Version 2.8.0.0

Technical Support Appliance Setup Guide

IBM

Note

Before using this information and the product it supports, read the information in "Notices" on page 137.

Twenty-fourth edition (January 2021)

This edition applies to version 2, release 8, modification 0 of IBM® Technical Support Appliance and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Chapter 1. Introduction

The Technical Support Appliance (TSA) is an easy-to-use tool that enables you to get more value from your IBM Support contracts. TSA discovers key information technology elements and their relationships within your IT infrastructure, and then securely transmits the data to IBM Support for analysis. This data provides IBM Support with insight into the complex relationships between the applications, middleware, servers, and network components in your data center.

TSA includes a web-based user interface (UI) to set up and customize access to your system and data. The UI also enables you to modify schedules for data discovery and transmission.

As part of the discovery process, TSA initially attempts to detect endpoints within the defined scope without using discovery credentials. This involves the use of Nmap and attempts to discover and classify devices with minimum intrusive IP scanning, stack fingerprinting, and port mapping. Generally, this activity is not significant enough to set off an intrusion detection system (IDS), but might do so if there are stringent local settings.

The General scope sets allows you to discover individual IT network elements. The scope set contains one or more scopes that identify the location of these network elements using an IP address or host name, a range of IP addresses, or a network or subnet.

For HMCs and VMware vCenter Servers / ESXi, using dynamic scope sets is recommended. Dynamic scope sets require far less configuration effort in TSA versus creating and managing discovery scopes for individual LPARs/virtual machines. Also, for environments where the LPARs or virtual machines are added and deleted over time, dynamic scope sets can handle this without the need to modify any scope sets.

User accounts and user groups

Executing any TSA function requires a certain authority level. If an authenticated user attempts to perform a function without the appropriate authority level, an error is displayed and the function is not executed.

Within an organization, roles can be created for various job functions. The permissions to perform certain operations are assigned to specific roles. TSA users are assigned particular roles, and through those role assignments have the necessary permissions to perform particular system functions. That way, any user assigned to a role will have the authority levels associated with that role and it is easy to add a user to a role, to change users from one role to another, or to remove users from a role.

In TSA, roles are managed with user groups that have associated authority levels. Users are managed with user accounts. User accounts can be assigned membership in one or more user groups, and through those memberships, users have the authority level to perform particular functions.

In addition, user groups can be further restricted to selected scope sets. A scope set is a collection of IP addresses or host names, address ranges, or subnets that identify the IT elements that TSA can discover. Specifying scope set restrictions for a user group is a way to further limit access of the members of that user group. For example, it is possible to create platform-specific user groups, such as users responsible for maintaining Linux® systems, through a combination of authority level and scope set restrictions associated with a particular user group.

Discovery Scopes and Scope Sets

Discovery scopes identify the resources that you want TSA to discover. Discovery scopes are grouped into discovery scope sets.

You can specify discovery scopes by using an IP address or host name, a range of IP addresses, or a network or subnet to define the resources that are accessed during discovery. A discovery scope can be as small as a single IP address or host name, or as large as a range of IP addresses or a network.

To simplify creation of a scope set, a file can be used to import a list of containing IP addresses and host names. For more information, see section “Importing a scope set” on page 72.

The more IP addresses that are in the discovery scope, the longer the discovery takes. You can modify the discovery size by disabling or enabling discovery scope sets or by excluding IP addresses, ranges of IP addresses, or networks or subnets from a scope within a scope set.

Note: For better performance, limit the cumulative number of IP addresses (IP address, ranges, subnets, and exclusions) in a scope set to 400 or less.

Note: Scopes or import lists that are defined with host names have the host name resolved to an IP address when the scope is created or edited. TSA does not use the host name when discovering network resources.

Related tasks

Adding user accounts and user groups
You can add user accounts and groups to control access to TSA functions.

Discovery credentials

Discovery credentials are a collection of user names, passwords or SSH keys, and Simple Network Management Protocol (SNMP) community strings that TSA uses to access resources during the discovery.

You must set up and maintain discovery credentials for the resources that you want to discover. The access information that you provide varies by the type of credential, but usually includes at least user name and password or SSH key.

A discovery credential can apply to all scope sets or be restricted to a single scope set. Defining credentials that apply to a single scope set improves performance and prevents invalid login attempts, which can result in the account being locked.

When you access a resource, TSA sequentially uses each credential that is associated with a particular scope in the order that is listed on the **Discovery Credentials** page until the resource allows TSA permission to access it. For example, when you are accessing a computer system, TSA uses the first user name and password that is specified in the credential list for computer systems and is associated with the containing scope set. If the user name and password are incorrect for a particular computer system, TSA automatically uses the next user name and password that is specified in the credential list for computer systems.

Tip: Before you save the credentials, you can test whether you specified valid credentials for system types, such as **Computer System**, **Computer System (Windows)**, **SNMP**, or **SNMPV3**. By this testing you can ensure that the credentials are validly defined.

Tip:

- Use a service account with a common password for all devices of a certain type, such as AIX® or Windows. A single credential can then be defined to discover all instances of this device type.
- Use accounts with non-expiring passwords.
- Use SSH keys, wherever needed.

Discovery schedule

Discoveries are run on scheduled days and times to ensure that discovered data is always current and accurate. TSA has a default "Full Discovery" schedule that does a discovery of all defined scope sets. This default schedule can be modified for your needs. You can also create schedules that allow the discovery of scope sets to be spread out between different times and dates. You can also view details, history, and the state of the last discovery that was run.

When you modify a discovery schedule, you specify the name, the scope sets, the start time, and the frequency of discoveries. If the discovery schedule is the default discovery, you can modify only the start time and the frequency for discoveries. You can also run discoveries on demand.

The duration of the discovery depends on a number of factors that also include the number and complexity of resources and can take up to 72 hours to complete.

Transmission schedule

Discovered data is securely packaged and transmitted to IBM Support on scheduled days and times to ensure that IBM has the most current and accurate information. TSA has a default transmission schedule that you can modify for your needs. You can also run transmissions on demand. You can also view the state of the last transmission that was run.

The elapsed time for a transmission varies depending on the amount of discovered data.

Chapter 2. Prerequisites

To set up and use TSA, you need to ensure that you meet prerequisites, such as the required credentials for the discovery environment and configuration requirements for connecting to IBM Support.

Download TSA image

TSA images are available for both Microsoft Hyper-V [*TSA-HYPERV-<version>*] and VMware [*TSA-VMWARE-<version>*] servers.

You can get the download instructions at: https://ibm.biz/TSAdemo

Requirements for TSA

Before you set up and use TSA, ensure that you meet the following prerequisites.

x86 64-bit hardware
TSA must be loaded on x86 64-bit systems.

Hypervisor
TSA requires VMware ESXi or Microsoft Hyper-V

Note: Only use versions of ESXi or Hyper-V that are currently supported by the manufacturer.

Processor
TSA requires a minimum of 2.26 GHz, four core processor.

CPU
TSA requires four 64-bit CPUs.

Memory
TSA requires 16 GB memory.

Direct access storage device (DASD)
TSA requires 150 GB of DASD.

Network
TSA requires a 1-Gigabit Ethernet adapter.

Required web browsers

A web-based user interface is used to set up and monitor discovery and transmission.

TSA supports the following internet browsers:

- Mozilla Firefox V78.4.0 Extended Support Release (ESR)
- Microsoft Edge V86.0.622.56 for Windows 10
- Google Chrome V86.0.4240.111 (64-bit)

You can download these browsers from the following sites:

- 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)

Configuration requirements for connections to IBM Support

TSA can connect to IBM Support through a direct connection or through a user-supplied proxy that you must configure to allow communication with IBM. If you are using a proxy, TLS/SSL inspection is not supported. Any requests through a proxy must be allowed to flow directly to IBM without TLS/SSL termination.

Ensure that your firewall allows connections to the IBM server host name and IP addresses as explained in the Network connections table. If your network does not allow access to the IBM servers, TSA transactions to IBM Support will fail.

Table 1. Network connections

DNS name	IP address	Port	Protocol
esupport.ibm.com	129.42.54.189	443	HTTPS (to IBM)
	129.42.56.189		
	129.42.60.189		

The IBM server environment is fully NIST SP800-131A compliant, supporting TLS 1.2 protocol, SHA-256 or stronger hashing functions, and at least 2048-bit strength RSA keys.

Note: SSL inspection is not supported, if utilizing it on the proxy, disable it for these flows.

For Blue Coat proxies, disable "protocol detection" to IBM servers. Add these configuration rules:

- 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)

Credential and software requirements for the discovery environment

In order to discover endpoints or resources in your environment, TSA must have access to those resources. It is recommended that you create a service account on each resource that is specifically for TSA to use when accessing that resource.

After you create a service account on a resource, you must define and maintain credentials on TSA that match the credentials defined on the resource for that service account. TSA uses these credentials to access the resource. Requirements for credentials vary according to the environment and the type of resource that you want to discover, but typically include a user name and password or SSH key. Some resources have specific software requirements as well.

Type of credential	Access information
Computer System	**User name:** User name to access the device. **Password / Passphrase:** Password / passphrase to access the device. **Authentication type:** The type of authentication for the device. • **Password** - Use the provided password. • **PKI** - Use SSH key associated with the specific scope set.
Computer System (Windows)	**User name:** User name to access the Windows computer system. **Password:** Password to access the Windows computer system.

Type of credential	Access information
Network Element (SNMP)	**Community string:** The community string for the device.
Network Element (SNMPV3)	**User name:** The user name to access the device. **Password:** The password to access the device. **Private password:** The password that is used if data encryption is set for SNMP. **Authentication protocol:** The type of authentication protocol that is used by SNMP. • None • MD5 • SHA
Other (Cisco Device)	**User name:** The user name to access the Cisco device. **Password:** The password for the Cisco device. **Enable password:** The enable password for the Cisco device.
Other (Cisco Works)	**User name:** The user name to access the CiscoWorks server. **Password:** The password to access the CiscoWorks server.

Note: For more information about credentials and software requirements, refer to the Configuration Assistant Guide.

Chapter 3. Installing the Technical Support Appliance

TSA includes preinstalled software. It is packaged and distributed as an image for VMware installations or as a VHDX image for Microsoft Hyper-V installations. For VMware, TSA can be installed by using the VMware web interface (for ESXi). For Hyper-V, TSA can be installed by using the Hyper-V Manager. This section provides the steps for installing TSA using either of these methods.

