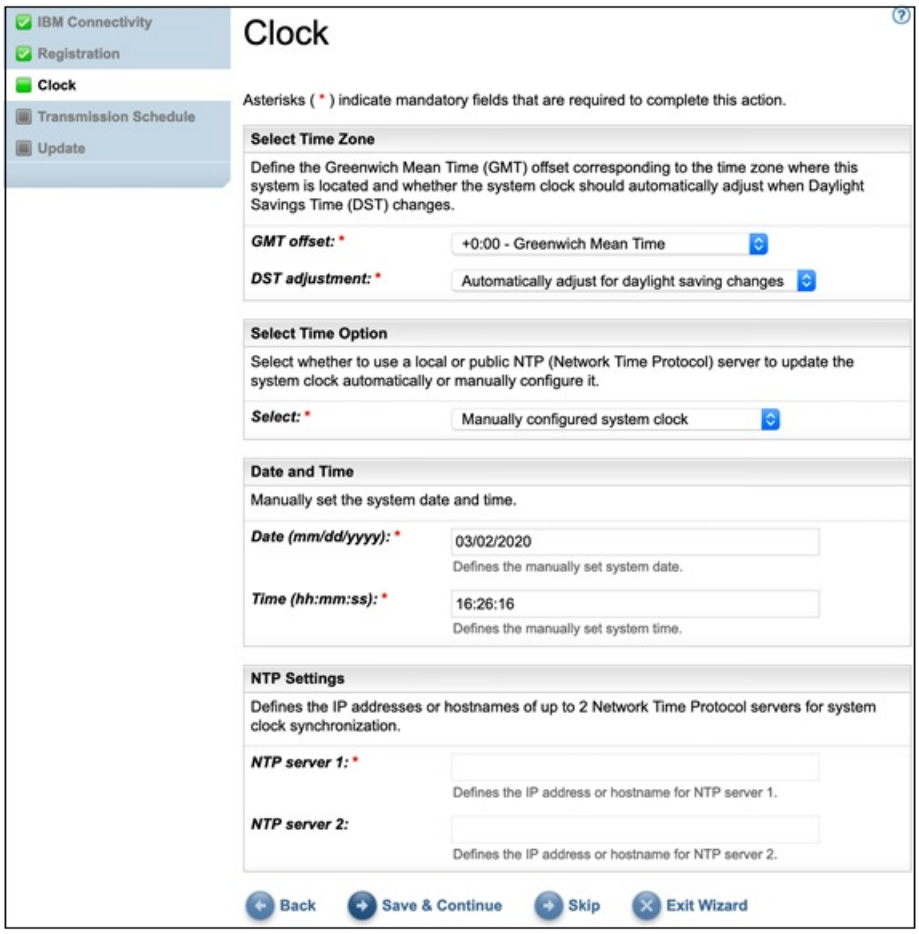

图 *25.* 时钟

1. 从 **GMT 偏移量**下拉列表中选择本地时区。
2. 从 **DST 调整**下拉列表中选择夏令时 (DST) 调整。

   注: 并非所有时区都允许 DST。如果针对不允许 DST 的时区选择了此选项，那么将显示一条错误消息。
3. 从**选择时间选项**下拉列表中选择一种方法来更新系统时钟。

   选项包括同步系统时钟与网络时间协议 (NTP) 服务器来自动更新系统时钟，或者手动配置系统时钟。

   a) 如果选择了手动配置系统时钟，那么必须设置系统日期和时间。在**日期**和**时间**字段中，输入日期和时间信息。

   b) 如果选择了同步系统时钟与网络时间协议 (NTP) 服务器来自动更新系统时钟，那么必须指定 NTP 服务器的 IP 地址和主机名。在 **NTP 服务器**字段中，输入最多两台服务器的 IP 地址或主机名信息。

      注: 确保 TSA 可通过网络来访问 NTP 服务器。

下一步做什么

· 单击**保存并继续**，以保存时钟信息，并继续完成“**传输计划安排**”页面。

-或者-

· 单击**跳过**以跳至“**传输计划安排**”页面。

修改前一个向导页面上的设置

· 单击**后退**以返回到“**注册**”页面。

退出向导

· 单击**退出向导**以退出“**设置向导**”并转至**摘要**页面。

设置传输计划安排

TSA 提供缺省计划安排以使传输过程在指定的时间运行。 您可以根据需求修改此计划安排。

过程

1. 使用**按小时**和**按分钟**下拉列表以选择新时间。
2. 选择**日期选择模式**。

周日期（周日-周六）

要将传输操作安排在一周中的某一天（或某几天），请选择**周日期（周日-周六）**选项。

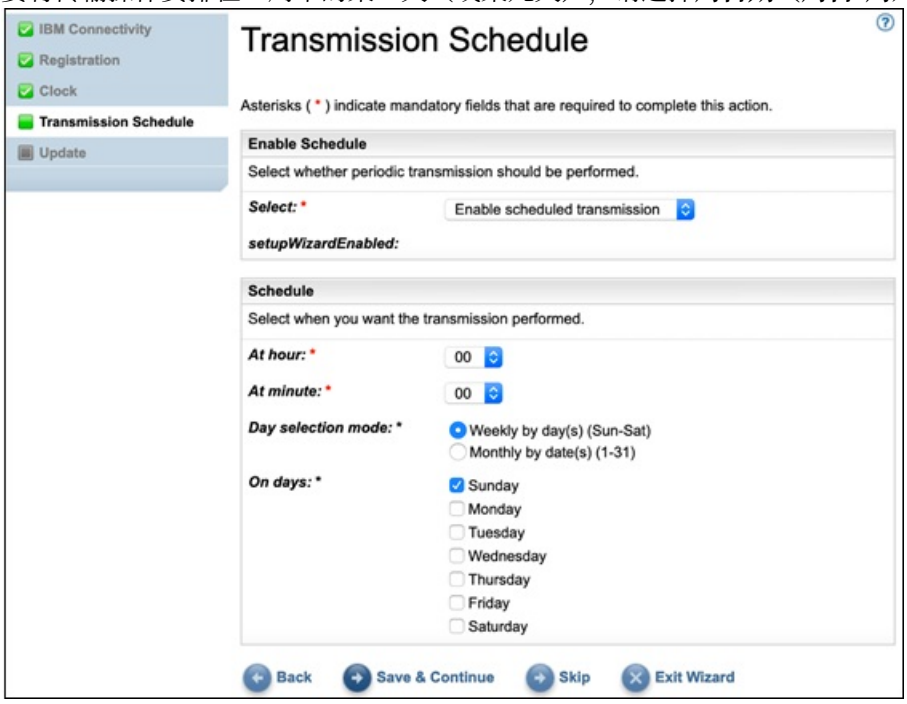

图 *26.* 周日期（周日-周六）

对于**日期**字段，选中相应复选框以选择一周中的一天或多天。

月日期 (1-31)

要将传输操作安排在一个月中的某一天（或某几天），请选择**月日期 (1-31)** 选项。

对于**日期**字段，选中相应复选框以选择一月中的一天或多天。

注: 如果选择了超过特定月份最后一天的日期，那么将在此特定月份的最后一天触发作业。

注: 确保发现开始时间早于传输时间，以避免在传输新收集数据的过程中出现长时间延迟。

下一步做什么

· 单击**保存并继续**，以保存传输计划安排，并继续完成“**更新**”页面。

-或者-

· 单击**跳过**以跳至“**更新**”页面。

修改前一个向导页面上的设置

· 单击**后退**以返回到“**时钟**”页面。

退出向导

· 单击**退出向导**以退出“**设置向导**”并转至“**摘要**”页面。

更新 Technical Support Appliance

您可以将 TSA 更新为可用的最新版本。

如果更新可用，那么会显示以下“**更新**”页面。

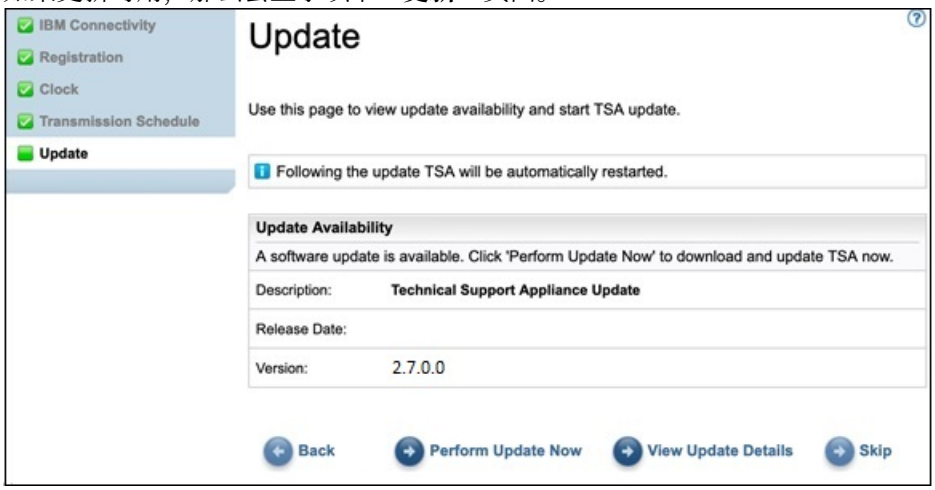

图 *27.* 更新可用性

· 单击**立即更新**以安装更新并完成“**设置向导**”。

-或者-

· 单击**查看更新详细信息**以查看更新内容的信息。

修改前一个向导页面上的设置

· 单击**后退**以返回到“**传输计划安排**”页面。

完成向导

· 单击**跳过**以完成“**设置向导**”，而不应用更新。

如果更新不可用，那么会显示以下“**更新**”页面。

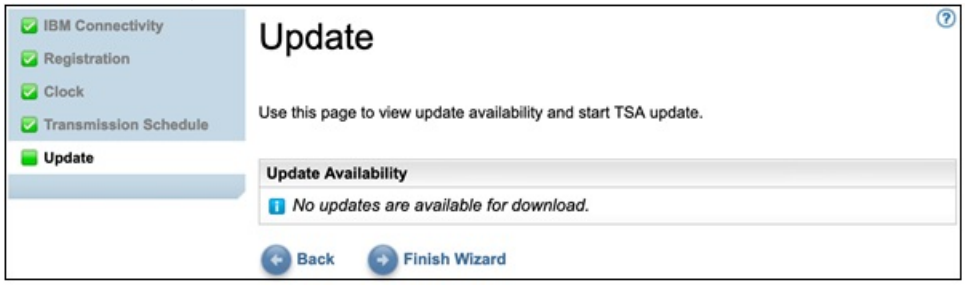

图 *28.* 无可用更新

· 单击**完成向导**以完成“**设置向导**”。 这样会显示“**已完成设置向导**”页面。

-或者-

· 单击**后退**以返回到“**传输计划安排**”页面。

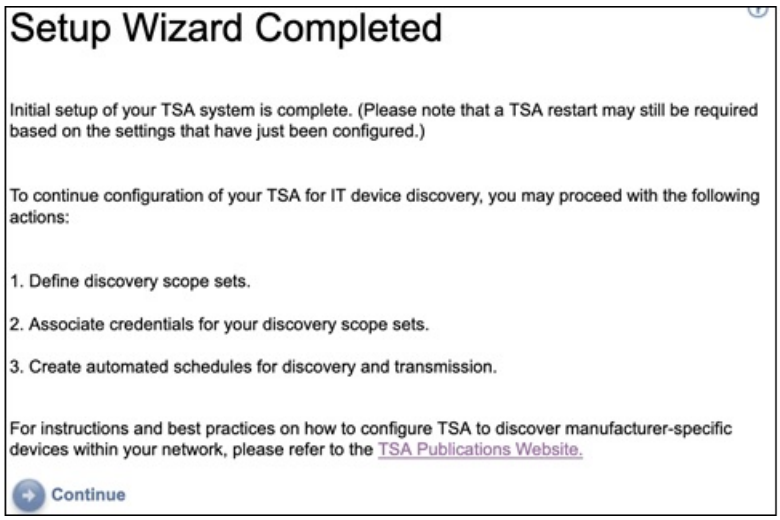

图 *29.* 设置向导已完成

· 单击**继续**以转至“**摘要**”页面。

注: 可能需要重新启动，“**时钟**”页面中的一些更改才会生效。例如，如果设置了日期或时间，或者将手动配置更改为 NTP 服务器配置，那么将提示您重新启动系统。

– 单击**确定**以完成“**设置向导**”并返回至“**摘要**”页面。这样会显示“**摘要**”页面，系统重新启动。

注: 如果退出或跳过在“**设置向导**”中配置任何设置，那么可以从 TSA 的导航窗格中手动配置。有关配置这些设置的更多信息，请参阅第 109 页的『附录 B 配置 Technical Support Appliance 』。

配置网络设置

安装 TSA 要求配置基本网络设置。如果这些设置适合您的 IT 网络，那么可以跳过此部分。

开始之前

使用“**网络**”页面执行以下任一操作：

· 更改初始基本网络设置

· 配置 TSA 以访问多个网络

要通过控制台配置基本网络设置，请执行第 17 页的『配置网络详细信息』部分中的步骤。

配置基本网络设置

使用“**网络**”页面以更改任何初始网络设置。

过程

1. 在导航窗格中，单击**管理 > 网络**。
   这样会显示“**网络**”页面。

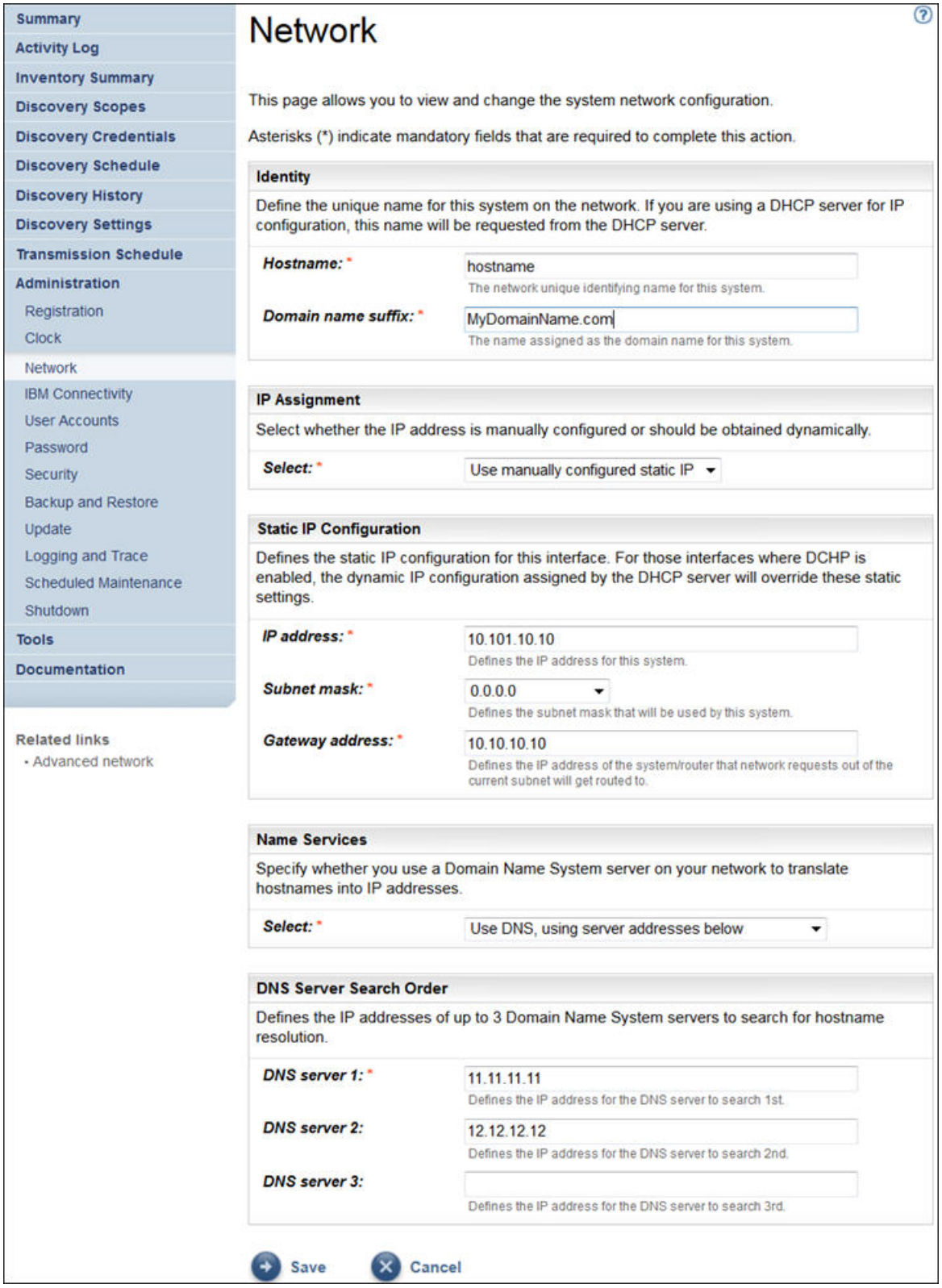

图 *30.* 网络

2. 在**主机名**字段中，指定此系统在本地网络上的唯一名称。
3. 在**域名后缀**字段中，指定在本地网络上用作此系统域名的名称。
4. 对于 *IP* 分配，选择**使用手动配置的静态 IP**。有关 DHCP 地址分配，请参阅第 119 页的『附录 C 配置 DHCP 网络详细信息』部分。
5. 配置静态 IP 地址：

a) 在 **IP 地址**字段中，输入此系统的 IP 地址。

b) 在**子网掩码**下拉列表中，选择此系统要使用的子网掩码。

c) 在**网关地址**字段中，输入处理当前子网之外的请求的系统或路由器的 IP 地址。

6. 根据 IP 分配指定“**名称服务**”。

a) 对于手动配置的静态 IP，选择**使用 DNS，使用以下服务器地址**选项。

b) 对于 DHCP IP 地址分配，选择**使用 DNS，但通过 DHCP 获取服务器地址**选项。

7. 针对域名系统 (DNS) 服务器最多输入 3 个 IP 地址以在解析主机名时使用。

   TSA 按照服务器显示顺序搜索服务器。

8. 单击**保存**可保存网络设置。

   将提示您重新启动系统。

   警告: 请谨慎更改网络设置。如果网络配置发生错误，TSA UI 可能不可访问。在此情况下，必须使用 TSA 控制台来修复网络配置：

   · 对于 VMware，使用 VMware ESXi Web 界面或 VMware vSphere Client

   · 对于 Microsoft Hyper-V，使用 Hyper-V Manager

9. 单击**取消**可退出“**网络**”页面而不保存设置。

配置高级网络设置

如果要配置 TSA 以访问多个网络，请使用“**网络（高级）**”页面来指定这些网络设置。

要配置高级网络设置，请执行以下步骤：

1. 在导航窗格中，单击**管理 > 网络**。
2. 在下方导航窗格的**相关链接**下，单击**高级网络**。

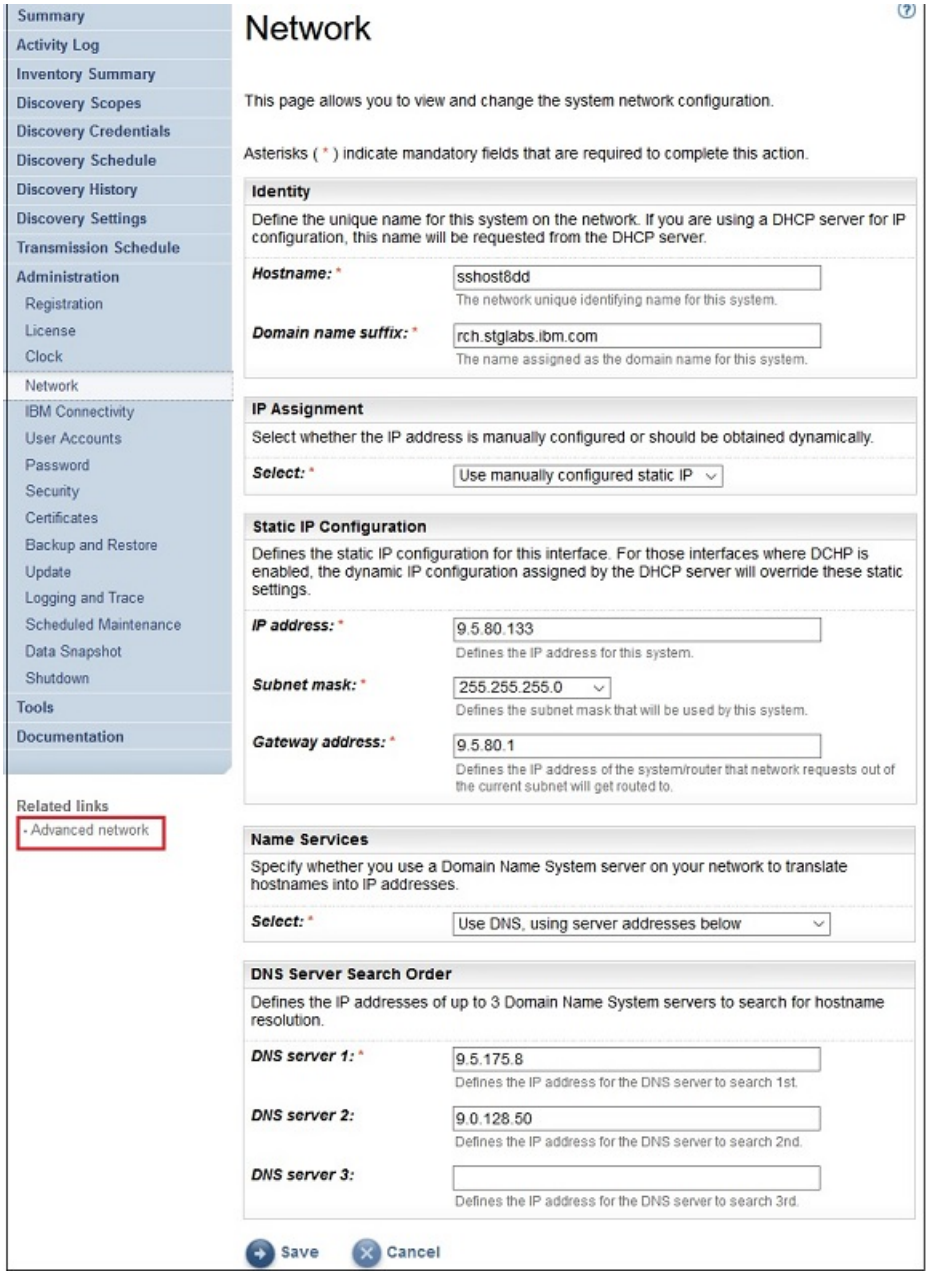

图 *31.* “访问网络（高级）”页面

这样会显示“**网络（高级）**”页面。

“**网络（高级）**”页面分为以下单独的页面：

· 全局

· 网络接口

· DNS 设置

· 网络路由

要访问这些单独的页面，请单击要显示的页面的选项卡。

要点: 在离开页面前必须单击**保存**以保存对此页面上的字段进行的更改。系统将提示您重新启动系统以使更改生效。

全局

使用此页面，可以查看和更改全局网络设置：

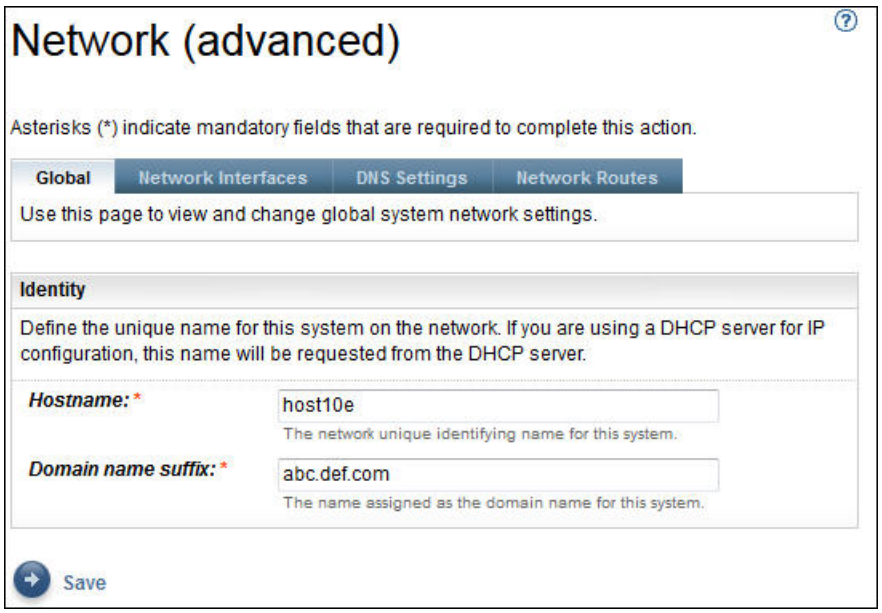

图 32. 网络（高级）- 全局

身份

定义此系统在网络上的身份。

1. 在**主机名**字段中，指定此系统的唯一名称。
2. 在**域名后缀**字段中，指定用作此系统的域名的名称。

网络接口

TSA 配置为具有两个网络接口控制器 (NIC) - eth0 和 eth1。使用此页面，可以查看和更改所选网络接口的当前设置。

1. 单击 **eth0** 以选择 eth0 网络接口。
2. 单击 **eth1** 以选择 eth1 网络接口。

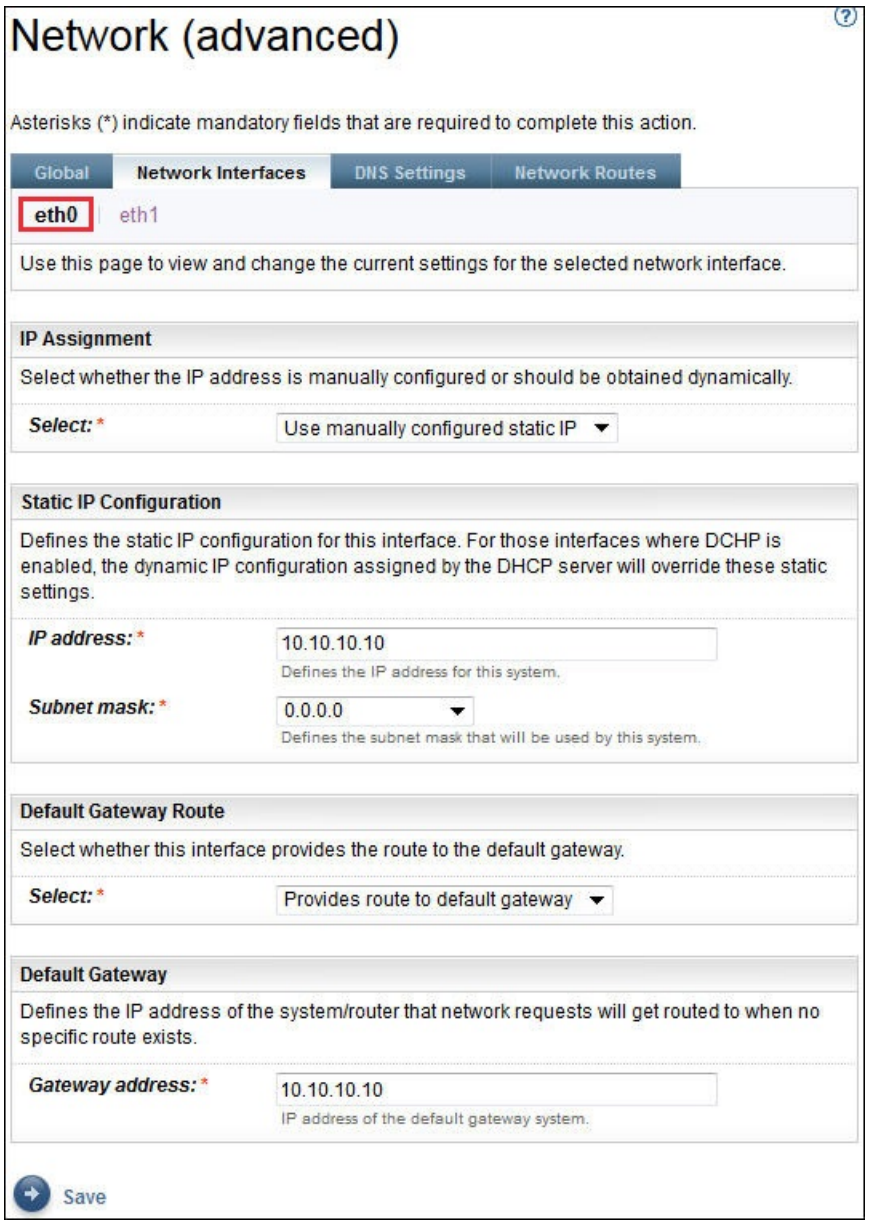

图 *33.* 网络（高级）- 网络接口

IP 分配

选择为此系统分配 IP 地址的方法。选项包括从 DHCP 服务器动态获取 IP 地址或者使用手动配置的静态 IP 地址。如果选择使用手动配置的静态 IP 地址，必须在此页面上配置系统 IP 地址。

静态 IP 配置

如果选择手动配置静态 IP 地址，请指定此网络接口的 IP 信息，如下所示：

1. 在 **IP 地址**字段中，指定此系统的 IP 地址。
2. 在**子网掩码**下拉列表中，选择此系统要使用的子网掩码。

缺省网关路由

指定此网络接口是否提供到缺省网关的路由。

缺省网关

在**网关地址**字段中，指定此系统的缺省网关的 IP 地址。

DNS 设置

使用此页面，可以查看和更改 DNS 设置。

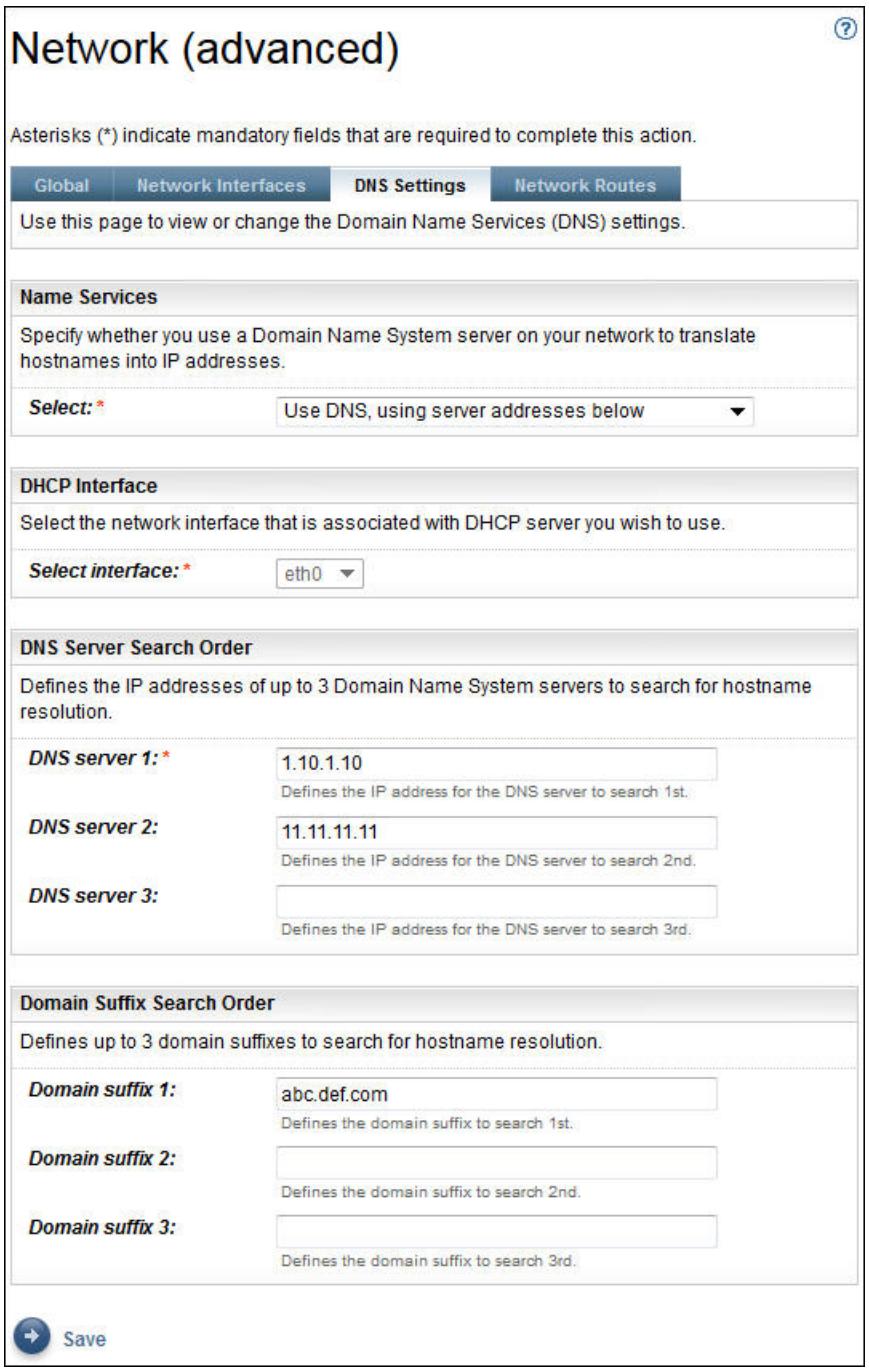

图 *34.* 网络（高级）- *DNS* 设置

名称服务

指定网络上的域名系统 (DNS) 以将主机名转换为 IP 地址。 您可以从以下选项进行选择：

- 使用 DNS，但是从 DHCP 服务器获取服务器地址。

  如果选择此选项，那么必须选择与要使用的 DHCP 服务器关联的网络接口。
- 使用 DNS 以及您指定的服务器地址。

  如果选择此选项，那么必须在此页面上至少指定一台 DNS 服务器。

DHCP 接口

选择与要使用的 DHCP 服务器关联的网络接口。

DNS 服务器搜索顺序
如果选择使用 DNS 以及您指定的服务器地址，那么针对域名系统 (DNS) 服务器最多输入 3 个 IP 地址以在解析主机名时使用。TSA 按照服务器显示顺序搜索服务器。

域后缀搜索顺序
如果选择使用 DNS 以及您指定的服务器地址，那么最多输入 3 个域名后缀以在解析主机名时使用。TSA 按照域名后缀显示顺序搜索这些域名后缀。

网络路由

使用此页面可查看、添加、更改或删除静态路由条目。

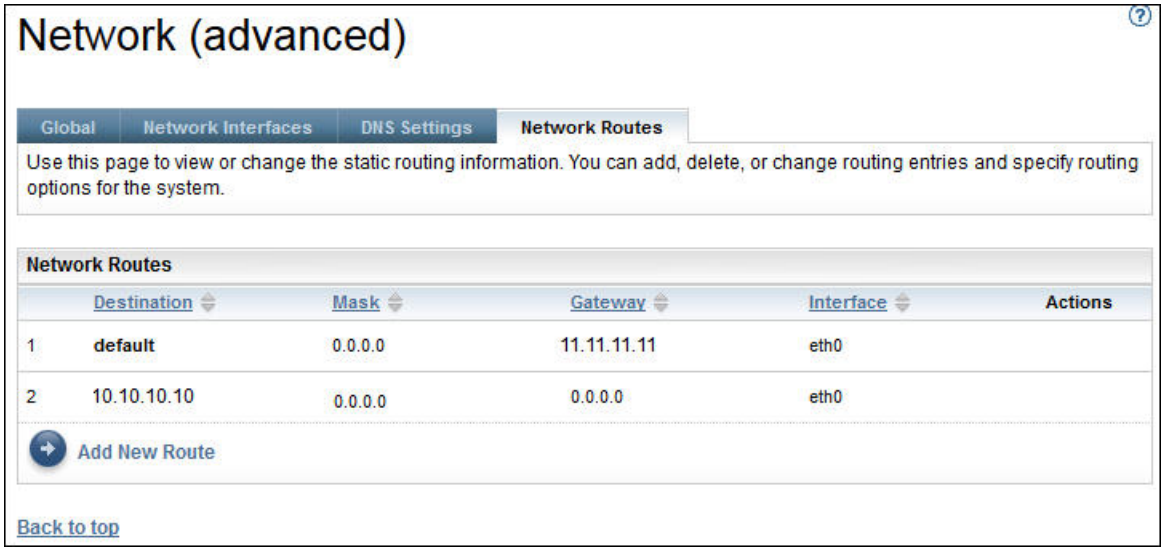

图 *35.* 网络（高级）- 网络路由

将显示每个网络路由的以下信息：

目标
指定 TCP/IP 目标网络主机或子网地址。

掩码
指定在添加路由时要用作网络掩码的子网掩码。这是 IP 地址的主机部分的子网地址。网络接口可以使用不同的子网掩码，因此能够通过选择子网掩码（可变子网路由）来添加路由。在添加路由时必须选择子网掩码，采用 32 位点分十进制表示法。

网关
指定用于路由 IP 数据包的 TCP/IP 网关地址。

接口
从菜单中选择适配器。这是与表条目相关联的网络适配器的名称。

操作
单击**删除**图标 以删除路由。

注: 图中显示的两个路由无法进行修改或删除。

单击**添加新路由**以定义新的静态网络路由。这样会显示“**网络路由**”页面。

添加网络路由

您可以添加静态网络路由。

过程

要添加网络路由，请执行以下步骤：

1. 在“**网络（高级）- 网络路由**”页面上，单击**添加新路由**。 这样会显示“**网络路由**”页面。

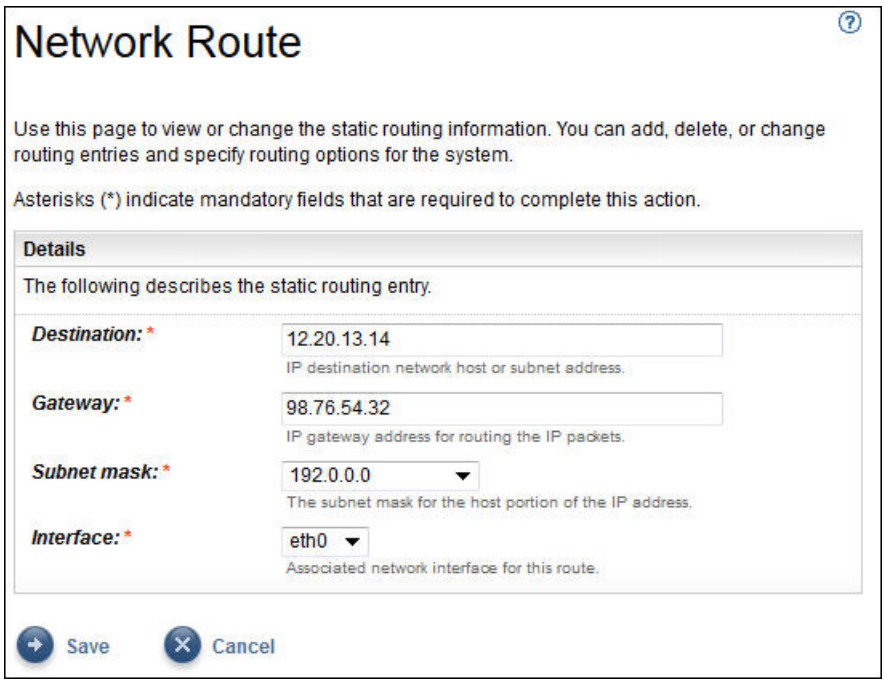

图 *36.* 新建网络路由

2. 在**目标**字段中，输入 TCP/IP 目标网络主机或子网的 IP 地址。
3. 在**网关**字段中，输入用于路由信息的 TCP/IP 网关地址。此地址必须采用 32 位点分十进制表示法。例如：`xxx.xxx.xxx.xxx`。
4. 在**子网掩码**下拉列表中，选择要用作此路由的网络掩码的子网掩码。
5. 从**接口**下拉列表中，选择要与此路由关联的网络适配器。
6. 单击**保存**以保存此网络路由。

设置证书

使用**证书**页面，可以查看证书签名信息、生成并安装证书或者导入证书。这些是访问用户界面时 TSA 向 Web 服务器提供的服务器证书。

TSA 的缺省配置实施了通用的自签名 SSL 服务器证书来简化设置过程。为了增强安全性，建议在完成初始部署和配置步骤后替换缺省证书。通过使用 TSA，可以生成并安装对于此 TSA 唯一的自签名 SSL 服务器证书、生成并安装由所选认证中心签署的自定义证书，或者上传包含自定义 SSL 服务器证书的自有 Java 密钥库文件。

您可以使用两种方法之一来安装定制证书：

· 第 40 页的『安装自定义证书（使用签署者）』
· 第 40 页的『安装自定义证书（备用方法）』

查看 SSL 服务器证书状态

配置 TSA 将安装 Technical Support Appliance 随附的缺省 TSA 证书。

过程

1. 在导航窗格中，单击**管理 > 证书**。
   这样会显示“**证书**”页面。

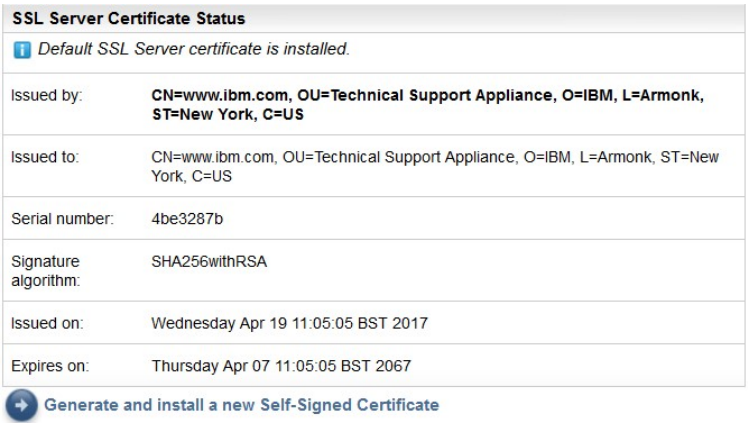

图 *37. SSL* 服务器证书状态

“**SSL 服务器证书状态**”部分显示有关安装在 TSA 中的 SSL 服务器证书的信息。证书信息包括颁发者、颁发对象、颁发日期、到期日期、序列号和签名算法。