Installing using VMware ESXi web interface

Before you begin

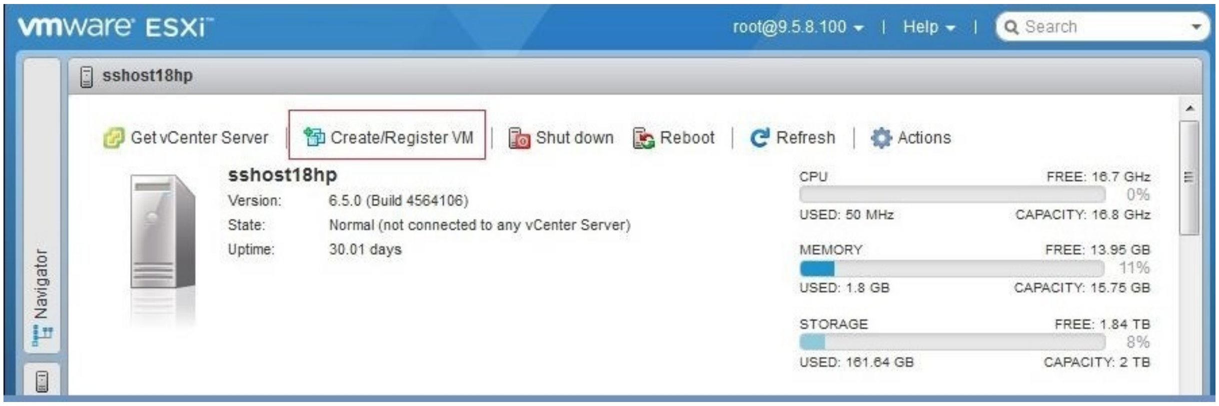
TSA requires VMware ESXi 6.5 or higher to be loaded to control the hardware.

About this task

Follow these steps to install the TSA image.

Procedure

1. Log in to the ESXi system through the VMware ESXi web interface.
2. Click **Create/Register VM**. The **New virtual machine** wizard displays.

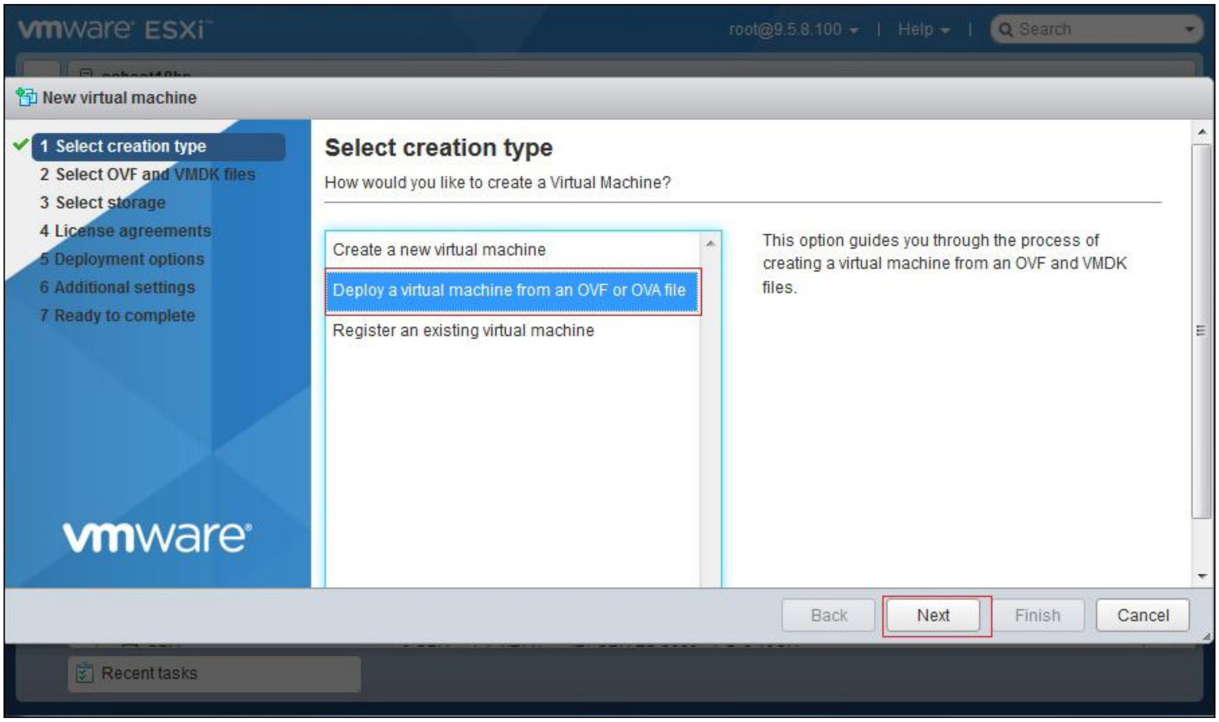


sshost18hp
Version: 6.5.0 (Build 4564106)
State: Normal (not connected to any vCenter Server)
Uptime: 30.01 days

CPU FREE: 16.7 GHz 0% USED: 50 MHz CAPACITY: 16.8 GHz
MEMORY FREE: 13.95 GB 11% USED: 1.8 GB CAPACITY: 15.75 GB
STORAGE FREE: 1.84 TB 8% USED: 161.64 GB CAPACITY: 2 TB

Figure 1. Create / Register VM

3. On the **Select creation type** screen, select the **Deploy a virtual machine from an OVF or OVA file** option and click **Next**.



Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine

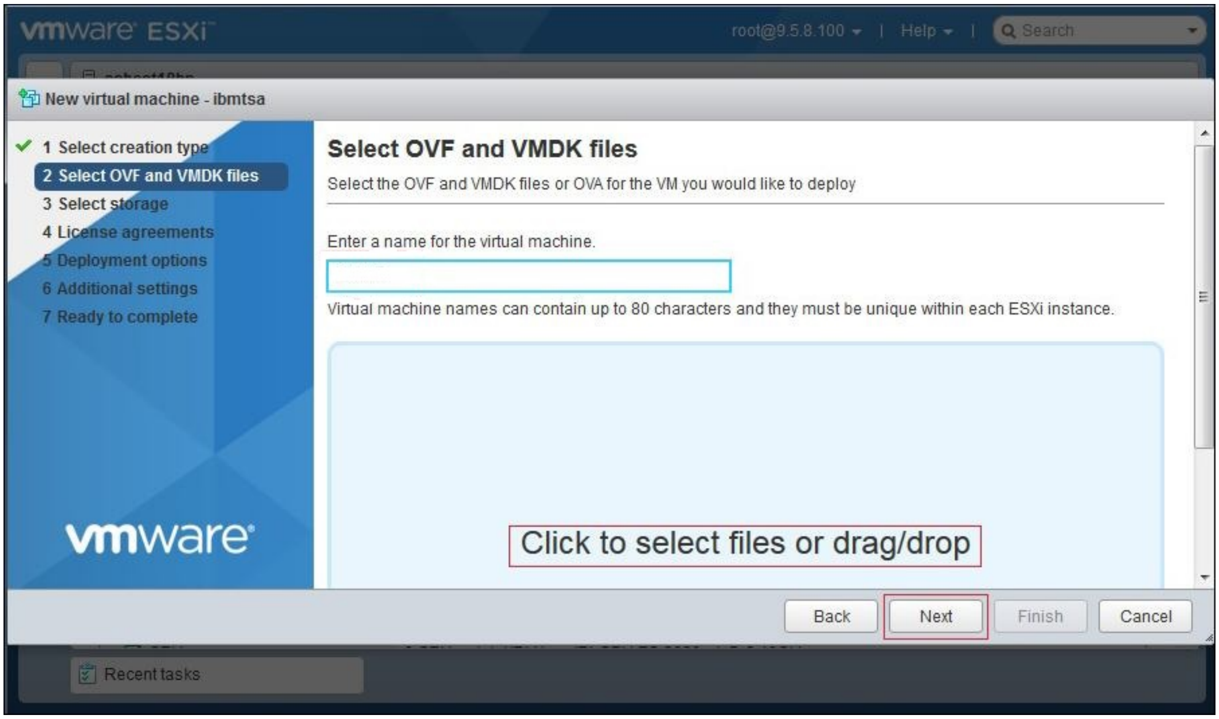
Deploy a virtual machine from an OVF or OVA file

Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

Figure 2. Select creation type

4. On the **Select OVF and VMDK** files screen, click inside the **Click to select files or drag/drop** box and select the image file that you have downloaded from Fix Central. Enter a unique name for your virtual machine or you can use the default value, then click **Next**.



Select OVF and VMDK files

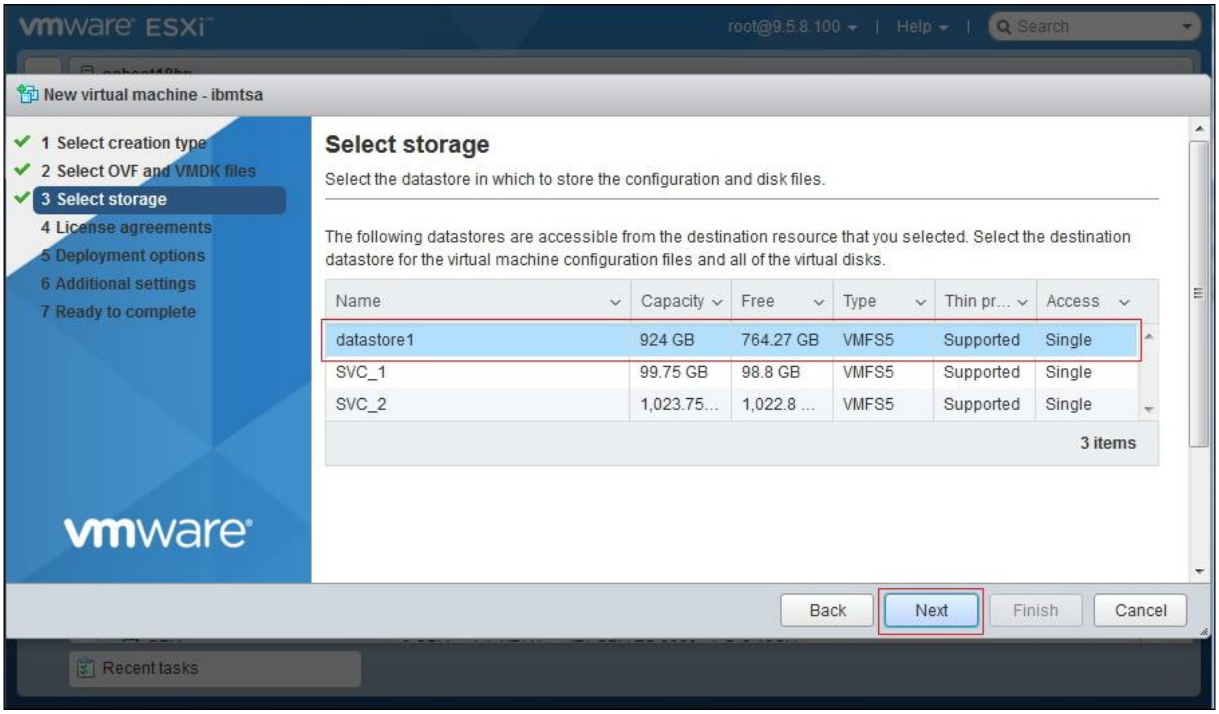
Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Figure 3. Select OVF and VMDK files

5. On the **Select storage** screen, from the displayed list, select a data store in which to store the configuration and disk files. Then, click **Next**.



New virtual machine - ibmtsa

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files.

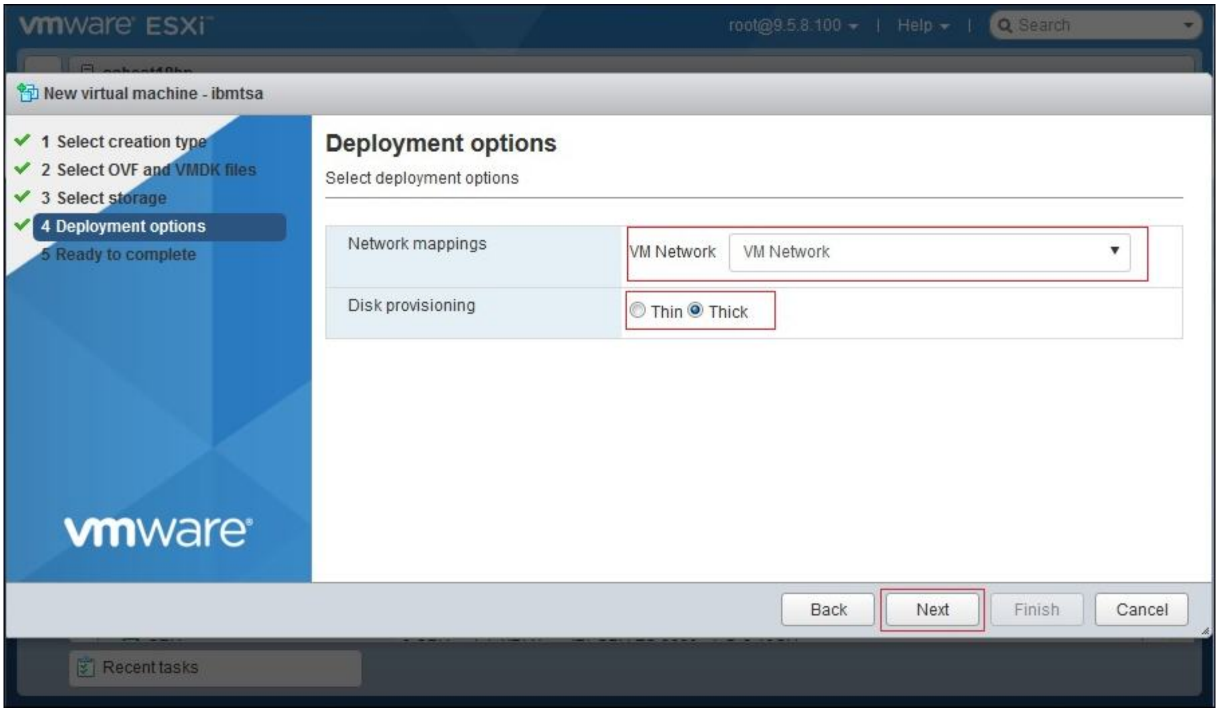
The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pr...	Access
datastore1	924 GB	764.27 GB	VMFS5	Supported	Single
SVC_1	99.75 GB	98.8 GB	VMFS5	Supported	Single
SVC_2	1,023.75...	1,022.8 ...	VMFS5	Supported	Single

3 items

Figure 4. Select storage

6. On the **Deployment options** screen, select network mappings from the **VM Network** drop-down list.



New virtual machine - ibmtsa

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Ready to complete

Deployment options

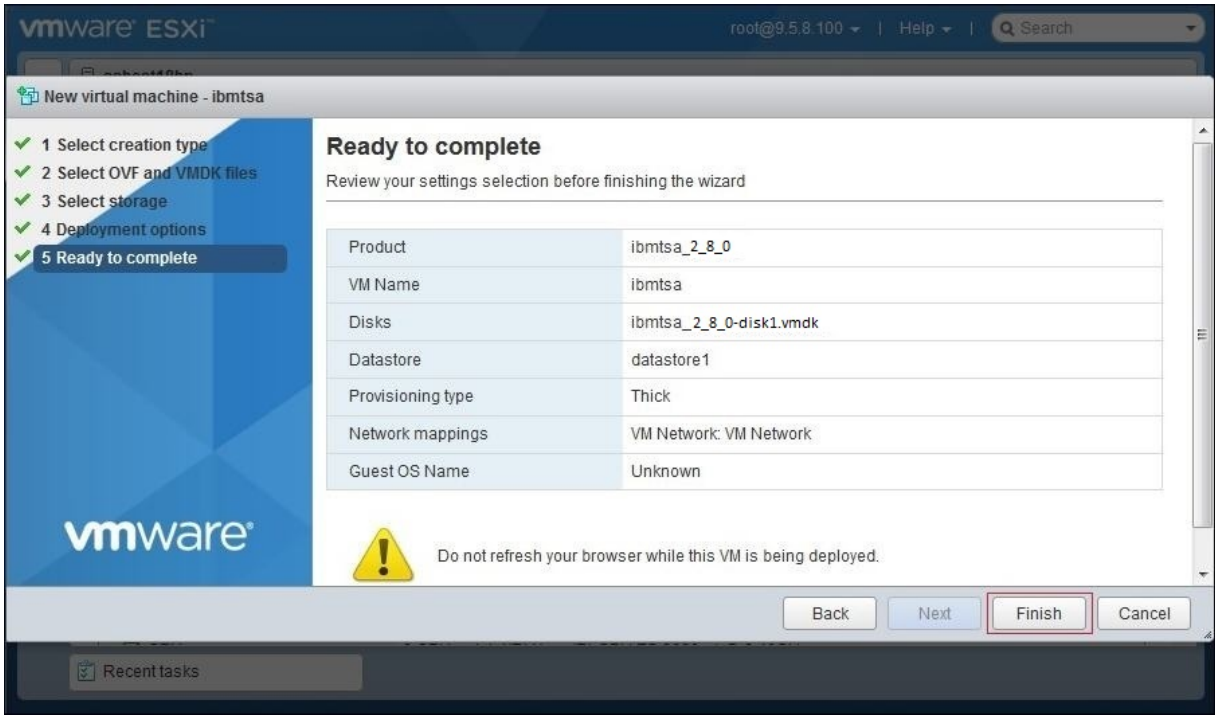
Select deployment options

Network mappings	VM Network: VM Network ▾
Disk provisioning	○ Thin ● Thick

Figure 5. Deployment options

7. Select the **Thick** option for disk provisioning, then click **Next**.
8. On the **Ready to complete** screen, review all the settings that you have specified. If you want to make any changes click **Back** and make changes to the relevant options. If you are satisfied, click **Finish**.

   Important: Do not refresh your browser while the virtual machine is being deployed.



Ready to complete

Review your settings selection before finishing the wizard

Product	ibmtsa_2_8_0
VM Name	ibmtsa
Disks	ibmtsa_2_8_0-disk1.vmdk
Datastore	datastore1
Provisioning type	Thick
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

Do not refresh your browser while this VM is being deployed.

Figure 6. Review settings selection

The TSA virtual machine is installed on your system.

9. In the TSA console, enter the **ibmtsa login** as **`tsausr`** and **Password** as **`configTsa`**.
10. Required: To change the login password, continue with the steps that are listed in the section "Changing tsausr password (required)" on page 19.
11. To complete the installation, continue with the steps that are listed in the section "Configuring the network details" on page 19.

Installing TSA on Microsoft Hyper-V

Before you begin

Before you set up and use TSA on Hyper-V, ensure that you meet the following prerequisites:

- Hyper-V Server 2016 or 2019
- Hyper-V Manager
- Virtual Network Switch has been created through Hyper-V Manager

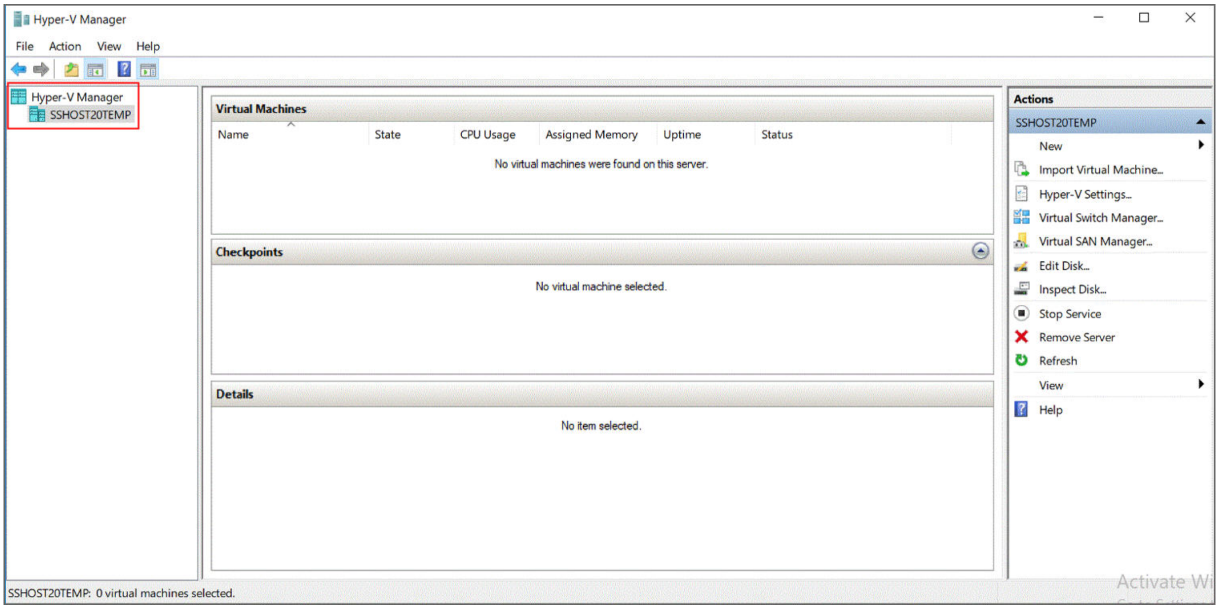
About this task

Follow these steps to install TSA on Hyper-V.

Procedure

To install TSA on Hyper-V, follow these steps:

1. After downloading the TSA image, extract the *ibmtsa_2800.vhdx* file from *ibmtsa_2800.zip* file from ibmtsa_2800.zip and move it to a directory on the Hyper-V server.
2. Start the Hyper-V Manager and connect to the Hyper-V server from the client system.
3. Click **Browse** and select the image that is saved on your system.