2. 单击**生成并安装新的自签名证书**可安装此 TSA 特有的自签名证书。此时会显示一条警告消息，提示在生成并安装自签名证书后设备将自动重新启动。

   注: 生成并安装新的自签名证书按钮仅在 TSA 上安装缺省证书时才可见。

生成和下载 CSR

要申请由认证中心认证的 SSL 证书，您需要提供以下信息来生成和下载证书签名请求 (CSR) 文件。

过程

1. 在导航窗格中，单击**管理 > 证书**。
   这样会显示“**证书**”页面。

图 *38.* 证书签名请求

2. 在**通用名**字段中，输入 TSA 的标准主机名称 (FQDN)。最小字符数限制为 1，最大字符数限制为 64。
3. 在**组织单位**字段中，指定组织名称以区分组织内的各个部门。
4. 在**组织**字段中，指定公司、有限合伙公司、大学或政府机构的名称。
5. 在**城市**字段中，指定运行 TSA 的城市或地区的名称。
6. 在**省/自治区/直辖市**字段中，指定运行 TSA 的省/自治区/直辖市的名称。如果您不确定省/自治区/直辖市，或者省/自治区/直辖市不适用于您的国家或地区，请输入未知。
7. 在**国家或地区**下拉菜单中，指定运行 TSA 的国家或地区的名称。
8. 在**距离到期的天数**字段中，指定证书从创建时起算的有效天数。

9. 单击**生成并下载证书签名请求 (CSR) 文件**可创建和下载含指定信息的 CSR 文件。

   注: 要复原与 TSA 打包在一起的缺省证书，请参阅第 41 页的『复原缺省证书』部分。

安装自定义证书（使用签署者）

使用此功能可安装自定义证书。您需要由认证中心生成的服务器证书、认证中心的根证书以及认证中心的任何中级证书。

开始之前

确保证书文件（根证书、中级证书和服务器证书）采用以下任何格式:

- *.crt*
- *.der*
- *.pem*

过程

请执行以下步骤来上传证书并将其安装在 TSA 上:

1. 在导航窗格中，单击**管理 > 证书**。

   这样会显示“**证书**”页面。

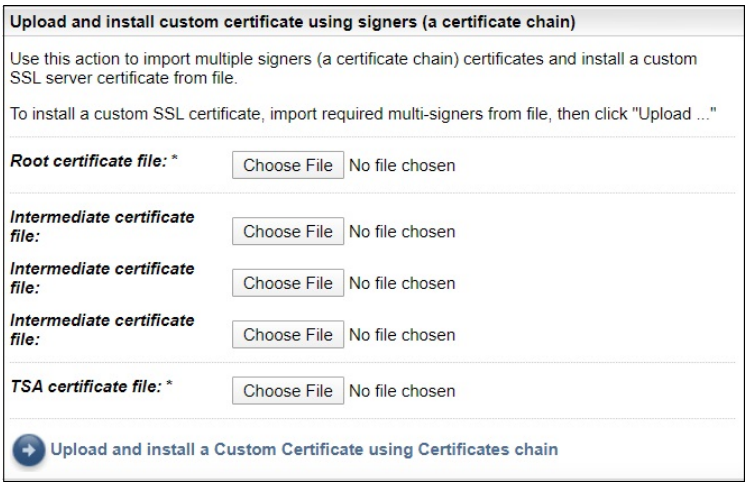

   图 *39.* 安装自定义证书

2. 在**根证书文件**字段中，指定要在 TSA 上安装的根证书文件的位置。
3. 在**中间证书文件**字段中，指定要在 TSA 上安装的中间证书文件的位置。

   注: 根据导入的多个签署者，可能存在多个（最多 3 个）中级证书文件。
4. 在 **TSA 证书文件**字段中，指定要在 TSA 上安装的 TSA 服务器证书文件的位置。
5. 单击**上传并安装使用证书链的自定义证书**可上传您指定的所有文件（根证书文件、中级证书文件 和 *TSA* 证书文件）并使用证书链安装自定义证书。

   注: 要复原与 TSA 打包在一起的缺省证书，请参阅第 41 页的『复原缺省证书』部分。

安装自定义证书（备用方法）

使用此功能可安装自定义证书。您可以使用此功能来部署已经构建的完整 Java 密钥库文件。

开始之前

建议从“**证书**”页面使用“**证书权限签名请求**”和“**使用签署者更新和安装定制证书（证书链）**”功能部署定制证书。但是，如果已单独构建完整的 Java 密钥库文件（包含密钥、自定义证书和相关 CA 证书），那么可以使用此功能来部署密钥库文件。您必须提供密钥库文件的位置和此文件的密码。

注: 在创建密钥库文件时，确保密钥输入密码和密钥库密码相同。

过程

1. 在导航窗格中，单击**管理 > 证书**。
   这样会显示“**证书**”页面。

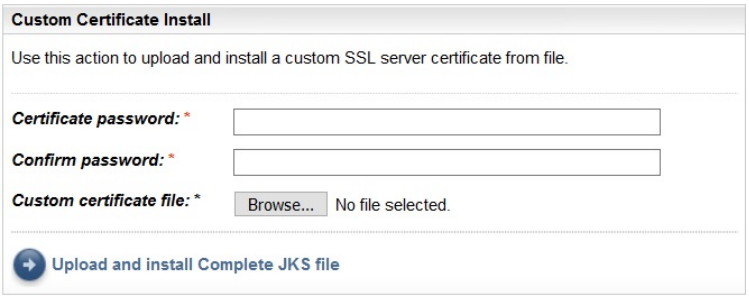

   图 *40.* 安装自定义证书

2. 要安装自定义服务器证书，请执行以下步骤。
   a) 在**证书密码**字段中输入证书的密码。
   b) 在**确认密码**字段中重新输入密码。
      比较您输入的两个密码以确认它们相互匹配，然后再保存密码。
   c) 在**自定义证书文件**字段中输入包含自定义证书的 Java 密钥库文件的位置。
   d) 单击**上传并安装完整 JKS 文件**可上传您指定的 Java 密钥库文件并安装自定义证书。Java 密钥库文件必须包含自定义证书和任何相关认证中心根证书及中级证书。设备将重新启动以激活使用新证书。

   注: 要复原与 TSA 打包在一起的缺省证书，请参阅第 41 页的『复原缺省证书』部分。

结果

安装新证书后，TSA 将自动重新启动。完成重新启动后，您的浏览器可能会显示有关是否信任新证书的安全提示。

复原缺省证书

要复原与 TSA 打包在一起的缺省证书，请使用 TSA 控制台并选择**将设备证书设置为缺省证书**选项。

过程

1. 启动 TSA 控制台。
2. 从“**TSA 配置菜单**”中选择 **3) 将设备证书设置为缺省证书**选项。

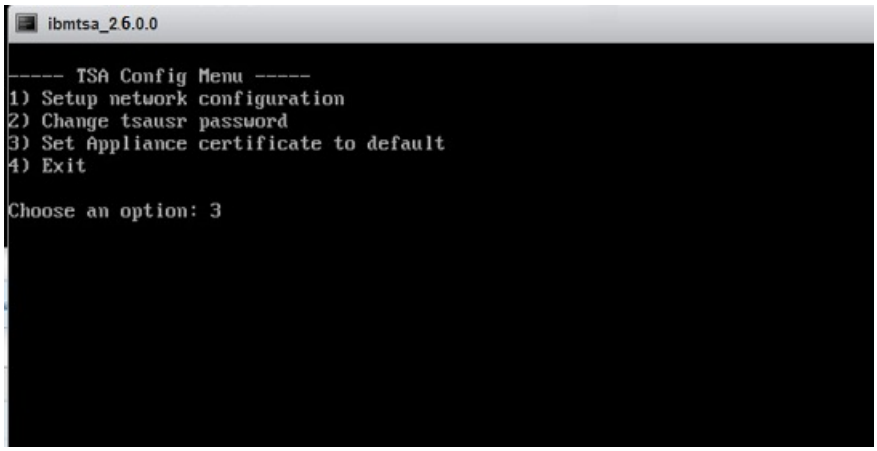

   图 *41.* 将设备证书设置为缺省证书

3. **确认将设备证书设置为缺省证书 [y|n]:** 输入 **y** 可确认将 TSA 证书设置为缺省证书。

结果

安装缺省证书后，TSA 将在 5 秒内自动重新启动。完成重新启动后，您的浏览器可能会显示有关是否信任缺省证书的安全提示。

计划库存数据清理

您可以针对在资源上收集的所有库存数据计划安排或手动运行清理任务（从发现时间开始）。

关于此任务

注意: 建议对于大多数安装，每周运行一次清理任务。

要查看库存清理任务的当前计划安排，请选择**库存摘要 > 库存清理计划安排**。

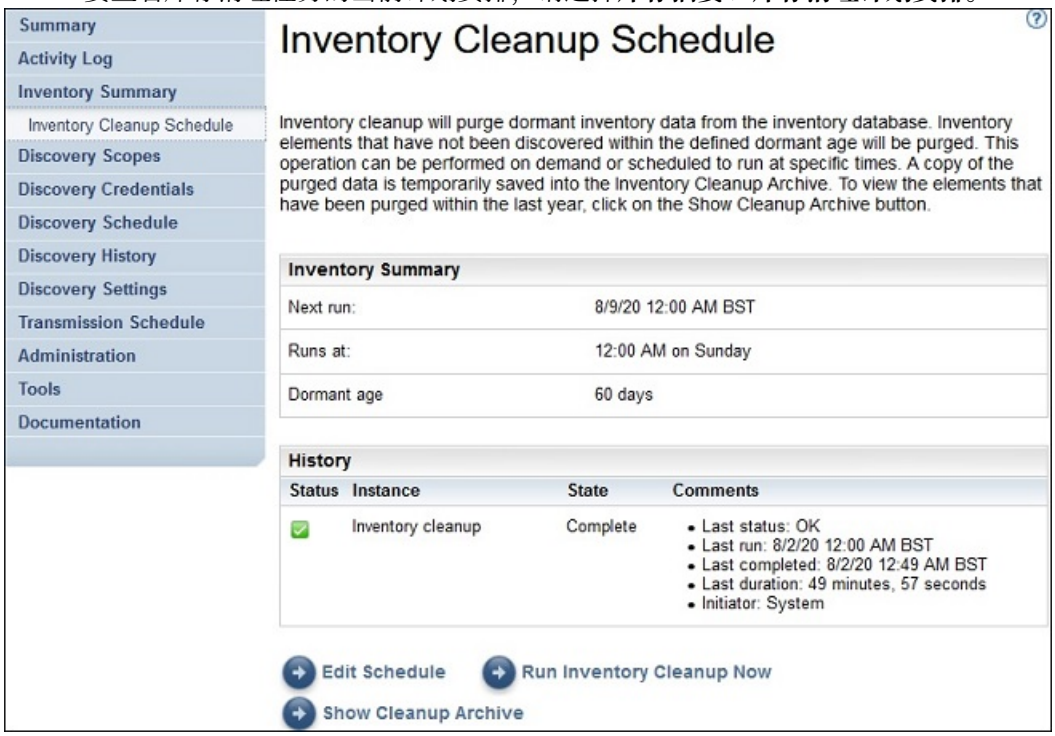

图 *42.* 库存清理计划安排

要手动运行库存清理，请单击**立即运行库存清理**。

要编辑、启用或禁用当前库存清理计划安排，请执行以下步骤：

过程

1. 在“**库存清理计划安排**”页面上，单击**编辑计划安排**。
2. 在“**库存设置**”页面上，选择**启用计划安排的库存清理**以启用库存清理任务，或者选择**禁用计划安排的库存清理**以禁用库存清理任务。
3. 如果选择启用库存清理任务，请完成以下步骤：
   a) 选择**按小时**和**按分钟**下拉列表以选择新时间。
   b) 选择**日期选择模式**。要将库存清理安排在一周中的某一天（或某几天），请选择**周日期（周日-周六）**选项；要将库存清理安排在一个月中的某一天（或某几天），请选择**月日期 (1-31)** 选项。
   c) 对于**日期**字段，选择相应的复选框以选择周或月份中的不同日期或其他日期。

   注: 如果选择了超过特定月份最后一天的日期，那么将在此特定月份的最后一天触发作业。
4. 从**休眠期**列表选择要保留库存数据的时间段。
5. 单击**保存**。

第 5 章 设置到 IBM 的发现和传输

在完成 TSA 设置后，您可以使用各种管理功能来管理发现、传输和作业。

发现作用域

发现作用域指定要用于发现 IT 元素的 IP 地址、IP 地址范围或网络。发现作用域可分组为不同的发现作用域集。

TSA 提供多种类型的发现作用域：

- HMC 动态作用域集 - 可用于发现 HMC 及其管理的所有分区。
- VMware 动态作用域集 - 可用于发现 VMware vCenter 或 ESXi 主机以及 ESXi 主机上的所有虚拟机。
- 常规发现作用域 - 用于发现使用动态作用域集未发现的所有其他资源。可手动输入 IP 地址、IP 地址范围或网络，也可以将 IP 地址列表从文件导入到 TSA 中。

HMC 动态作用域

您可以定义 HMC 动态作用域，以从 HMC、其管理的 IBM Power Systems 以及系统上的 VIOS、AIX 和 Linux LPAR 收集详细库存。

关于此任务

除了从已定义的 HMC 检索库存信息外，TSA 还会查询这些 HMC 动态管理的 LPAR，而无需创建和维护多个作用域定义。您必须为 HMC 定义一个作用域，并选择在发现这些 HMC 时要自动扫描的 LPAR 类型（AIX、VIOS 和 Linux）。其优势在于：即使 LPAR 发生更改，也无需重新配置 TSA。

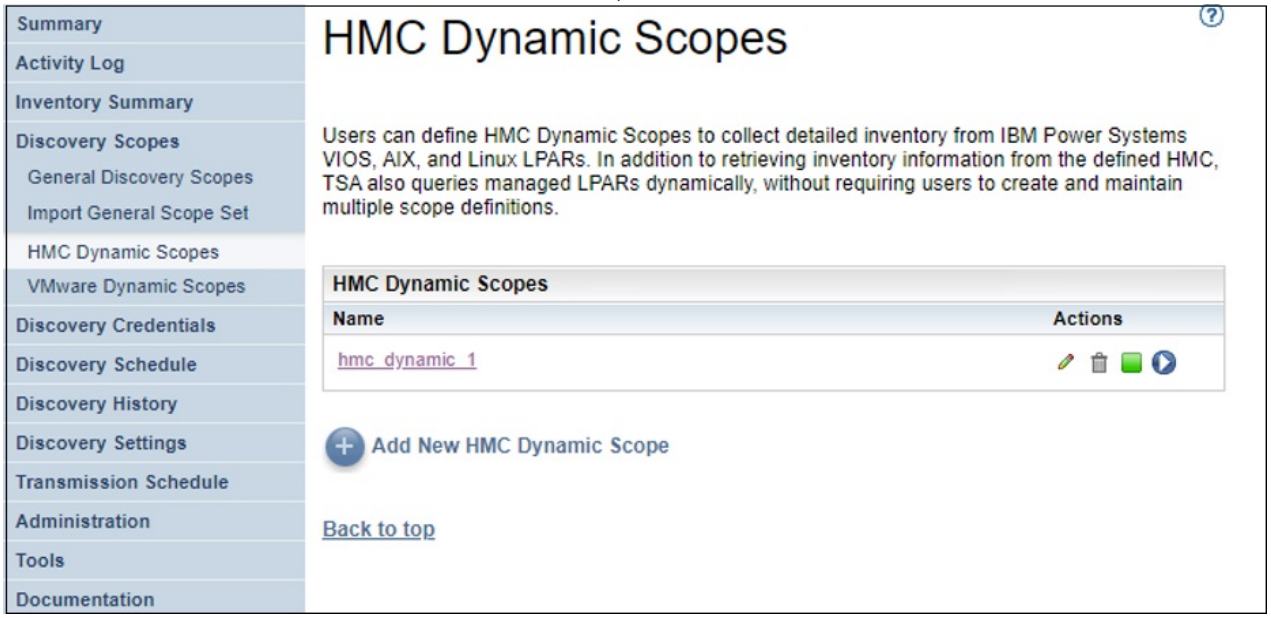

图 *43. HMC* 动态作用域

显示 HMC 动态作用域

您可以显示现有 HMC 动态作用域。

关于此任务

要显示现有 HMC 动态作用域，请单击导航窗格中的**发现作用域 > HMC 动态作用域**。这样会显示“**HMC 动态作用域**”页面。“**HMC 动态作用域**”窗格包含 HMC 动态作用域的列表。

要显示与特定动态作用域集相关联的作用域和凭证，请单击“**名称**”列中的作用域集名称。这样会显示“**HMC 动态作用域集**”页面。

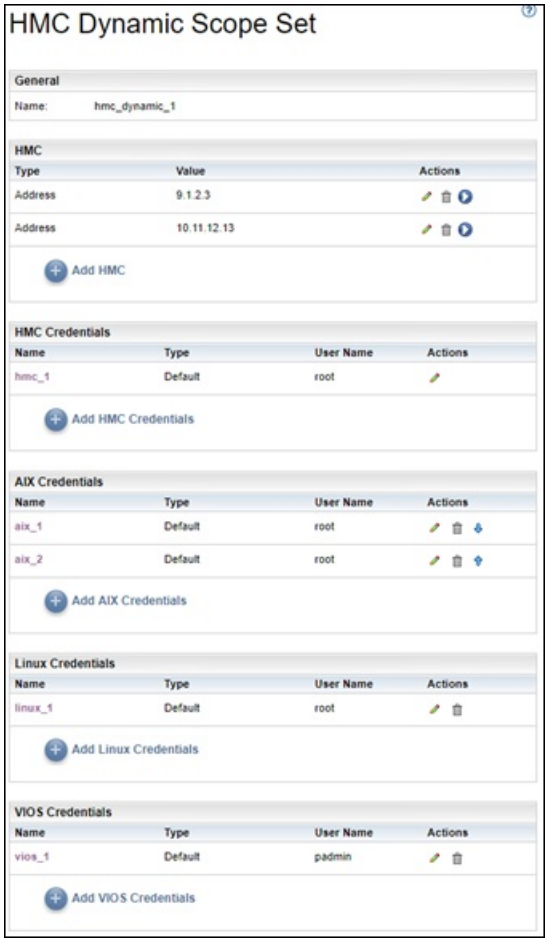

图 *44.* 查看 *HMC* 动态作用域集

HMC 窗格显示动态作用域集发现的 HMC 的 IP 地址列表。各种凭证窗格（如，“**AIX 凭证**”）列出了在作用域集中配置的凭证。

添加 HMC 动态作用域

要添加 HMC 动态作用域集，请指定单个 HMC 的 IP 地址以及用于访问 HMC 的单个凭证。（可选）您可以指定 AIX、Linux 和 VIOS 的凭证，以允许发现 HMC 管理的 IBM Power Systems 的 LPAR。创建 HMC 动态作用域集后，可以对其进行编辑以定义其他 HMC IP 地址。同时还可以编辑 HMC 动态作用域集，以支持用于访问 HMC 的多个凭证以及用于访问 LPAR 的多个凭证。

关于此任务

要添加作用域集，请执行以下步骤：

过程

1. 在导航窗格中，单击**发现作用域 > HMC 动态作用域**。
   这样会显示“**HMC 动态作用域**”页面。
2. 要定义新 HMC 动态作用域集，请单击**添加新 HMC 动态作用域**。
   这样会显示“**HMC 动态作用域集**”页面。

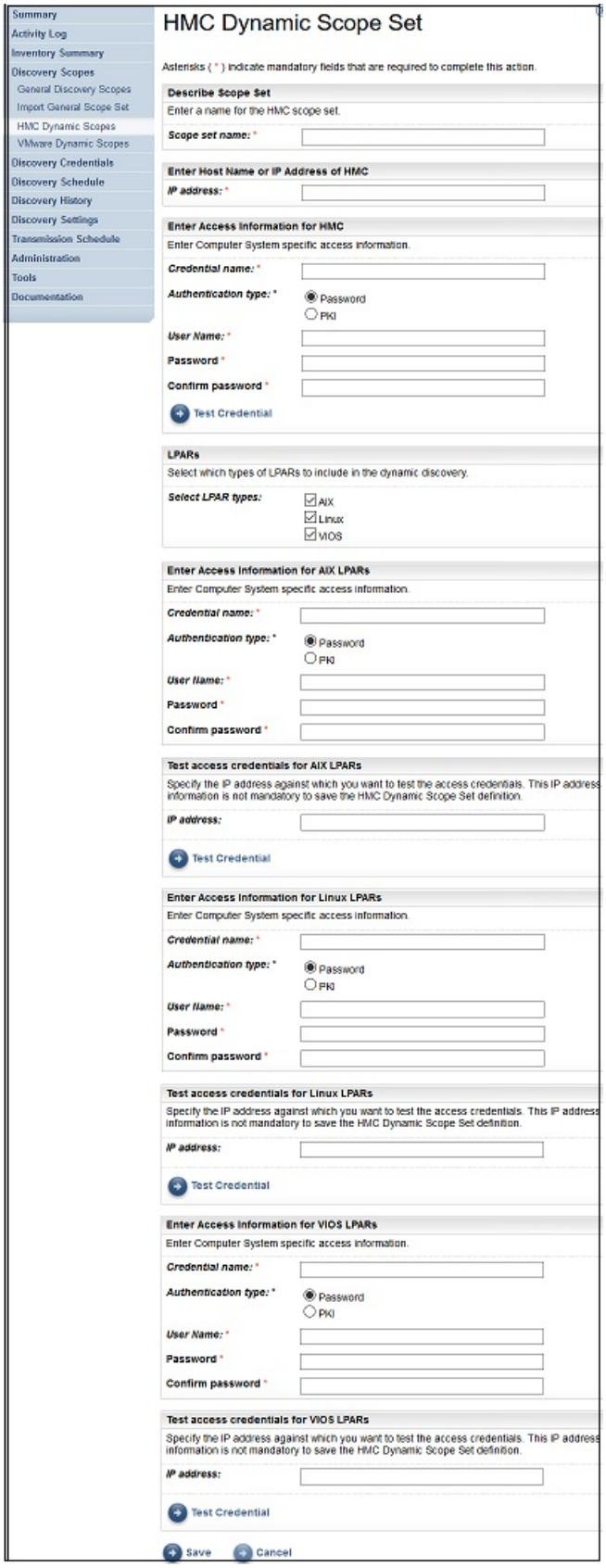

图 *45.* 添加 *HMC* 动态作用域集

3. 在“**描述作用域集**”窗格中的**作用域集名称**字段中，输入唯一名称。
4. 在“**输入 HMC 的主机名或 IP 地址**”窗格中，输入 HMC 的 IP 地址或主机名。

5. 在“**输入 HMC 的访问信息**”窗格中，输入以下详细信息 -
   a) 输入**凭证名称**
   b) 选择**认证类型**
      · **密码** - 使用所提供的密码。
      · **PKI** - 使用与特定作用域集关联的 SSH 密钥。
   c) 输入用于向 HMC 认证的**用户名**。
   d) 当**认证类型**为**密码**时，输入**密码**和**确认密码**。
   e) 当**认证类型**为 **PKI** 时，输入**口令**和**确认口令**（如果 SSH 密钥已加密）。如果 SSH 密钥未加密，请保留这两个字段为空。
   f) 如果**认证类型**为 **PKI**，请单击**选择文件**并将专用密钥上传到 TSA。必须在 HMC 上外部部署公钥。
   g) 可选： 单击**测试凭证**可测试目标 HMC 的凭证。
6. 在“**LPAR**”窗格中，选择要在动态发现中包含的 LPAR 类型（AIX、LINUX 或 VIOS）。
7. 如果您选择了任何 LPAR 类型（AIX、Linux 或 VIOS），请输入相应的访问信息。

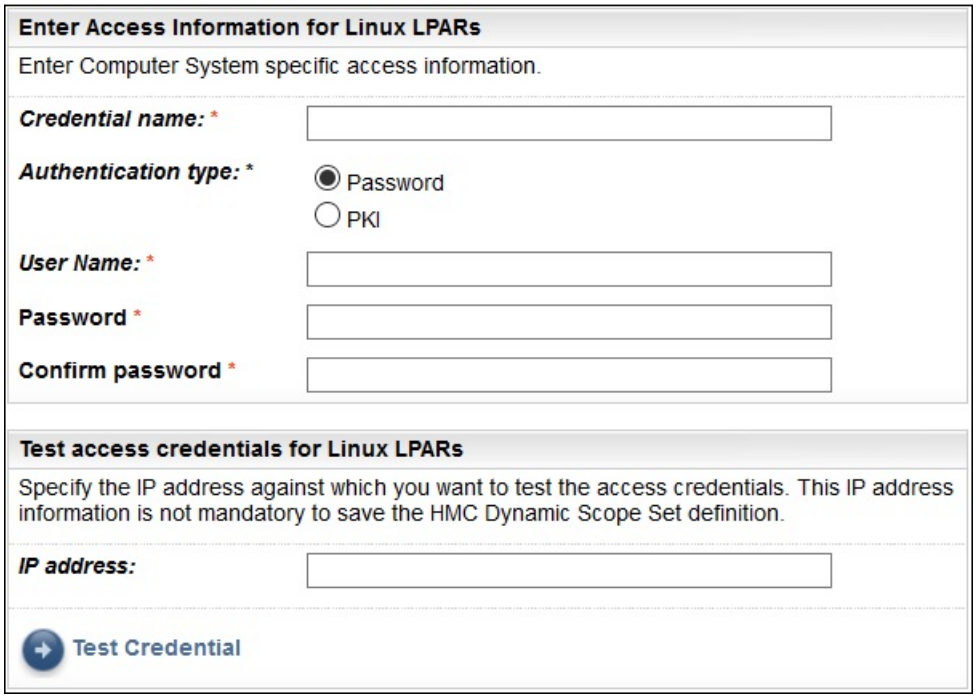

图 *46.* 示例：输入 *Linux LPAR* 的访问信息

   a) 输入**凭证名称**。
   b) 选择**认证类型**
      · **密码** - 使用所提供的密码。
      · **PKI** - 使用与特定作用域集关联的 SSH 密钥。
   c) 输入在向相应的 LPAR 进行认证时要使用的**用户名**。
   d) 当**认证类型**为**密码**时，输入**密码**和**确认密码**。
   e) 当**认证类型**为 **PKI** 时，输入**口令**和**确认口令**（如果 SSH 密钥已加密）。如果 SSH 密钥未加密，请保留这两个字段为空。
   f) 如果**认证类型**为 **PKI**，请单击**选择文件**并将专用密钥上传到 TSA。必须在每个 LPAR 上外部部署公钥。
   g) 可选： 输入此 HMC 管理的 LPAR 的 **IP 地址**，并单击**测试凭证**以测试目标 LPAR 的凭证。
8. 单击**保存**以保存该 HMC 动态作用域集。

修改 HMC 动态作用域 - HMC IP 地址

您可以修改与现有 HMC 动态作用域集关联的 HMC IP 地址的列表。

关于此任务

要修改 HMC IP 地址的列表，请执行以下步骤。

过程

1. 在导航窗格中，单击**发现作用域** > **HMC 动态作用域**。
   这样会显示“**HMC 动态作用域**”页面。
2. 要编辑作用域集，请单击 图标。
   这样会显示“**HMC 动态作用域集**”页面。
   - 要将 HMC IP 地址添加到作用域集，请执行以下步骤：
     a. 在“**HMC**”窗格中，单击**添加 HMC**。这样会显示“**HMC 动态作用域**”页面。
     b. 在“**描述地址或主机**”窗格中输入 HMC 的 **IP 地址**。
     c. 单击**保存**以添加 HMC。
   - 要编辑作用域集中的现有 HMC IP 地址，请执行以下步骤：
     a. 在 **HMC** 窗格中，单击 图标。这样会显示“**HMC 动态作用域**”页面。
     b. 在“**描述地址或主机**”窗格中修改 HMC 的 **IP 地址**。
     c. 单击**保存**以修改 HMC。
   - 要删除作用域集中的现有 HMC IP 地址，请执行以下步骤：
     a. 在 **HMC** 窗格中，单击 图标。
     b. 在对话框中，单击**确定**以确认删除。

        注: HMC 动态集作用域集必须始终至少定义一个 HMC IP 地址。TSA 不允许删除所有 HMC IP 地址。

修改 HMC 动态作用域 - 凭证

您可以修改与现有 HMC 动态作用域集关联的凭证的列表。

关于此任务

HMC 动态集作用域集必须始终至少定义一个 HMC 凭证。TSA 不允许删除所有 HMC 凭证。如果没有用于 AIX、Linux 或 VIOS 的凭证，那么 TSA 不会收集该 LPAR 类型的详细信息。

过程

1. 在导航窗格中，单击**发现作用域** > **HMC 动态作用域**。
   这样会显示“**HMC 动态作用域**”页面。
2. 要编辑作用域集，请单击 图标。
   这样会显示“**HMC 动态作用域集**”页面。
   - 要为 HMC、AIX、Linux 或 VIOS、HMC 添加凭证，请执行以下步骤：
     a. 在相应“**凭证**”窗格中，单击**添加凭证**。 例如，要添加 HMC 凭证，请在“**HMC 凭证**”窗格中单击**添加 HMC 凭证**。这样会显示“**新建 HMC 发现凭证**”页面。
     b. 输入**凭证名称**
     c. 选择**认证类型**
        – **密码** - 使用所提供的密码。
        – **PKI** - 使用与特定作用域集关联的 SSH 密钥。
     d. 输入在向 HMC 或相应的 LPAR 进行认证时要使用的**用户名**。

e. 当**认证类型**为**密码**时，输入**密码**和**确认密码**。

f. 当**认证类型**为 **PKI** 时，输入**口令**和**确认口令**（如果 SSH 密钥已加密）。如果 SSH 密钥未加密，请保留这两个字段为空。

g. 如果**认证类型**为 **PKI**，请单击**选择文件**并将专用密钥上传到 TSA。必须在 HMC 或 LPAR 上外部部署公钥。

h. **可选：** 输入 HMC 或 LPAR 的 **IP 地址**并单击**测试凭证**以测试目标 LPAR 的凭证。

i. 单击**保存**以保存该 HMC 动态作用域集凭证。

- 要编辑适用于 HMC、AIX、Linux 或 VIOS、HMC 的凭证，请执行以下步骤：

a. 在相应“**凭证**”窗格中，单击要修改的凭证的 图标。例如，要编辑 HMC 凭证，请在要修改的凭证的“**HMC 凭证**”窗格中单击 。这样会显示**编辑 HMC 发现凭证**页面。

b. 在“**输入访问信息**”窗格中，您可以修改以下详细信息 -

1) 输入在向 HMC 或相应的 LPAR 进行认证时要使用的**用户名**。

2) 选择**认证类型**

- **密码** - 使用所提供的密码。
- **PKI** - 使用与特定作用域集关联的 SSH 密钥。

3) 当**认证类型**为**密码**时，输入**密码**和**确认密码**。

4) 当**认证类型**为 **PKI** 时，输入**口令**和**确认口令**（如果 SSH 密钥已加密）。如果 SSH 密钥未加密，请保留这两个字段为空。

5) 如果**认证类型**为 **PKI**，请单击**选择文件**并将专用密钥上传到 TSA。必须在每个 HMC 或 LPAR 上外部部署公钥。

c. **可选：** 输入 HMC 或 LPAR 的 **IP 地址**并单击**测试凭证**以测试目标 LPAR 的凭证。

d. 单击**保存**可更新相应凭证的修改。

- 要删除适用于 HMC、AIX、Linux 或 VIOS 的凭证，请执行以下步骤：

a. 在相应“**凭证**”窗格中，单击相应凭证的**删除**图标。例如，要删除 HMC 凭证，请在要删除的凭证的“**HMC 凭证**”窗格中单击 图标。此时会显示一条确认消息。

b. 单击**确定**可删除相应的凭证。

- 要修改适用于 HMC、AIX、Linux 或 VIOS 的凭证的顺序，请执行以下步骤：

a. 如果存在适用于 HMC、AIX、Linux 或 VIOS 的多个凭证，那么可以修改 HMC 或 LPAR 的凭证顺序。存在单个凭证时，向上和向下箭头不会显示在凭证窗格的“**操作**”列中。

b. 在相应“**凭证**”窗格中，单击 图标或 图标，以对相应凭证进行重新排序。

启用或禁用动态作用域集

您可以启用或禁用 HMC 动态作用域集。

关于此任务

在计划的发现过程中会跳过禁用的作用域集。

注: 无论作用域集的状态如何，始终可以执行手动发现。

禁用动态作用域集

过程

要禁用 HMC 动态作用域集，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域** > **HMC 动态作用域**。
   这样会显示“**HMC 动态作用域**”页面。
2. 单击要禁用的作用域集旁边的**启用**图标。

启用动态作用域集

过程

要启用 HMC 动态作用域集，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > HMC 动态作用域**。
   这样会显示“**HMC 动态作用域**”页面。
2. 单击要启用的作用域集旁边的**禁用**图标 。

发现 HMC
您可以手动启动 HMC 动态作用域集内单个 HMC 的发现。该发现收集有关 HMC 以及与其关联的 LPAR 的信息。

过程

要手动启动 HMC 的发现，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > HMC 动态作用域**。
   这样会显示“**HMC 动态作用域**”页面。
2. 单击所需 HMC 动态作用域集的 图标。这样会显示“**HMC 动态作用域集**”页面。
3. 单击要发现的 HMC IP 地址旁边的 图标。

发现动态作用域集
您可以手动启动 HMC 动态作用域集的发现。该发现收集有关定义到作用域集的所有 HMC 的信息以及与其关联的 LPAR。

过程

要手动启动 HMC 动态作用域集的发现，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > HMC 动态作用域**。
   这样会显示“**HMC 动态作用域**”页面。
2. 单击要发现的作用域集旁边的**运行**图标 。

删除 HMC 动态作用域
您可以删除现有的 HMC 动态作用域集。

过程

要删除 HMC 动态作用域集，请执行以下步骤：

1. 在导航窗格中，单击 **HMC 动态作用域**。
   这样会显示“**HMC 动态作用域**”页面。
2. 单击要删除的作用域集旁边的**删除**图标 。
3. 单击**确定**以确认要删除 HMC 动态作用域集。

   注: 在确认删除 HMC 动态作用域集后，也会删除 AIX、Linux 或 VIOS LPAR 各自的访问信息。

VMware 动态作用域

您可以定义 VMware 动态作用域以从 VMware vCenter Server 和 ESXi 实例收集详细存库。VMware 动态作用域还收集有关 VMware vCenter Server 或 ESXi 实例管理的 x86 服务器和这些系统上 Linux 和 Windows 虚拟机的信息。

TSA 从定义的 VMware vCenter Server 和 ESXi 实例检索库存信息。TSA 还可动态查询由 VMware 实例管理的虚拟机，而无需创建和维护多个作用域定义。您必须为 VMware 实例定义一个作用域，并选择在发现这些 VMware 实例时要自动扫描的虚拟机类型（Linux 和 Windows）。其优势在于：即使虚拟机发生更改，也无需重新配置 TSA。

VMware vCenter Server 发现会查找其管理的所有 VMware ESXi 实例，而无需直接发现 VMware ESXi 实例。对于不是由 VMware vCenter Server 管理的任何 VMware ESXi 实例，可以通过在 VMware 动态作用域中定义 VMware ESXi，由 TSA 直接发现这些实例。

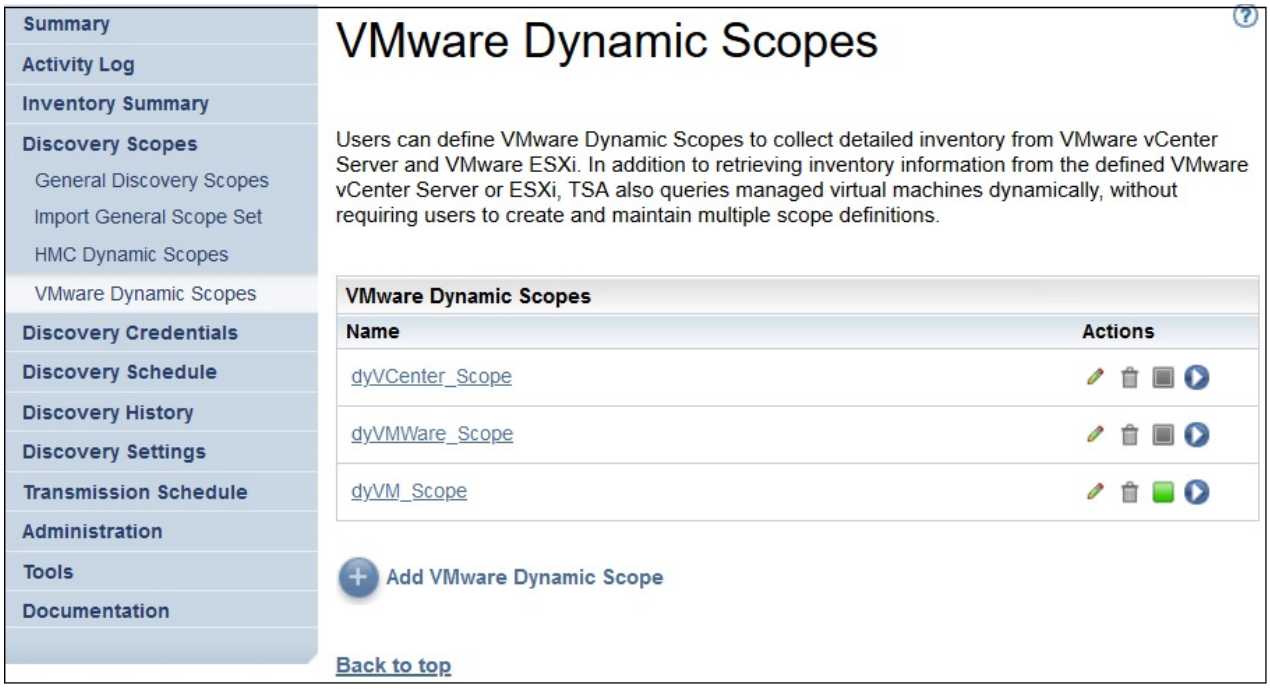

图 *47. VMware* 动态作用域

显示 VMware 动态作用域、作用域集和凭证
您可以显示现有 VMware 动态作用域和作用域集。

关于此任务

要显示现有 VMware 动态作用域集，请单击导航窗格中的**发现作用域 > VMware 动态作用域**。这样会显示“**VMware 动态作用域**”页面。“**VMware 动态作用域**”窗格包含 VMware 动态作用域的列表。

要显示与特定动态作用域集相关联的作用域和凭证，请单击“**名称**”列中的作用域集名称。这样会显示“**VMware 动态作用域集**”页面。

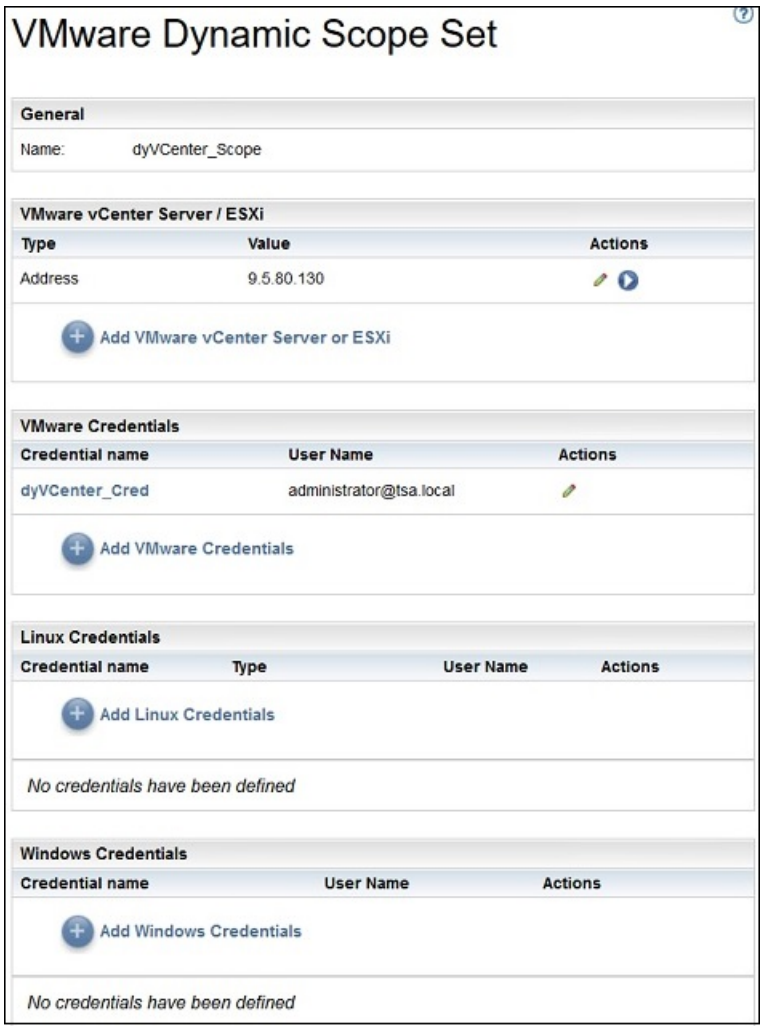

图 *48.* 查看 *VMware* 动态作用域集

VMware vCenter Server/ESXi 窗格显示动态作用域集发现的 VMware vCenter Server 和 ESXi 实例的 IP 地址列表。各种凭证窗格（如，“**Linux 凭证**”）列出了在作用域集中配置的凭证。