No virtual machines were found on this server.

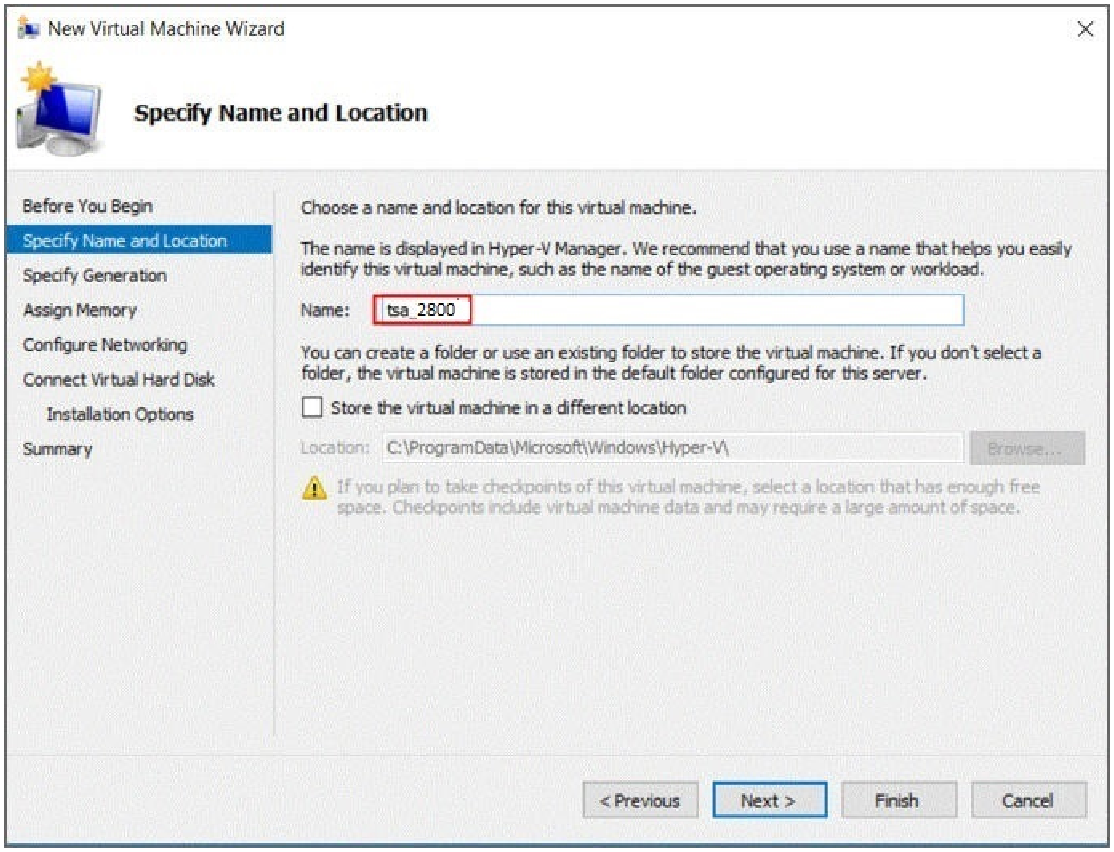
No virtual machine selected.

No item selected.

SSHOST20TEMP: 0 virtual machines selected.

Figure 7. Hyper-V Manager

4. From the **Action** menu, select **New** → **Virtual Machine**. The **New Virtual Machine Wizard** displays.
5. Enter the **Name** for the new virtual machine and click **Next**.



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: tsa_2800

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

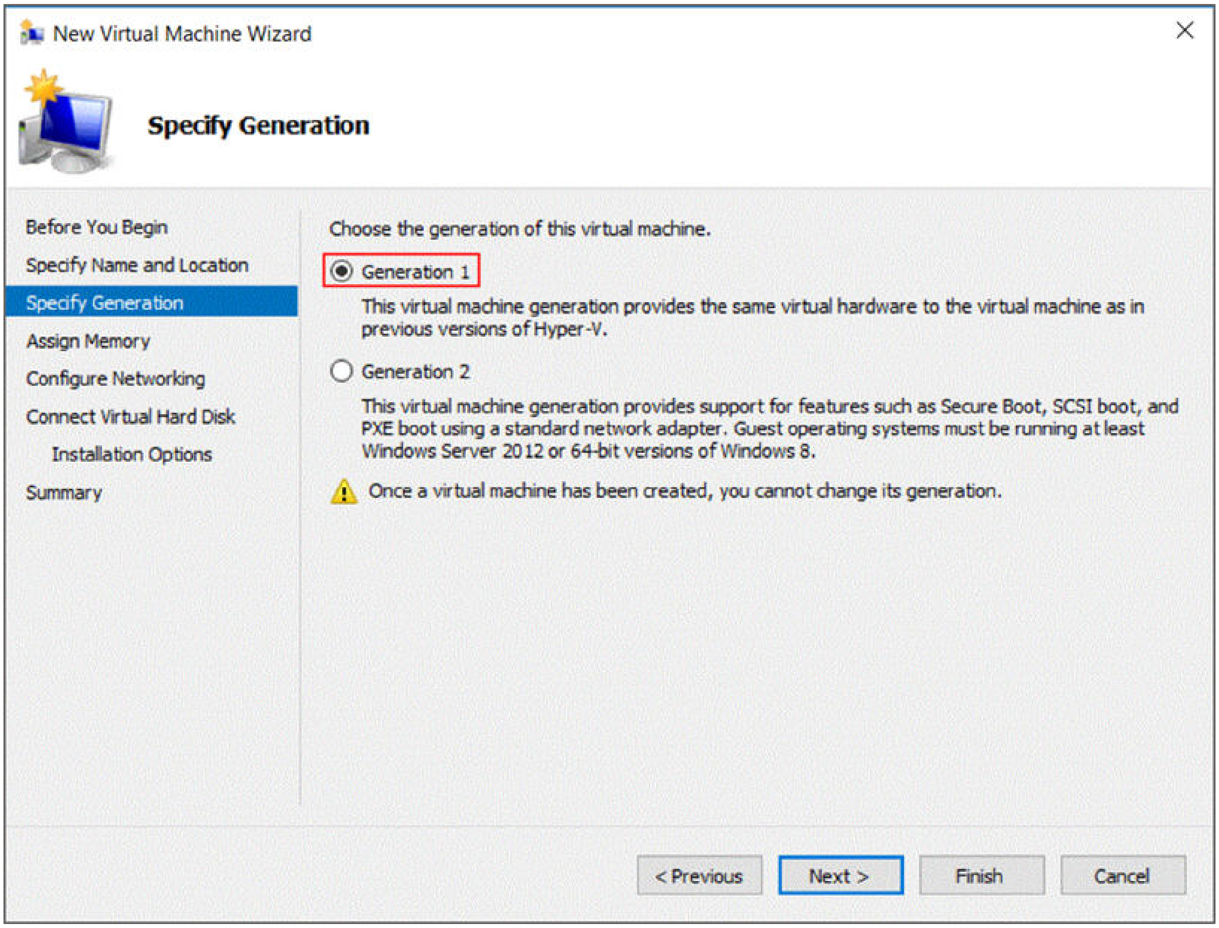
☐ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

Figure 8. Virtual Machine Name

6. Select **Generation 1** as the generation of the virtual machine and click **Next**.



Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.

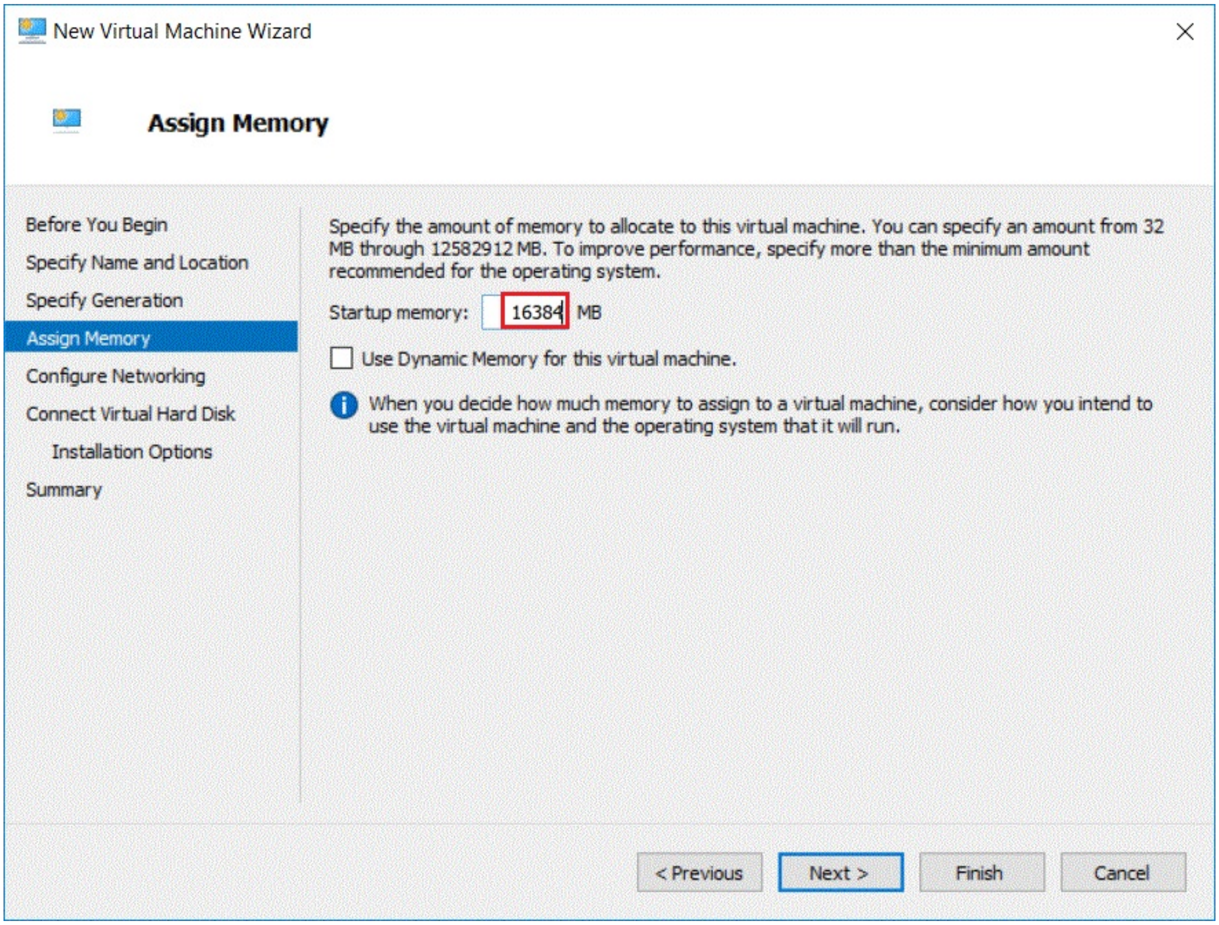
○ Generation 2

This virtual machine generation provides support for features such as Secure Boot, SCSI boot, and PXE boot using a standard network adapter. Guest operating systems must be running at least Windows Server 2012 or 64-bit versions of Windows 8.