添加 VMware 动态作用域

要添加 VMware 动态作用域集，请指定单个 VMware vCenter Server 或 ESXi 实例的 IP 地址以及用于访问 VMware 实例的单个凭证。（可选）您可以指定 Linux 和 Windows 的凭证，以允许发现 VMware 实例管理的 x86 服务器的虚拟机。创建 VMware 动态作用域集后，可以对其进行编辑以定义其他 VMware vCenter Server 或 ESXi IP 地址。同时还可以编辑 VMware 动态作用域集，以支持用于访问 VMware 实例的多个凭证以及用于访问虚拟机的多个凭证。

关于此任务

要添加 VMware 动态作用域集，请执行以下步骤：

过程

1. 在导航窗格中，单击**发现作用域 > VMware 动态作用域**。
   这样会显示“**VMware 动态作用域**”页面。
2. 要定义新 VMware 动态作用域集，请单击**添加 VMware 动态作用域**。
   这样会显示“**VMware 动态作用域集**”页面。

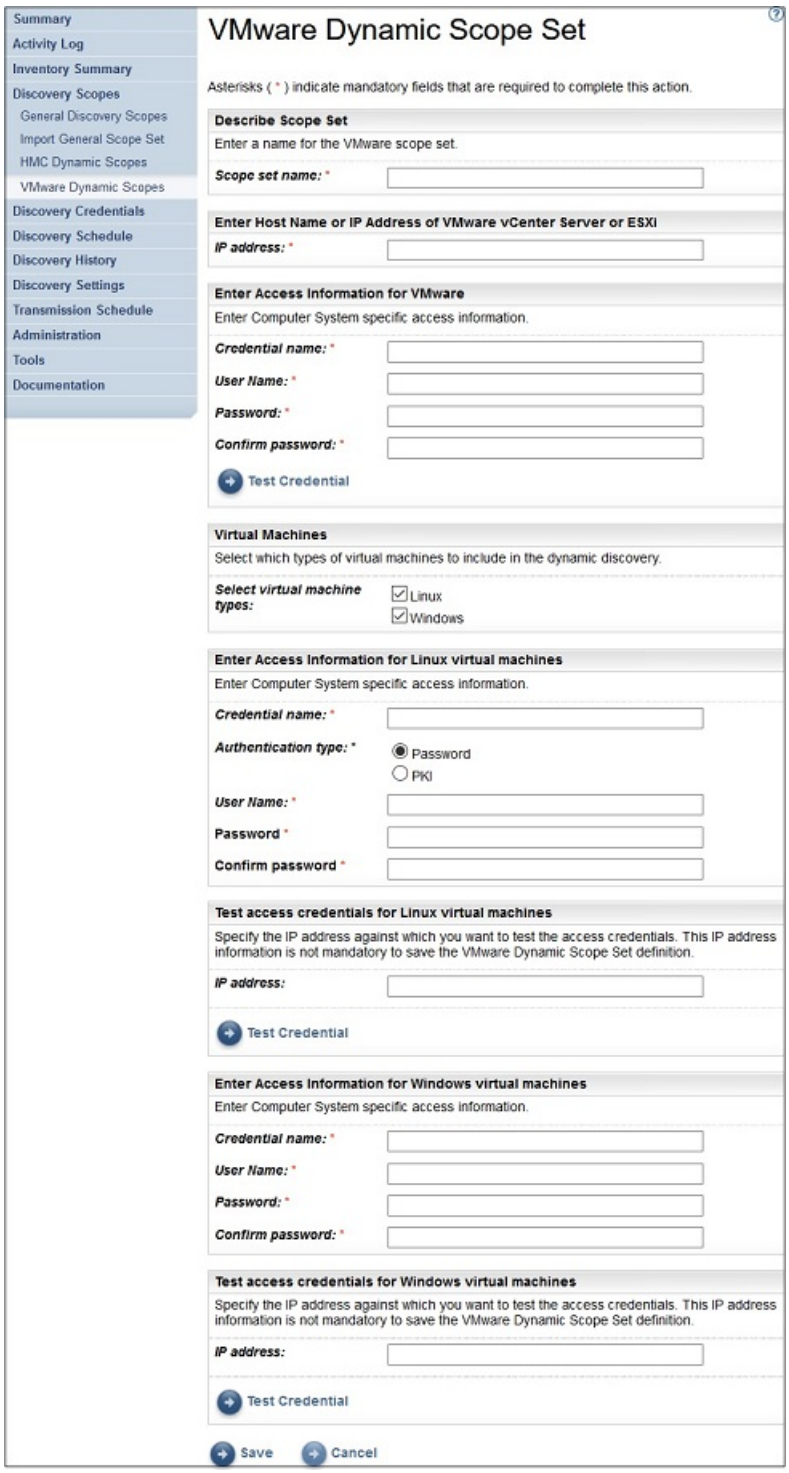

图 *49.* 添加 *VMware* 动态作用域集

3. 在“**描述作用域集**”窗格中的**作用域集名称**字段中，输入唯一名称。
4. 在“**输入 VMware vCenter Server 或 ESXi 的主机名或 IP 地址**”窗格中，输入 vCenter Server 或 ESXi 实例的 IP 地址或主机名。
5. 在“**输入 VMware 的访问信息**”窗格中，输入以下详细信息 -
   a) 输入**凭证名称**
   b) 输入向 VMware vCenter Server 或 ESXi 实例认证所用的**用户名**。
   c) 输入**密码**和**确认密码**
   d) 可选： 单击**测试凭证**以测试目标 VMware vCenter Server 或 ESXi 实例的凭证。

6. 在“**虚拟机**”窗格中，选择要在动态发现中包含的虚拟机（Linux 或 Windows）。
7. 如果选择 Linux 虚拟机，请输入相应的访问信息。

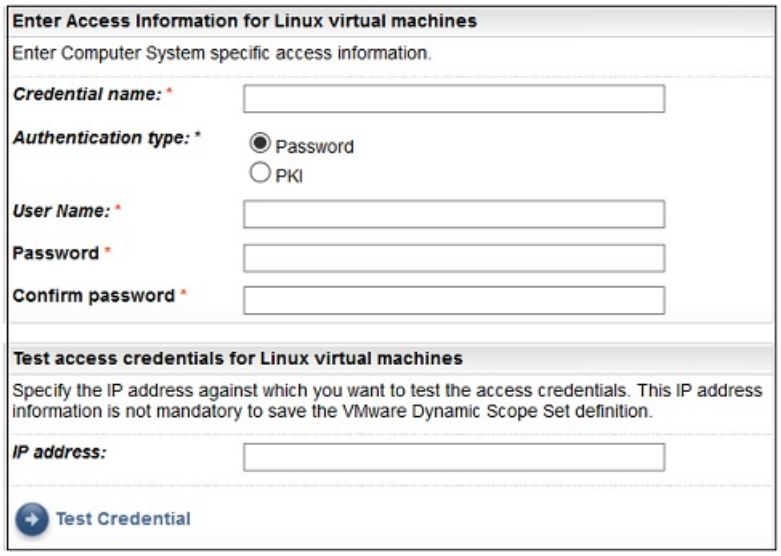

图 *50.* 输入 *Linux* 虚拟机的访问信息

a) 输入**凭证名称**。

b) 选择**认证类型**

- **密码** - 使用所提供的密码。
- **PKI** - 使用与特定作用域集关联的 SSH 密钥。

c) 输入在向相应的虚拟机进行认证时要使用的**用户名**。

d) 当**认证类型**为**密码**时，输入**密码**和**确认密码**。

e) 当**认证类型**为 **PKI** 时，输入**口令**和**确认口令**（如果 SSH 密钥已加密）。如果 SSH 密钥未加密，请保留这两个字段为空。

f) 如果**认证类型**为 **PKI**，请单击**选择文件**并将专用密钥上传到 TSA。必须在每个虚拟机上外部部署公钥。

g) 可选： 输入虚拟机的 **IP 地址**，并单击**测试凭证**以测试目标虚拟机的凭证。

8. 如果选择 Windows 虚拟机，请输入相应的访问信息。

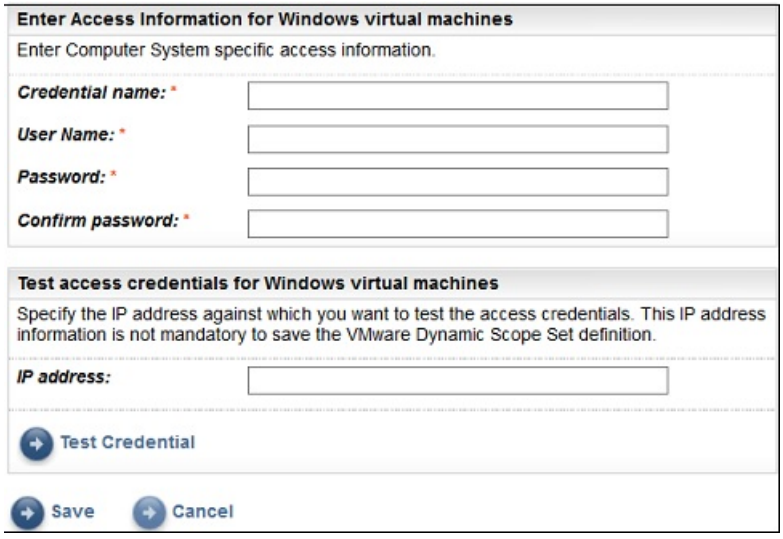

图 *51.* 输入 *Windows* 虚拟机的访问信息

a) 输入**凭证名称**。

b) 输入在向相应的虚拟机进行认证时要使用的**用户名**。

c) 输入**密码**和**确认密码**。

d) 可选： 输入虚拟机的 **IP 地址**，并单击**测试凭证**以测试目标虚拟机的凭证。

9. 单击**保存**以保存该 VMware 动态作用域集。

修改 VMware 动态作用域 - VMware vCenter Server 或 ESXi IP 地址

您可以修改与现有 VMware 动态作用域集关联的 VMware vCenter Server 或 ESXi IP 地址的列表。

关于此任务

要修改 IVMware vCenter Server 或 ESXi IP 地址的列表，请执行以下步骤。

过程

1. 在导航窗格中，单击**发现作用域 > VMware 动态作用域**。
   这样会显示“**VMware 动态作用域**”页面。
2. 要编辑作用域集，请单击 图标。
   这样会显示“**VMware 动态作用域集**”页面。
   - 要将 VMware vCenter Server 或 ESXi IP 地址添加到作用域集，请执行以下步骤：
     a. 在 **VMware vCenter Server/ESXi** 窗格中，单击**添加 VMware vCenter Server 或 ESXi**。这样会显示“**VMware 动态作用域**”页面。
     b. 在“**描述地址或主机**”窗格中输入 VMware vCenter Server 或 ESXi 的 **IP 地址**。
     c. 单击**保存**以添加 VMware vCenter Server 或 ESXi 实例。
   - 要编辑作用域集中的现有 VMware vCenter Server 或 ESXi IP 地址，请执行以下步骤：
     a. 在 **VMware vCenter Server/ESXi** 窗格中，单击 图标。这样会显示“**VMware 动态作用域**”页面。
     b. 在“**描述地址或主机**”窗格中修改 VMware vCenter Server 或 ESXi 实例的 **IP 地址**。
     c. 单击**保存**。
   - 要删除作用域集中的现有 VMware vCenter Server 或 ESXi IP 地址，请执行以下步骤：
     a. 在 **VMware vCenter Server/ESXi** 窗格中，单击 图标。
     b. 在对话框中，单击**确定**以确认删除。

        注: VMware 动态作用域集必须始终至少定义一个 VMware vCenter Server 或 ESXi IP 地址。TSA 不允许删除所有 VMware IP 地址。

修改 VMware 动态作用域 - 凭证

您可以修改与现有 VMware 动态作用域集关联的凭证的列表。

关于此任务

VMware 动态作用域集必须始终至少定义一个 VMware 凭证。TSA 不允许删除所有 VMware 凭证。如果没有用于 Linux 或 Windows 的凭证，那么 TSA 不会收集有关该虚拟机类型的详细信息。

过程

1. 在导航窗格中，单击**发现作用域 > VMware 动态作用域**。
   这样会显示“**VMware 动态作用域**”页面。
2. 要编辑作用域集，请单击 图标。
   这样会显示“**VMware 动态作用域集**”页面。
   - 要添加 VMware 或 Windows 的凭证，请执行以下步骤：
     a. 在相应“**凭证**”窗格中，单击**添加凭证**。 例如，要添加 VMware 凭证，请在“**VMWare 凭证**”窗格中单击**添加 VMWare 凭证**。这样会显示“**新建 VMware 发现凭证**”页面。

b. 输入**凭证名称**

c. 输入用于向 VMware vCenter Server、ESXi 实例或 Windows 虚拟机进行认证的**用户名**。

d. 输入**密码**和**确认密码**。

e. **可选：**输入 VMware vCenter Server、ESXi 实例或 Windows 虚拟机的 **IP 地址**，并单击**测试凭证**以测试目标的凭证。

f. 单击**保存**可保存相应的凭证。

- 要添加 Linux 的凭证，请执行以下步骤：

a. 在“**Linux 凭证**”窗格中，单击**添加 Linux 凭证**。这样会显示“**新建 VMware 发现凭证**”页面。

b. 输入**凭证名称**

c. 选择**认证类型**

- **密码** - 使用所提供的密码。
- **PKI** - 使用与特定作用域集关联的 SSH 密钥。

d. 输入用于向 Linux 虚拟机进行认证的**用户名**。

e. 当**认证类型**为**密码**时，输入**密码**和**确认密码**。

f. 当**认证类型**为 **PKI** 时，输入**口令**和**确认口令**（如果 SSH 密钥已加密）。如果 SSH 密钥未加密，请保留这两个字段为空。

g. 如果**认证类型**为 **PKI**，请单击**选择文件**并将专用密钥上传到 TSA。必须在 Linux 虚拟机上外部部署公钥。

h. **可选：**输入 Linux 虚拟机的 **IP 地址**并单击**测试凭证**以测试目标 Linux 虚拟机的凭证。

i. 单击**保存**以保存 Linux 凭证。

- 要编辑 VMware 或 Windows 的凭证，请执行以下步骤：

a. 在相应“**凭证**”窗格中，单击要修改的凭证的 图标。例如，要编辑 VMware 凭证，请在要修改的凭证的“**VMware 凭证**”窗格中单击 。这样会显示“**编辑 VMware 发现凭证**”页面。

b. 在“**输入访问信息**”窗格中，您可以修改以下详细信息 -

1) 输入连接到 VMware vCenter Server、ESXi 实例或 Windows 虚拟机时要用于认证的**用户名**。

2) 输入**密码**和**确认密码**。

c. **可选：**输入 VMware vCenter Server、ESXi 实例或 Windows 虚拟机的 **IP 地址**，并单击**测试凭证**以测试目标的凭证。

d. 单击**保存**可更新相应凭证的修改。

- 要编辑 Linux 的凭证，请执行以下步骤：

a. 在“**Linux 凭证**”窗格中，单击要修改的凭证的 图标。这样会显示“**编辑 VMware 发现凭证**”页面。

b. 在“**输入访问信息**”窗格中，您可以修改以下详细信息 -

1) 选择**认证类型**

- **密码** - 使用所提供的密码。
- **PKI** - 使用与特定作用域集关联的 SSH 密钥。

2) 输入用于向 Linux 虚拟机进行认证的**用户名**。

3) 当**认证类型**为**密码**时，输入**密码**和**确认密码**。

4) 当**认证类型**为 **PKI** 时，输入**口令**和**确认口令**（如果 SSH 密钥已加密）。如果 SSH 密钥未加密，请保留这两个字段为空。

5) 如果**认证类型**为 **PKI**，请单击**选择文件**并将专用密钥上传到 TSA。必须在 Linux 虚拟机上外部部署公钥。

6) **可选：**输入虚拟机的 **IP 地址**并单击**测试凭证**以测试目标 Linux 虚拟机的凭证。

c. 单击**保存**可更新相应凭证的修改。

- 要删除 VMware、Linux 或 Windows 的凭证，请执行以下步骤：
  a. 在相应“**凭证**”窗格中，单击相应凭证的**删除**图标。例如，要删除 VMware 凭证，请在要删除的凭证的“**VMware 凭证**”窗格中单击 图标。此时会显示一条确认消息。
  b. 单击**确定**可删除相应的凭证。
- 要修改 VMware、Linux 或 Windows 的凭证的顺序，请执行以下步骤：
  a. 如果存在适用于 VMware、Linux 或 Windows 的多个凭证，那么可以修改 VMware 或虚拟机的凭证顺序。存在单个凭证时，向上和向下箭头不会显示在凭证窗格的“**操作**”列中。
  b. 在相应“**凭证**”窗格中，单击 图标或 图标，以对相应凭证进行重新排序。

启用或禁用动态作用域集
您可以启用或禁用 VMware 动态作用域集。

关于此任务

在计划的发现过程中会跳过禁用的作用域集。

注: 无论作用域集的状态如何，始终可以执行手动发现。

禁用动态作用域集

过程

要禁用 VMware 动态作用域集，请执行以下步骤：
1. 在导航窗格中，单击**发现作用域 > VMware 动态作用域**。
   这样会显示“**VMware 动态作用域**”页面。
2. 单击要禁用的作用域集旁边的**启用**图标。

启用动态作用域集

过程

要启用 VMware 动态作用域集，请执行以下步骤：
1. 在导航窗格中，单击**发现作用域 > VMware 动态作用域**。
   这样会显示“**VMware 动态作用域**”页面。
2. 单击要启用的作用域集旁边的**禁用**图标。

发现 VMware vCenter 或 ESXi
您可以手动启动 VMware 动态作用域集内单个 VMware vCenter Server 或 ESXi 的发现。该发现收集有关 VMware 实例以及与其关联的虚拟机的信息。

过程

要手动启动 VMware vCenter Server 或 ESXi 的发现，请执行以下步骤：
1. 在导航窗格中，单击**发现作用域 > VMware 动态作用域**。
   这样会显示“**VMware 动态作用域**”页面。
2. 单击所需 VMware 动态作用域集的 图标。这样会显示“**VMware 动态作用域集**”页面。
3. 单击要发现的 VMware vCenter Server 或 ESXi IP 地址旁边的 图标。

发现动态作用域集

您可以手动启动 VMware 动态作用域集的发现。该发现收集有关定义到作用域集的所有 VMware vCenter Server 或 ESXi 实例以及与其关联的虚拟机的信息。

过程

要手动启动 VMware 动态作用域集的发现，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > VMware 动态作用域**。
   这样会显示“**VMware 动态作用域**”页面。
2. 单击要发现的作用域集旁边的**运行**图标 。

删除 VMware 动态作用域

您可以删除现有的 VMware 动态作用域集。

过程

要删除 VMware 动态作用域集，请执行以下步骤：

1. 在导航窗格中，单击 **VMware 动态作用域**。
   这样会显示“**VMware 动态作用域**”页面。
2. 单击要删除的作用域集旁边的**删除**图标 。
3. 单击**确定**以确认要删除 VMware 动态作用域集。

   注: 在确认删除 VMware 动态作用域集后，也会删除 Linux 或 Windows 虚拟机各自的访问信息。

常规发现作用域

发现过程会搜索基础架构中的 IT 元素。发现作用域会定义发现过程中所发现的单个 IP 地址或范围。发现作用域可分组为用户命名的作用域集。

显示发现作用域和作用域集

您可以显示现有发现作用域和作用域集。

关于此任务

要显示现有发现作用域集，请单击导航窗格中的**发现作用域 > 常规发现作用域**。这样会显示“**常规发现作用域**”页面。“**常规发现作用域**”窗格包含作用域集列表。

要显示某个作用域集包含的作用域，请单击该作用域集。这样会显示“**发现作用域集**”页面。

- “**常规**”窗格显示作用域集的名称。
- “**IP 地址计数**”窗格显示特定作用域集中的 IP 地址总数。
- “**作用域**”窗格显示有关作用域集中作用域的详细信息。

添加发现作用域

您可以添加作用域集并向其中添加新作用域、向现有作用域集添加作用域或者将作用域移到其他作用域集。要添加作用域，请指定有效的 IP 地址、IP 地址范围、网络或子网。

关于此任务

提示: 以下是设置发现作用域和作用域集的实际注意事项。

- 发现作用域中的 IP 地址越多，发现所需的时间就越长。通过禁用或启用作用域集或从作用域集内的作用域中排除 IP 地址、IP 地址范围、网络或子网，可以修改发现规模。

  为了最大程度地缩短发现所需的时间，请将发现作用域的目标设置为仅要发现的这些元素，并禁用作用域集或者排除不想要或不需要发现的 IP 地址、IP 地址范围、网络或子网。

  注: 为提高性能，请将作用域集中的 IP 地址总数限制为 400 或更少。 有关导入作用域集的信息，请参阅第 61 页的『导入作用域集』部分

· 并非所有元素都相等。例如，与单个主机相比，具有数十个接口的路由器可能需要更长的时间才能完全发现。

· 如果将 PKI 认证用于设备发现，那么只能将一个 SSH 密钥与每个作用域集相关联。

有关设置发现作用域的最佳实践的更多信息，请参阅《TSA 配置助手指南》。

要添加作用域集和作用域，请执行以下步骤：

过程

1. 在导航窗格中，单击**发现作用域 > 常规发现作用域**。
   这样会显示“**常规发现作用域**”页面。
2. 要定义新的发现作用域集，请单击**添加新作用域集**。
   这样会显示“**发现作用域集**”页面。

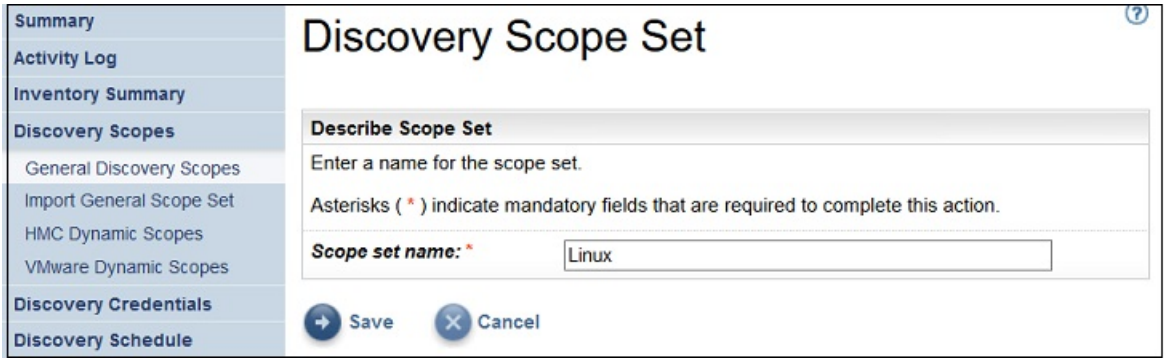

图 *52.* 发现作用域集

a) 在**作用域集**名称字段中，输入唯一作用域集名称。

b) 单击**保存**。
这样会创建新的作用域集，并显示**常规发现作用域**页面。

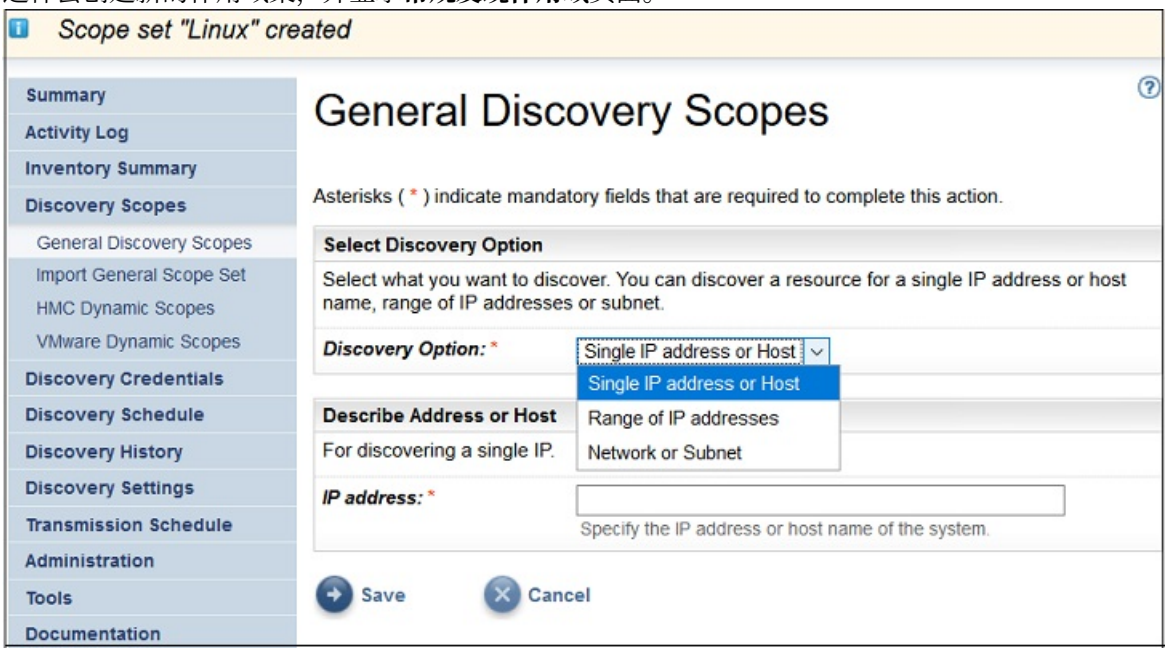

图 *53.* 常规发现作用域

3. 在“**选择发现选项**”窗格中，指定以下选项之一：

   · 单个 IP 地址或主机

   对于**描述地址或主机**，输入 IP 地址或主机名。

- IP 地址范围

  对于**描述地址范围**，在所提供的字段中输入起始 IP 地址、结束 IP 地址和可选的描述。
- 网络或子网

  对于**描述网络或子网**中，在所提供的字段中输入 IP 地址、掩码和可选的描述。

4. 如果要从发现中排除主机、IP 地址、IP 地址范围或子网，请单击**添加排除项**并执行以下步骤：
   a) 选择**主机**、**范围**或**子网**。
   b) 指定要从发现中排除的 IP 地址、IP 地址范围或子网。
   c) 可选： 为要从发现中排除的 IP 地址、IP 地址范围或子网指定描述。

      注: 排除项仅适用于使用 IP 地址范围或子网定义的作用域。

      注: 您不能复用作用域集中任何作用域或排除项的 IP 地址、IP 地址范围、子网或描述。
   d) 要添加更多排除项，请单击**添加排除项**并执行上述步骤来定义更多排除项。
5. 单击**保存**可保存作用域和排除项。这样会显示“**发现作用域集**”页面，其中列出了该新作用域。
6. 要向此作用域集添加更多作用域，请单击**添加新作用域**并执行先前步骤以定义更多作用域。

注: 为提高性能，请将作用域集中的 IP 地址总数限制为 400 或更少。

向现有作用域集添加发现作用域

您可以向现有作用域集添加作用域。

过程

要向现有作用域集添加作用域，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > 常规发现作用域**。
   这样会显示“**常规发现作用域**”页面。
2. 在“**常规发现作用域**”窗格中，单击要向其中添加作用域的作用域集。
   这样会显示“**发现作用域集**”页面。
3. 单击**添加新作用域**。
   这样会显示“**常规发现作用域**”页面。
4. 在“**选择发现选项**”窗格中，指定以下选项之一。
   - 单个 IP 地址或主机

     对于**描述地址或主机**，输入 IP 地址或主机名。
   - IP 地址范围

     对于**描述地址范围**，在所提供的字段中输入起始 IP 地址、结束 IP 地址和可选的描述。
   - 网络或子网

     对于**描述网络或子网**中，在所提供的字段中输入 IP 地址、掩码和可选的描述。
5. 如果要从发现中排除主机、IP 地址、IP 地址范围或子网，请单击**添加排除项**并执行以下步骤：
   a) 选择**主机**、**范围**或**子网**。
   b) 指定要从发现中排除的 IP 地址、IP 地址范围或子网。
   c) 可选： 为要从发现中排除的 IP 地址、IP 地址范围或子网指定描述。

      注: 排除项仅适用于使用 IP 地址范围或子网定义的作用域。

      注: 您不能复用作用域集中任何作用域或排除项的 IP 地址、IP 地址范围、子网或描述。
   d) 要添加更多排除项，请单击**添加排除项**并执行上述步骤来定义更多排除项。
6. 单击**保存**以保存该作用域和排除项。
   这样会显示“**发现作用域集**”页面，其中列出了该新作用域。

修改发现作用域集

您可以通过更改作用域集的设置来修改现有发现作用域集。

关于此任务

要修改现有发现作用域集，请执行以下步骤。

过程

1. 在导航窗格中，单击**发现作用域 > 常规发现作用域**。
   这样会显示“**常规发现作用域**”页面。
2. 要编辑作用域集，请单击作用域集旁边的**编辑**图标 。
   这样会显示“**发现作用域集**”页面。您可以通过编辑作用域、添加作用域、将作用域移至其他作用域集或者删除作用域来编辑作用域集。
   - 要添加作用域，请执行以下步骤：
     a. 单击**添加新作用域**。
     b. 在“**选择发现选项**”窗格中，指定以下选项之一：
        – 单个 IP 地址/主机
          对于“**描述地址或主机**”，输入 IP 地址或主机名。
        – IP 地址范围
          对于“**描述地址范围**”，在所提供的字段中输入起始 IP 地址、结束 IP 地址和可选的描述。
        – 网络或子网
          对于**描述网络或子网**中，在所提供的字段中输入 IP 地址、掩码和可选的描述。

        注: 提供**描述**的唯一名称。如果指定此作用域集中任何其他作用域已存在的描述，那么 TSA 将不允许您创建新作用域。如果**描述**字段保留为空，那么 TSA 使用 IP 地址范围/子网掩码自动创建描述。
     c. 如果要从发现中排除主机、IP 地址或子网，请单击**添加排除项**并执行以下步骤：
        1) 选择**主机**、**范围**或**子网**。
        2) 指定要从发现中排除的 IP 地址、IP 地址范围或子网。
        3) 要添加更多排除项，请单击**添加排除项**并执行上述步骤来定义更多排除项。
     d. 单击**保存**可保存作用域和排除项。这样会显示“**发现作用域集**”页面，其中列出了该新作用域。
   - 要将作用域移至另一个作用域集，请执行以下步骤：
     a. 单击**移动作用域**。
     b. 在“**将作用域从一个作用域集移动至另一个**”页面上，从**作用域**列表中选择要移动的作用域。
     c. 从**目标作用域集**列表中选择要将作用域移动到的作用域集。
     d. 单击**移动**。
   - 要编辑作用域，请执行以下步骤：
     a. 单击特定作用域的**编辑** 图标。
     b. 您可以修改**发现选项**、**IP 地址**和**排除项**等。
     c. 单击**保存**可保存作用域和排除项。这样会显示“**发现作用域集**”页面，其中列出了该新作用域。
   - 要删除作用域，请执行以下步骤：
     a. 单击要删除的作用域旁边的**删除**图标 。
     b. 单击**确定**以确认要删除该发现作用域。

删除发现作用域

您可以删除作用域集中的现有发现作用域，也可以删除整个作用域集。

关于此任务

过程

要删除发现作用域，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > 常规发现作用域**。
   这样会显示“**常规发现作用域**”页面。
2. 通过单击作用域集旁边的**编辑**图标 ，编辑包含要删除的发现作用域的作用域集。
   这样会显示“**发现作用域集**”页面。
3. 单击要删除的作用域旁边的**删除**图标 。
4. 单击**确定**以确认要删除该发现作用域。

删除发现作用域集

您可以删除现有发现作用域集。

过程

注: 在删除作用域集之前，必须先删除与该作用域集相关联的所有凭证。

要删除发现作用域集，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > 常规发现作用域**。
   这样会显示“**常规发现作用域**”页面。
2. 单击要删除的作用域集旁边的**删除**图标 。
3. 单击**确定**以确认要删除该发现作用域集。

导入作用域集

您可以导入 IP 地址列表来定义新的作用域集。

关于此任务

可根据指定的名称和输入文件中的 IP 地址列表来创建新的作用域集。导入作用域集时，TSA 将执行以下验证：

- 检查作用域集名称是否已存在。
- 逐行验证该文件，以检查它是否为有效的 IP 地址。
- 在验证 IP 地址时，忽略尾部空格和前导空格。
- 忽略重复的 IP 地址。

过程

要导入 IP 地址，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > 导入常规作用域集**。
   这样会显示“**导入常规作用域集**”页面。
2. 输入**新作用域集名称**。

   注: 输入任何现有作用域集都未使用过的唯一名称。如果输入现有的作用域集名称，那么将显示以下错误消息：作用域集名称已存在。
3. 单击**选择文件**以选择文本文件。

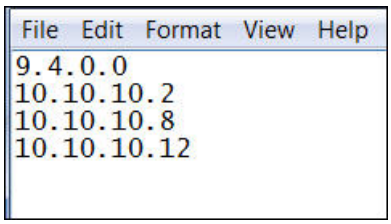

图 *54.* 导入作用域集

注: 必须将该文本文件格式化为单列，其中每一行都包含一个 IP 地址，但不包含其他数据。

4. 单击**导入作用域集文件**可导入作用域集。成功完成导入后，将显示以下状态消息：**已成功导入作用域集**。

   注: 如果作用域集文件包含的 IP 地址超过 400 个，那么将显示以下警告消息：**已成功导入作用域集。但作用域元素的数量超出了建议的准则，请将其限制为 400 个，以便获得更佳性能。**

5. 在导入作用域集之后，可以在用户界面的“**常规发现作用域**”部分中编辑该作用域集，并在“**发现凭证**”部分中关联凭证。

发现设置

使用“**发现设置**”页面，可以调整高级发现设置。

配置连接设置

使用“**连接设置**”页面，可以配置 SLP 发现并通过 EMC SMI-S Provider 发现 EMC 存储设备。

关于此任务

缺省情况下，发现作业会尝试通过运行 SLP 查询来查找 EMC SMI-S Provider，以确定其 IP 地址和端口。如果在网络中无法使用 SLP（例如，如果存在阻止 SLP 消息的任何安全策略），仍然可以通过禁用 SLP 发现并配置 EMC SMI-S Provider 用于侦听查询请求的端口来完成 EMC 存储设备的发现。

过程

1. 选择**启用**或**禁用**选项可启用或禁用 SLP 发现。

   注: 缺省情况下，已启用 SLP 发现。

2. 如果禁用 SLP 发现，那么必须设置一个或多个 EMC SMI-S Provider 连接端口 -

   a) **EMC SMI-S HTTPS 端口：** 5989 是 EMC SMI-S Provider 用于侦听查询请求的缺省 HTTPS 端口。如果您指定了多个端口，请用逗号将它们分隔开。EMC SMI-S 侦听这些端口以获取连接请求（例如，来自于 TSA）。TSA 需要识别此端口才能启动连接。

   b) **EMC SMI-S HTTP 端口：** 5988 是 EMC SMI-S Provider 用于侦听查询请求的缺省 HTTP 端口。TSA 首先尝试 HTTPS 连接（如果已配置），如果失败，它将尝试通过已定义的 HTTP 端口进行连接。如果要避免 HTTP 连接，请勿定义 HTTP 端口。如果您指定了多个 HTTP 端口，请用逗号将它们分隔开。EMC SMI-S 侦听这些端口以获取连接请求（例如，来自于 TSA）。TSA 需要识别此端口才能启动连接。

3. 单击**保存**以保存连接设置。将显示以下消息：已成功保存发现连接设置。

发现凭证

发现凭证是用户名、密码或 SSH 密钥以及简单网络管理协议 (SNMP) 共用名字符串（TSA 用于在发现期间访问“**常规发现作用域**”中配置的资源）。

显示凭证

发现过程需要使用凭证（例如，用户标识和密码）来访问资源。

关于此任务

要点: 您指定的访问信息必须与发现目标资源的访问信息相匹配。如果您更改了目标资源的访问信息（例如密码），请务必同时更改相关的 Technical Support Appliance 访问信息。

您可以通过单击导航窗格中的**发现凭证**来显示现有凭证。这样会显示“**发现凭证**”页面。

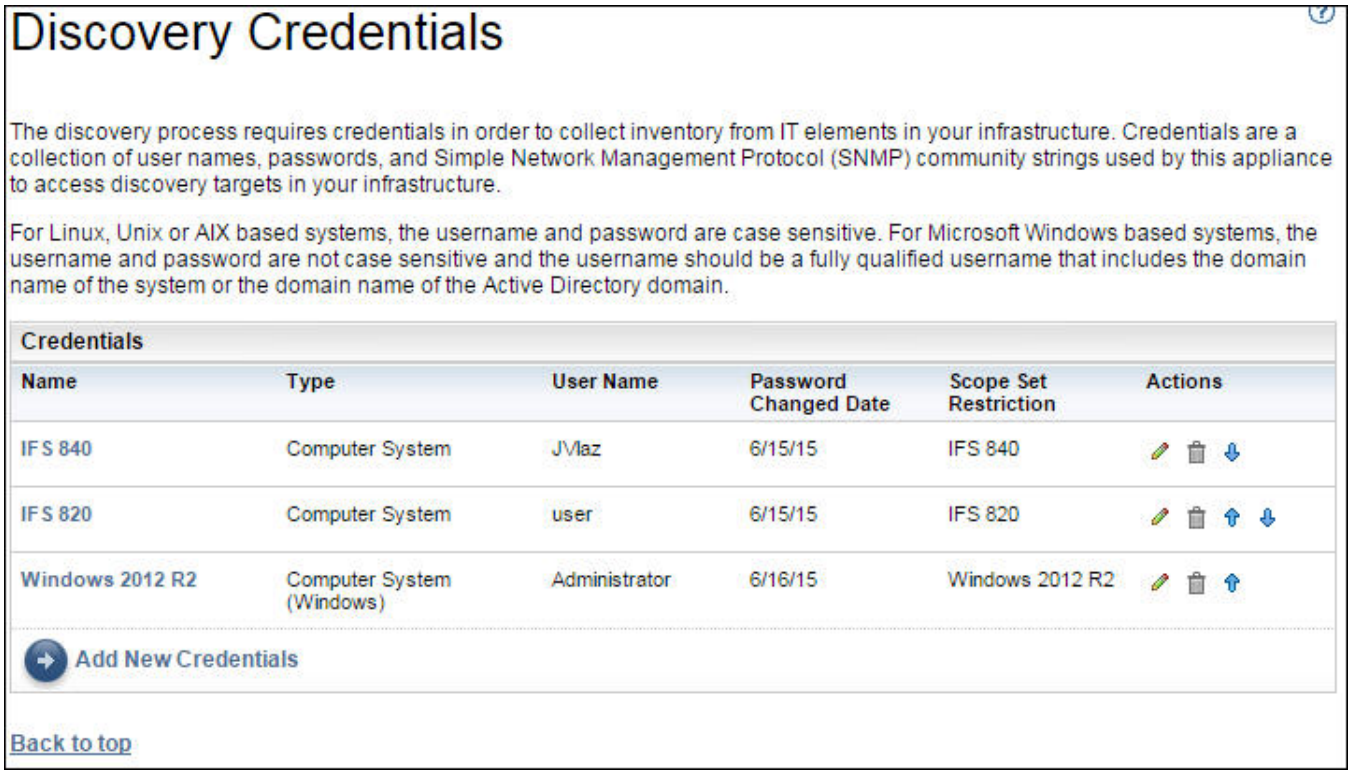

图 *55.* 新建发现凭证

查看凭证详细信息

您可以查看有关特定发现凭证的详细信息。

关于此任务

要查看凭证详细信息，请执行以下步骤：

过程

1. 在导航窗格中，单击**发现凭证**。
   这样会显示“**发现凭证**”页面并列出所有现有凭证。
2. 要查看特定凭证的详细信息，请单击凭证的名称。
   这样会显示“**发现凭证**”页面以及选中凭证的信息。

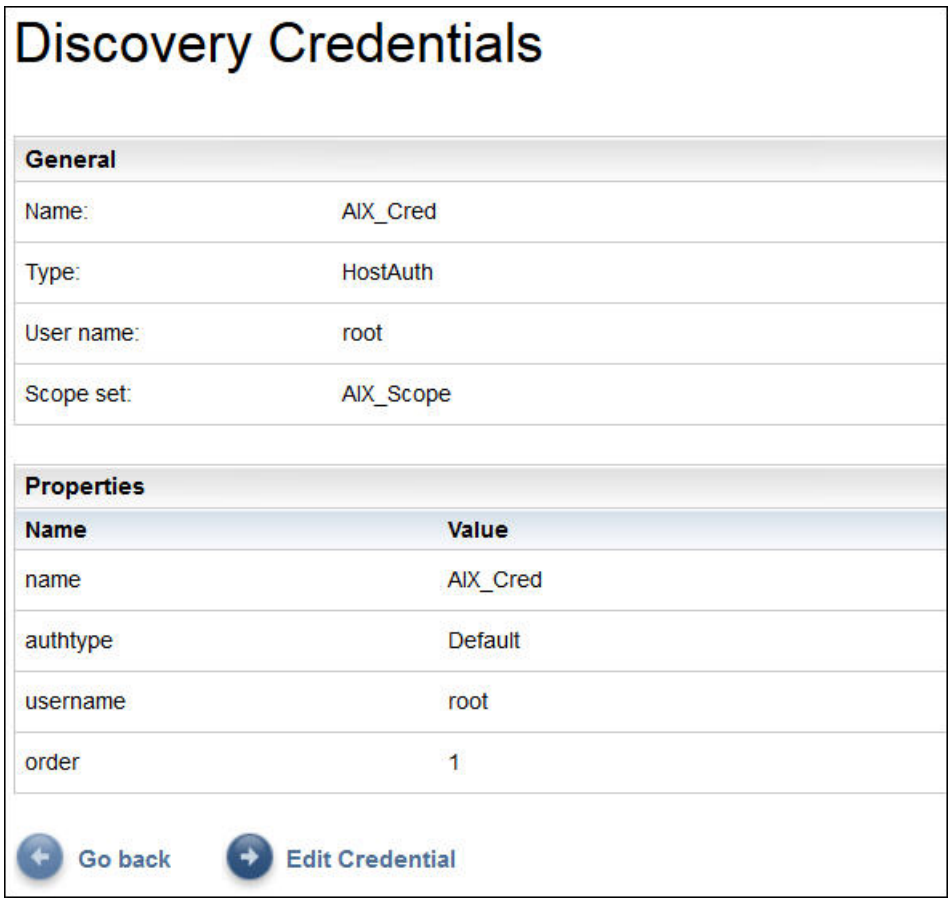

图 56. 发现凭证详细信息

相关任务

修改凭证

您可以修改现有凭证以提供发现过程的访问控制。

添加凭证

可添加凭证来提供对发现过程的访问控制。

关于此任务

要添加凭证，请执行以下步骤：

过程

1. 在导航窗格中，单击**发现凭证**。
   这样会显示“**发现凭证**”页面。
2. 要创建凭证，请单击**添加新凭证**。
   这样会显示“**新建发现凭证**”页面。

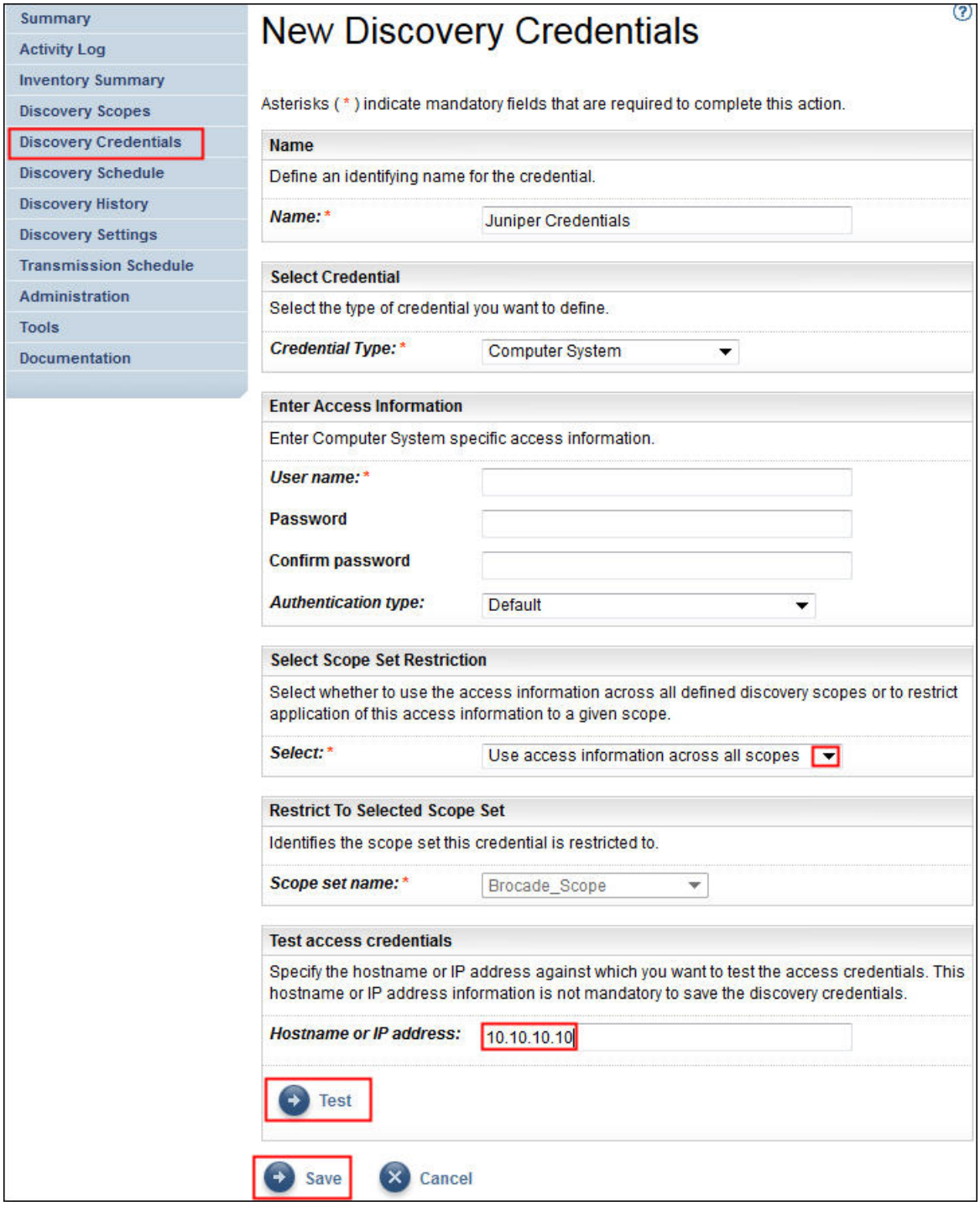

图 *57.* 新建发现凭证

a) 在**名称**字段中，输入凭证的标识名称。

b) 在“**凭证类型**”下拉列表中，选择要创建的凭证的类型。

c) 在“**输入访问信息**”窗格中，指定选择的凭证类型的信息：

所需信息取决于凭证类型。有关每种类型的凭证所需的访问信息的信息，请参阅第 4 页的『发现环境的凭证和软件需求』。

要点: 您指定的访问信息必须与发现目标资源的访问信息相匹配。如果更改有关目标资源的访问信息，请务必同时更改关联的 TSA 访问信息。有关更多信息，请参阅《IBM Technical Support Appliance 配置助手指南》。

提示: “**发现凭证**”页面显示上次更改密码的时间。如果定期更改目标资源上的密码，那么可以使用此信息来确保还更改了 TSA 上的密码以匹配目标资源的新密码。有关显示发现凭证的信息，请参阅第 63 页的『显示凭证』。

d) “**选择作用域集限制**”窗格用于指定凭证是限制为单个作用域集还是应用于所有作用域集。如果**凭证类型**是**计算机系统**并且**认证类型**为 **PKI**，那么不显示此窗格。PKI 凭证必须始终限定为单个作用域集。

提示: 创建限制为特定作用域集的发现凭证可通过减少针对要发现的资源尝试的凭证数量来提高性能。

e) **限制为所选作用域集**窗格用于将凭证限制为单个作用域集。在以下两个条件之一下会显示此窗格。

- **选择作用域集限制**窗格已选择**将访问信息仅用于指定的作用域**，或者
- **凭证类型**为**计算机系统**并且**认证类型**为 **PKI**。

凭证仅用于发现选中的作用域集。在使用不同作用域集进行发现时，不使用凭证。此方法可阻止可能导致帐户锁定的无效登录尝试。

f) 如果凭证类型为**计算机系统**、**计算机系统 (Windows)**、**SNMP** 或 **SNMPV3**，那么可以验证凭证是否正确。**计算机系统**凭证类型的**测试**功能支持以下设备:

- 使用基于 SSH 或 Telnet 的认证的设备
- XIV®
- DS6000™ & DS8000®
- VMware ESXi
- VMware vCenter Server
- EMC CLARiiON/VNX/VMAX（通过 EMC SMI-S）
- IBM TS3100/TS3200
- IBM TS3310
- IBM TS3500
- IBM TS4500
- IBM TS7700
- IBM DS3000、DS4000 和 DS5000（如果密码受保护）
- Windows
- Palo Alto Networks (PAN-OS)

要测试凭证，请输入要用于测试凭证的目标设备的 IP 地址或主机名，然后单击**测试**。

注:

- 输入的主机名不得包含下划线 (“_”)。
- 要在运行 Linux、AIX、IBM i 或 HP-UX 操作系统的系统上运行发现或测试凭证，请启用 SSH。

g) 单击**保存**。
这样会在“**发现凭证**”页面中显示该新凭证。

注: 最佳实践是在创建或修改发现凭证时备份 TSA 配置。

3. 要更改 TSA 访问资源所使用的凭证的顺序，请单击凭证旁边的**向上箭头**图标 或**向下箭头**图标 ，以将其在列表中向上或向下移动。
有关如何使用顺序的信息，请参阅第 2 页的『发现凭证』。
此时会再次显示包含新顺序的“**发现凭证**”页面列表。

修改凭证

您可以修改现有凭证以提供发现过程的访问控制。

关于此任务

要修改凭证，请执行以下步骤：

过程

1. 在导航窗格中，单击**发现凭证**。
   这样会显示“**发现凭证**”页面并列出所有现有凭证。
2. 通过单击凭证旁边的**编辑**图标 ，编辑凭证。
   这样会显示“**编辑发现凭证**”页面。
   a) 在“**修改访问信息**”窗格中，您可以更改此凭证的访问信息。

      要点： 您指定的访问信息必须与发现目标资源的访问信息相匹配。如果更改有关目标资源的访问信息，请务必同时更改关联的 TSA 访问信息。有关更多信息，请参阅《IBM Technical Support Appliance 配置助手指南》。

      提示： “**发现凭证**”页面显示上次更改密码的时间。如果定期更改目标资源上的密码，那么可以使用此信息来确保还更改了 TSA 上的密码以匹配目标资源的新密码。有关显示发现凭证的信息，请参阅第 63 页的『显示凭证』。

   b) “**选择作用域集限制**”窗格用于指定凭证是限制为单个作用域集还是应用于所有作用域集。如果**凭证类型**是**计算机系统**并且**认证类型**为 **PKI**，那么不显示此窗格。PKI 凭证必须始终限定为单个作用域集。

      提示： 创建限制为特定作用域集的发现凭证可通过减少针对要发现的资源尝试的凭证数量来提高性能。

   c) **限制为所选作用域集**窗格用于将凭证限制为单个作用域集。在以下两个条件之一下会显示此窗格：

      · **选择作用域集限制**窗格已选择**将访问信息限于指定的作用域**，或者

      · **凭证类型**为**计算机系统**并且**认证类型**为 **PKI**。

      仅在发现选中的作用域集时使用凭证。此凭证不用于任何其他作用域集。此方法可阻止可能导致用户帐户锁定的无效登录尝试。

   d) 如果凭证类型为**计算机系统**、**计算机系统 (Windows)**、**SNMP** 或 **SNMPV3**，那么可以验证凭证是否正确。要测试这些凭证，请输入要用于测试凭证的目标的 IP 地址或主机名，然后单击**测试**。

      注： 输入的主机名不得包含下划线 (“_”)。

   e) 单击**保存**。
      将在“**发现凭证**”页面中显示更改的凭证。
3. 要更改 TSA 访问资源所使用的凭证的优先级顺序，请单击凭证旁边的**向上箭头**图标 或**向下箭头**图标 ，以将其在列表中向上或向下移动。
   有关如何使用顺序的信息，请参阅第 2 页的『发现凭证』。
   此时会再次显示包含新顺序的“**发现凭证**”页面列表。

相关概念

发现凭证
发现凭证是用户名、密码或 SSH 密钥以及简单网络管理协议 (SNMP) 共用名字符串（供 TSA 用来在发现期间访问资源）的集合。

发现环境的凭证和软件需求

为发现您的环境中的端点或资源，TSA 必须有权访问这些资源。建议针对每个资源创建一个服务帐户，以专门供 TSA 访问此资源时使用。

删除凭证

您可以删除 TSA 在访问资源时使用的凭证。

关于此任务

要删除凭证，请执行以下步骤：

过程

1. 在导航窗格中，单击**发现凭证**。
   这样会显示“**发现凭证**”页面。
2. 单击要删除的凭证旁边的**删除**图标 。
3. 单击**确定**以确认要删除该凭证。

发现计划安排

计划安排发现以确保发现的数据总是最新且准确。您可以查看发现计划安排和最后一次发现的详细信息、修改发现计划安排以及禁用计划安排的发现。您还可以随时选择运行发现。

开始之前

缺省情况下，TSA 使用“完全发现”计划安排来发现在 HMC 和“VMware 动态作用域”以及“常规发现作用域”中定义的所有 IT 元素。TSA 在发现过程中自动分布 IT 元素检测，以将影响降至最低。

替代方法是创建多个用户定义的计划安排。这允许特定发现作用域的发现分布在对网络和 IT 元素影响最小（或理想情况下）的不同日期和时间。在此情况下，应禁用完全发现计划安排以支持用户定义的计划安排。

在任何计划安排的发现开始时，设备运行预发现维护作业，在此期间，一些功能不可用，例如，“库存摘要”、“发现作用域”、“发现计划安排”和“凭证”。在预发现维护作业期间，“**摘要**”屏幕上的**发现作业管理器**状态设置为警告符号 ()。此外，将在 TSA 屏幕上显示一条警告消息，指示某些功能暂时不可用：在执行“预发现维护”过程中，“发现作业管理器”暂时脱机。在此时间内（通常最多 10 分钟），与发现或库存相关的一些 UI 功能可能显示部分信息或者不显示信息。

在成功预发现维护后，“**摘要**”页面上的**发现作业管理器**状态变为正常() 状态，并且恢复完全发现活动（在 10 分钟内）。

查看发现计划安排

您可以查看有关发现计划安排的摘要信息。

关于此任务

要查看发现计划安排，请执行以下步骤：

过程

在导航窗格中，单击**发现计划安排**。
这样会显示“**发现计划安排**”页面。

“**计划安排**”窗格显示计划安排的名称、下一次安排的运行、运行计划安排和每个计划安排的操作（“编辑”()、“删除”()、“启用/禁用”(/) 和“运行”）。

单击 图标以查看针对计划安排指定的所有作用域集。有关完全发现计划安排，此图标列出在 TSA 中定义且缺省情况下分配给计划安排的所有作用域集。

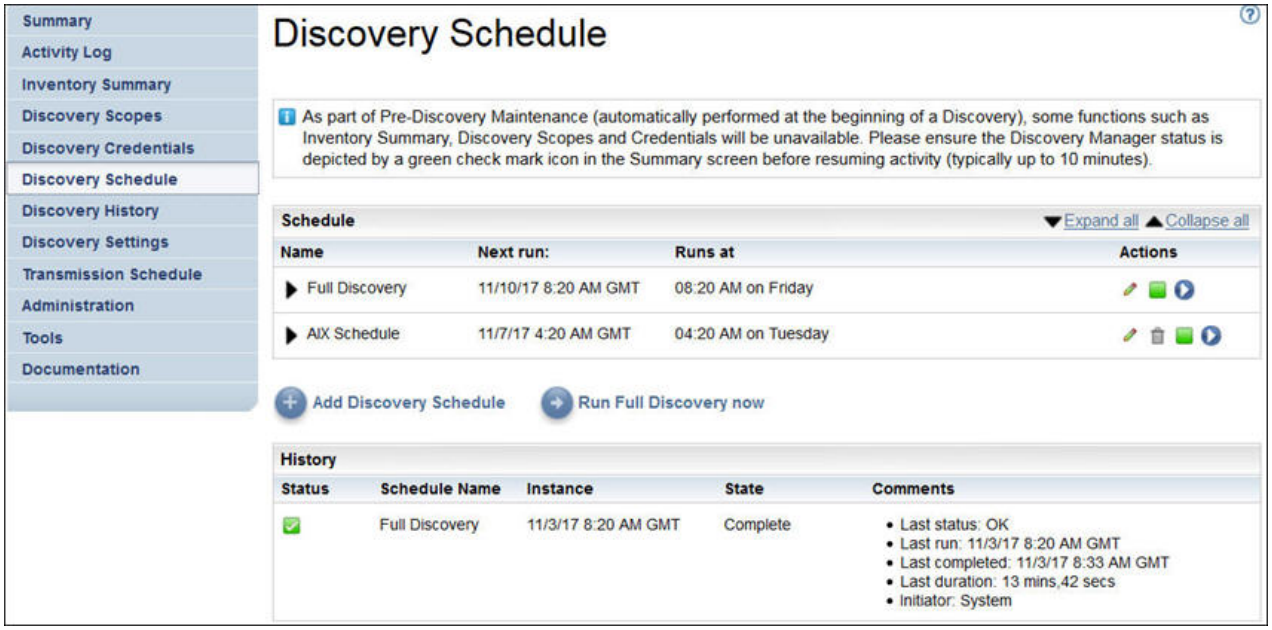

图 *58.* 发现计划安排

注: 如果您的 TSA 是全新安装的，或者已迁移或更新到最新版本，那么新 TSA 具有使用缺省日期（星期二凌晨 2:15）创建且名为**完全发现**的发现计划安排。可编辑或禁用“完全发现”计划安排，但是无法将其删除。如果具有任何预先定义的发现计划安排（已启用/已禁用），那么将在迁移后复原相同值。

“**历史记录**”窗格显示当前正在运行以及先前发现的作业的状态、计划安排名称和更多详细信息。

添加发现计划安排

您可以添加新的计划安排，以使发现过程在指定的时间运行。新的计划安排允许 TSA 在安排的日期和时间发现 IT 元素的子集。

过程

1. 在导航窗格中，单击**发现计划安排**。
   这样会显示“**发现计划安排**”页面。
2. 单击**添加发现计划安排**。这样会显示“**添加发现计划安排**”页面。

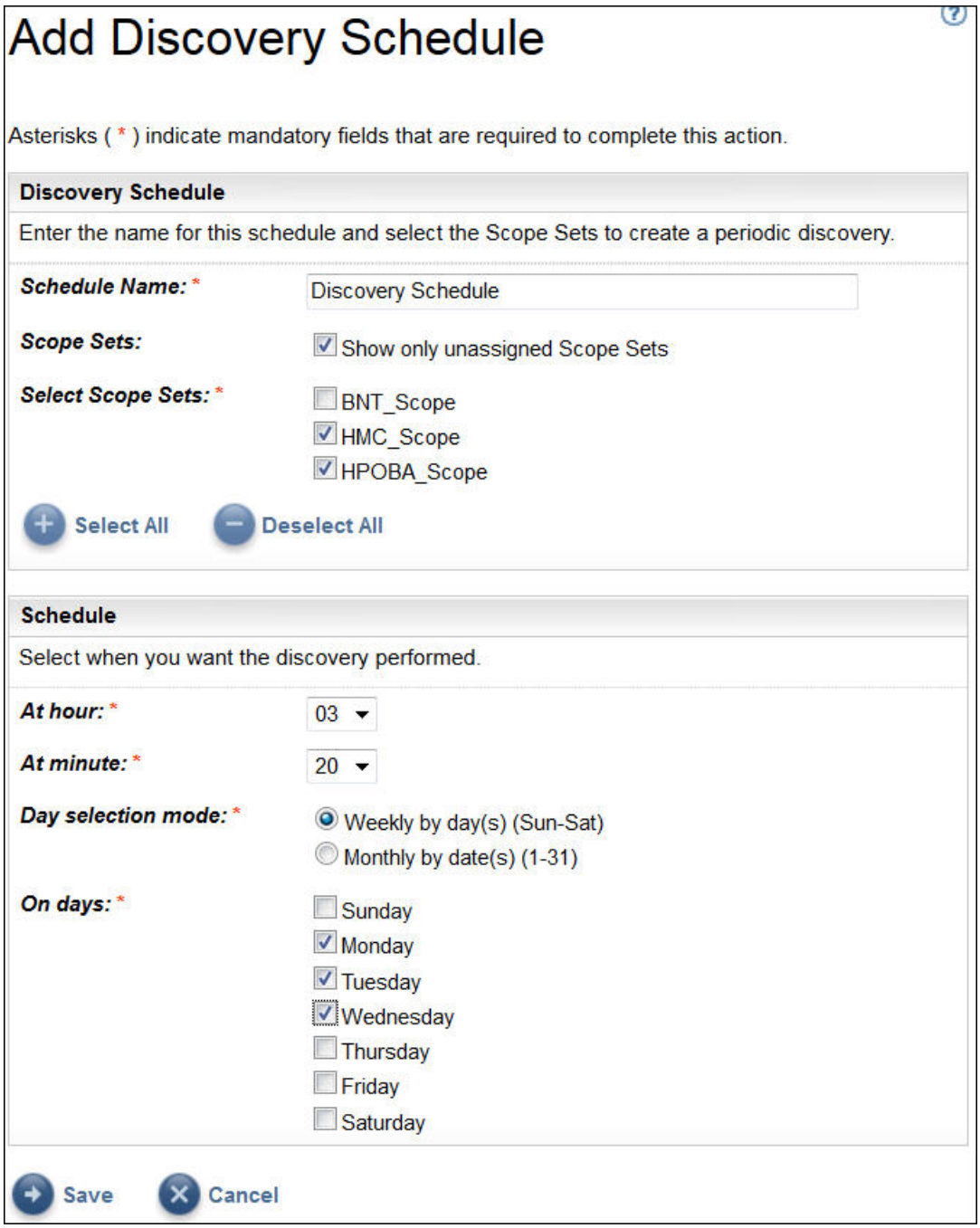

图 *59.* 添加发现计划安排

3. 在**计划安排名称**字段中，输入计划安排的标识名称。
4. 选择**仅显示未分配的作用域集**选项，以仅查看未分配给任何其他用户定义的发现计划安排的作用域集。
5. 从**选择作用域集**列表中选择期望的作用域集。
   您可以使用**全选/取消全选**来选择所有作用域集或不选择任何作用域集。
6. 使用**按小时**和**按分钟**列表来选择新时间。
7. 选择**日期选择模式**。

周日期（周日-周六）

要将发现操作安排在一周中的某一天（或某几天），请选择**周日期（周日-周六）**选项。

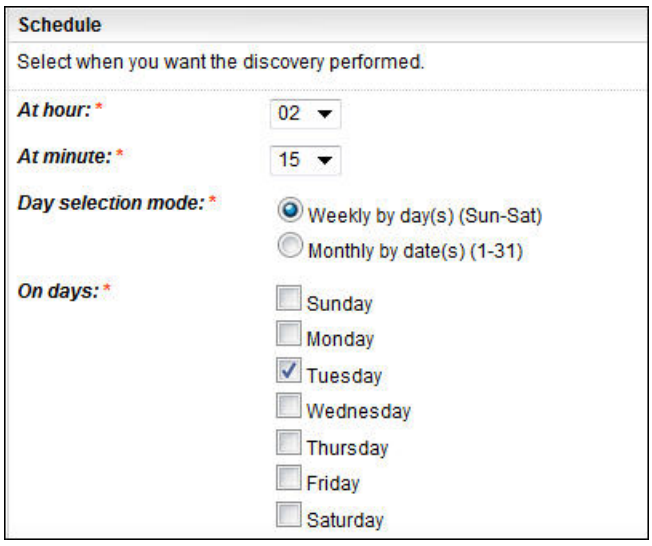

图 60. 周日期（周日-周六）

对于**日期**字段，选中相应复选框以选择一周中的一天或多天。

月日期 (1-31)

要将发现操作安排在一个月中的某一天（或某几天），请选择**月日期 (1-31)** 选项。

对于**日期**字段，选中相应复选框以选择一个月中的一天或多天。

注: 如果选择了超过特定月份最后一天的日期，那么将在此特定月份的最后一天触发作业。

8. 单击**保存**。
   此时会再次显示“**发现计划安排**”页面，其中显示了该新计划安排。

修改发现计划安排

TSA 提供缺省计划安排以使发现过程在指定的时间运行。 您可以根据需要修改缺省计划安排或使用定制计划安排。

关于此任务

过程

1. 在导航窗格中，单击**发现计划安排**。
   这样会显示“**发现计划安排**”页面。
2. 单击**编辑计划安排** ( ) 图标。
   这样会显示“**编辑发现计划安排**”页面。
   a) 根据需要，编辑“**发现计划安排**”窗格中的**计划安排名称**、**作用域集**和**选择作用域集**。
   注: 您无法编辑缺省“完全发现”的这些字段。
   b) 根据需要，编辑“**计划安排**”窗格中的**按小时**、**按分钟**、**日期选择模式**和**日期**。
3. 单击**保存**。
   此时会再次显示“**发现计划安排**”页面以及修改的计划安排。

禁用发现计划安排

您可以禁用计划安排的发现。

开始之前

注: 如果已配置用户定义的发现计划安排，那么建议禁用**完全发现**计划安排，以避免重复发现相同的 IT 元素。

过程

要禁用计划安排的发现，请执行以下步骤：

1. 在导航窗格中，单击**发现计划安排**。
   这样会显示“**发现计划安排**”页面。
2. 单击相应计划安排的 /  图标以禁用/启用发现计划安排。

删除发现计划安排

您可以删除计划安排的发现。

过程

要删除计划安排的发现，请执行以下步骤：

1. 在导航窗格中，单击**发现计划安排**。
   这样会显示“**发现计划安排**”页面。
2. 单击要删除的计划安排旁边的 图标。

   注： 无法删除缺省完全发现计划安排，但可以在需要时禁用缺省完全发现计划安排。

   此时会显示一条确认消息，要求确认删除所选的发现计划安排。
3. 单击**确定**以删除该计划安排。

运行发现

您可以按需运行发现而不是等待下一个计划安排的发现。您可以在所有定义的发现作用域、特定发现计划安排或特定发现作用域集或作用域上运行发现。

过程

要在所有定义的作用域上运行发现，请执行以下步骤：

1. 在导航窗格中，单击**发现计划安排**。这样会显示“**发现计划安排**”页面。
2. 单击**立即运行完全发现**。“历史记录”部分将进行更新，指示发现正在运行。

   注： TSA 将尝试最大程度地降低对网络环境的影响。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。您可以在**摘要**页面上的**作业摘要**部分中监视发现过程。
3. 要在特定作用域上运行发现，请单击该作用域的**运行**图标 。
4. 检查“**摘要**”页面（单击导航窗格中的**摘要**）。在“**作业摘要**”窗格中将显示该发现。“**摘要**”页面将定期进行刷新以显示 TSA 的当前状态。如果在“**作业摘要**”窗格中不再列出该作业，请检查“**活动日志**”（单击导航窗格中的**活动日志**）。该发现应该已经成功完成。

在常规作用域集上运行发现

过程

要在特定作用域集上运行发现，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > 常规发现作用域**。
   这样会显示“**常规发现作用域**”页面。此页面显示针对此 TSA 定义的所有作用域集的列表。

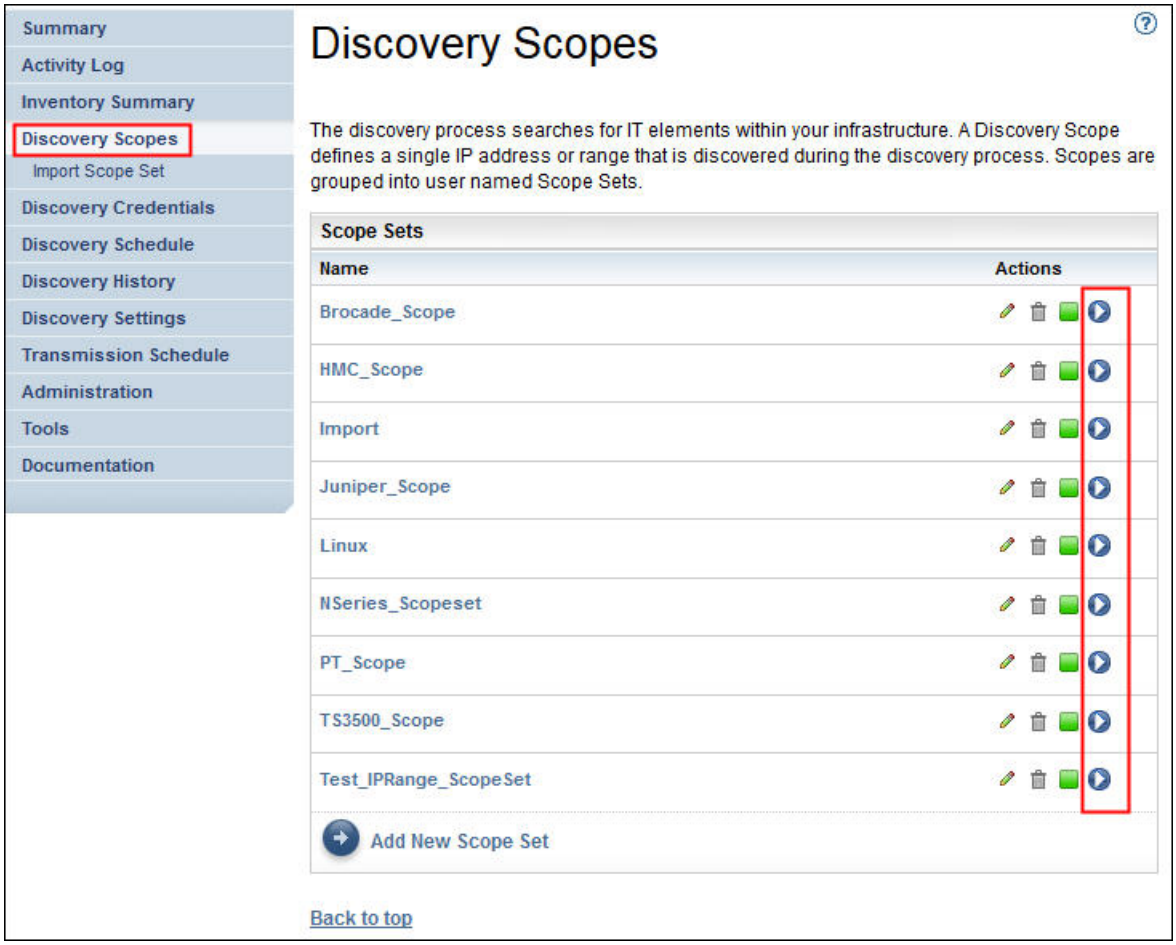

图 *61.* 在特定作用域上运行发现

2. 要在特定作用域集上运行发现，请单击此作用域集的**运行**图标 。
3. 检查“**摘要**”页面（单击导航窗格中的**摘要**）。在“**作业摘要**”窗格中将显示该发现。“**摘要**”页面将定期进行刷新以显示 TSA 的当前状态。如果在“**作业摘要**”窗格中不再列出该作业，请检查“**活动日志**”（单击导航窗格中的**活动日志**）。该发现应该已经成功完成。

在 HMC 动态作用域集上运行发现

过程

要在特定作用域集上运行发现，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > HMC 动态作用域**。
   这样会显示“**HMC 动态作用域**”页面。此页面显示针对此 TSA 定义的所有作用域集的列表。

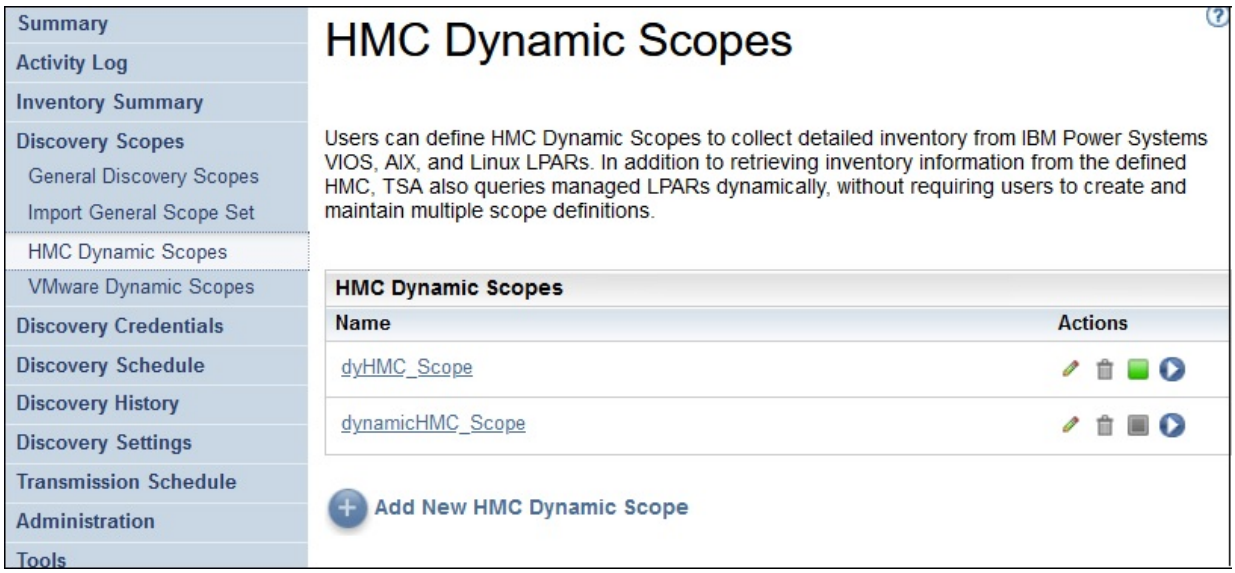

图 *62. HMC* 动态作用域

2. 要在特定作用域集上运行发现，请单击此作用域集的**运行**图标 。
3. 检查“**摘要**”页面（单击导航窗格中的**摘要**）。在“**作业摘要**”窗格中将显示该发现。“**摘要**”页面将定期进行刷新以显示 TSA 的当前状态。如果在“**作业摘要**”窗格中不再列出该作业，请检查“**活动日志**”（单击导航窗格中的**活动日志**）。该发现应该已经成功完成。

在 VMWare 作用域集上运行发现

过程

要在特定作用域集上运行发现，请执行以下步骤：

1. 在导航窗格中，单击**发现作用域 > VMWare 动态作用域集**。
   这样会显示“**VMWare 动态作用域**”页面。此页面显示针对此 TSA 定义的所有作用域集的列表。

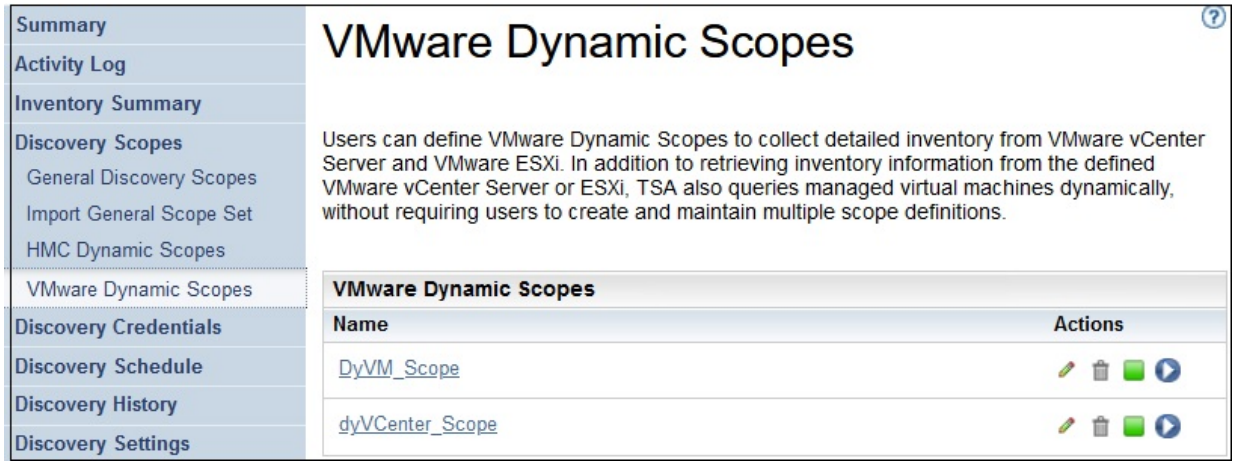

图 *63.* 在 *VMware* 动态作用域上运行发现

2. 要在特定作用域集上运行发现，请单击此作用域集的**运行**图标 。
3. 检查“**摘要**”页面（单击导航窗格中的**摘要**）。在“**作业摘要**”窗格中将显示该发现。“**摘要**”页面将定期进行刷新以显示 TSA 的当前状态。如果在“**作业摘要**”窗格中不再列出该作业，请检查“**活动日志**”（单击导航窗格中的**活动日志**）。该发现应该已经成功完成。

在作用域集上运行发现

您可以按需运行发现而不是等待下一个计划安排的发现。您可以在所有定义的发现作用域、特定发现计划安排或特定发现作用域集或作用域上运行发现。

在常规作用域上运行发现

过程

1. 在导航窗格中，单击**发现作用域 > 常规发现作用域**。这样会显示“**常规发现作用域**”页面。

图 *64.* 发现作用域

2. 单击包含要发现的作用域的作用域集。
   这样会显示“**发现作用域集**”页面。此页面显示针对该作用域集定义的所有作用域。

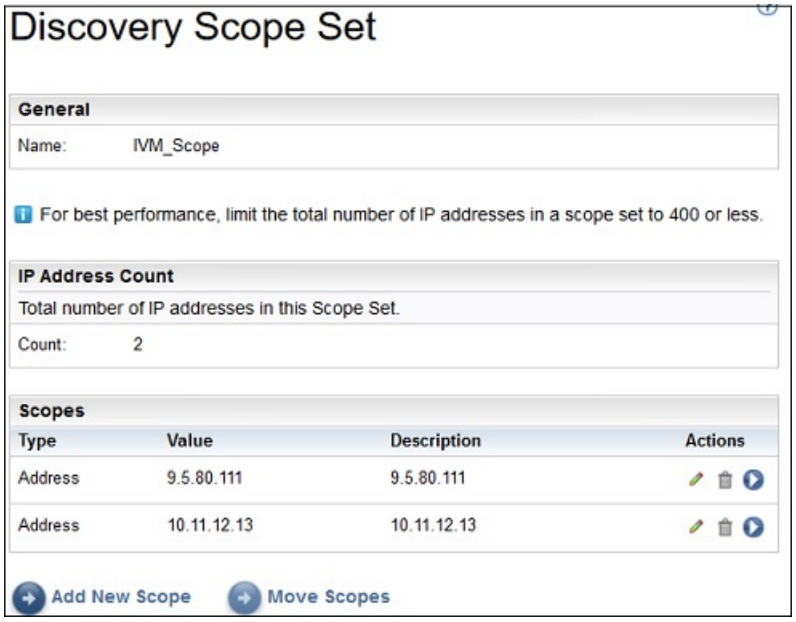

图 *65.* 在特定作用域上运行发现

3. 要在特定作用域上运行发现，请单击该作用域的**运行**图标 。
4. 检查“**摘要**”页面（单击导航窗格中的**摘要**）。在“**作业摘要**”窗格中将显示该发现。“**摘要**”页面将定期进行刷新以显示 TSA 的当前状态。如果在“**作业摘要**”窗格中不再列出该作业，请检查“**活动日志**”（单击导航窗格中的**活动日志**）。该发现应该已经成功完成。