⚠ Once a virtual machine has been created, you cannot change its generation.

Figure 9. Specify Generation

7. Enter **Startup memory** as *16384* MB and click **Next**.



Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

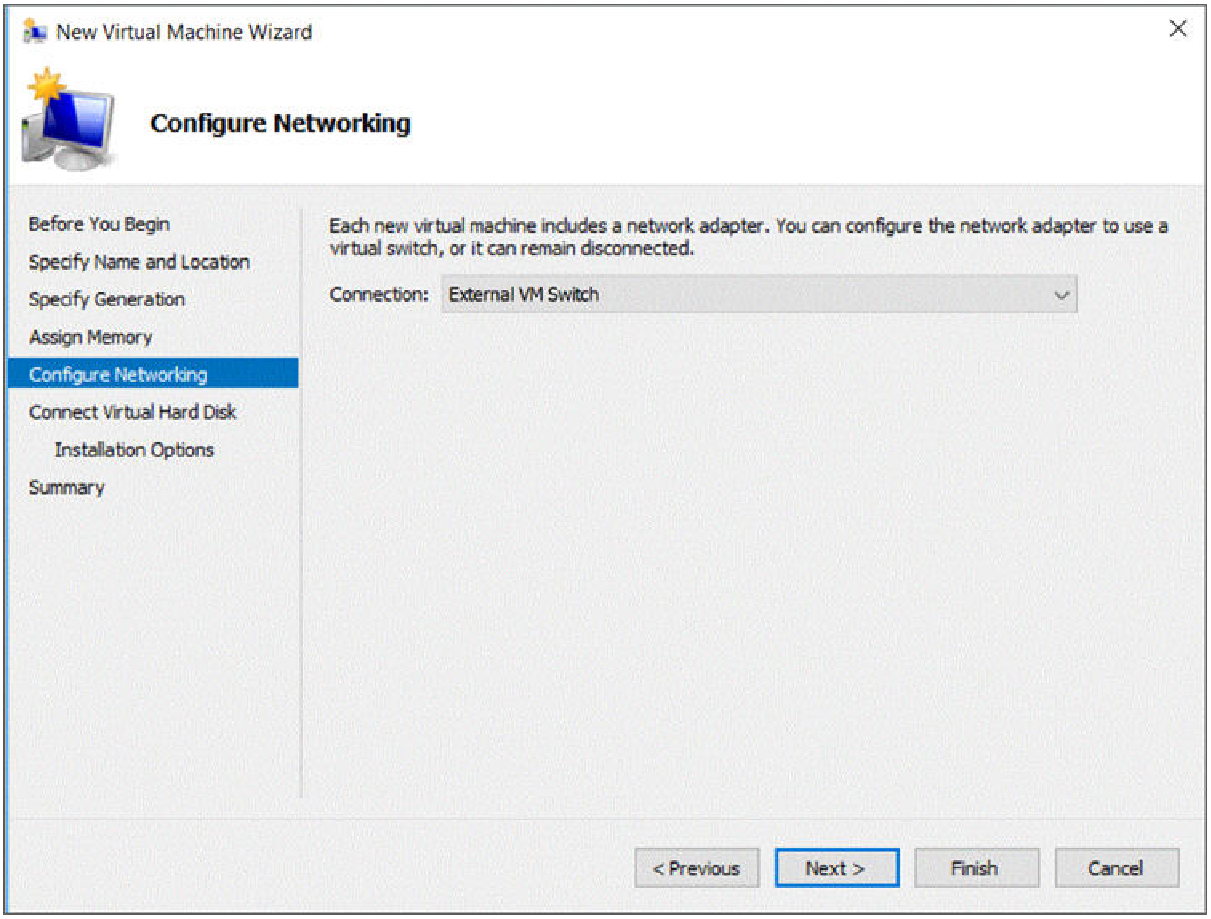
Startup memory: 16384 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

Figure 10. Startup Memory

8. Select a preconfigured virtual switch and click **Next**.

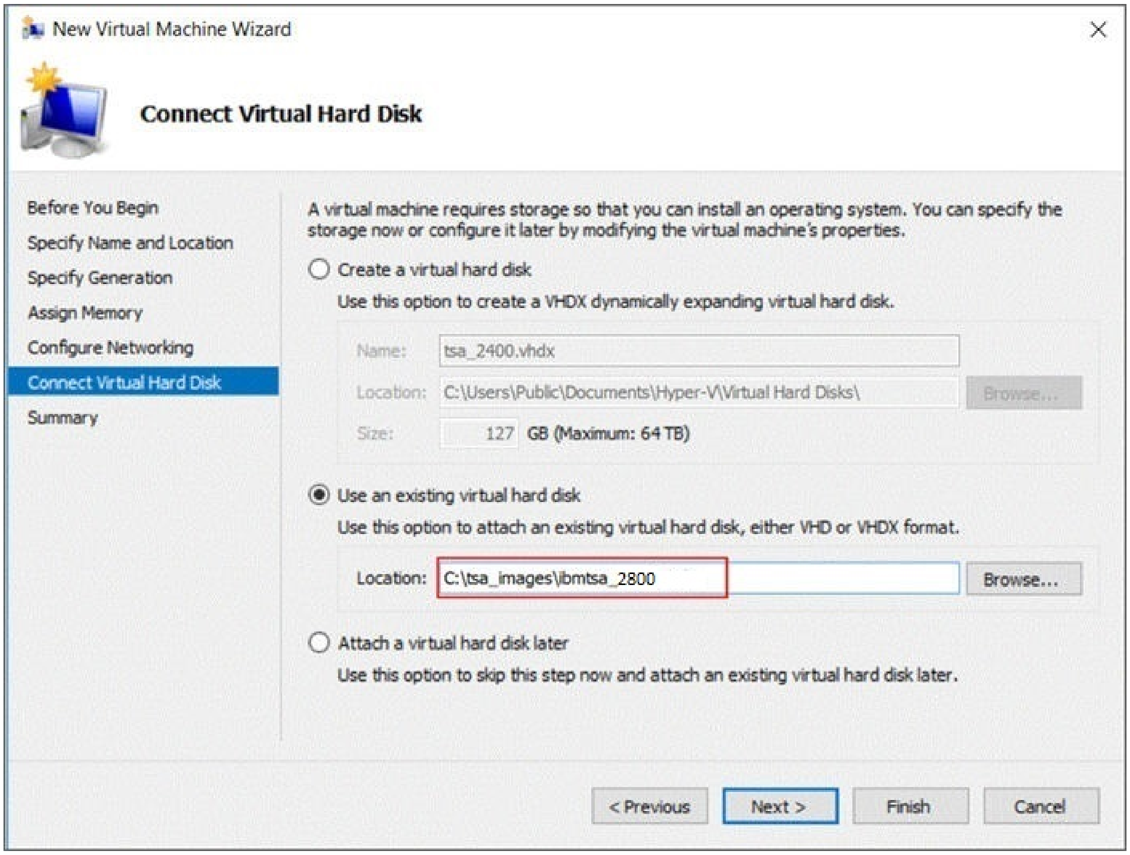


Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: External VM Switch

Figure 11. Configure Networking

9. Select the **Use an existing virtual hard disk** option and browse for the *ibmtsa_2800.vhdx* file that you copied to Hyper-V server in Step 2 and click **Next**.



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: tsa_2400.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

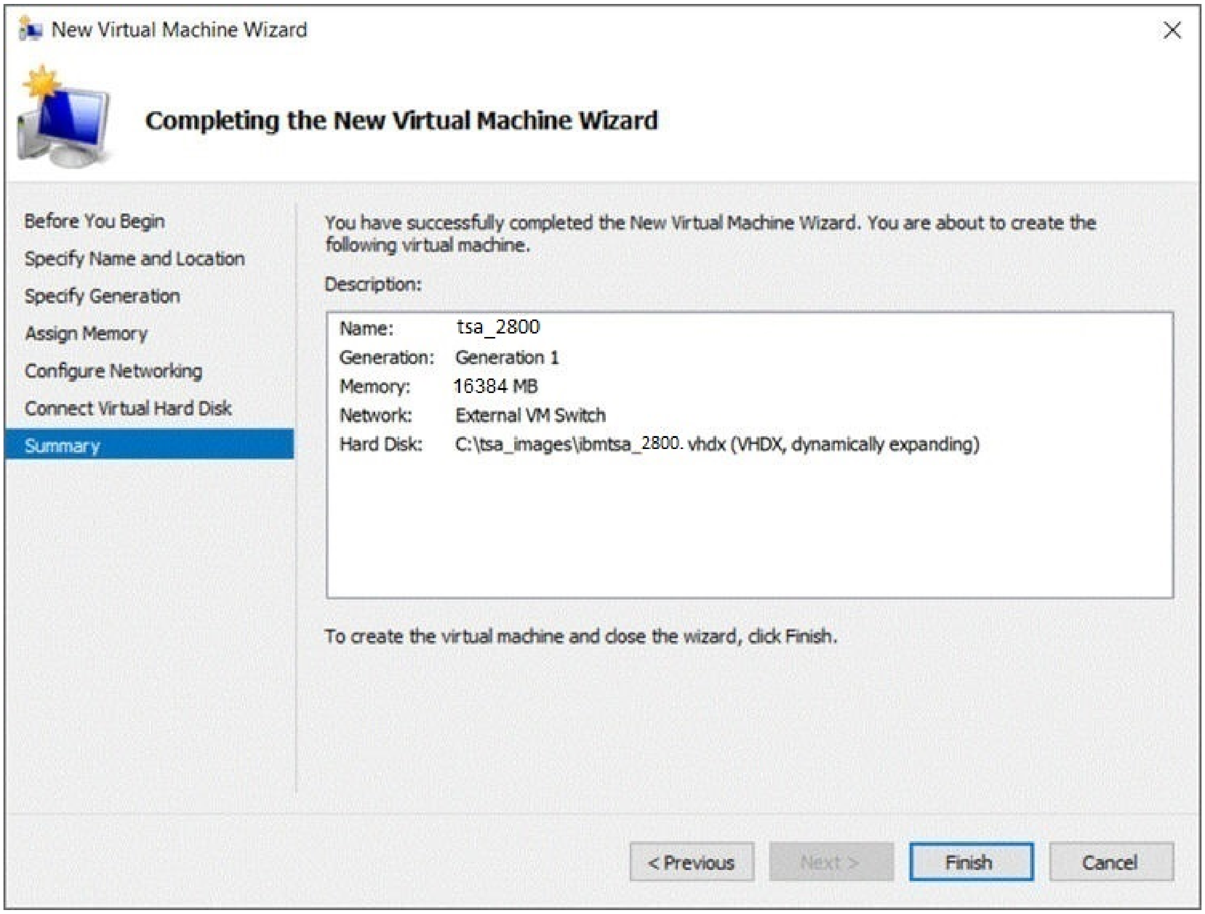
Location: C:\tsa_images\ibmtsa_2800

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

Figure 12. Connect Virtual Hard Disk

10. In the **Summary** page, review the settings and click **Finish**.


New Virtual Machine Wizard
Completing the New Virtual Machine Wizard
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary
< Previous
Next >
Finish
Cancel