在 HMC 动态作用域上运行发现

过程

1. 在导航窗格中，单击**发现作用域 > HMC 动态作用域**。这样会显示“**HMC 动态作用域**”页面。

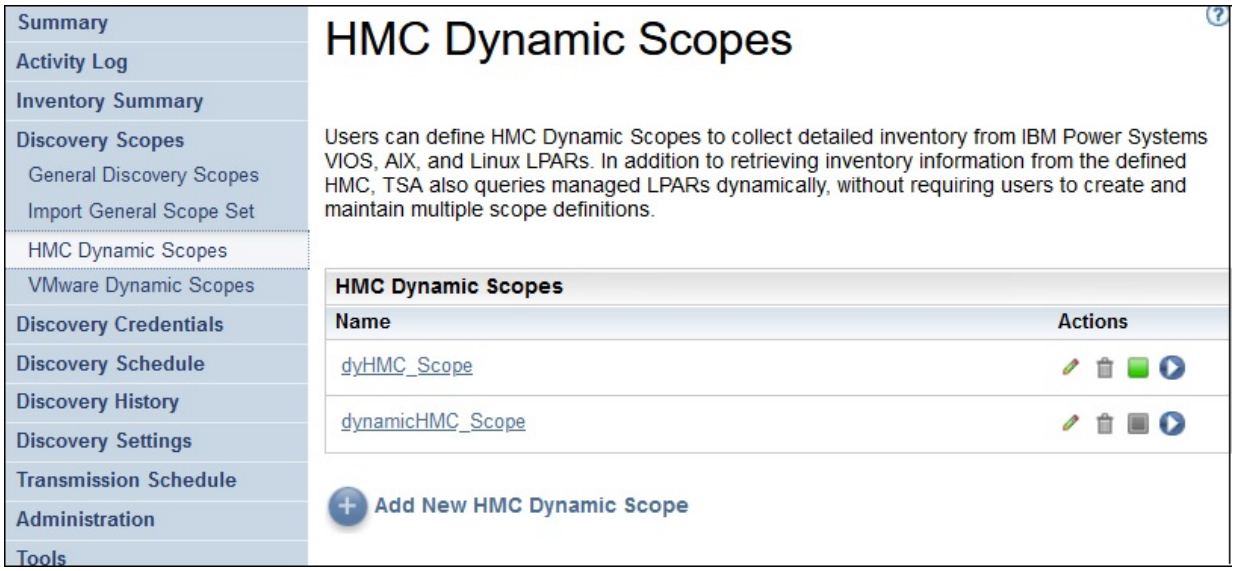

图 *66. HMC* 动态作用域

2. 单击包含要发现的作用域的作用域集。
   这样会显示“**HMC 动态作用域集**”页面。此页面显示针对该作用域集定义的所有作用域。

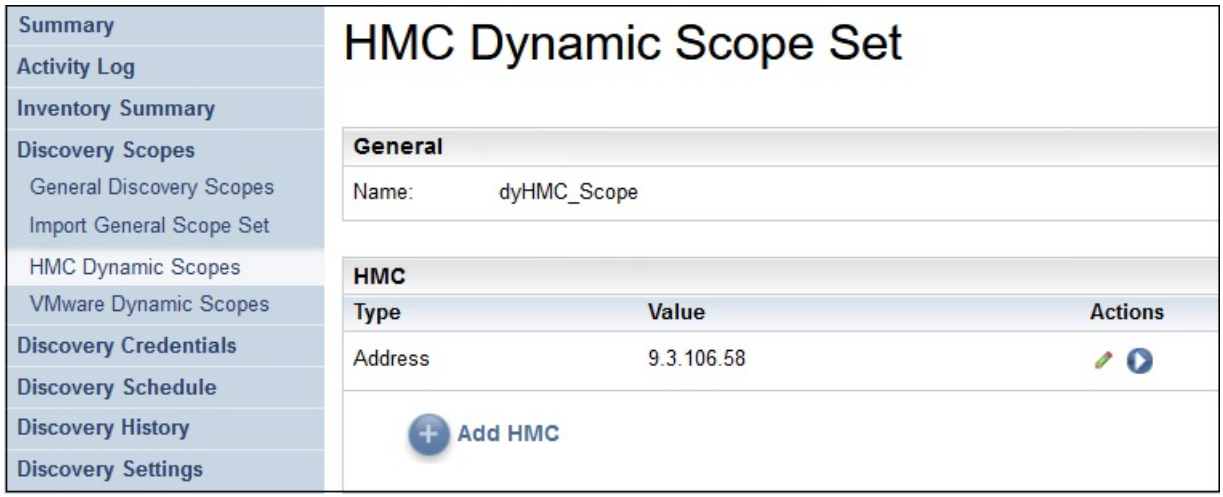

图 *67.* 在特定作用域上运行发现

3. 要在特定作用域上运行发现，请单击该作用域的**运行**图标 。
4. 检查“**摘要**”页面（单击导航窗格中的**摘要**）。在“**作业摘要**”窗格中将显示该发现。“**摘要**”页面将定期进行刷新以显示 TSA 的当前状态。如果在“**作业摘要**”窗格中不再列出该作业，请检查“**活动日志**”（单击导航窗格中的**活动日志**）。该发现应该已经成功完成。

在 VMWare 动态作用域上运行发现

过程

1. 在导航窗格中，单击**发现作用域 > VMWare 动态作用域**。这样会显示“**VMWare 动态作用域**”页面。

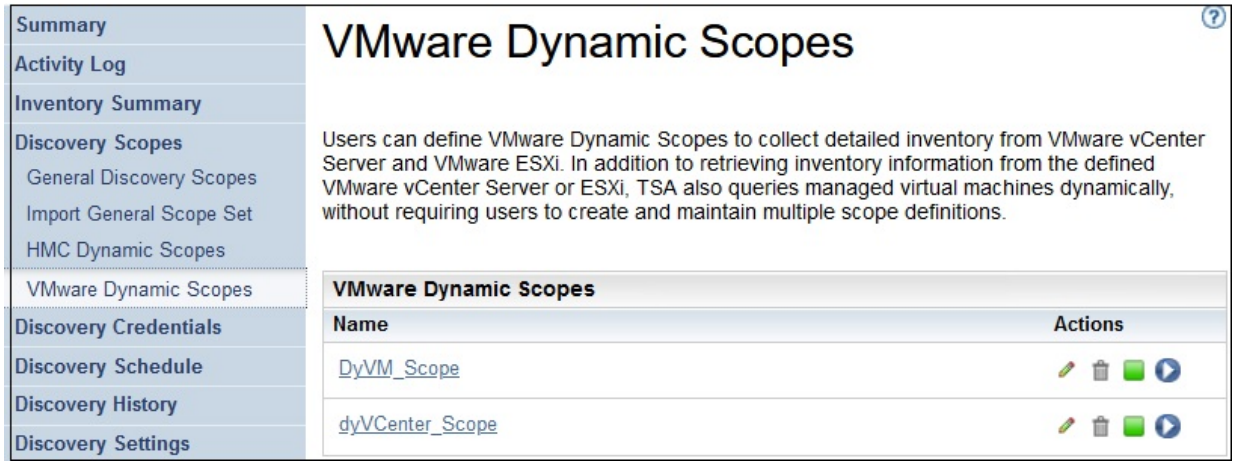

图 *68. VMWare* 动态作用域

2. 单击包含要发现的作用域的作用域集。
   这样会显示“**VMWare 动态作用域集**”页面。此页面显示针对该作用域集定义的所有作用域。

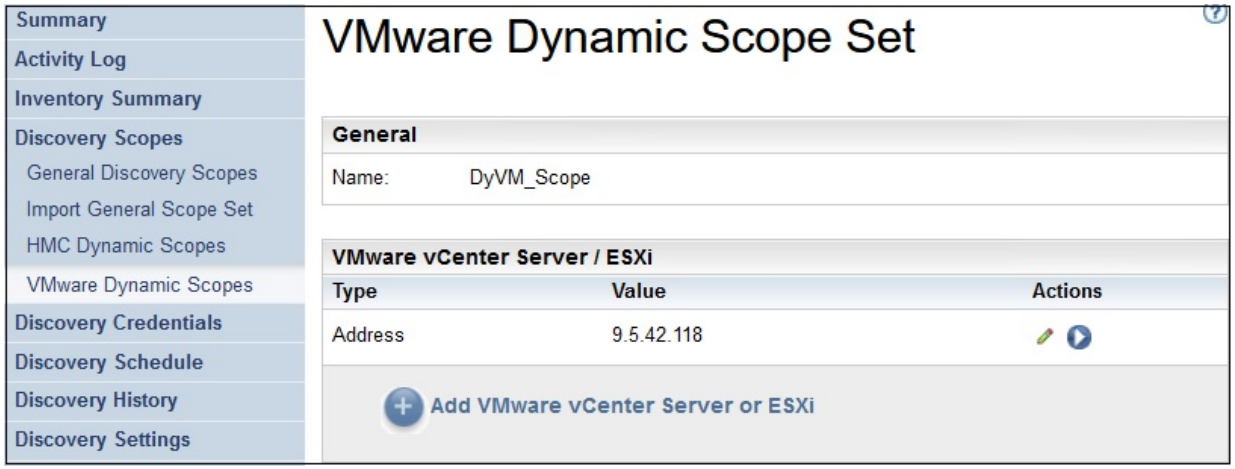

图 *69.* 在 *VMware* 动态作用域上运行发现

3. 要在特定作用域上运行发现，请单击该作用域的**运行**图标 。
4. 检查“**摘要**”页面（单击导航窗格中的**摘要**）。在“**作业摘要**”窗格中将显示该发现。“**摘要**”页面将定期进行刷新以显示 TSA 的当前状态。如果在“**作业摘要**”窗格中不再列出该作业，请检查“**活动日志**”（单击导航窗格中的**活动日志**）。该发现应该已经成功完成。

发现历史记录

您可以在发现完成后查看其详细信息，并下载发现的诊断日志文件。

过程

要查看发现历史记录或下载诊断日志文件，请执行以下步骤：

1. 在导航窗格中，单击**发现历史记录**。
   这样会显示“**发现历史记录**”页面。此时会显示发现条目列表。 每个条目显示一个发现的状态、名称以及开始和结束时间。

图 *70.* 发现历史记录

2. 要在“**历史记录条目**”列表中显示有关条目的更多信息，请单击历史记录条目的名称。

   “**条目信息**”窗格显示有关选中的发现的信息。
3. 要下载发现的诊断日志文件，请单击发现的**下载**图标 。
4. 要删除发现的诊断日志文件，请单击发现的**删除**图标 。

传输计划安排

计划安排数据传输以确保定期将发现的数据发送给 IBM 支持人员。 您可以查看传输计划安排和最后一次传输的详细信息、修改传输计划安排以及禁用计划安排的传输。您还可以随时选择将数据发送到 IBM。

查看传输计划安排

您可以查看有关传输计划安排的摘要信息。

关于此任务

要查看传输计划安排，请执行以下步骤:

过程

在导航窗格中，单击**传输计划安排**。

这样会显示“**传输计划安排**”页面。

“**计划安排**”窗格显示下一个计划安排的运行以及计划安排的运行时间。“**历史记录**”窗格显示当前正在运行和先前的传输作业的状态以及其他详细信息。

修改传输计划安排

TSA 提供缺省计划安排以使传输过程在指定的时间运行。 您可以根据需求修改此计划安排。

过程

1. 在导航窗格中，单击**传输计划安排**。

   这样会显示“**传输计划安排**”页面。

   “**计划安排**”窗格显示下一个计划安排的运行以及计划安排的运行时间。“**历史记录**”窗格显示当前正在运行和先前的传输作业的状态以及其他详细信息。
2. 单击**编辑计划安排**。

   这样会显示“**传输计划安排**”页面。

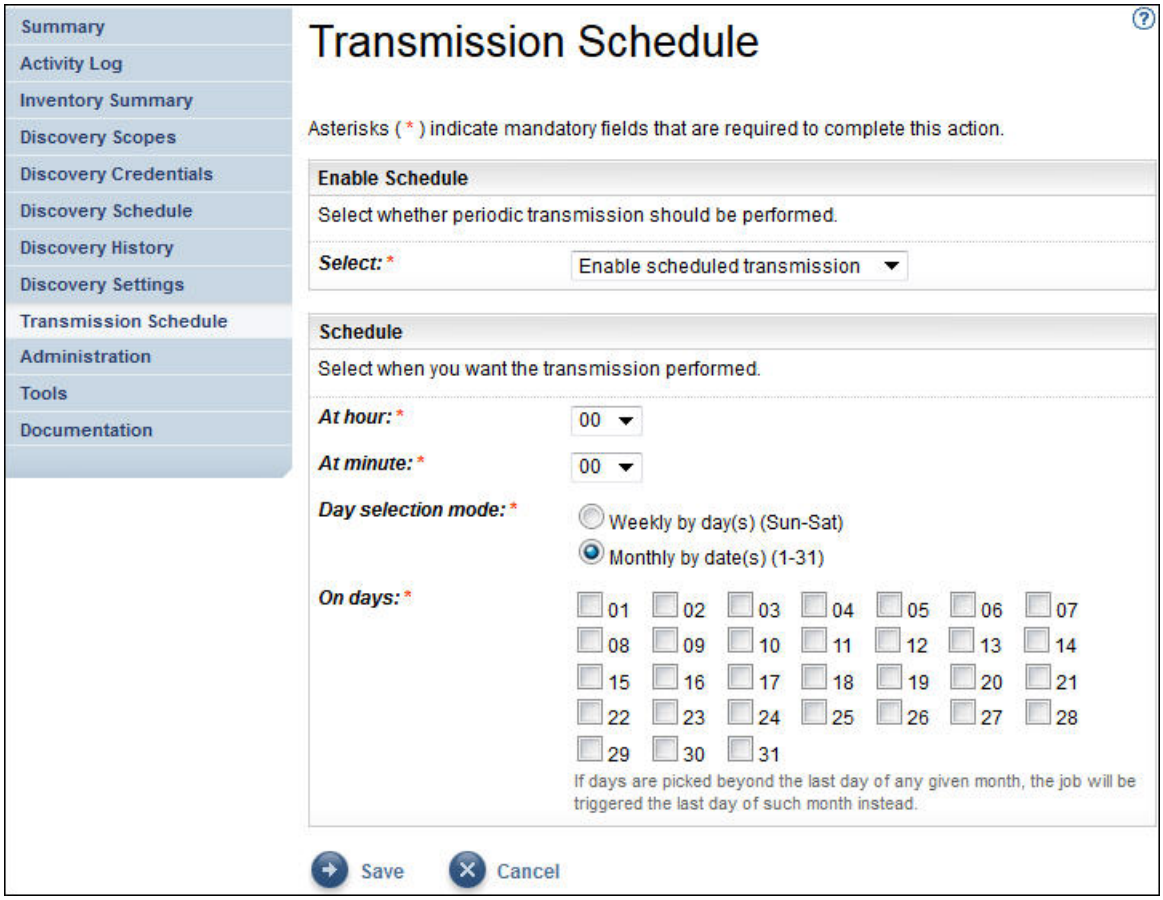

图 71. 编辑传输计划安排

a) 使用**按小时**和**按分钟**下拉列表以选择新时间。

b) 选择**日期选择模式**。

周日期（周日-周六）

要将传输操作安排在一周中的某一天（或某几天），请选择**周日期（周日-周六）**选项。

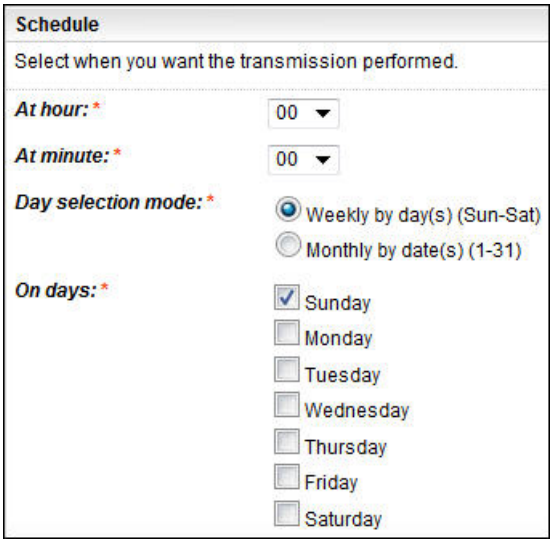

图 72. 周日期（周日-周六）

对于**日期**字段，选中相应复选框以选择一周中的一天或多天。

月日期 (1-31)

要将传输操作安排在一个月中的某一天（或某几天），请选择**月日期 (1-31)** 选项。

对于**日期**字段，选中相应复选框以选择一个月中的一天或多天。

注: 如果选择了超过特定月份最后一天的日期，那么将在此特定月份的最后一天触发作业。

3. 单击**保存**。
   此时会再次显示“**传输计划安排**”页面以及新计划安排。

禁用传输计划安排

您可以禁用计划安排的数据传输。

过程

要禁用计划安排的传输，请执行以下步骤:

1. 在导航窗格中，单击**传输计划安排**。
   这样会显示“**传输计划安排**”页面。
2. 单击**编辑计划安排**。
   这样会显示“**传输计划安排**”页面。
3. 在“**启用计划安排**”窗格中，选择**禁用计划安排的传输**。
4. 单击**保存**。
   这样会显示“**发现计划安排**”页面，并且“**计划安排**”窗格会显示已禁用计划安排的发现。您可以通过单击**启用计划安排的传输**来启用计划安排的传输。

运行传输

您可以按需运行传输，而不是等待下一个计划安排的传输。

过程

1. 在导航窗格中，单击**传输计划安排**。
   这样会显示“**传输计划安排**”页面。

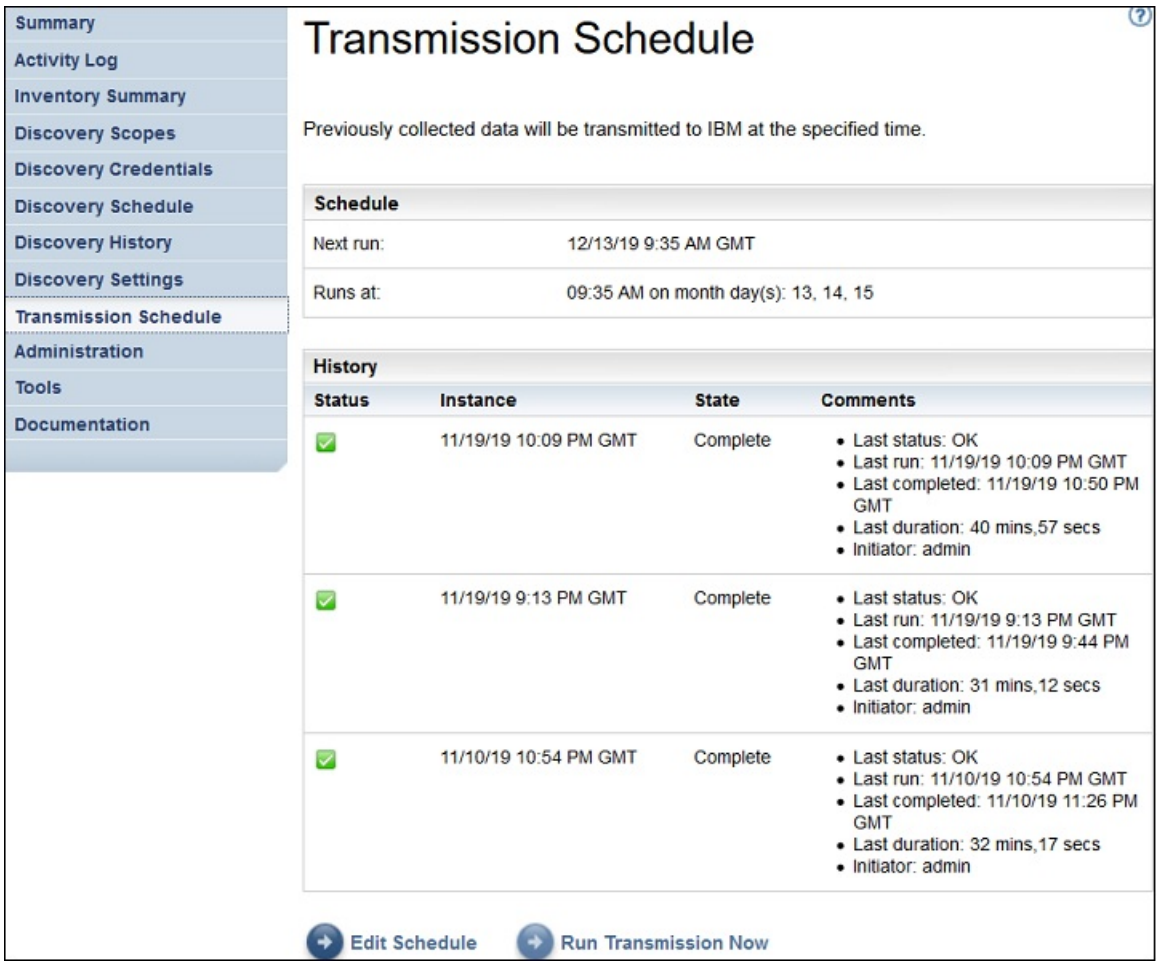

图 *73.* 立即运行传输

2. 单击**立即运行传输**。

   “**历史记录**”窗格将进行更新，指示传输正在运行。

3. 检查“**摘要**”页面（单击导航窗格中的**摘要**）。在“**作业摘要**”窗格中将显示该传输。“**摘要**”页面将定期进行刷新以显示 TSA 的当前状态。如果在“**作业摘要**”窗格中不再列出该作业，请检查“**活动日志**”（单击导航窗格中的**活动日志**）。该传输应该已经成功完成。

数据快照

您可生成并保存 TSA 收集的未经格式处理的原始数据的本地副本，而无需将数据传输到 IBM。您还可以查看已传输给 IBM 的最新数据。

1. 在导航窗格中，单击**管理 > 数据快照**。这样会显示“**数据快照**”页面。

图 *74.* 数据快照

注: 当存在已完成的传输或数据快照时，才会启用**下载最新数据快照**按钮。

2. 单击**立即生成数据快照**，收集 TSA 发现的最新数据并生成新的数据快照。这样会显示以下消息 - 正在生成数据快照。这最多可能需要 2 小时。可查看“活动日志”或“摘要”页面以了解状态。单击导航菜单中的**摘要**，查看“**摘要**”页面。 “**作业摘要**”窗格显示数据快照收集的状态，直至其完成。单击导航菜单中的**活动日志**，查看数据快照请求的完成状态。
3. 如果传输或数据快照服务完成，那么将显示**数据快照日期**。

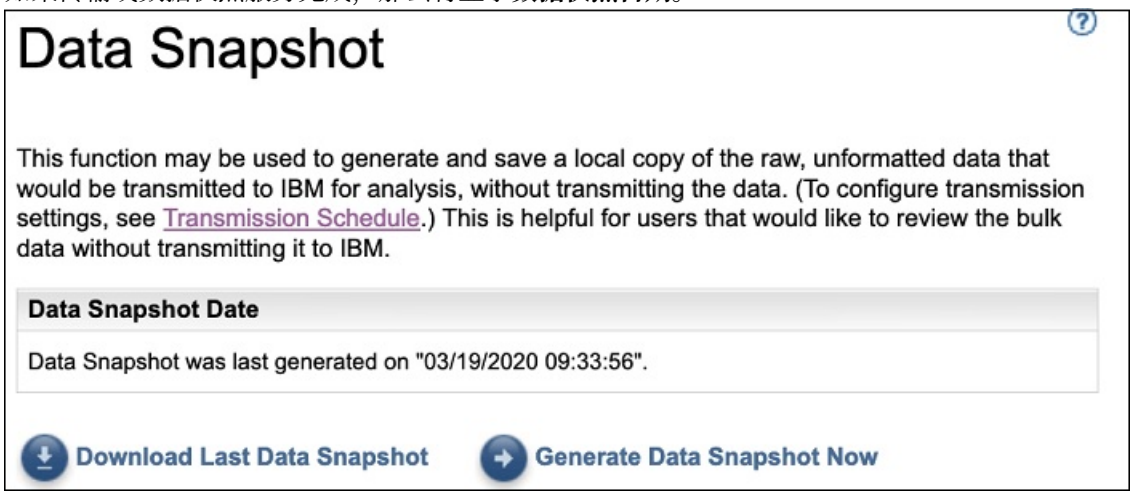

图 *75.* 数据快照日期

4. 单击**下载上一个数据快照**，下载最新数据快照。指定生成的文件 (*collection.tar.xz*) 的位置。根据数据量，下载操作可能需要一段时间。要抽取 *.tar.xz* 归档的内容，请使用 *tar* 实用程序（用于 Linux）或 *7-Zip* 实用程序（同时适用于 Linux 和 Windows）。

   注:

   - 如果传输或收集作业正在进行，那么会显示以下消息 - 收集作业当前正在运行。在 `<<timestamp>>` 生成了最新数据快照。是否确定要下载收集的信息？。
     - 单击**确定**可继续下载。
     - 单击**取消**可取消下载并等待当前正在运行的收集作业完成。
   - 如果传输或收集作业未在运行，那么会显示以下消息 - 在 `<<timestamp>>` 生成了最新数据快照。是否确定要下载收集的信息？。单击**确定**可继续下载。

查看库存摘要

使用“**库存摘要**”页面，可以查看 IT 元素（例如，已发现的计算机系统、操作系统和存储子系统）的摘要。

单击导航窗格中的**库存摘要**以显示“**库存摘要**”页面。

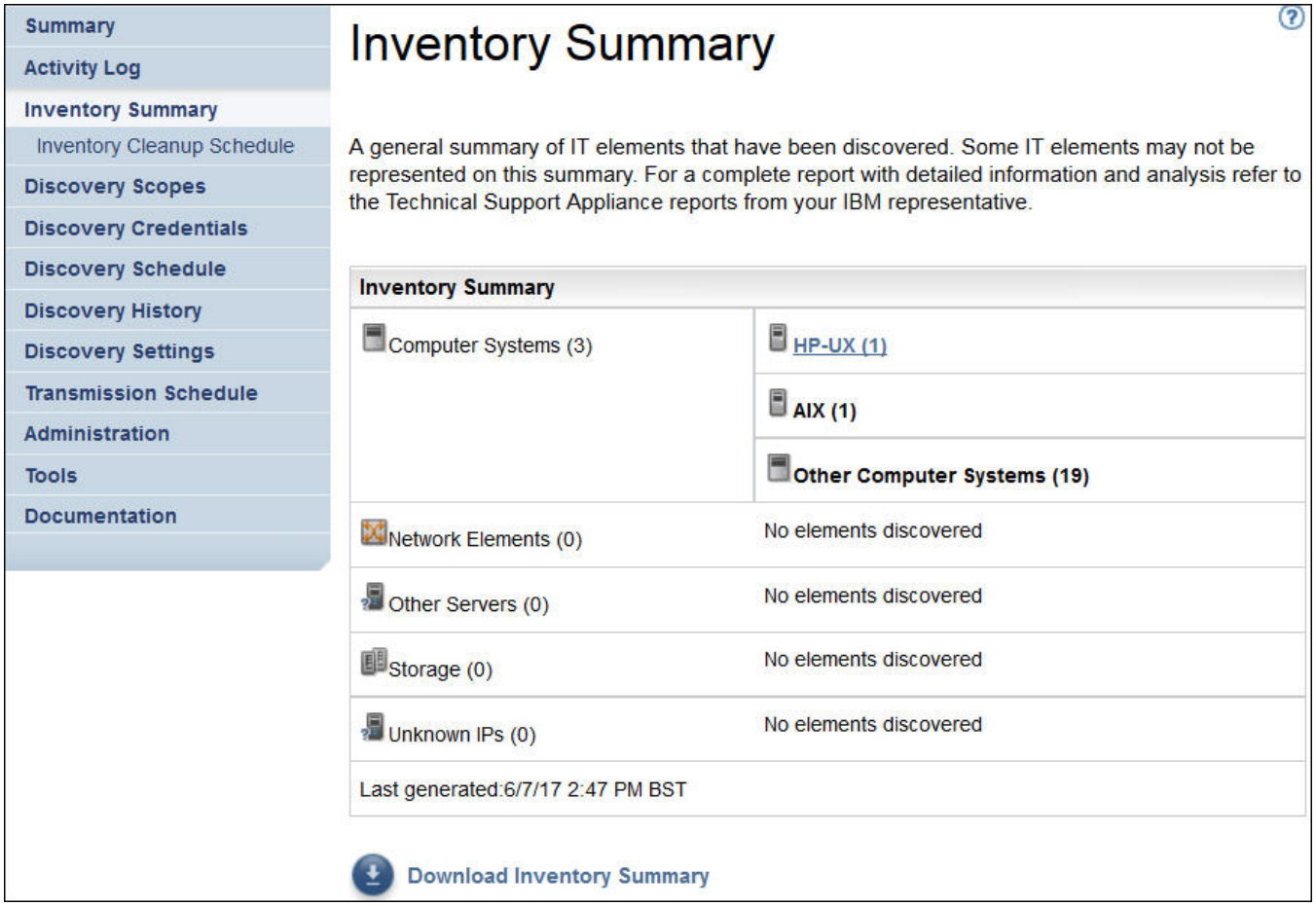

图 76. 库存摘要

“库存摘要”页面显示 6 个不同的 IT 元素组：

- **虚拟机管理器**：包括 HMC、IBM Flex System Manager、VMware 和 VIOS 等管理程序。
- **计算机系统**：包括物理计算机系统。
- **操作系统**：包括在裸机或虚拟环境中运行的 AIX 和 Linux 等操作系统。
- **网络元素**：包括交换机和路由器。
- **存储**：包括 IBM XIV、IBM FlashSystem、EMC 和 HP 存储设备等存储子系统。此外，它还包括磁带设备。
- **未知 IP**：可能由于如下原因而未归类的设备：
  - 防火墙阻止访问该设备。
  - 没有为设备定义任何凭证。请查看“**认证状态**”页面（**工具 → 认证状态**），以了解有关 IP 地址和关联凭证的信息。
  - 不存在该设备类型的传感器。
- **上次生成时间**行指示库存摘要作业的上次完成时间。

注: TSA 启动后不久就会显示此窗格中的数据。如果您在此时间范围内查看该页面，那么将显示以下参考消息：**正在生成库存摘要**。在最初填充摘要信息后，大约每 30 分钟刷新一次。要手动刷新，请单击浏览器的**刷新**图标。

每个组将显示设备类型列表和每种设备类型的计数。

1. 单击任何设备类型超链接以查看“**库存摘要详细信息**”页面。

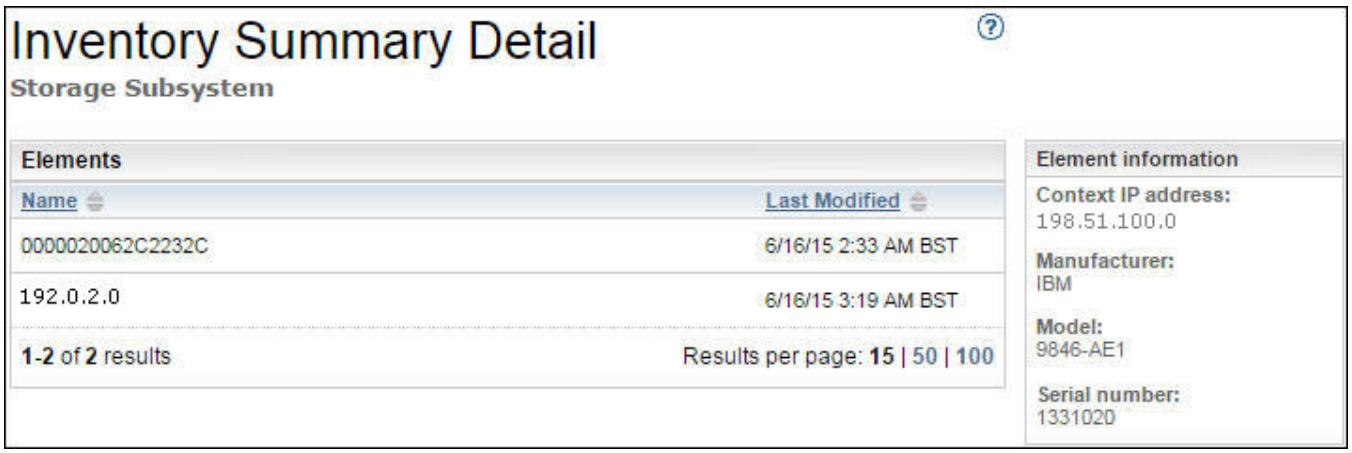

图 *77.* 库存摘要详细信息

2. 选择列表中的任何设备以查看**要素信息**，例如，上下文 *IP* 地址、制造商、型号和序列号。

   注: 对于 TSA 已检测到但没有为其定义有效凭证的设备，不填写**要素信息**。TSA 需要成功登录到设备以提供这些详细信息。

单击**下载库存摘要**可下载包含已发现设备的摘要的文件。

调试发现问题

认证状态

使用“**认证状态**”页面，可以查看在作用域集中定义且存在凭证问题的 IT 元素的摘要。

要查看认证状态，请单击导航窗格中的**工具 > 认证状态**。这样会显示“**认证状态**”页面。

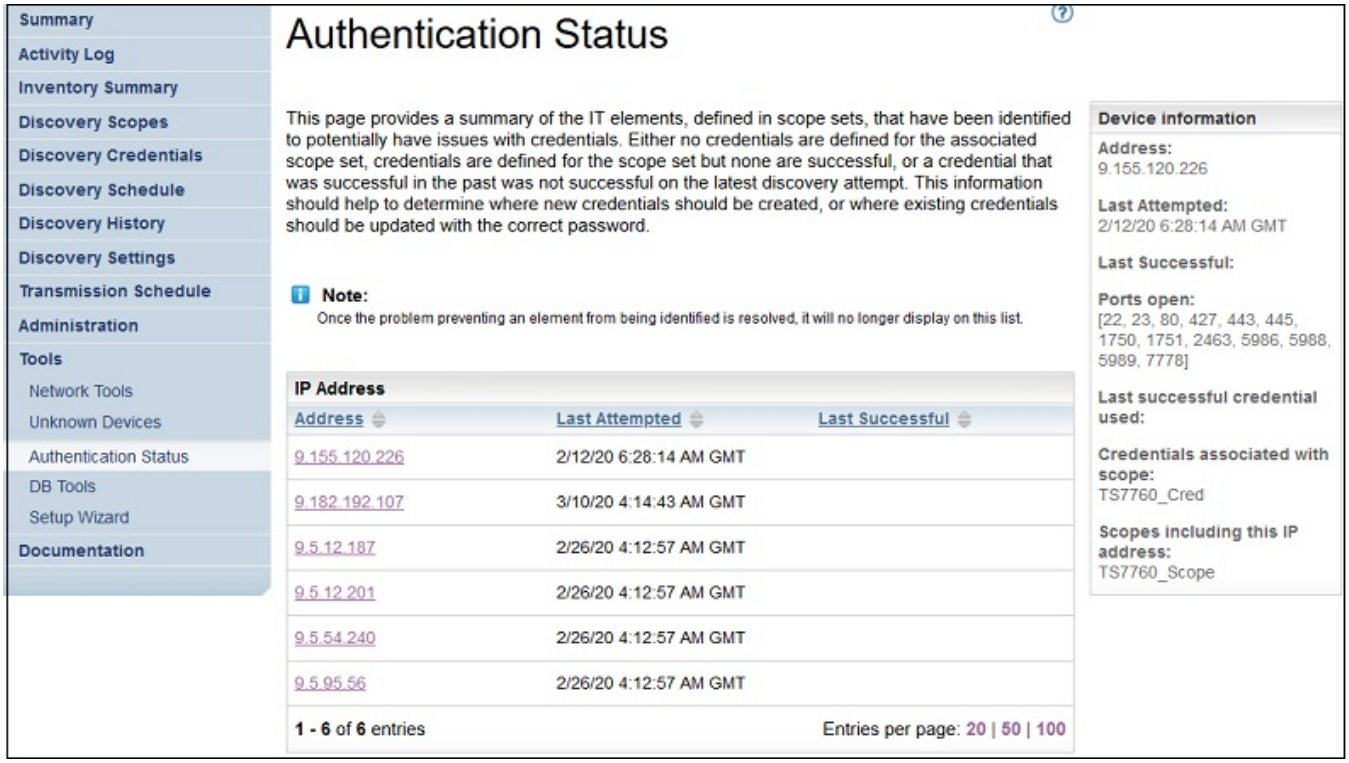

图 *78.* 认证状态

该状态将显示报告了凭证问题的所有设备 IP。这些问题可能由于以下任何原因引起：

· 没有为相关作用域集定义凭证。

· 为相关作用域集定义凭证失败。

· 过去成功的凭证在最近的发现尝试中失败。

单击相应的 IP 地址链接可查看设备信息，例如，上次尝试时间、上次成功时间、打开的端口、使用的上一个成功凭证、凭证的上次更改日期、与作用域关联的凭证以及包含此 *IP* 地址在内的作用域。这些信息有助于确定需要创建新凭证的情况或者需要使用正确密码更新现有凭证的情况。

注: 解决了设备的凭证问题后，列表中将不会再显示相应的设备 IP。

未知设备

您可以显示有关 TSA 已发现但是无法完全识别的设备的信息。

要显示这些未知设备，请单击导航窗格中的**工具 > 未知设备**。这样会显示“**未知设备**”页面。

您可以单击“未知 IP”列表中的任何条目以显示有关此设备的其他信息。

第 6 章 设置管理任务

状态信息

TSA 提供摘要信息、日志和报告以支持您快速查找有关作业、发现的库存和产品信息的信息。

您可以通过单击导航窗格中的**摘要**，显示有关作业、库存和产品信息的高级摘要信息。“**摘要**”页面频繁刷新以显示最新的摘要信息。“**摘要**”页面包含以下信息：

- **系统状态**

  “**系统状态**”窗格显示正在执行的当前服务和任务的状态。 您可以通过单击“**系统状态**”窗格中的服务名称，显示服务页面。

- **作业摘要**

  “**作业摘要**”窗格显示当前作业的摘要。

- **库存摘要**

  “**库存摘要**”窗格显示已发现的库存的列表。

- **产品信息**

  “**产品信息**”窗格显示 TSA 的主机名和标识。

查看活动日志

活动日志将显示发现和传输过程的日志消息。您可以单击活动日志中的条目以查看更多信息。

您可以通过单击导航窗格中的**活动日志**来显示活动日志。此时会显示日志条目列表。 每个条目都会显示消息、严重性和活动发生时间。

图 *79.* 活动日志

注: 由于是在单个作用域集上运行发现，因此一个完整发现可能存在多个日志条目。

要显示有关任何活动日志条目的扩展详细信息，请单击此条目的消息。

要将日志文件保存到计算机，请单击**下载所有日志**。

要清除日志，请单击**清除日志**。

查看库存清理归档

您可以查看根据在**库存清理计划安排**中指定的休眠期清理的库存

关于此任务

要查看已删除的库存，请执行以下步骤：

过程

1. 在“**库存清理计划安排**”页面上，单击**显示清除归档**。这样会显示“**库存清理归档**”页面。

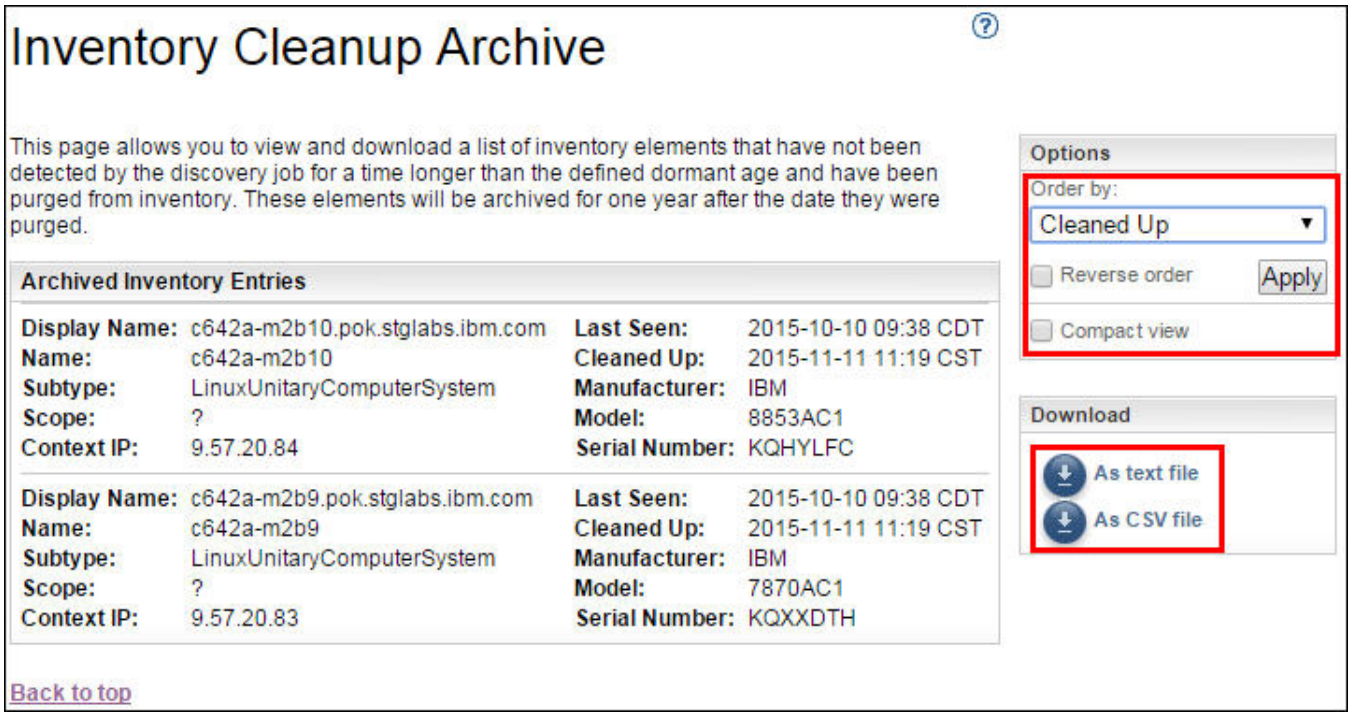

图 *80.* 库存清理归档

2. 在“**库存清理归档**”页面上，您可以查看在清理过程中从库存清除的元素。

   注:

   · 您只能在此归档中查看一年的库存信息。一年后，将清除归档信息。

   · 如果所有定义的目标都是在去年主动发现的，那么归档将为空（也就是，没有要清理的对象）。

3. 使用**选项**窗格可对库存详细信息进行重新排序。

   a) 在“**选项**”窗格中选择**排序依据**属性，然后单击**应用**，以对库存详细信息视图进行排序。

   b) 选择**倒序**选项以按选定属性的倒序顺序来查看详细信息。

   c) 选择**紧凑视图**选项可查看库存的摘要。

4. 单击**另存为文本文件**或**另存为 CSV 文件**以下载库存详细信息。保存库存详细信息可在本地处理数据，而且可以在计算机上将数据保留更长时间（超过一年）。保存在此归档中的数据仅保留一年，然后将其清除。

密码

使用密码来保护 TSA 用户帐户。

更改密码

可以更改 TSA 用户密码。

过程

1. 在导航窗格中，单击**管理 > 密码**。
   这样会显示“**密码**”页面。
2. 在**当前密码**字段中输入当前密码。
3. 在**新密码**字段中输入新密码。
   密码必须遵守以下规则：
   - 必须至少包含 8 个字符
   - 必须至少包含 1 个字母字符和 1 个非字母字符
   - 不得包含用户名
   - 不得与之前的 8 个密码相同
   - 必须每 90 天至少更改一次，但每天不能更改多次。
4. 在**确认密码**字段中重新输入新密码。
   比较您输入的两个密码以确认它们相互匹配，然后再保存密码。
5. 单击**保存**。

下一步做什么

要点: 无法恢复密码，因此，如果丢失或忘记密码，那么您将无法登录到 TSA 来更改凭证。如果丢失或忘记用户帐户或者管理员帐户（如果有多个帐户）的密码，请与 TSA 管理员联系。如果丢失或忘记缺省管理员帐户（随设备一起提供）的密码，请与 IBM 支持人员联系。有关更多信息，请参阅第 19 页的『登录到 Technical Support Appliance』部分。

安全

您可以访问和修改 TSA 的安全功能和实用程序。

“**安全**”页面列出可用的安全实用程序。在此页面上，您可以修改会话超时设置，或者修改所有用户帐户的最长密码使用期限。

修改会话超时设置

出于安全原因，在一段时间没有活动后 TSA 将注销用户。您可以阻止 TSA 自动注销用户，或者更改用户注销前的时间量。

禁用会话超时

您可以通过禁用会话超时，阻止 TSA 在一段时间没有活动后自动注销用户。

过程

1. 选中**禁用会话超时**复选框。
2. 单击**更改会话超时设置**。

修改会话超时值

缺省情况下，用户在持续 20 分钟不活动后注销。您可以通过修改会话超时值来增加用户注销前的时间量。

过程

1. 清除**禁用会话超时**复选框。
2. 在**会话超时**字段中，输入 TSA 注销用户前的时间量（以秒为单位）。

   注: 会话超时值不能小于 20 分钟。
3. 单击**更改会话超时设置**。

修改密码使用期限

作为一项安全措施，每个用户都必须在指定天数后更改其 TSA 登录密码。缺省情况下，密码的最长使用期限为 90 天，但是您可以将密码的最长使用期限更改为 30 天或 60 天。

过程

1. 在导航窗格中，单击**管理 > 安全**。这样会显示“**安全**”页面。
2. 在“**安全**”页面上，向下滚动以查看**最长密码使用期限**窗格。
3. 在**最长密码使用期限**窗格中，从**最长使用期限**下拉列表中选择使用期限（30 天、60 天或 90 天）。
4. 单击**更改最长密码使用期限**来进行更新。此时会显示以下确认消息：已更新最长密码使用期限。

备份与复原

您可以备份和复原 TSA 配置。

要点: 强烈建议定期执行备份。在更改作用域集或凭证后也应该执行备份。

备份日期

显示发生最新备份的日期和时间。

配置摘要

使用此选项可在保存前查看当前 TSA 配置的摘要。

要显示 TSA 配置摘要，请执行以下步骤:

1. 在导航窗格中，单击**管理 > 备份与复原**。这样会显示“**备份与复原**”页面。
2. 单击**查看摘要**以查看当前 TSA 配置摘要。所示信息将显示在执行备份时 TSA 保存的配置。

   注: 将通过弹出窗口来显示此信息。如果 Web 浏览器拦截了弹出窗口，那么可能需要允许浏览器显示来自 TSA 的弹出窗口。

   在**摘要**页面中，**备份**部分会显示与备份状态相关的信息以及以下消息:

   · 正常 () 图标（如果在 60 天内执行过备份）。

   · 警告 () 图标（如果在超过 60 天但不超过 90 天的时间内未执行过备份）。

   · 错误 () 图标（如果超过 90 天未执行过备份）。

备份

使用此选项可保存 TSA 配置的副本。

要备份 TSA 配置，请执行以下步骤:

1. 在导航窗格中，单击**管理 > 备份与复原**。这样会显示“**备份与复原**”页面。

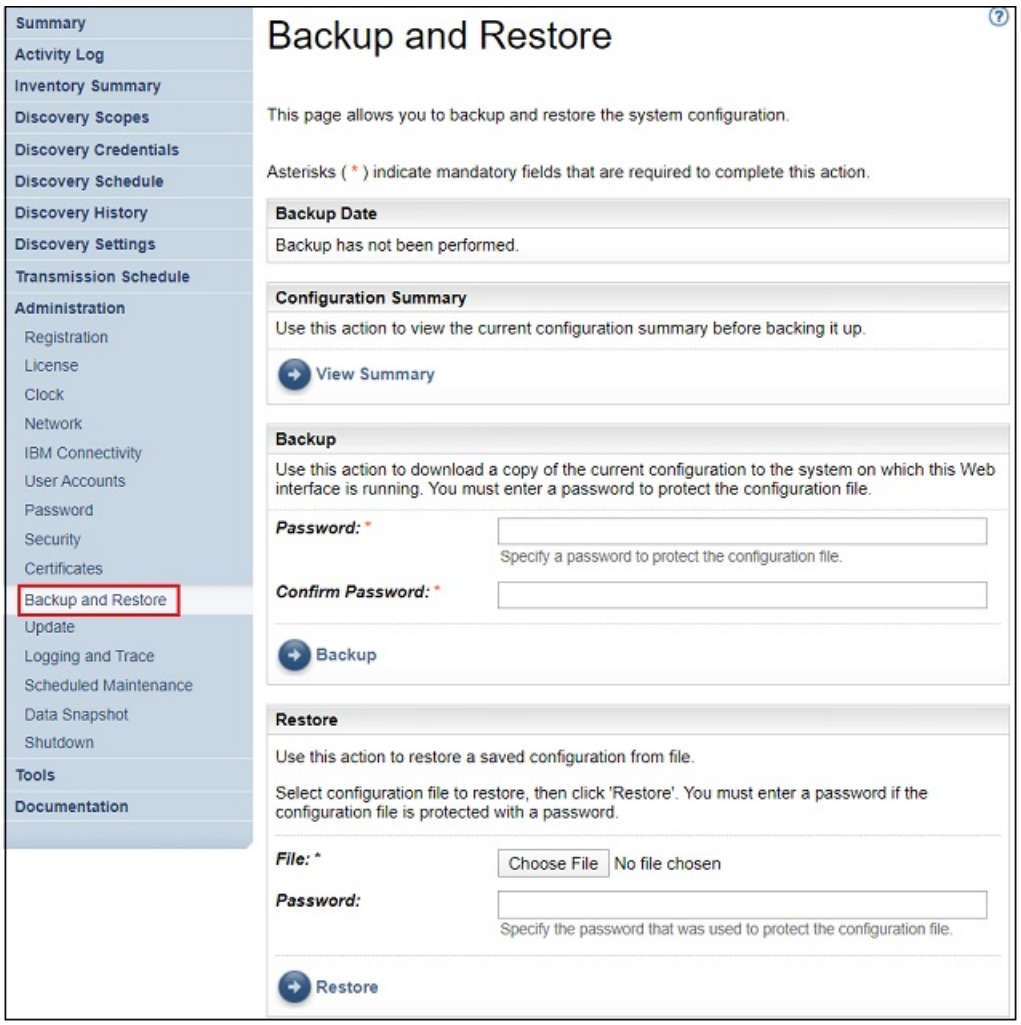

图 *81.* 备份与复原

2. 在**备份**窗格中输入用于保护配置文件的密码。
3. 在**确认密码**字段中重新输入密码。比较您输入的两个密码以确认它们相互匹配，然后再保存密码。

   注: 您需要安全地保存此密码，因为在复原期间需要使用此密码。
4. 单击**备份**并在系统上保存备份配置压缩文件。

   注: 生成的备份配置文件只能由 TSA 打开。

   注: 如果最近更改了管理员密码，请在更改密码后生成备份并使用最新备份文件进行复原。

复原

使用此选项可复原先前保存的配置副本。

要复原 TSA 配置，请执行以下步骤:

1. 在导航窗格中，单击**管理 > 备份与复原**。这样会显示“**备份与复原**”页面。
2. 单击**选择文件**以找到并选择要复原的配置文件。
3. 输入用于备份配置文件的密码。
4. 单击**复原**。

   这样会在“**摘要**”页面的“作业摘要”窗格中显示该复原作业。在完成复原后，将提示您重新启动系统。

   注: 从备份复原将删除现有配置。包括作用域定义和凭证在内的所有配置都将替换为备份文件中的配置。

注: 执行备份或复原操作时，确保“**摘要**”页面中的发现作业管理器状态为“正常”( )。 如果发现作业管理器未在运行，那么您将收到一条消息 -“发现作业管理器未在运行。在恢复活动 (通常最多需要 10 分钟) 之前，请确保在“摘要”屏幕中通过绿色复选标记描述了发现作业管理器的状态。”如果 10 分钟后发现作业管理器未在运行，请联系 IBM 支持人员。

更新

您可以检查和下载 TSA 的更新。

过程

1. 在导航窗格中，单击**管理** > **更新**。
   这样会显示“**更新**”页面。

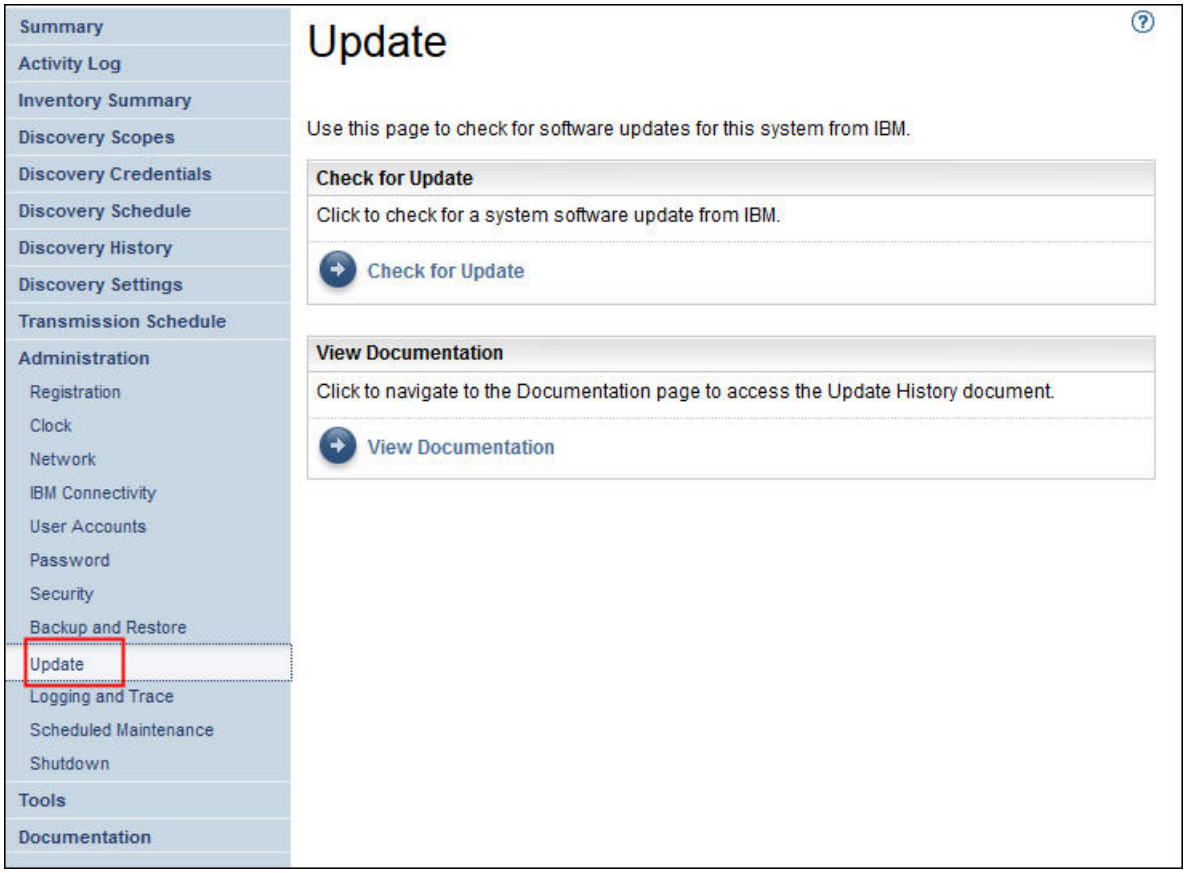

图 *82.* 更新

2. 单击**检查更新**。
   “**更新可用性**”页面将列出任何可用更新。

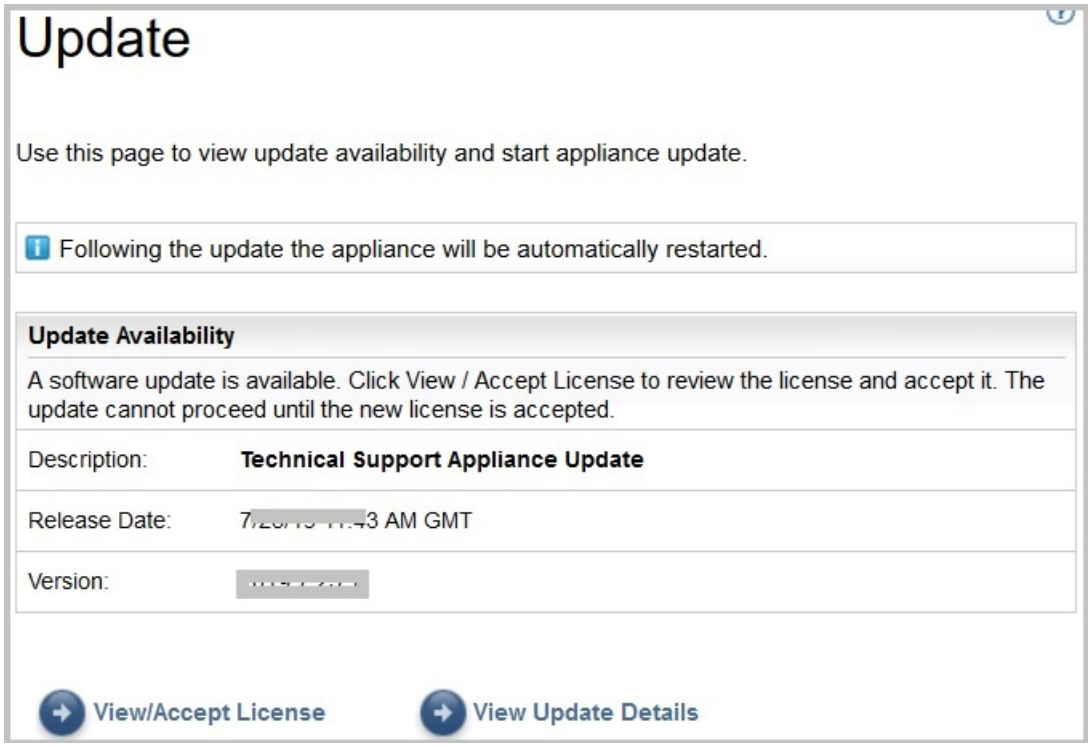

图 *83.* 更新可用性

a) 对于某些新版本的 TSA，您必须先接受新的许可协议，然后才能继续执行更新。如果有新许可证，请单击**查看/接受许可证**，这样会显示“**许可协议**”页面。

b) 单击“**许可协议**”页面上的**接受**按钮以接受新的许可协议。将再次显示“**更新**”页面以及**立即执行更新**按钮。如果不需要接受新的许可协议，那么不会显示**查看/接受许可证**按钮，单击**立即执行更新**以继续。

注:

· 接受许可证后，将不再显示**查看/接受许可证**按钮。

· 在导航窗格中，单击**管理** > **许可证**以查看已接受的最新许可协议。

c) 要安装更新，请单击**立即更新**。

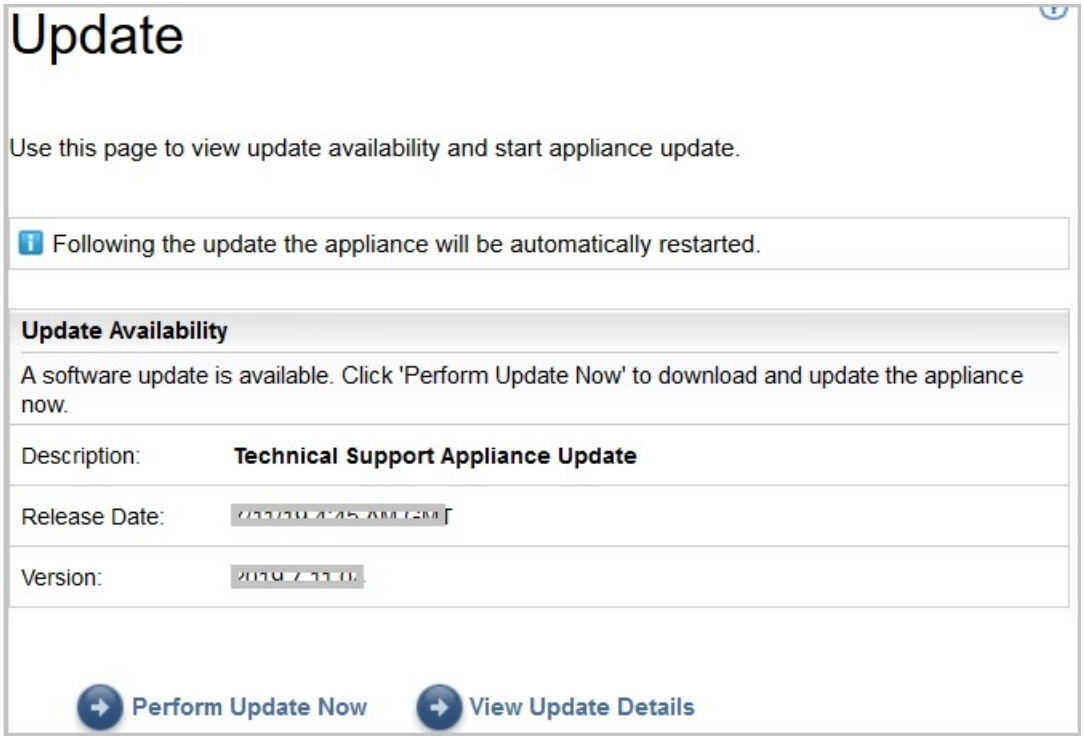

图 *84.* 立即更新

在完成更新后，TSA 会自动重新启动。

d) 要查看有关更新内容的信息，请单击**查看更新详细信息**。

启用计划安排的维护

要保持 TSA 以最佳性能运行，建议启用计划安排的维护功能。

关于此任务

计划安排的维护作业可确保 TSA 的最佳性能。您可以始终启用或禁用此功能。如果启用了计划安排的维护，那么可以设置自动运行维护的日期和时间。计划安排的维护的状态显示在“**摘要**”页面的“**系统状态**”部分中。

如果安排了维护作业，那么系统将在维护后自动重新启动，并在系统重新启动前一小时通知您。例如，由于计划安排的维护，系统重新启动作业将进入排队并在 59 分钟后启动。

要点: 请勿在其他计划安排作业（例如，发现、传输或库存清理）的 30 分钟内安排设备维护。如果在其他计划安排的作业的 30 分钟内安排维护，那么 TSA 无法运行这些作业。

过程

要编辑维护计划安排，请完成以下步骤：

1. 在导航窗格中，单击**计划安排的维护**。

   “**计划安排的维护**”页面显示**计划安排**的下一个计划安排的运行以及计划安排的运行时间。“**历史记录**”部分显示当前正在运行和先前的维护作业的状态以及更多详细信息。

2. 在“**计划安排的维护**”页面上，单击**编辑计划安排**。
   a) 在“**启用计划安排**”窗格中，选择是想要启用还是禁用计划安排的维护。
   b) 如果选择启用计划安排的维护任务，那么选择**按小时**和**按分钟**下拉列表以选择新时间。
   c) 选择**日期选择模式**。要将维护安排在一周中的某几天，请选择**周日期（周日-周六）**选项；要将维护安排在一个月中的某几天，请选择**月日期 (1-31)** 选项。

d) 选择**日期**字段的相应复选框，从而选择周或月份的不同日期或其他日期。

注: 如果选择了超过特定月份最后一天的日期，那么将在此特定月份的最后一天触发作业。

3. 单击**保存**。

这样会再次显示“**计划安排的维护**”页面以及新计划安排。

日志记录和跟踪

您可以查看和修改 TSA 诊断跟踪设置。您还可以修改发现作业管理器跟踪级别的设置。修改这些设置可能影响性能，因此仅在 IBM 支持人员的指示下才能执行此操作。

1. 在导航窗格中，单击**管理 > 日志记录和跟踪**。这样会显示“**日志记录和跟踪**”页面。**TSA 跟踪级别**窗格显示当前跟踪设置（错误、警告、信息、调试或跟踪）。

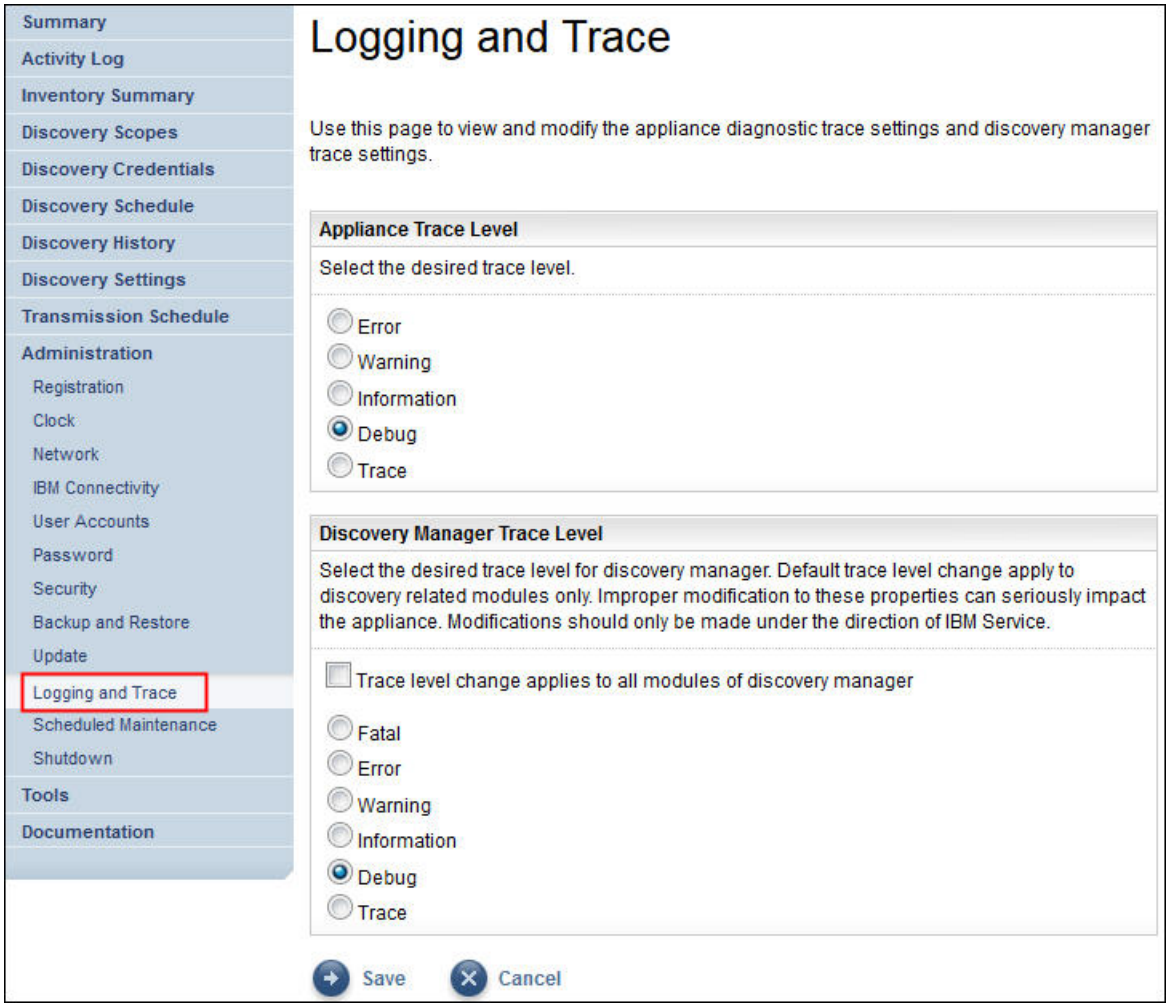

图 *85.* 日志记录和跟踪

2. 如果需要，您可以通过单击想要的跟踪设置旁边的单选按钮，更改 **TSA 跟踪级别**窗格中的跟踪设置。
3. 单击**保存**。

注: 缺省情况下，*TSA* 跟踪级别与其发现作业管理器跟踪级别窗格的跟踪级别设置为**调试**级别。

要查看和修改“**发现作业管理器跟踪级别**”设置，请执行以下步骤:

要点: 只有在 IBM 服务人员的指示下才能对此部分进行修改。

1. 在导航窗格中，单击**管理 > 日志记录和跟踪**。这样会显示“**日志记录和跟踪**”页面，以指示当前跟踪设置。

2. 如果想要将跟踪级别应用于发现作业管理器的所有模块，请选中**跟踪级别变更适用于发现作业管理器的所有模块**。
3. 选择想要的跟踪设置旁边的单选按钮。
4. 单击**保存**。

关闭

您可以暂挂或恢复 TSA 操作，或者关闭然后重新启动 TSA 或者切断其电源。

关闭可能需要几分钟才能完成。

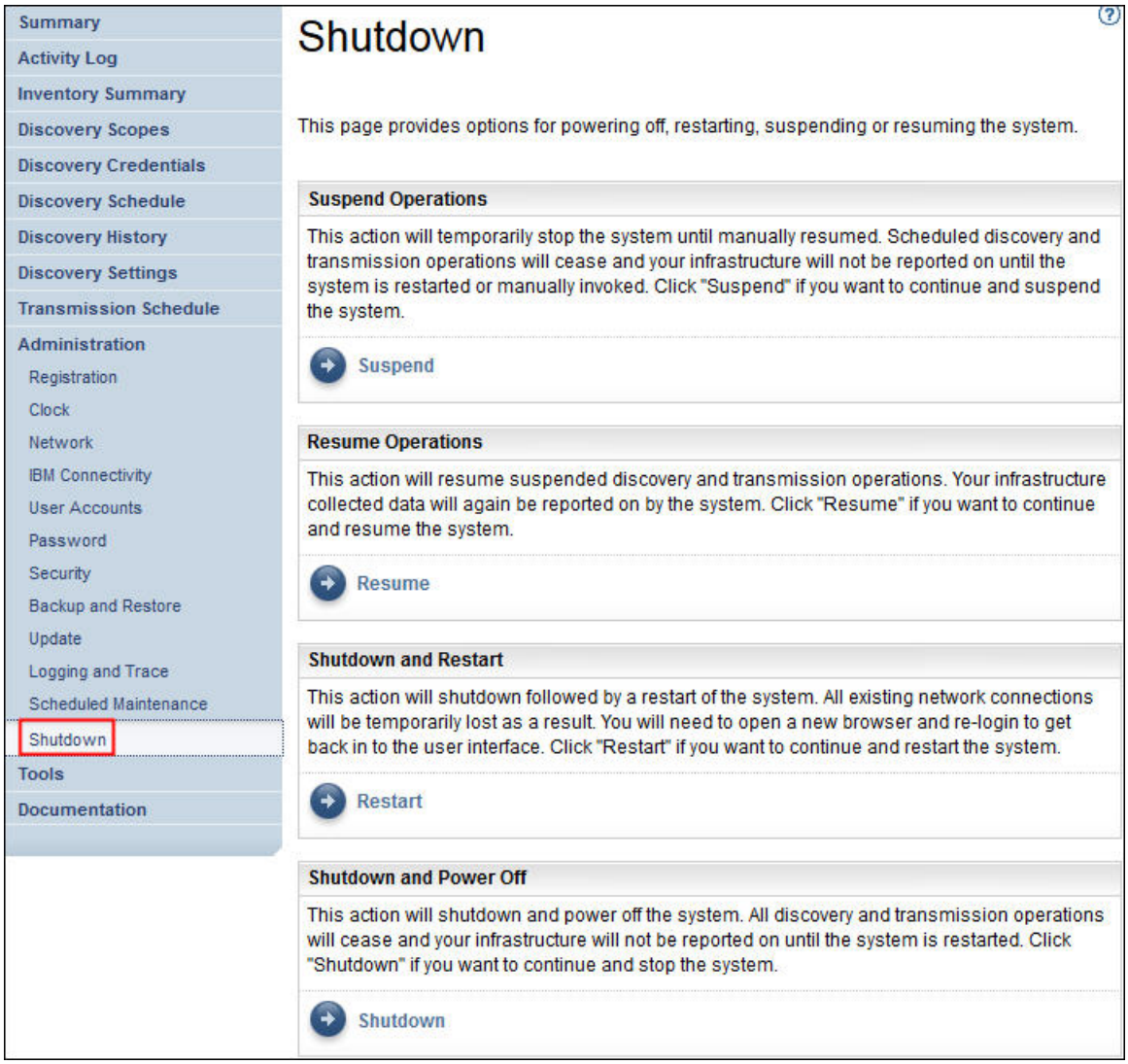

图 *86.* 关闭

暂挂操作

此操作将暂时停止 TSA。所有发现和传输操作都将停止，并且不会向 IBM 报告任何信息，直至恢复操作为止。

要暂挂 TSA 操作，请执行以下步骤：

1. 在导航窗格中，单击**管理 > 关闭**。这样会显示“**关闭**”页面。
2. 单击**暂挂**。

恢复操作

此操作将恢复暂时停止的 TSA。所有发现和传输操作将恢复，并且将按计划安排向 IBM 报告信息。

要恢复 TSA 操作，请执行以下步骤：

1. 在导航窗格中，单击**管理 > 关闭**。这样会显示“**关闭**”页面。
2. 单击**恢复**。

关闭并重新启动

此操作关闭然后重新启动 TSA。所有现有的网络连接都会暂时断开。您必须打开新浏览器并重新登录。

要关闭并重新启动 TSA，请执行以下步骤：

1. 在导航窗格中，单击**管理 > 关闭**。这样会显示“**关闭**”页面。
2. 单击**重新启动**。

关闭并切断电源

此操作关闭 TSA 并切断电源。所有发现和传输操作停止并且将不会报告基础结构，直至 TSA 重新启动。

要关闭 TSA 并切断电源，请执行以下步骤：

1. 在导航窗格中，单击**管理 > 关闭**。这样会显示“**关闭**”页面。
2. 单击**关闭**。

注: 关闭设备后，必须使用 VMware ESXi Web 界面或 Hyper-V Manager 打开 TSA 的电源。

工具

TSA 提供工具来帮助您设置 TSA 环境。

您可以通过单击导航窗格中的**工具**来访问这些工具。

网络工具

使用“**网络工具**”页面以获取 TSA 使用的网络协议的诊断工具和信息。

要访问这些诊断工具，请单击导航窗格中的**工具 > 网络工具**。这样会显示“**网络工具**”页面。

“网络工具”页面划分为选项卡式页面。单击任何选项卡可显示对应于此选项卡的页面。

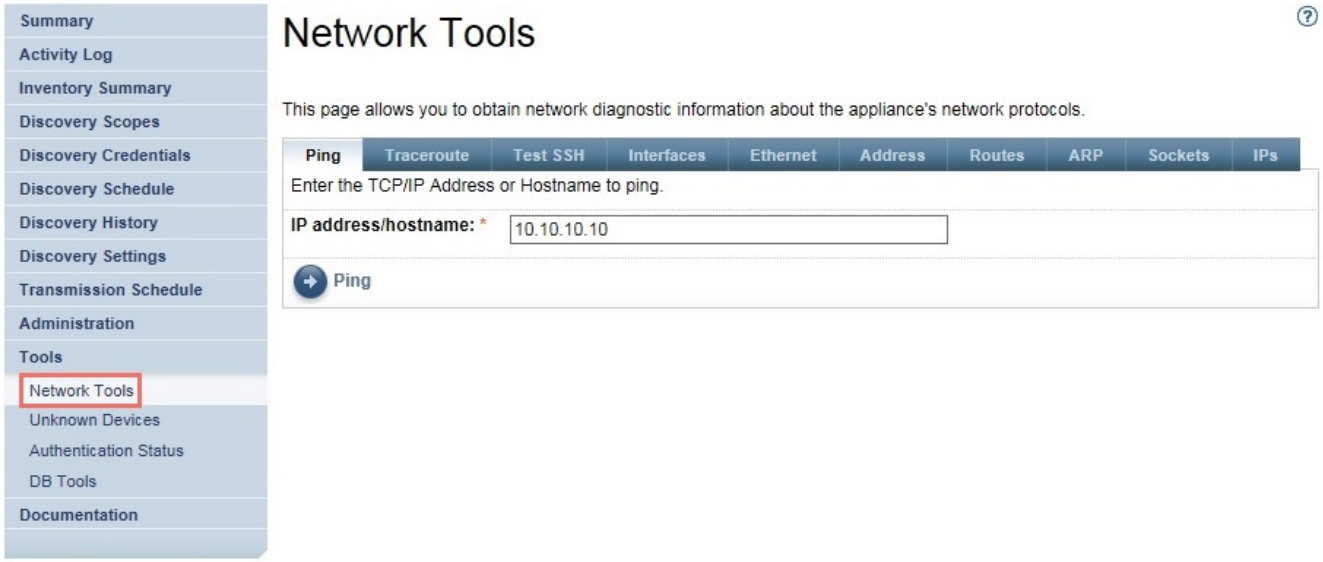

图 *87.* 网络工具

Ping
使用此页面可向远程主机发送回传请求，以检查该主机是否可访问并接收有关主机名或 IP 地址的信息。

跟踪路由
使用此页面可显示数据包到达远程主机所采取的路径。

测试 SSH
使用此页面可测试是否可使用针对主机定义的发现凭证通过 SSH 访问远程主机。

接口
使用此页面可以显示当前配置的网络接口的统计信息。

以太网
使用此页面可以显示当前配置的以太网卡的设置。

地址
使用此页面可以显示当前配置的网络接口的 IP 地址。

路由
使用此页面可以显示内核 IP 路由表和相应的网络接口。

ARP
使用此页面可以显示地址解析协议 (ARP) 连接的内容。

套接字
使用此页面可以显示有关 TCP/IP 套接字的信息。

IP
使用此页面可以显示有关 IP 数据包过滤规则的信息。

注: 输入的主机名不得包含下划线 (“_”)。

数据库工具

使用“**数据库工具**”页面，可以运行数据维护操作。建议仅在 IBM 支持人员指示时使用这些功能。

您可以对数据库运行以下操作:

重新创建库存数据库

在重新创建库存数据库时，所有库存数据都会丢失。此外，如果清除了**保留凭证**复选框或者发现作业管理器不可用，那么凭证将丢失。

要重新创建数据库，请完成以下步骤:

1. 在导航窗格中，单击**工具** > **数据库工具**。
2. 在“**重新创建库存数据库**”部分中，选中**保留凭证**复选框以保留所有发现凭证。如果未选中该复选框，那么凭证将丢失并且您需要重新设置所有凭证。有关发现凭证的更多信息，请参阅第 62 页的『发现凭证』。

   注: 仅当发现作业管理器正在运行（绿色状态）时，才能保留凭证。
3. 单击**重新创建库存数据库**。将显示以下警告消息：执行此操作将暂时关闭发现作业管理器。是否确定要重新创建库存数据库？
4. 单击**确定**以重新创建库存数据库。这样会显示以下消息 - 已开始重新创建数据库。重新创建数据库大约需要 6 小时，在此期间，会在“摘要”页面中显示以下消息：`dbinit 正在启动`。6 小时后，您可以检查“**活动日志**”以查看状态是否为成功重新创建库存数据库。

   注: 在重新创建库存数据库时，发现作业管理器将暂时关闭，并且会清除库存清理归档。

执行 RUNSTATS

要运行 **RUNSTATS** 命令，请完成以下步骤:

1. 在导航窗格中，单击**工具** > **数据库工具**。
2. 单击**执行 RUNSTATS**。将显示以下警告消息：是否确定要对库存数据库表执行 RUNSTATS？

3. 单击**确定**。这样会显示以下消息 - 已开始执行 RUNSTATS。在约 30 分钟后，您可以检查活动日志。在作业完成时，会向活动日志添加以下消息：成功对库存数据库执行 RUNSTATS。

执行 REORG

要运行 **REORG** 命令，请完成以下步骤：

1. 在导航窗格中，单击**工具 > 数据库工具**。
2. 单击**执行 REORG**。将显示以下确认消息：是否确定要对库存数据库表执行 REORG？
3. 单击**确定**。将向活动日志添加以下消息：已开始执行 REORG。在约 30 分钟后，您可以检查活动日志。作业完成时，会向活动日志添加以下消息：成功对库存数据库执行 REORG。

文档

使用“**文档**”页面以开始使用 IBM Technical Support Appliance。您可以访问设置指南和安全文档，查看样本报告，以及从以下 TSA Web 站点下载 TSA 安装代码：https://ibm.biz/TSAdemo。

过程

要查看文档并了解有关 Technical Support Appliance 的更多信息，请执行以下步骤：

1. 单击左侧导航菜单中的**文档**。

图 *88.* 文档

2. 要了解有关 Technical Support Appliance 的更多信息，请单击链接：https://ibm.biz/TSAdemo
3. 在“**安装 TSA**”页面上，将找到指向 TSA 映像、设置指南、配置指南和相关教程的链接。

第 7 章 就 Technical Support Appliance (TSA) 问题联系 IBM 支持人员

IBM 支持人员在您当地时区星期一到星期五的工作时间内提供服务。

关于此任务

您可以通过以下两个选项中的任何一个来联系 IBM 支持人员：

1. 在 IBM 支持门户网站上建立案例
2. 通过 IBM 呼叫中心创建服务请求

在 IBM 支持门户网站上建立案例

过程

1. 登录到 https://www.ibm.com/mysupport/s/

   注： 您必须首先创建一个帐户以访问 IBM 支持门户网站。
2. 单击门户网站右上方的**建立案例**。这样会显示“**建立案例**”页面。
3. 选择**支持类型**。
4. 输入**标题**、**产品制造商**和**产品**。

   注： 要直接将请求发送给 Technical Support Appliance 团队，请在**产品**字段中输入 `Technical Support Appliance`。
5. 选择**严重性**
6. 输入**描述**，并选择首选语言。
7. 如果没有代理会说您的语言，并且您有兴趣用英语交流，请选择**是**。
8. 单击**提交案例**。

通过 IBM 呼叫中心创建服务请求

过程

1. 拨打原产地对应的电话号码：https://www.ibm.com/planetwide
2. 选择语言。
3. 选择 1（IBM 产品）。
4. 选择 2（软件支持）。
5. 使用产品标识 *5621IZX01* 或使用产品名称 *Technical Support Appliance*。
6. 系统将提示您提供：
   - 公司编号/地理位置
   - 客户/公司名称
   - 地址/城市/州或省/自治区/直辖市/邮政编码
   - 大厦/楼层房间
   - TSA 所在位置的电话号码
   - 联系人姓名/电子邮件/电话号码
   - 问题描述

· 严重性级别

附录 A 使用 VMware vSphere Client 安装 TSA

开始之前
TSA 需要装入 VMware ESXi 6.5 或更高版本来控制硬件。

关于此任务
请执行以下步骤以安装 TSA 映像。有关需求的更多信息，请参阅第 3 页的『TSA 需求』。

注: 此过程（从步骤 1 到步骤 12）可作为有关如何部署 TSA 映像的示例/参考。部分步骤可能会随虚拟机不同的本地部署过程而有所变化。

过程

要安装 TSA，请执行以下步骤:

1. 启动 VMware vSphere Client。
2. 登录以连接到 ESXi 系统。
3. 在 vSphere Client 上，单击**文件 > 部署 OVF 模板**。这样会显示“**部署 OVF 模板**”向导。