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

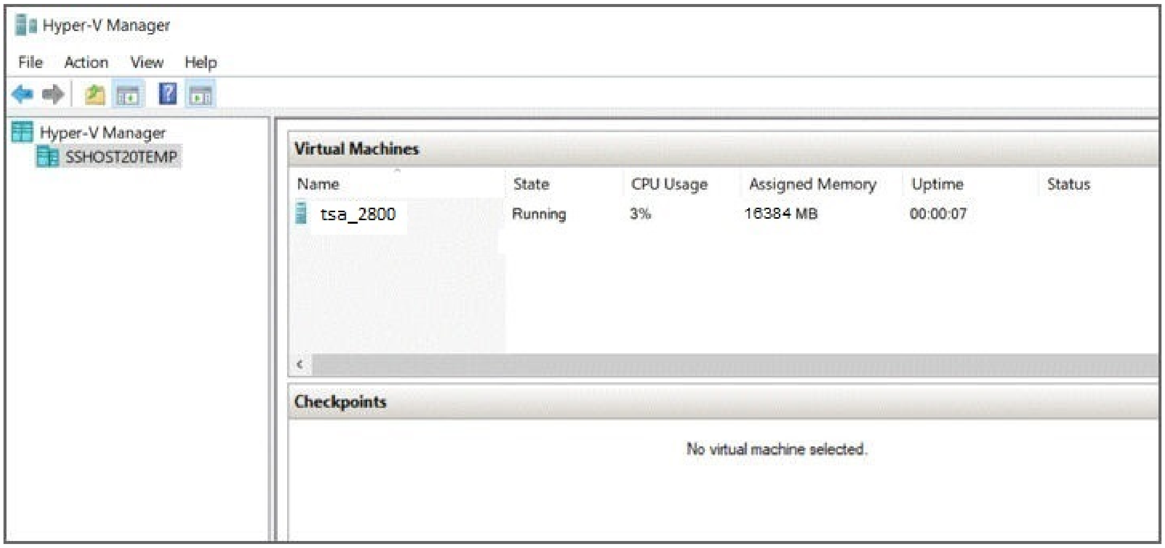
Description:

Name: tsa_2800
Generation: Generation 1
Memory: 16384 MB
Network: External VM Switch
Hard Disk: C:\tsa_images\ibmtsa_2800. vhdx (VHDX, dynamically expanding)

To create the virtual machine and close the wizard, click Finish.

Figure 13. Summary

11. The new virtual machine is added under the Hyper-V Manager. Select the virtual machine, go to **Action** menu and click **Start**.



Name	State	CPU Usage	Assigned Memory	Uptime	Status
tsa_2800	Running	3%	16384 MB	00:00:07	

No virtual machine selected.

Figure 14. Hyper-V Manager

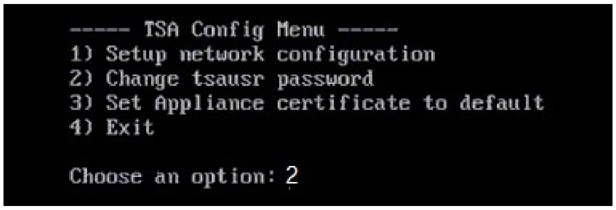
12. From the **Action** menu, select **Connect** to start a console session. In the TSA console, enter the **ibmtsa login** as **`tsausr`** and **Password** as **`configTsa`**.
13. Required: To change the login password, continue with the steps that are listed in the section "Changing tsausr password (required)" on page 19.
14. To complete the installation, continue with the steps that are listed in the section "Configuring the network details" on page 19.

Changing *tsausr* password (required)

For security purposes, it is recommended that the password for *tsausr* be changed from its initial value. Follow these steps to change the *tsausr* password.

Procedure

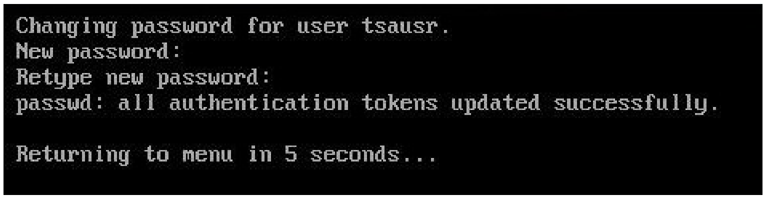
1. Select option **2) Change tsausr password** from the **TSA Config Menu**.



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

Choose an option: 2
```

Figure 15. Change Password

2. Enter the new password at the **New password** prompt. Enter the same password at the **Retype new password** prompt. The new password must be at least 7 characters long.



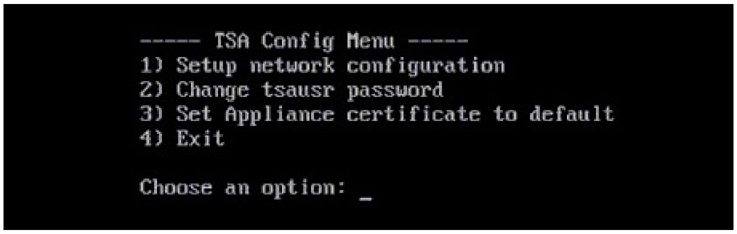
```
Changing password for user tsausr.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

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

Figure 16. New Password

Configuring the network details

Procedure

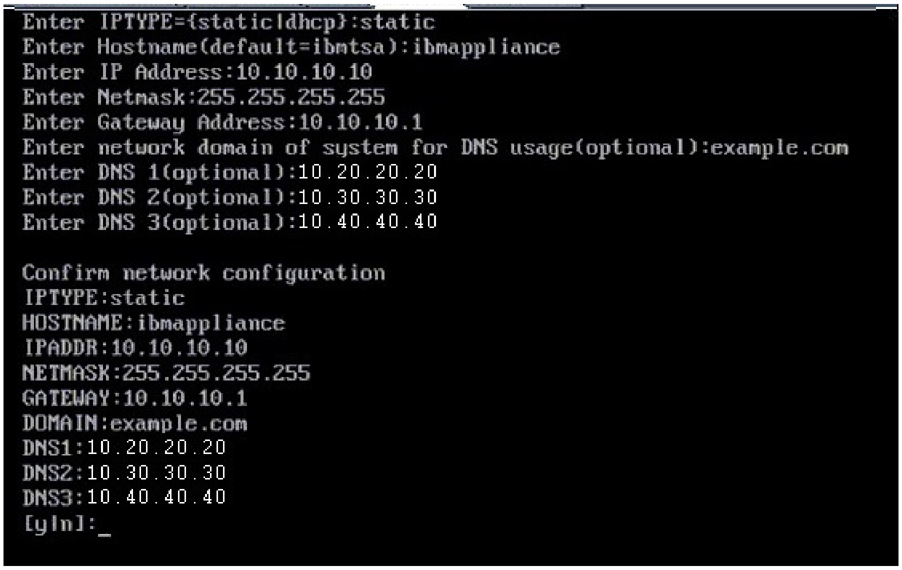
1. Select option **1) Setup network configuration** from the **TSA Config Menu**.



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

Choose an option: _
```

Figure 17. Setup network configuration

2. Enter the following network configuration details.



```
Enter IPTYPE={static|dhcp}:static
Enter Hostname(default=ibmtsa):ibmappliance
Enter IP Address:10.10.10.10
Enter Netmask:255.255.255.255
Enter Gateway Address:10.10.10.1
Enter network domain of system for DNS usage(optional):example.com
Enter DNS 1(optional):10.20.20.20
Enter DNS 2(optional):10.30.30.30
Enter DNS 3(optional):10.40.40.40