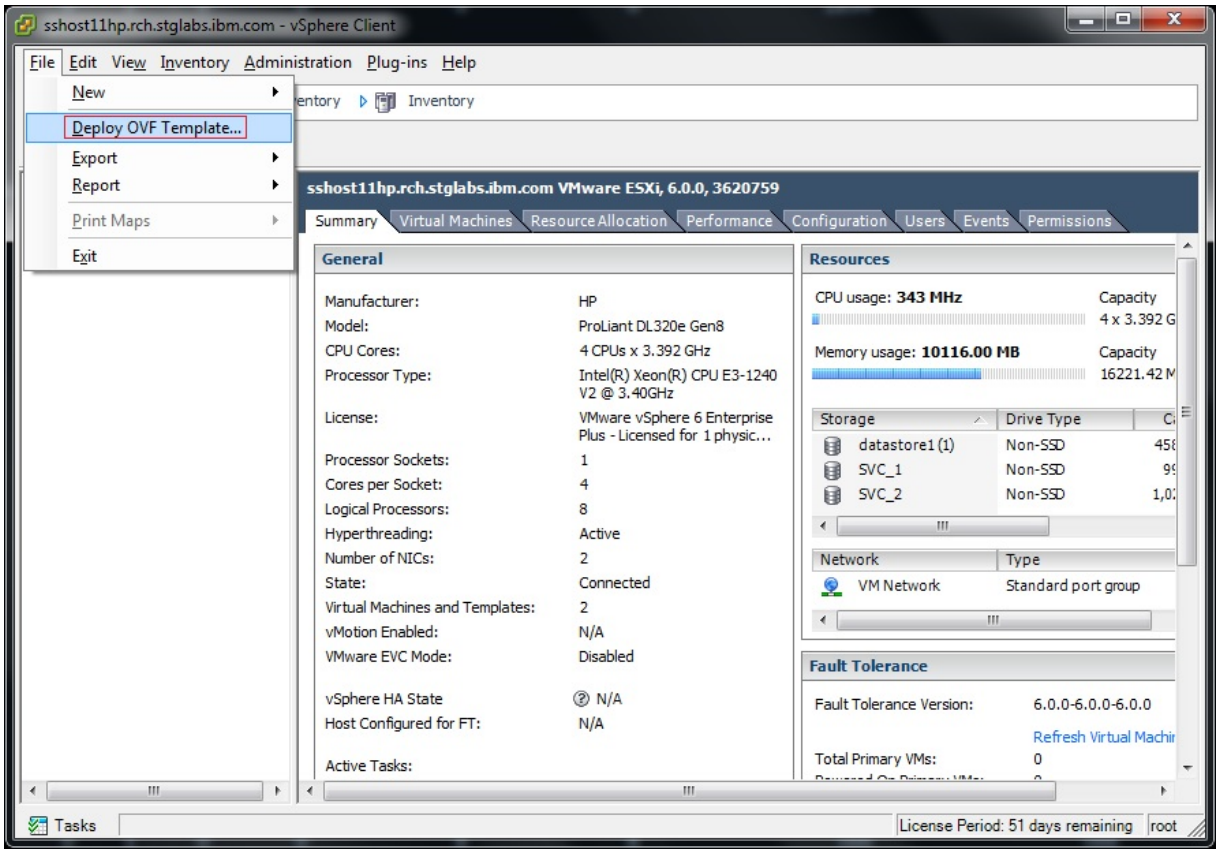

图 *89.* 部署 *OVF* 模板

4. 单击**浏览**并选择在系统上保存的映像。

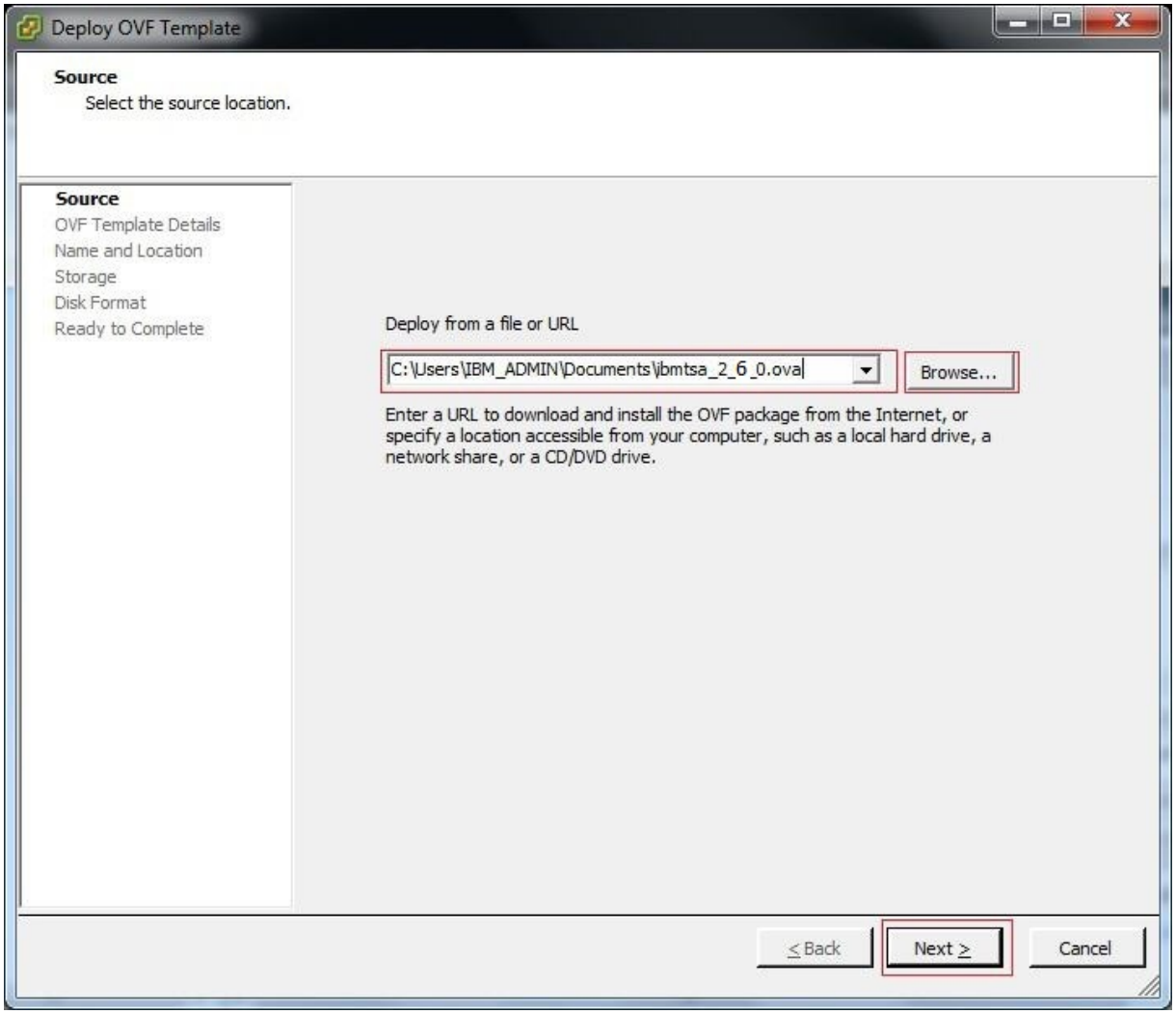

图 *90. OVF* 模板源

5. 单击**下一步**。 这样会显示 **OVF 模板详细信息**。
6. 单击**下一步**。 这样会显示**名称和位置**窗格。

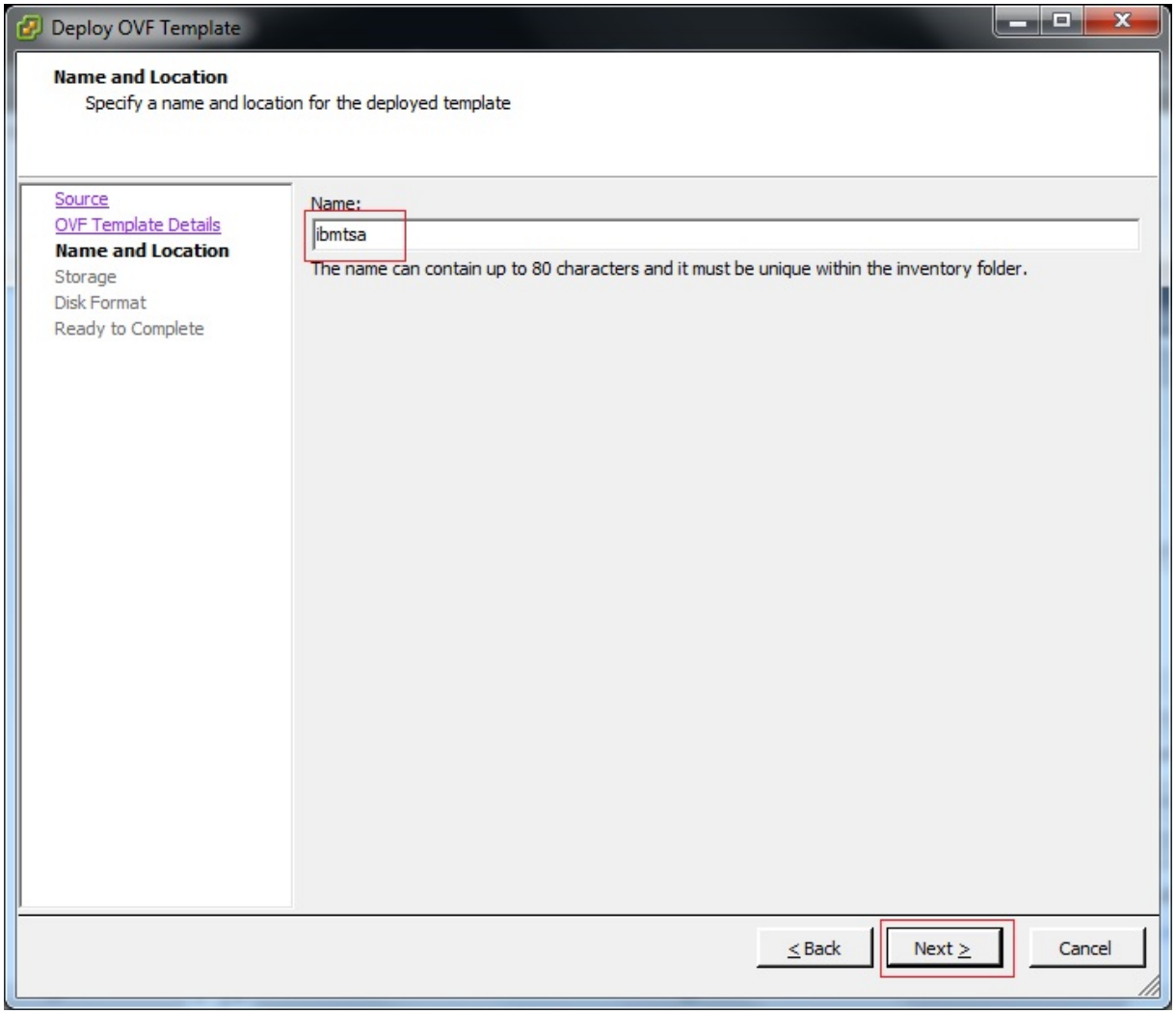

图 *91.* 名称和位置

7. 在**名称和位置**窗格上，输入虚拟机的**名称**或者使用缺省值，然后单击**下一步**。
8. 在**存储**窗格上，选择数据存储设备（用于存储虚拟机文件的存储设备），然后单击**下一步**。

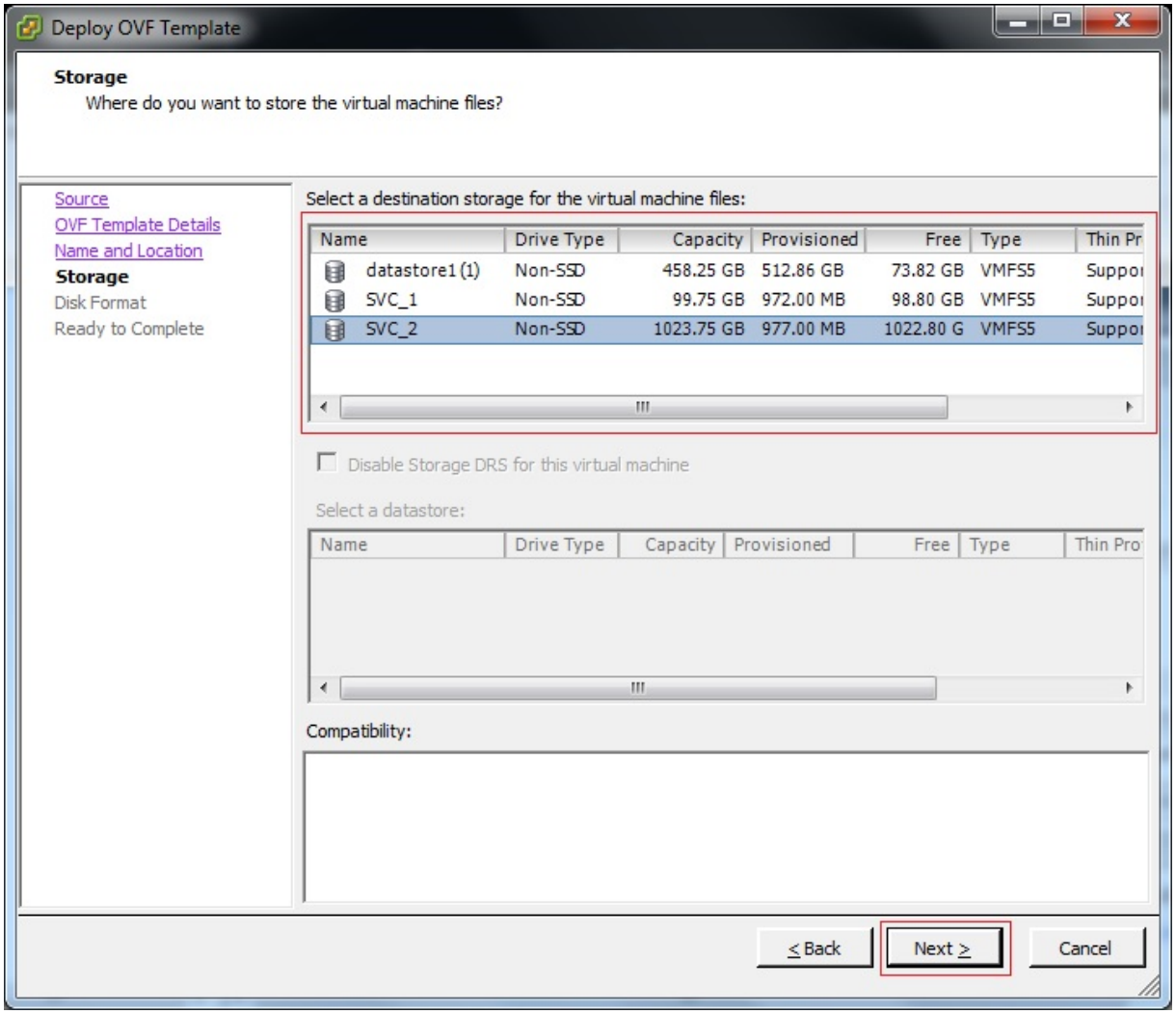

图 92. 存储

9. 在**磁盘格式**窗格上，选择 **Thick Provision Eager Zeroed** 选项，然后单击**下一步**。

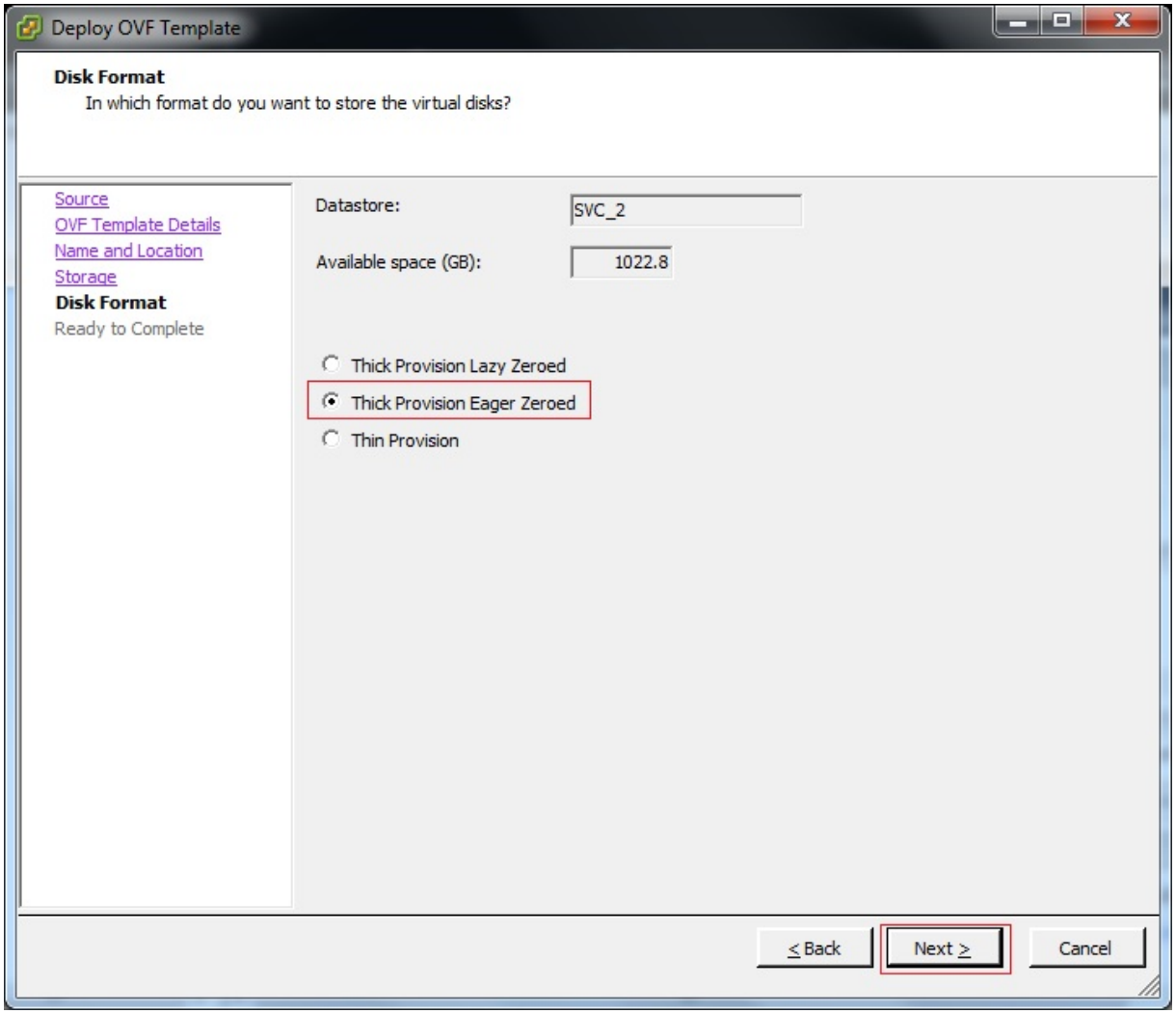

图 *93.* 磁盘格式

10. 如果 ESXi 具有单个网络连接，请继续到下一步。否则，在“**网络映射**”窗格上选择相应的网络，然后单击**下一步**。
11. 可选： 选择**部署后打开电源**选项以在部署后自动打开虚拟机电源。您还可以在完成部署后手动打开虚拟机电源。

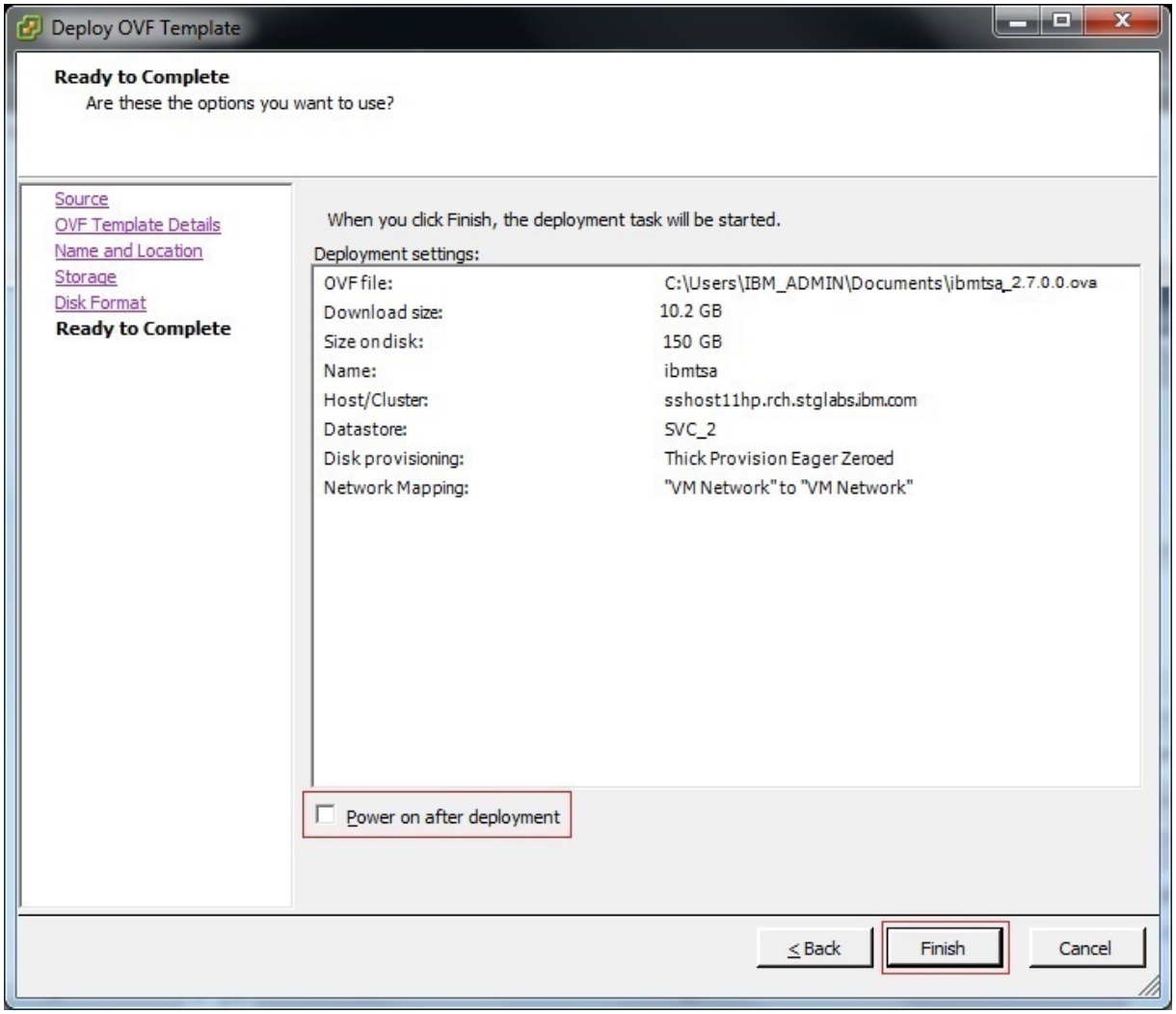

图 *94.* 准备完成

12. 单击**完成**。部署 TSA 可能需要 30 分钟左右，但是会因您的系统与 VMware ESXi 系统之间的网络连接速度而异。
13. 在成功部署 TSA 后，选择新部署的虚拟机，然后单击 vSphere Client 的**控制台**选项卡。
14. 登录到 TSA 控制台以设置网络配置。对于 **ibmtsa 登录**，输入 **tsausr**；对于**密码**，输入 **configTsa**。
15. 必需： 要更改登录密码，请继续执行第 17 页的『更改 tsausr 密码（必需）』部分中列出的步骤。
16. 要完成安装，请继续执行第 17 页的『配置网络详细信息』部分中列出的步骤。

附录 B 配置 Technical Support Appliance

如果退出或跳过在“**设置向导**”中配置任何设置，那么可以从 TSA 的左侧导航菜单中手动配置。

注册 Technical Support Appliance

注册收集在 TSA 向 IBM 报告信息进行分析时识别 TSA 所需的信息。

关于此任务
要进行注册，请执行以下步骤：

过程

1. 在导航窗格中，单击**管理** > **注册**。
   这样会显示“**注册**”页面。

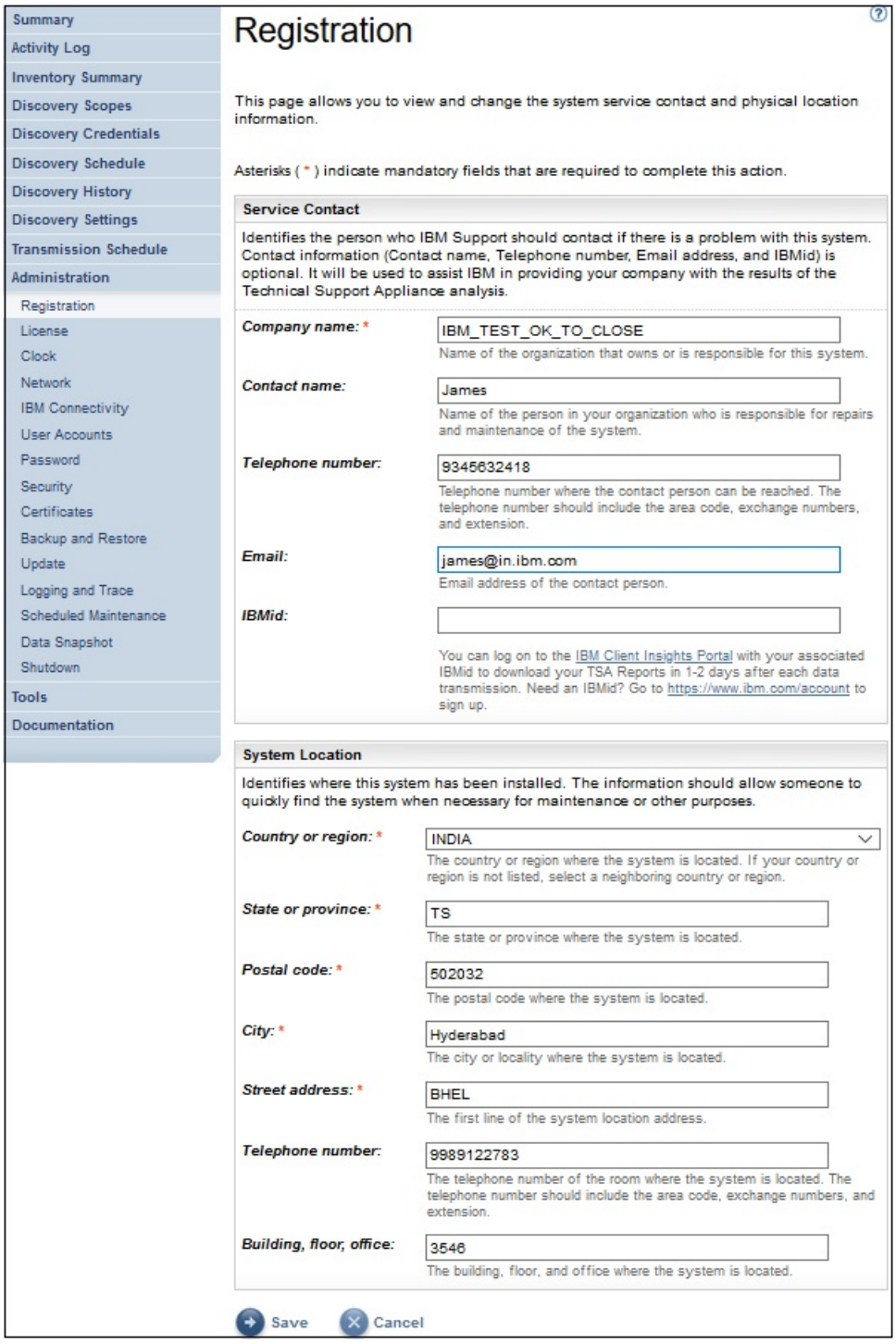

图 *95.* 注册

2. 在以下字段中指定服务联系人信息：

公司名称
使用 TSA 的组织的名称。

联系人姓名
（可选）组织中负责 TSA 的人员的姓名。

电话号码
（可选）可与联系人联系的电话号码。电话号码应包含区号、交换号和分机号。请勿在电话号码中使用括号。

电子邮件
（可选）联系人的电子邮件地址。

IBMid
（可选）您想要授权其在 IBM Client Insights 门户网站上查看报告的人员的 IBMid。

注: 在每次数据传输后 1-2 天内，您可以使用关联的 IBMid 登录到 https://clientinsightsportal.ibm.com/ 来下载 TSA 报告。要注册 IBMid，请转至 https://www.ibm.com/account。

注: 服务联系人标识当系统出现问题时 IBM 支持人员应联系的人员。联系人信息可帮助 IBM 向贵公司提供 Technical Support Appliance 分析的结果。

3. 在以下字段中指定 TSA 位置信息：

国家或地区
TSA 所在位置的国家或地区。

州或省/自治区/直辖市
TSA 所在位置的州或省/自治区/直辖市。如果您不确定州或省/自治区/直辖市，请输入未知

邮政编码
TSA 所在位置的邮政编码。

城市
TSA 所在位置的城市或地区。

街道地址
TSA 位置地址。

电话号码
（可选）TSA 所在房间的电话号码。电话号码应包含区号、交换号和分机号。请勿在电话号码中使用括号。

大厦、楼层和办公室
（可选）TSA 所在的大厦、楼层和办公室。

4. 单击**保存**以保存注册信息。

设置 IBM 连接

指定在连接到 IBM 时要使用的因特网连接信息。

开始之前
确保防火墙允许连接到 IBM 服务器主机名和 IP 地址（如第 4 页的表 1 中所述）。如果网络不允许访问 IBM 服务器，TSA 与 IBM 支持人员之间的事务将失败。

过程

1. 在导航窗格中，单击**管理** > **IBM Connectivity**。

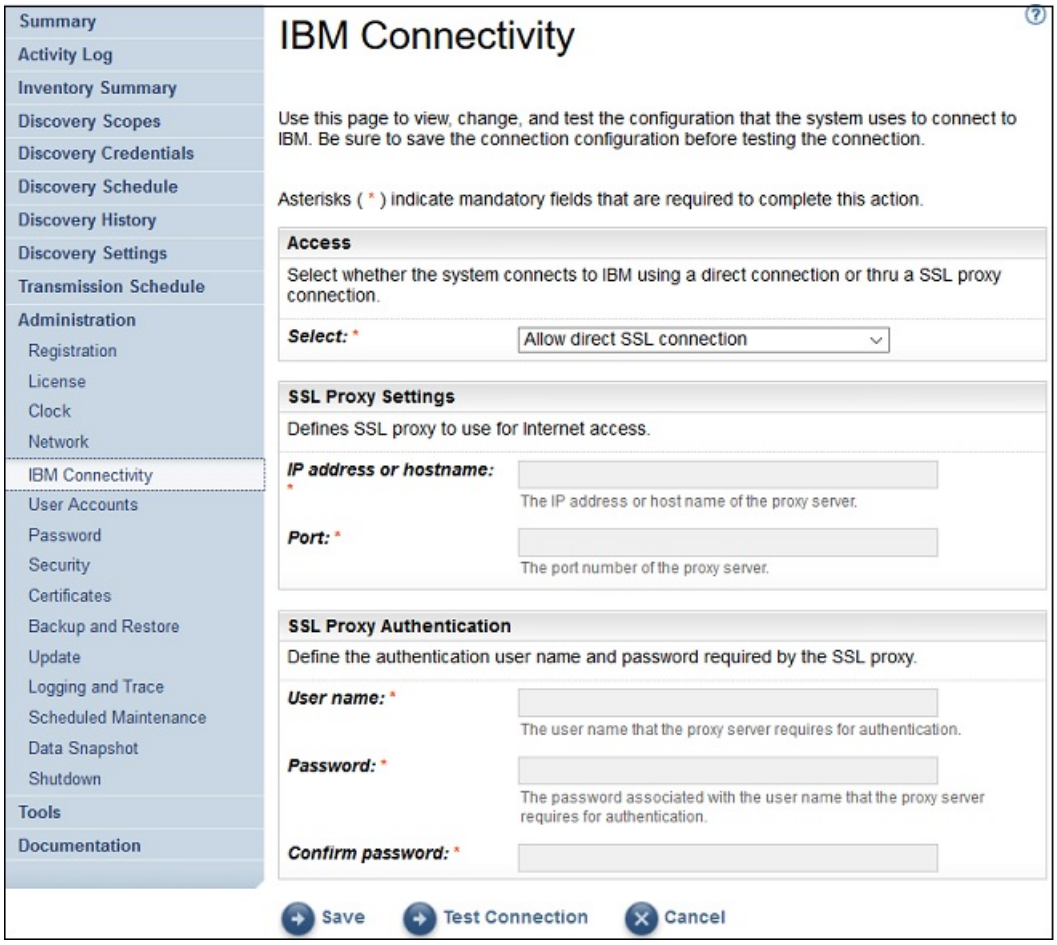

图 *96. IBM Connectivity*

2. 在“**访问**”窗格中，从以下因特网访问类型中进行选择：

   允许直接 SSL 连接
   TSA 使用直接连接来连接到 IBM。

   使用 SSL 代理连接
   TSA 使用 SSL 代理连接来连接到 IBM。

   使用认证 SSL 代理连接
   TSA 使用认证 SSL 代理连接来连接到 IBM。

3. 如果已选择**使用 SSL 代理连接**或**使用认证 SSL 代理连接**，请为代理服务器指定以下信息。

   IP 地址或主机名
   代理服务器的 IP 地址或主机名。

   注: 输入的主机名不得包含下划线 (“_”)。

   端口
   代理服务器的端口号。

4. 如果已选择**使用认证 SSL 代理连接**，请为代理服务器指定以下信息：

   用户名
   代理服务器进行认证所需的用户名。

   密码
   代理服务器进行认证所需的、与用户名关联的密码。

   确认密码
   再次输入密码。比较您输入的两个密码以确认它们相互匹配，然后再保存密码。

5. 单击**保存**可保存 IBM 连接信息。
6. 单击**测试连接**以测试指定的连接。

要点:

· 在测试连接之前保存连接设置。

· 您必须具有到 IBM 的正常运行的连接，否则 TSA 功能将不起作用。

相关概念

连接到 IBM 支持人员的配置需求

TSA 可通过直接连接或通过用户提供的代理（必须配置为允许与 IBM 通信）连接到 IBM 支持人员。如果使用代理，那么不支持 TLS/SSL 检查。必须允许通过代理的任何请求直接传递到 IBM，而不会发生 TLS/SSL 终止。

设置时钟

在设置期间，必须设置 TSA 系统时间、日期和本地时区。

过程

1. 在导航窗格中，单击**管理 > 时钟**。
   这样会显示“**时钟**”页面。

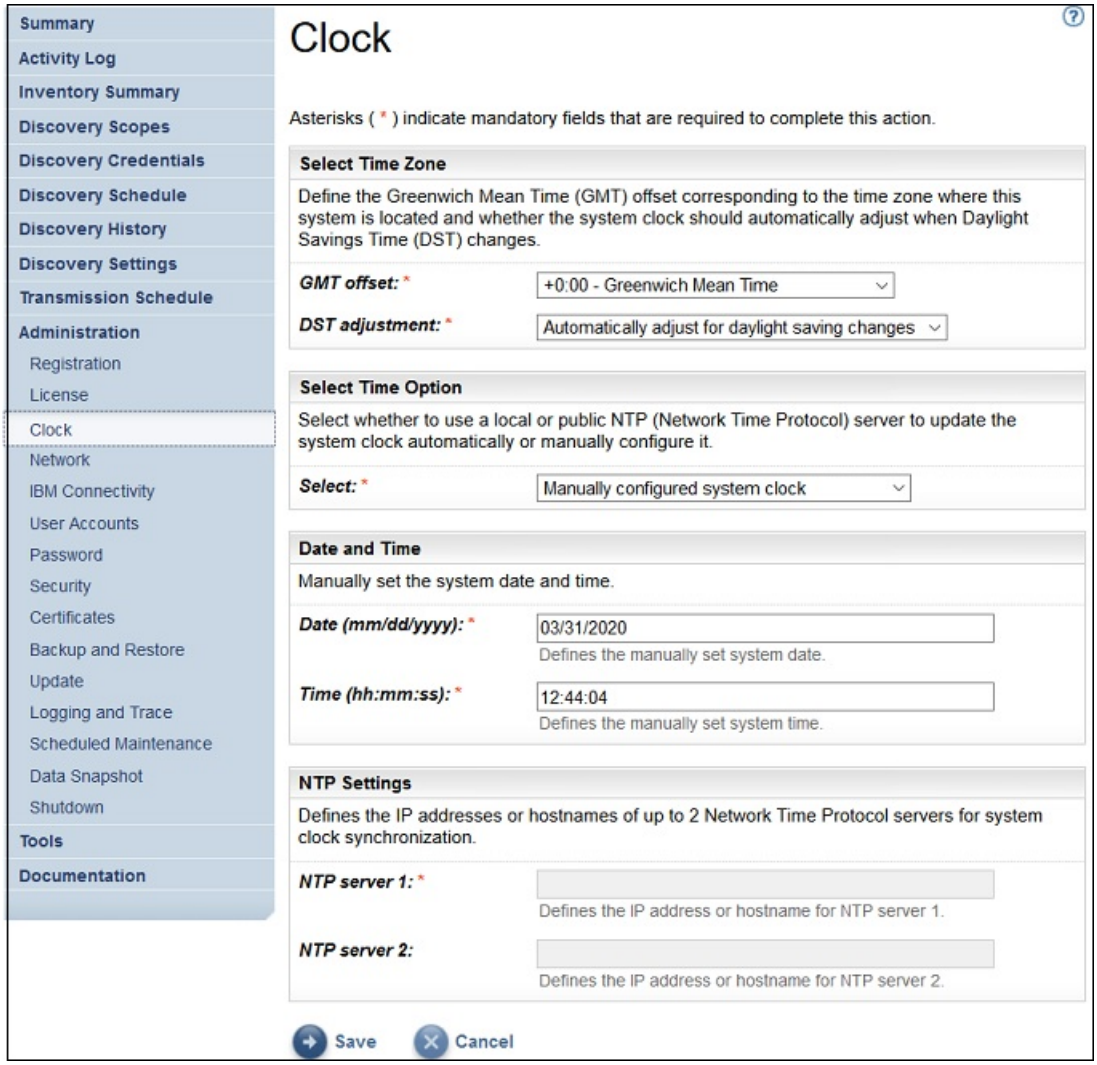

图 97. 时钟

2. 从 **GMT 偏移量**下拉列表中选择本地时区。
3. 从 **DST 调整**下拉列表中选择夏令时 (DST) 调整。

注: 并非所有时区都允许 DST。如果针对不允许 DST 的时区选择了此选项，那么将显示一条错误消息。

4. 从**选择时间选项**下拉列表中选择一种方法来更新系统时钟。

   选项包括同步系统时钟与网络时间协议 (NTP) 服务器来自动更新系统时钟，或者手动配置系统时钟。

   a) 如果选择了手动配置系统时钟，那么必须设置系统日期和时间。在**日期**和**时间**字段中，输入日期和时间信息。

   b) 如果选择了同步系统时钟与网络时间协议 (NTP) 服务器来自动更新系统时钟，那么必须指定 NTP 服务器的 IP 地址和主机名。在 **NTP 服务器**字段中，输入最多两台服务器的 IP 地址或主机名信息。

      注: 确保 TSA 可通过网络来访问 NTP 服务器。

5. 单击**保存**以保存时钟信息。

结果

注: 需要重新启动系统，某些更改才会生效。例如，如果设置了日期或时间，或者将手动配置更改为 NTP 服务器配置，那么将提示您重新启动系统。

设置传输计划安排

TSA 提供缺省计划安排以使传输过程在指定的时间运行。 您可以根据需求修改此计划安排。

过程

1. 在导航窗格中，单击**传输计划安排**。

   这样会显示“**传输计划安排**”页面。

   “**计划安排**”窗格显示下一个计划安排的运行以及计划安排的运行时间。“**历史记录**”窗格显示当前正在运行和先前的传输作业的状态以及其他详细信息。

2. 单击**编辑计划安排**。

   这样会显示“**传输计划安排**”页面。

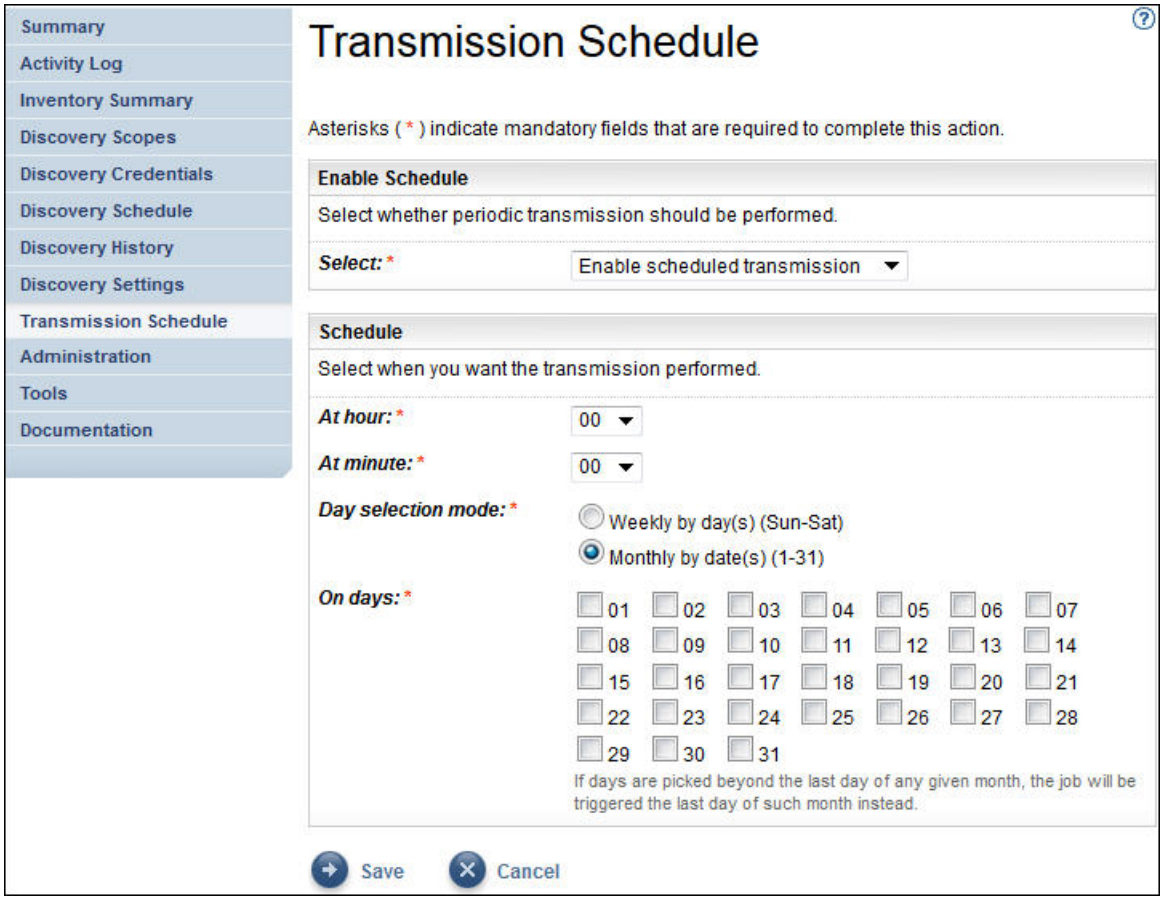

图 *98.* 编辑传输计划安排

a) 使用**按小时**和**按分钟**下拉列表以选择新时间。

b) 选择**日期选择模式**。

周日期（周日-周六）

要将传输操作安排在一周中的某一天（或某几天），请选择**周日期（周日-周六）**选项。

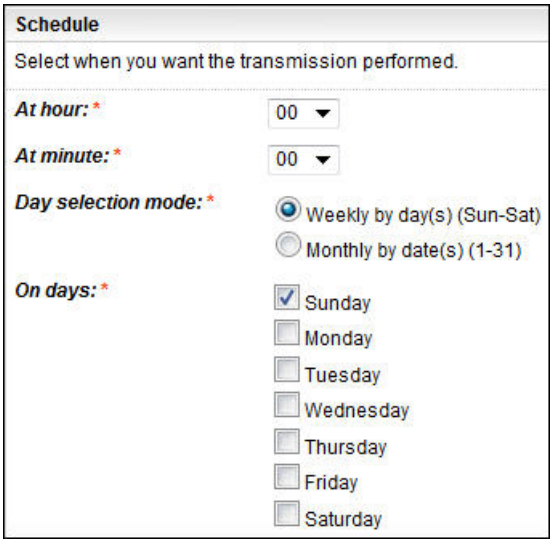

图 *99.* 周日期（周日-周六）

对于**日期**字段，选中相应复选框以选择一周中的一天或多天。

月日期 (1-31)