Confirm network configuration
IPTYPE:static
HOSTNAME:ibmappliance
IPADDR:10.10.10.10
NETMASK:255.255.255.255
GATEWAY:10.10.10.1
DOMAIN:example.com
DNS1:10.20.20.20
DNS2:10.30.30.30
DNS3:10.40.40.40
[y|n]:_
```

Figure 18. Network Configuration

a) **Enter IPTYPE = {static|dhcp}**. Enter `static` or `dhcp`. If `static`, follow these steps, else go through the `dhcp` configuration steps in the section, Appendix B, “Configuring the DHCP network details,” on page 125

IPTYPE: static

`Enter Hostname(default=ibmtsa)`. You can change the default host name. Ensure that the host name you use is unique.

`Enter IP Address`.

`Enter Netmask` and **`Enter Gateway`**.

`Enter network domain of system for DNS usage (optional)`.

`Enter DNS 1(optional)`, **`Enter DNS 2(optional)`**, and **`Enter DNS 3(optional)`**.

The specified network configuration details are displayed for confirmation.

b) Enter **[y|n]** to confirm or discard the network configuration. Entering **y** saves the network configuration and restarts the system automatically.

Note: For any incorrect configuration, you can change the details. Enter **n** to ignore the current settings and restart the configuration from step “2.a” on page 20

c) The system restarts in 15 seconds for the new network configuration to take effect.

d) Access TSA from the browser by using secure HTTP with the host name or IP address that is entered above.
For example, `https://<hostname | IP address>.`

Note: On the first connection, your browser might display a security exception. You must accept the security certificate and continue to login to TSA.

Note: To modify the basic network settings for TSA through the user interface, follow the steps in “Configuring basic network settings” on page 33. To configure the advanced network settings, follow the steps in “Configuring advanced network settings” on page 35.

3. Setup the Technical Support Appliance using the steps that are listed in Chapter 4, “Setting up the Technical Support Appliance,” on page 21

Results

After you successfully set up TSA, see Chapter 5, “Setting up discovery and transmission to IBM,” on page 49

Chapter 4. Setting up the Technical Support Appliance

About this task

Follow these steps to quickly get started with TSA. If you have not already done so, review Chapter 2, "Prerequisites," on page 5.

Procedure

1. "Logging in to the Technical Support Appliance" on page 21
2. "Accepting the License Agreement" on page 24
3. "Using the Setup Wizard for initial configuration" on page 25
   a) "Setting up IBM Connectivity" on page 26
   b) "Registering the Technical Support Appliance" on page 28
   c) "Setting the Clock" on page 30
   d) "Setting up the Transmission Schedule" on page 31
   e) "Updating the Technical Support Appliance" on page 32
4. "Configuring network settings" on page 33
5. "Setting up the certificates" on page 41.
6. Optional: Appendix C, "User accounts and user groups," on page 127

What to do next

When you finish setting up TSA, see Chapter 5, "Setting up discovery and transmission to IBM," on page 49 for information about how to perform other tasks.

Logging in to the Technical Support Appliance

Procedure

1. Open an internet browser from a system with network access to TSA.

   For more information, see "Required web browsers" on page 5.
2. Enter the following URL in the browser Address bar:

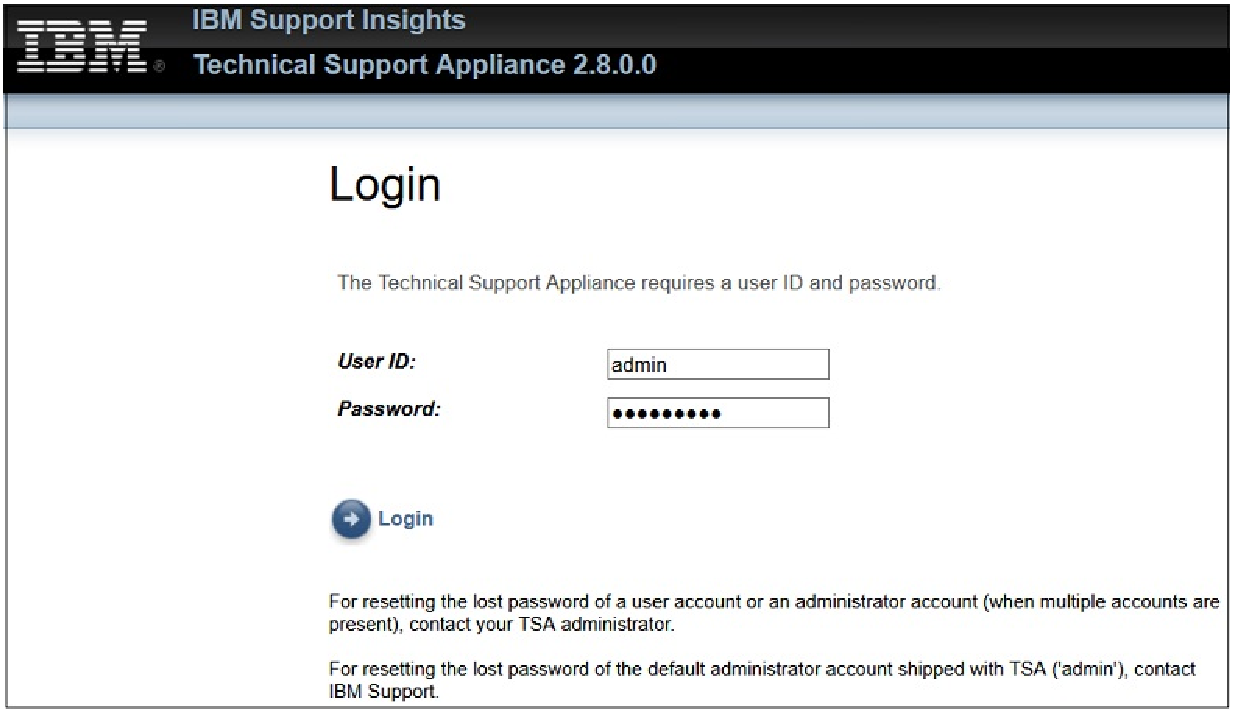
   ```
   https://<hostname or IP address>
   ```

   Note: If the `<hostname>` does not work, then try the assigned IP address of TSA.
3. When prompted, enter the following information:

   User ID:
   Enter `admin`

   Password:
   Enter the TSA administrator password.

   The initial password is `passw0rd`. You must change this initial password after you log on to TSA.



Login

The Technical Support Appliance requires a user ID and password.

User ID: admin

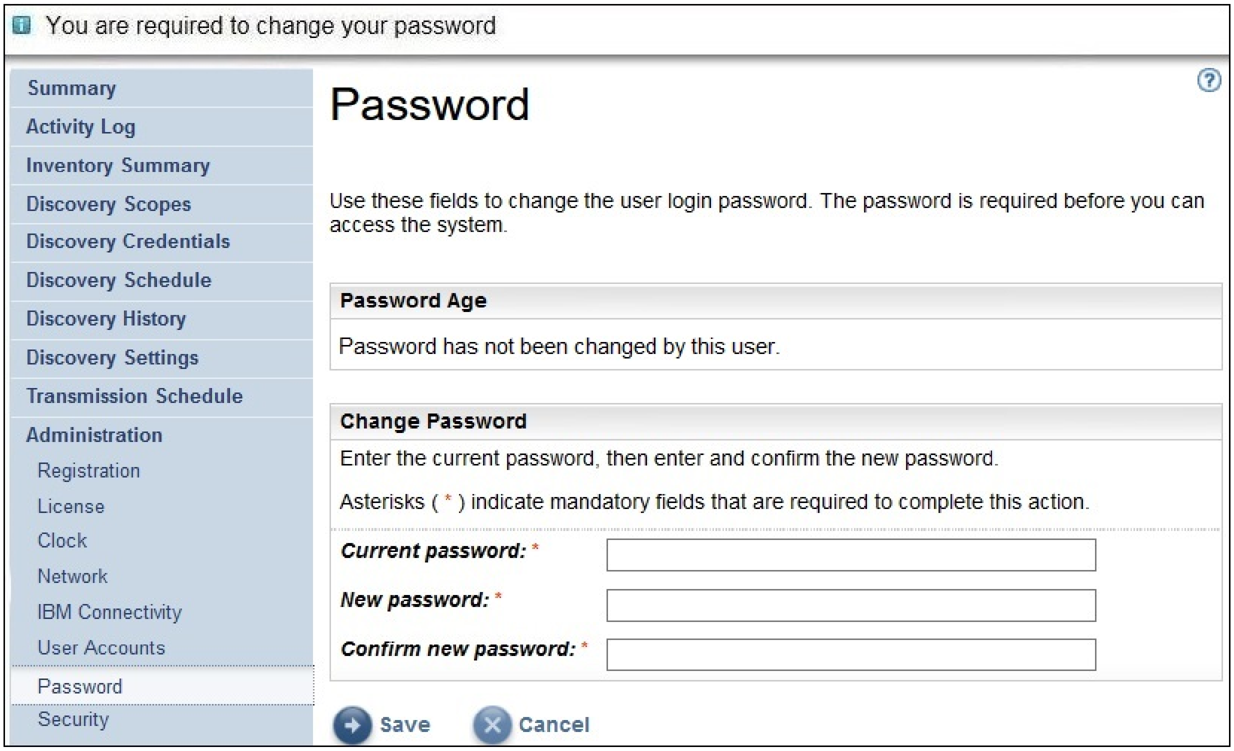
Password: ●●●●●●●●●

For resetting the lost password of a user account or an administrator account (when multiple accounts are present), contact your TSA administrator.

For resetting the lost password of the default administrator account shipped with TSA ('admin'), contact IBM Support.

Figure 19. Login

The **Change Password** page is displayed on your first login.



You are required to change your password

Password

Use these fields to change the user login password. The password is required before you can access the system.

Password Age

Password has not been changed by this user.

Change Password

Enter the current password, then enter and confirm the new password.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Current password: *

New password: *

Confirm new password: *

Figure 20. Change Password

To change the initial password, follow these steps:

a) Enter a new password.

The password must adhere to the following rules:

- Must be at least 8 characters long

- Must contain at least one alphabetic and one non-alphabetic character
- Must not contain the user name
- Must not be the same as any of the previous eight passwords
- Must be changed at least once every 90 days, but must not be changed more than once each day

b) Enter the new password again in the **Confirm new password** field.

The two passwords that you enter are compared to confirm that they match before the password is saved.

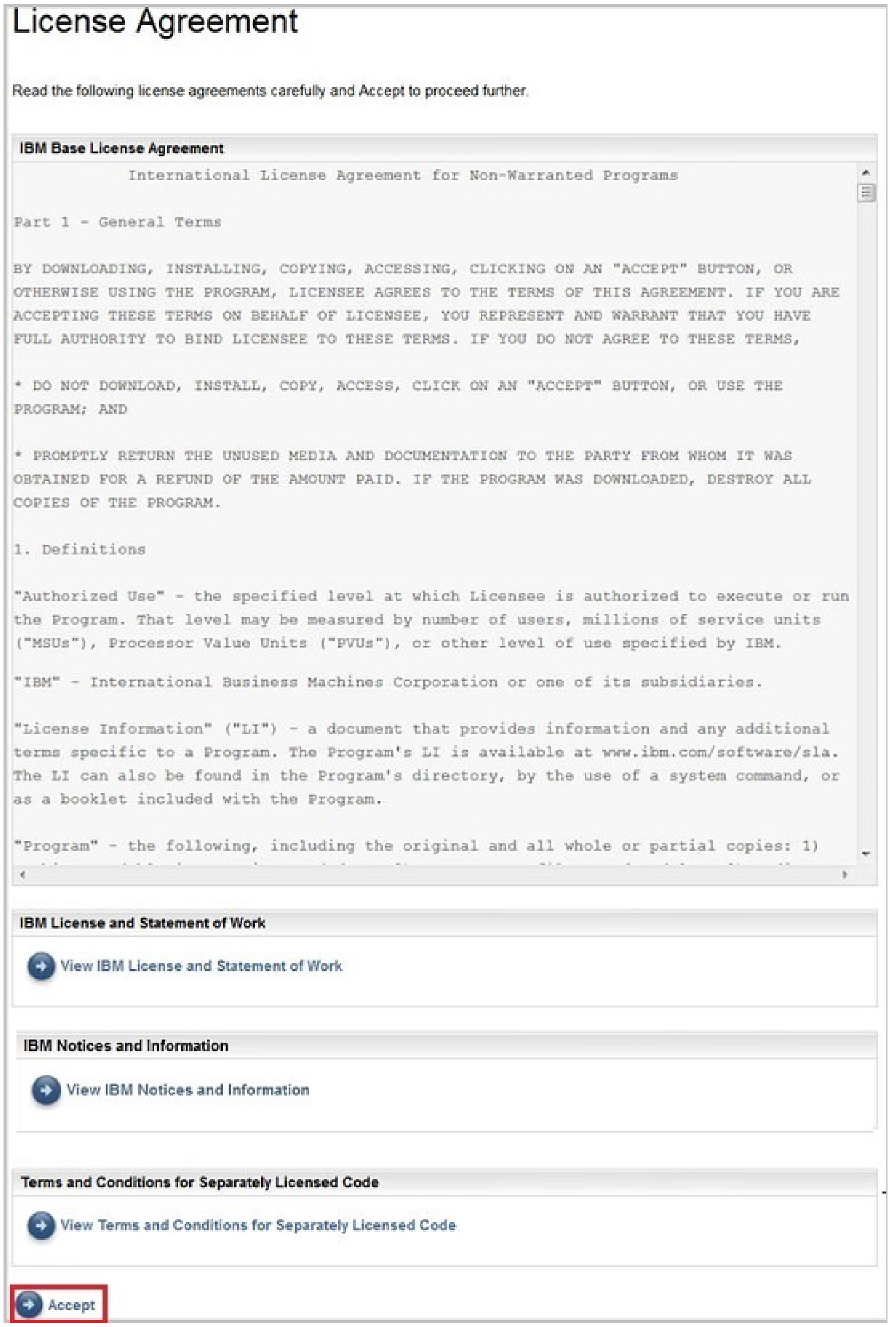
c) Record the new password for future reference.

Important: It is not possible to recover a password, so if the password is lost or forgotten, you cannot log on to TSA to change credentials. If you lose or forget your password for a user account or an administrator account (if you have multiple accounts), contact your TSA administrator. If you lose or forget your password for the default administrator account (shipped with TSA), contact IBM Support.

d) Click **Save**. For the first sign-on, the **License Agreement** page is displayed.

Accepting the License Agreement

Read and accept the License Agreement to proceed further.



License Agreement

Read the following license agreements carefully and Accept to proceed further.

IBM Base License Agreement

International License Agreement for Non-Warranted Programs

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND

* PROMPTLY RETURN THE UNUSED MEDIA AND DOCUMENTATION TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

1. Definitions

"Authorized Use" - the specified level at which Licensee is authorized to execute or run the Program. That level may be measured by number of users, millions of service units ("MSUs"), Processor Value Units ("PVUs"), or other level of use specified by IBM.

"IBM" - International Business Machines Corporation or one of its subsidiaries.

"License Information" ("LI") - a document that provides information and any additional terms specific to a Program. The Program's LI is available at www.ibm.com/software/sla. The LI can also be found in the Program's directory, by the use of a system command, or as a booklet included with the Program.

"Program" - the following, including the original and all whole or partial copies: 1)

IBM License and Statement of Work

View IBM License and Statement of Work

IBM Notices and Information

View IBM Notices and Information

Terms and Conditions for Separately Licensed Code

View Terms and Conditions for Separately Licensed Code

Figure 21. License Agreement

The License Agreement includes the following items:

- **IBM Base License Agreement**: Displays the IBM base license agreement.
- **IBM License and Statement of work**: Click **View IBM License and Statement of Work** to view the IBM license and statement of work.

  Note: TSA is GDPR compliant `[EU/2016/679]`. You can view the GDPR compliant information in the **IBM License and Statement of work** section.
- **IBM Notices and Information**: Click **View IBM Notices and Information** to view the IBM notices and information.

- **Terms and Conditions for Separately Licensed Code**: Click **View Terms and Conditions for Separately Licensed Code** to view the terms and conditions for separately licensed code.

Click **Accept** to accept the agreement. Once you have accepted the license, the **Setup Wizard** is displayed to configure TSA. You can either configure TSA through the **Setup Wizard**, or you can exit the wizard and configure TSA settings as per your requirements.

Note: To view the license agreement again after accepting it, click **Administration** > **License** in the navigation pane.

Related concepts

"Using the Setup Wizard for initial configuration" on page 25
Use the **Setup Wizard** to set up the TSA for the initial configuration.

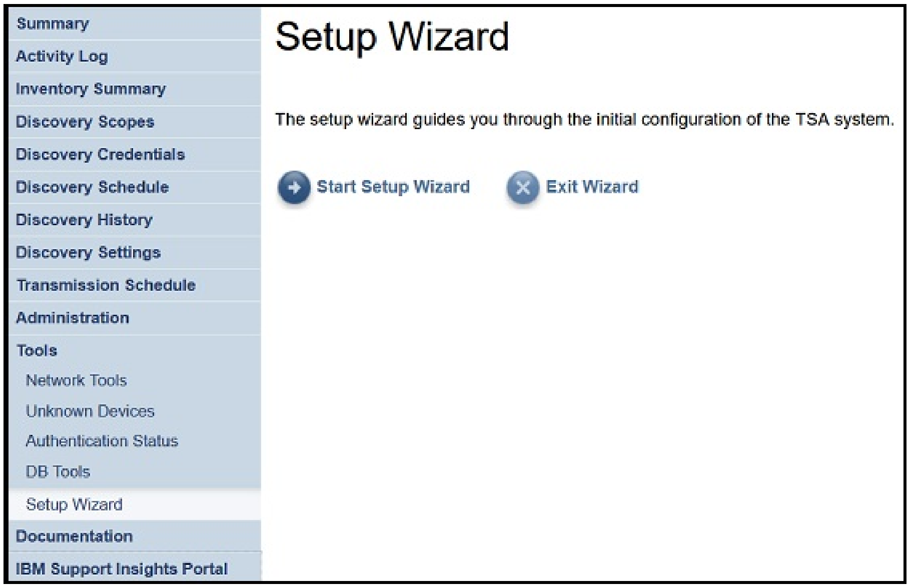
"Configuring the Technical Support Appliance" on page 115
If you exit or skip configuring any of the settings in the **Setup Wizard**, you can manually configure them from the left navigation menu of TSA.

Using the Setup Wizard for initial configuration

Use the **Setup Wizard** to set up the TSA for the initial configuration.

After you accept the license agreement, the **Setup Wizard** is displayed automatically.

Note: To start the **Setup Wizard** manually, in the navigation pane, click **Tools** > **Setup Wizard** > **Start Setup Wizard**.



The setup wizard guides you through the initial configuration of the TSA system.

Figure 22. Setup Wizard

The **Setup Wizard** guides you through the following steps:

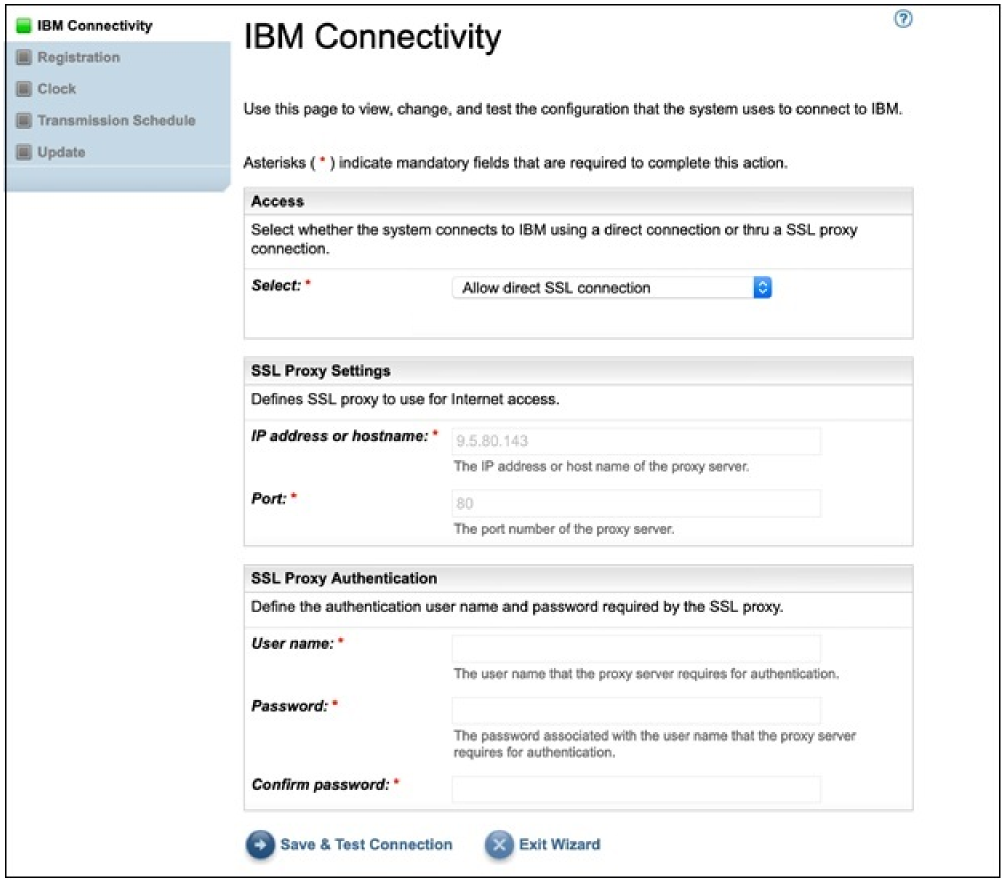
- "Setting up IBM Connectivity" on page 26
- "Registering the Technical Support Appliance" on page 28
- "Setting the Clock" on page 30
- "Setting up the Transmission Schedule" on page 31
- "Updating the Technical Support Appliance" on page 32

Note: If you exit or skip configuring any of the settings in the **Setup Wizard**, you can manually configure them from the navigation pane of TSA. For more information on configuring these settings, see Appendix A, "Configuring the Technical Support Appliance," on page 115.

Setting up IBM Connectivity

Procedure

You can view, change, and test the configuration that TSA uses to connect to IBM.



IBM Connectivity

Use this page to view, change, and test the configuration that the system uses to connect to IBM.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Access

Select whether the system connects to IBM using a direct connection or thru a SSL proxy connection.

Select: * Allow direct SSL connection

SSL Proxy Settings

Defines SSL proxy to use for Internet access.

IP address or hostname: * 9.5.80.143

The IP address or host name of the proxy server.

Port: * 80

The port number of the proxy server.

SSL Proxy Authentication

Define the authentication user name and password required by the SSL proxy.

User name: *

The user name that the proxy server requires for authentication.

Password: *

The password associated with the user name that the proxy server requires for authentication.

Confirm password: *

Figure 23. IBM Connectivity

1. In the **Access** pane, select from the following Internet access types:

   Allow direct SSL connection

   TSA connects to IBM by using a direct connection.

   Use SSL proxy connection

   TSA connects to IBM by using an SSL proxy connection.

   Use authenticating SSL proxy connection

   TSA connects to IBM by using an authenticating SSL proxy connection.

2. If you have selected **Use SSL proxy connection** or **Use authenticating SSL proxy connection**, specify the following information for the proxy server.

   IP address or hostname

   The IP address or host name of the proxy server.

   Note: The host name you enter must not contain an underscore ("_").

   Port

   The port number of the proxy server.

3. If you have selected **Use authenticating SSL proxy connection**, specify the following information for the proxy server:

   User name

   The user name that the proxy server requires for authentication.

Password

The password that is associated with the user name that the proxy server requires for authentication.

Confirm password

Enter the password again. The two passwords that you entered are compared to confirm that they match before the password is saved.

What to do next