要将传输操作安排在一个月中的某一天（或某几天），请选择**月日期 (1-31)** 选项。

对于**日期**字段，选中相应复选框以选择一个月中的一天或多天。

注: 如果选择了超过特定月份最后一天的日期，那么将在此特定月份的最后一天触发作业。

3. 单击**保存**。
   此时会再次显示“**传输计划安排**”页面以及新计划安排。

更新

您可以检查和下载 TSA 的更新。

过程

1. 在导航窗格中，单击**管理** > **更新**。
   这样会显示“**更新**”页面。

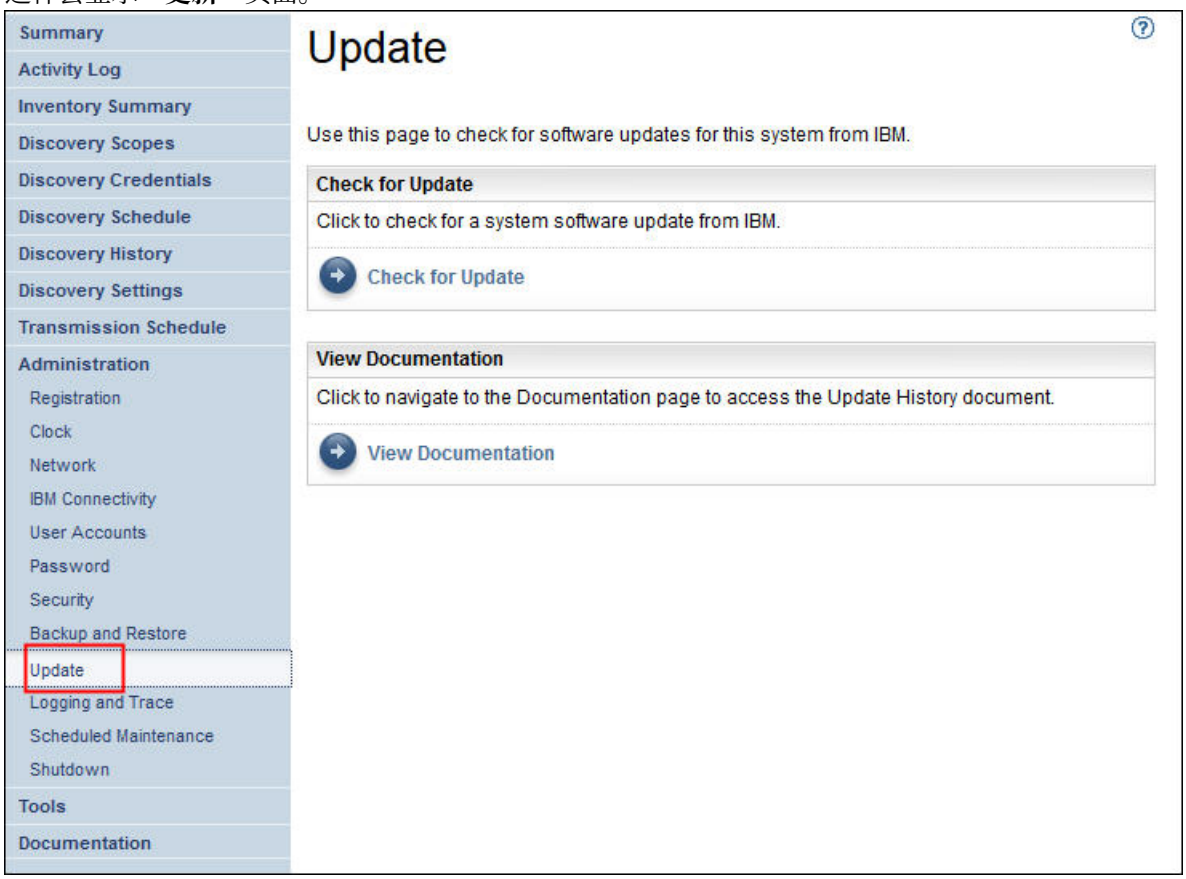

图 *100.* 更新

2. 单击**检查更新**。
   “**更新可用性**”页面将列出任何可用更新。

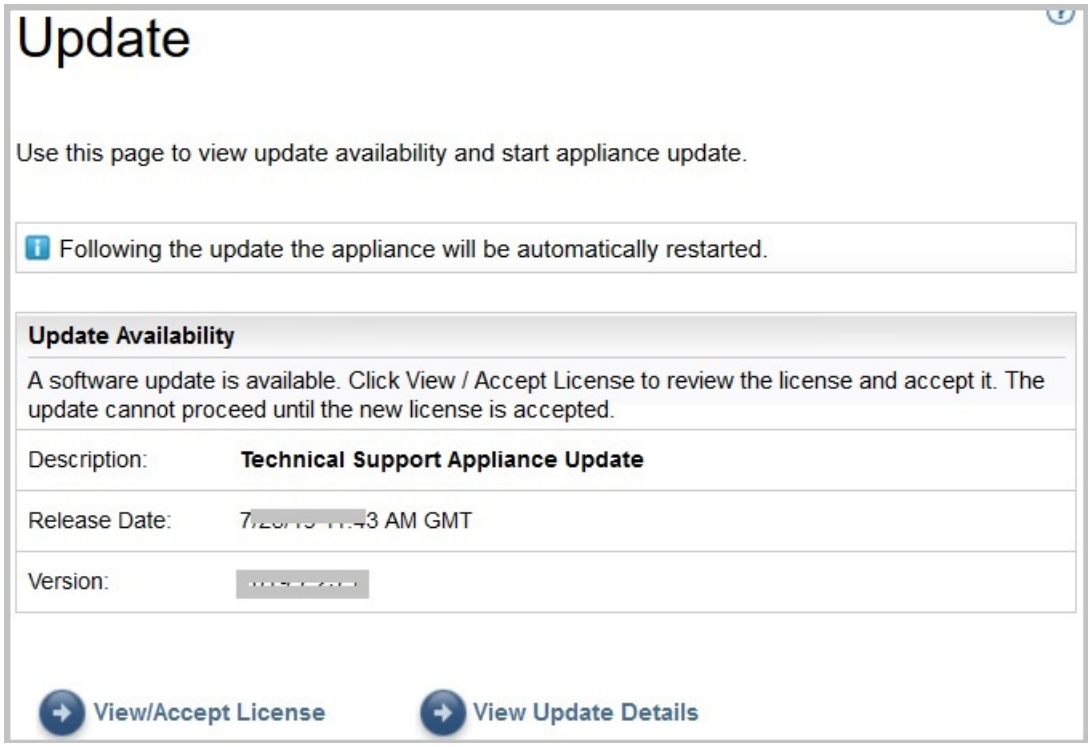

图 *101.* 更新可用性

a) 对于某些新版本的 TSA，您必须先接受新的许可协议，然后才能继续执行更新。如果有新许可证，请单击**查看/接受许可证**，这样会显示“**许可协议**”页面。

b) 单击“**许可协议**”页面上的**接受**按钮以接受新的许可协议。将再次显示“**更新**”页面以及**立即执行更新**按钮。如果不需要接受新的许可协议，那么不会显示**查看/接受许可证**按钮，单击**立即执行更新**以继续。

注:

- 接受许可证后，将不再显示**查看/接受许可证**按钮。
- 在导航窗格中，单击**管理** > **许可证**以查看已接受的最新许可协议。

c) 要安装更新，请单击**立即更新**。

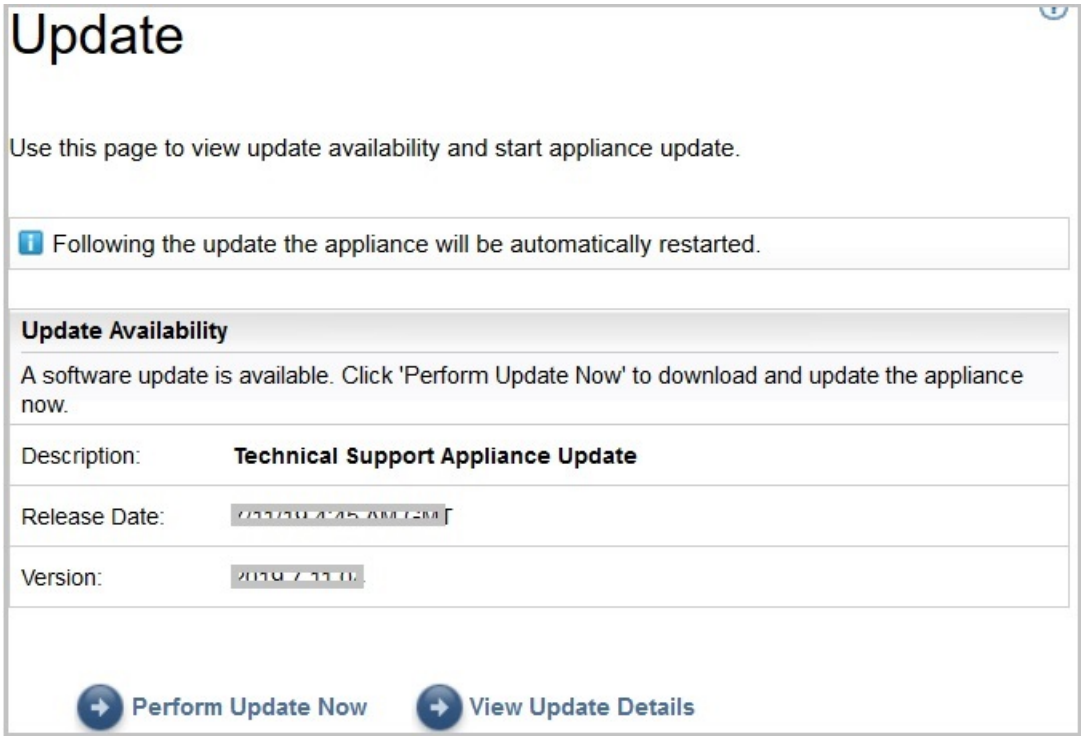

图 *102.* 立即更新

在完成更新后，TSA 会自动重新启动。

d) 要查看有关更新内容的信息，请单击**查看更新详细信息**。

附录 C 配置 DHCP 网络详细信息

请执行以下步骤以配置 DHCP 网络详细信息：

过程

1. 从“**TSA 配置菜单**”中选择选项 **1) 设置网络配置**。

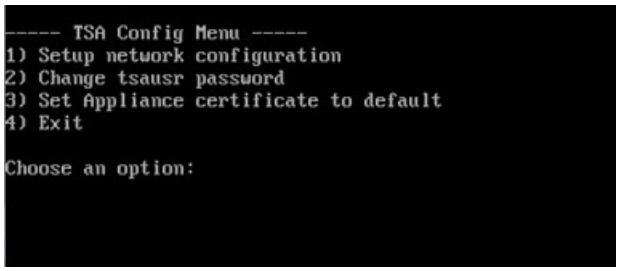

图 *103.* 设置网络配置

2. 输入以下网络配置详细信息。

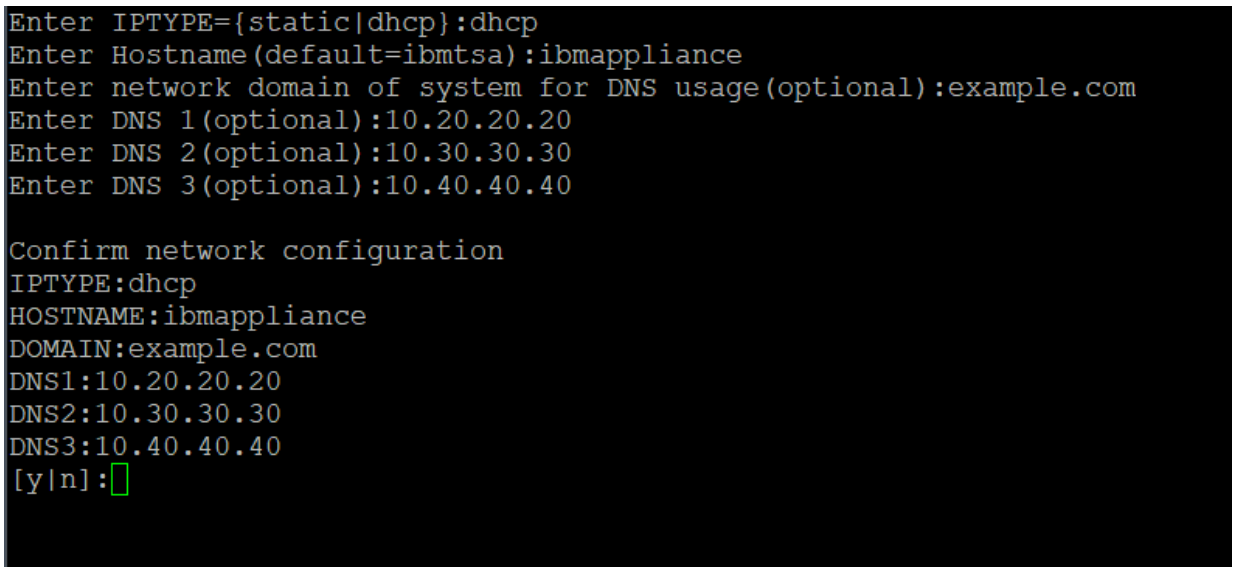

图 *104.* 网络配置

a) **输入 IPTYPE = {static|dhcp}**。输入 dhcp。

IPTYPE: dhcp

输入主机名（缺省值=ibmtsa）。您可以更改缺省主机名。 确保您使用的主机名是唯一的。

输入系统的网络域以供 DNS 使用（可选）。

输入 DNS 1（可选）、**输入 DNS 2（可选）**和**输入 DNS 3（可选）**。

此时会显示指定的网络配置详细信息以供确认。

b) 输入 **[y|n]** 以确认或丢弃网络配置。输入 **y** 将保存网络配置并自动重新启动系统。

注: 对于任何不正确的配置，您可以更改详细信息。输入 **n** 将忽略当前设置并从步骤第 119 页的『2.a』重新启动配置

c) 系统将在 15 秒内重新引导，以使新的网络配置生效。

d) 在系统重新引导后，登录到虚拟化管理器，并记录“**摘要**”选项卡上的 **IP 地址**。

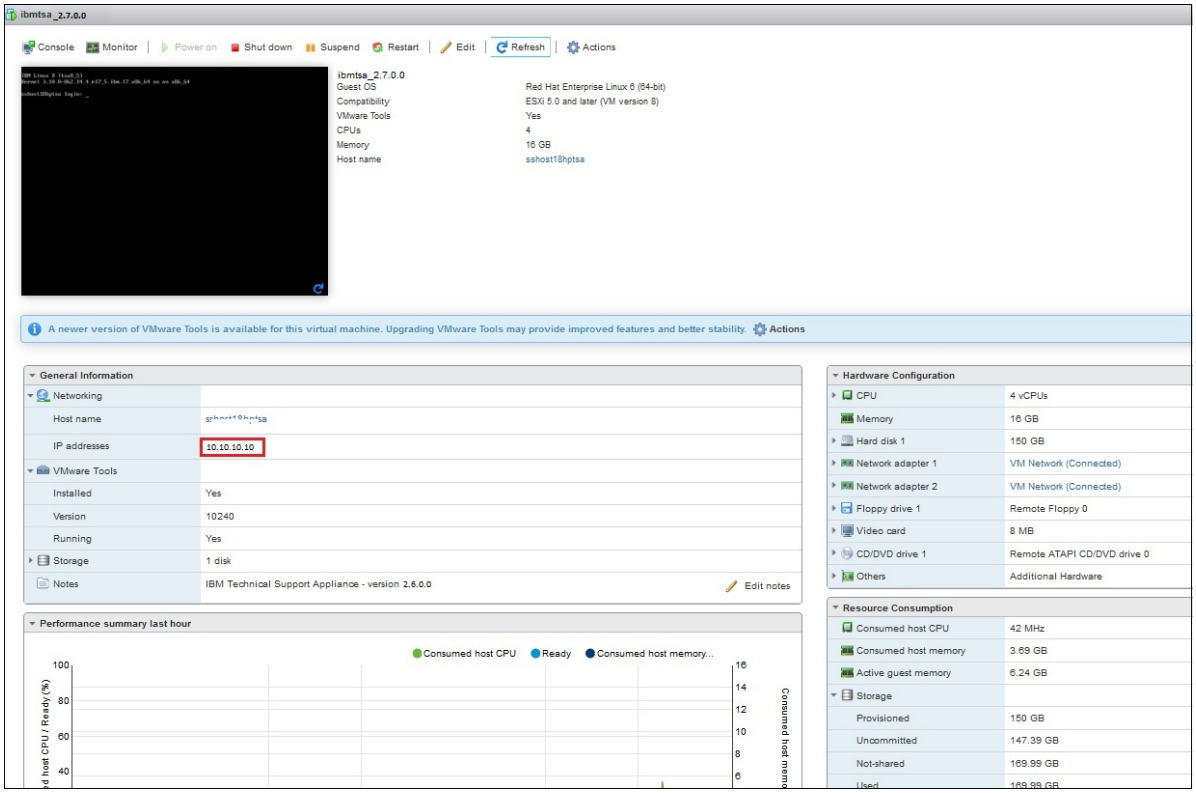

图 *105. DHCP IP* 地址

e) 在浏览器中，使用从先前步骤获取的 URL 来访问 TSA。
例如，`https://newhost1.new.abclabs.example.com`

注: 在第一个连接上，浏览器可能显示安全异常。您必须接受安全证书并继续登录到 TSA。

附录 D 用户帐户和用户组

您可以使用用户帐户和用户组以授权访问 TSA 功能。

开始之前

使用名为 **admin** 的用户帐户安装 TSA。此帐户有权执行任何 TSA 功能。由于以下原因，您可能想要添加用户帐户：

· 允许其他用户充当 **admin** 用户的备份。

· 允许某些用户访问 TSA 上有限数量的功能。

关于此任务

执行任何 TSA 功能都需要一定的权限级别。如果已认证的用户尝试在没有相应权限级别的情况下执行某个功能，那么将显示一条错误并且不会执行该功能。

在 TSA 中，权限级别与用户组相关联。将向用户分配一个或多个用户组中的成员资格，通过这些组成员资格，用户具备权限级别来执行特定功能。

TSA 随附一个**管理员**用户组和一个 **admin** 用户帐户。**管理员**用户组具有所有系统功能的无限制访问权。**admin** 用户帐户分配到**管理员**用户组。

显示用户帐户和用户组

您可以显示现有用户帐户和用户组。

过程

1. 在导航窗格中，单击**管理 > 用户帐户**。
   这样会显示“**用户帐户和组**”页面。
2. 要显示现有用户帐户，请单击**帐户**选项卡。
   “用户帐户”表将显示用户帐户。

   提示: 要查看特定用户帐户的详细信息，请单击该用户帐户的名称。右侧“**常规**”窗格显示与所选用户帐户相关联的用户名、全名和描述。单击右侧“**隶属于**”窗格，以查看此用户帐户所属的用户组。
3. 要显示现有用户组，请单击**组**选项卡。
   “用户组”表将显示用户组。

   提示: 要查看特定用户组的详细信息，请单击该用户组的名称。右侧“**常规**”窗格显示与用户组相关联的名称和权限级别。单击右侧“**作用域限制**”窗格，以查看所选用户组可发现的作用域集。单击“**成员**”窗格以查看与此用户组相关联的用户帐户。

添加用户帐户和组

您可以通过添加用户帐户和组来控制对 TSA 功能的访问。

相关概念

发现作用域和作用域集

发现作用域可标识您希望 TSA 发现的资源。 发现作用域可分组为不同的发现作用域集。

添加用户组

您可以通过添加用户组来控制对 TSA 功能的访问。

关于此任务

要添加用户组，请执行以下步骤：

过程

1. 在导航窗格中，单击**管理** > **用户帐户**。
   这样会显示“**用户帐户和组**”页面。
2. 单击**组**选项卡。

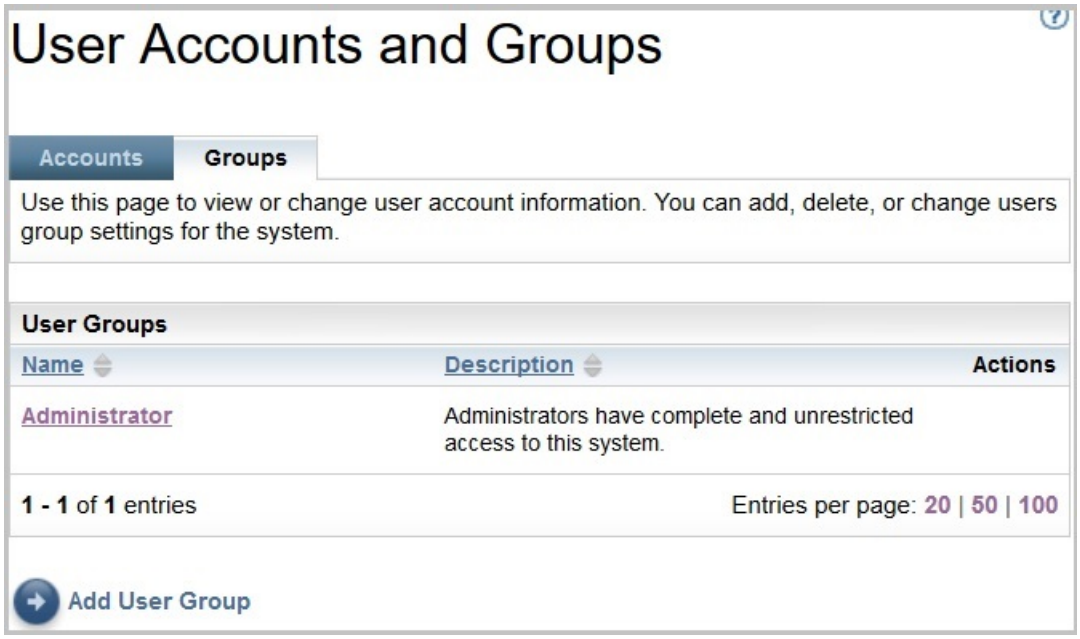

图 *106.* 组

3. 单击**添加用户组**。
   这样会显示“**用户组**”页面。

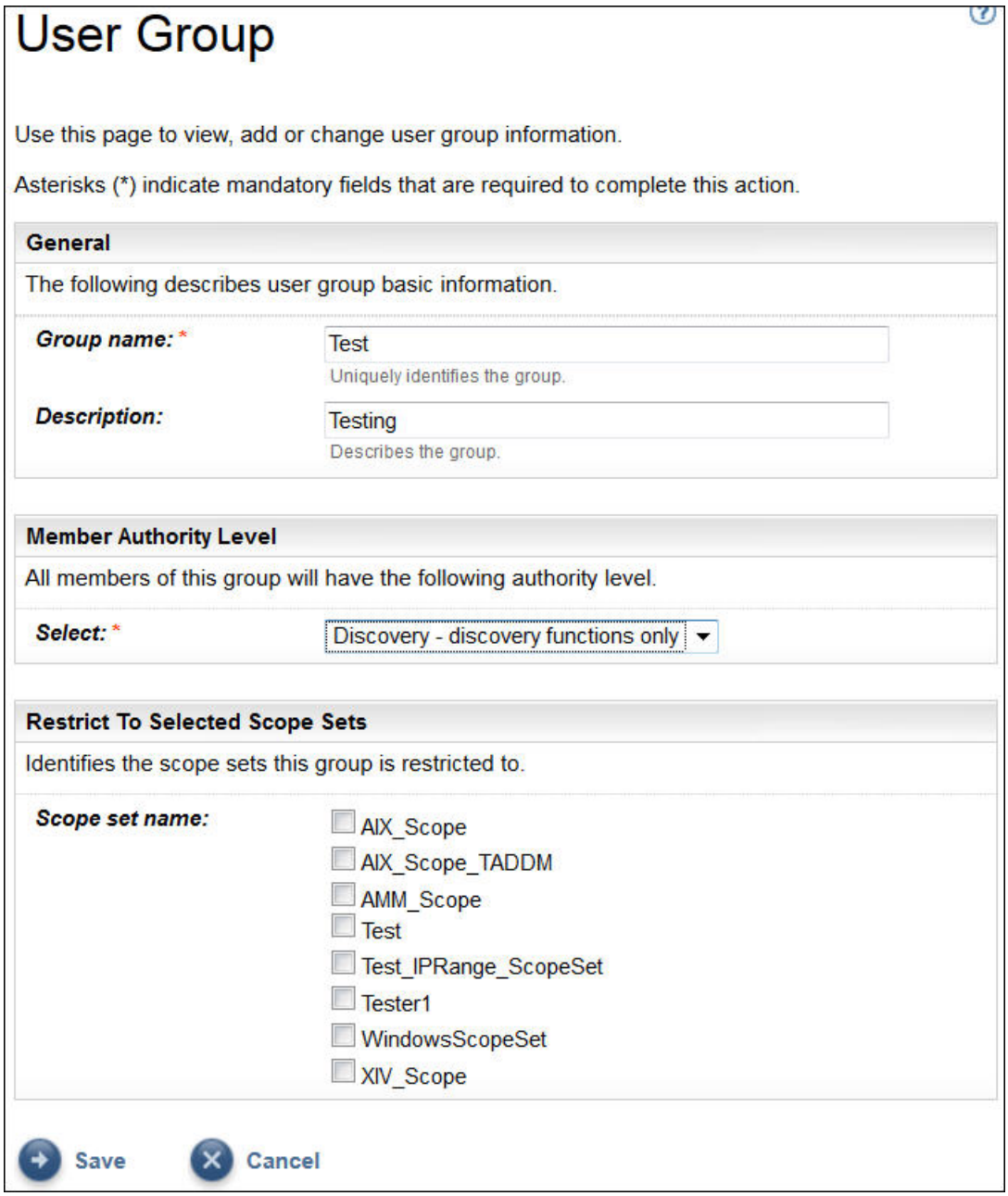

图 *107.* 添加用户组

4. 在**组名**字段中，输入该用户组的唯一名称。
5. 可选： 在**描述**字段中，输入该用户组的描述。
6. 选择您希望该用户组的成员拥有的权限级别。

   TSA 定义了以下组权限级别：

   · **管理员** - 无限制

   · **发现** - 仅限发现功能

   · **访问者** - 仅限读访问权
7. 如果针对该用户组指定了发现权限级别，那么至少应选择一个限定于该用户组的作用域集。
   有关作用域集的更多信息，请参阅 第 1 页的『发现作用域和作用域集』。
8. 单击**保存**可保存用户组。
   这样会显示“**用户帐户和组**”页面，其中列出了该新用户组。

添加用户帐户

您可以通过添加用户帐户来控制对 TSA 功能的访问。

关于此任务

要添加用户帐户，请执行以下步骤：

过程

1. 在导航窗格中，单击**管理** > **用户帐户**。
   这样会显示“**用户帐户和组**”页面。

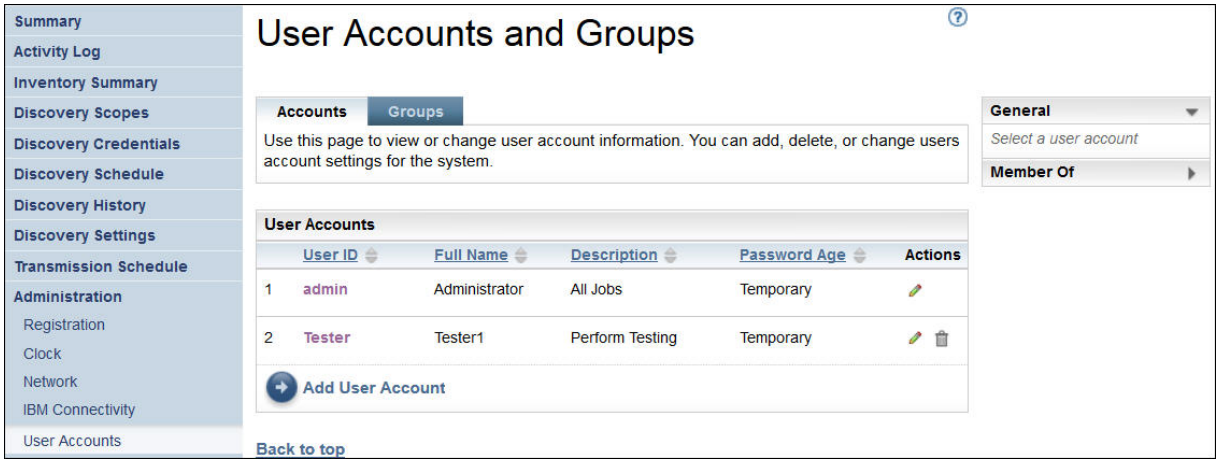

图 *108.* 用户帐户和组

2. 要定义新用户帐户，请单击**添加用户帐户**。
   这样会显示“**用户帐户**”页面。

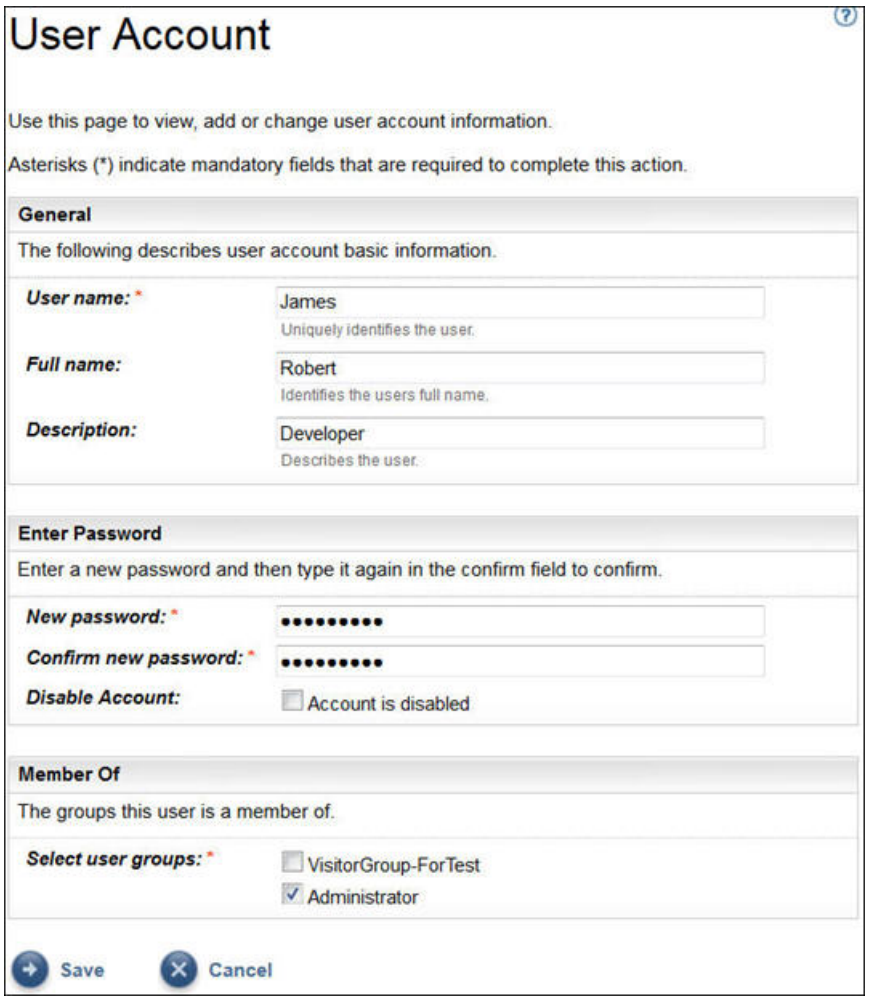

图 *109.* 添加用户帐户

3. 在**用户名**字段中，输入该用户帐户的名称。
4. 可选： 在**全名**字段中，输入该帐户的用户的全名。
5. 可选： 在**描述**字段中，输入该用户帐户的描述。
6. 在**新密码**字段中，输入该用户帐户的密码。

   密码必须遵守以下规则：

   · 必须至少包含 8 个字符
   · 必须至少包含 1 个字母字符和 1 个非字母字符
   · 不得包含用户名
   · 不得与之前的 8 个密码相同
   · 至少应每 30 天（缺省情况下）或按照第 90 页的『修改密码使用期限』部分中指定的期限更改一次，但每天不能更改多次。
7. 在**确认密码**字段中，再次输入该用户帐户的密码。

   比较您输入的两个密码以确认它们相互匹配，然后再保存密码。

   注: 首次登录该用户帐户时必须更改密码。
8. 如果要禁用此用户帐户，请选中**帐户已禁用**复选框。

   通过禁用该帐户，您可以在不删除该帐户的情况下阻止使用该帐户。

   注: 您既不能禁用**管理员**帐户，也不能更改**管理员**帐户的组。
9. 为该用户帐户选择用户组。至少应选择一个用户组。 该用户将拥有针对任何选定组定义的权限级别。
10. 单击**保存**可保存用户帐户。

这样会显示“**用户帐户和组**”页面，其中列出了该新用户帐户。

修改用户帐户和用户组

您可以修改现有用户帐户和用户组。

修改用户帐户

您可以修改现有用户帐户。

关于此任务

要修改用户帐户，请执行以下步骤：

过程

1. 在导航窗格中，单击**管理** > **用户帐户**。
   这样会显示“**用户帐户和组**”页面。
2. 单击**帐户**选项卡，然后单击用户帐户旁边的**编辑**图标 。
   这样会显示“**用户帐户**”页面。
3. 在“**常规**”窗格中，您可以更改此用户帐户的基本信息。
4. 在“**输入密码**”窗格中，您可以更改密码和密码管理信息。您还可以禁用此用户帐户。
   密码必须遵守以下规则：
   - 必须至少包含 8 个字符
   - 必须至少包含 1 个字母字符和 1 个非字母字符
   - 不得包含用户名
   - 不得与之前的 8 个密码相同
   - 必须每 90 天至少更改一次，但每天不能更改多次。

   注： 首次登录该用户帐户时必须更改密码。
5. 如果要禁用此用户帐户，请选择**帐户已禁用**。
   通过禁用该帐户，您可以在不删除该帐户的情况下阻止使用该帐户。有关删除用户帐户的信息，请参阅第 128 页的『删除用户帐户和用户组』。
   注： 您既不能禁用**管理员**帐户，也不能更改**管理员**帐户的组。

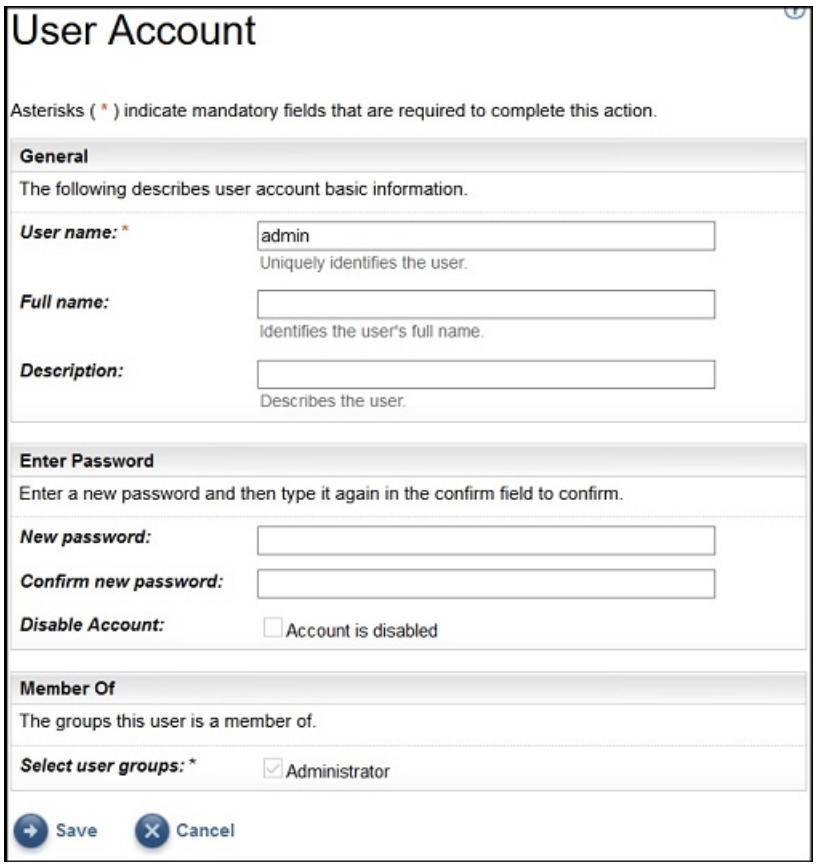

图 *110.* 修改管理员用户帐户

6. 在“**隶属于**”窗格中，您可以更改此用户帐户所属的用户组。用户帐户至少是一个用户组的成员。
7. 单击**保存**可保存您的更改。
   将在“**用户帐户和组**”页面中显示更改的信息。

修改用户组

您可以修改现有用户组。

开始之前

注: 您无法更改**管理员**组。

关于此任务

要修改用户组，请执行以下步骤:

过程

1. 在导航窗格中，单击**管理 > 用户帐户**。
   这样会显示“**用户帐户和组**”页面。
2. 单击**组**选项卡，然后单击用户组旁边的**编辑**图标 。
   这样会显示“**用户组**”页面。
3. 在“**常规**”窗格中，您可以更改此用户组的基本信息。
4. 在“**成员权限级别**”窗格中，您可以更改此用户组是具有管理员、发现还是读权限。
5. 如果在“**成员权限级别**”中指定发现权限级别，那么可以在“**限制为所选作用域集**”窗格中更改此用户组有权发现的作用域集。
6. 单击**保存**可保存您的更改。
   将在“**用户帐户和组**”页面中显示更改的信息。

删除用户帐户和用户组

您可以删除现有用户帐户和用户组。

删除用户帐户

您可以删除现有用户帐户。

关于此任务

注: 无法删除**管理员**用户帐户。

要删除用户帐户，请执行以下步骤:

过程

1. 在导航窗格中，单击**管理 > 用户帐户**。
   这样会显示“**用户帐户和组**”页面。
2. 单击**帐户**选项卡，然后单击要删除的用户帐户旁边的“删除”图标 。
3. 单击**确定**以确认要删除该用户帐户。

删除用户组

您可以删除现有用户组。

关于此任务

注: 无法删除**管理员**用户组。

要删除用户组，请执行以下步骤:

过程

1. 单击**管理 > 用户帐户**。
   这样会显示“**用户帐户和组**”页面。
2. 单击**组**选项卡，然后单击要删除的用户组旁边的“删除”图标 。
3. 单击**确定**以确认要删除该用户组。

   注: 仅当没有分配用户时，才能删除该用户组。

辅助功能选项

Technical Support Appliance 不会干扰受支持的浏览器的辅助功能。要获取辅助功能的全面列表，请访问所使用的受支持浏览器的辅助功能选项支持页面。有关受支持浏览器的列表，请参阅第 3 页的『必需的 Web 浏览器』。

本产品的出版物采用 Adobe 可移植文档格式 (PDF) 并且应符合辅助功能选项标准。如果您在使用 PDF 文件时遇到困难并且想要请求基于 Web 的格式的出版物，可以通过电子邮件将请求发送到以下地址：

icfeedbk@us.ibm.com

也可以通过邮寄方式将请求邮寄到以下地址：

International Business Machines Corporation
Information Development
3605 Hwy 52 North
Rochester, MN, U.S.A 55901

在请求中，请务必在信件主题行中包含出版物标题“IBM Technical Support Appliance 设置指南”。

当您发送信息给 IBM 后，即授予 IBM 非专有权，IBM 对于您所提供的任何信息，有权利以任何它认为适当的方式使用或分发，而不必对您负任何责任。

声明

本信息是为在美国国内供应的产品和服务而编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户任何使用这些专利的任何许可。您可以用书面形式将许可查询寄往：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

有关双字节 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

以下段落对于英国和与当地法律有不同规定的其他国家或地区均不适用： INTERNATIONAL BUSINESS MACHINES CORPORATION“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。 因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的，实际结果可能会有差别。本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问 题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或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。

本信息仅用于规划的目的。在所描述的产品上市之前，此处的信息会有更改。

商标

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corp., 在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。当前的 IBM 商标列表，可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上“版权和商标信息”部分获取。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的商标。

Microsoft、Windows、Hyper-V 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

Java™ 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

VMware、VMware 徽标、VMware Cloud Foundation、VMware Cloud Foundation Service、VMware vCenter Server 和 VMware vSphere 是 VMware, Inc. 或其子公司在美国和/或其他管辖区域中的注册商标或商标。

部件号:

(1P) P/N: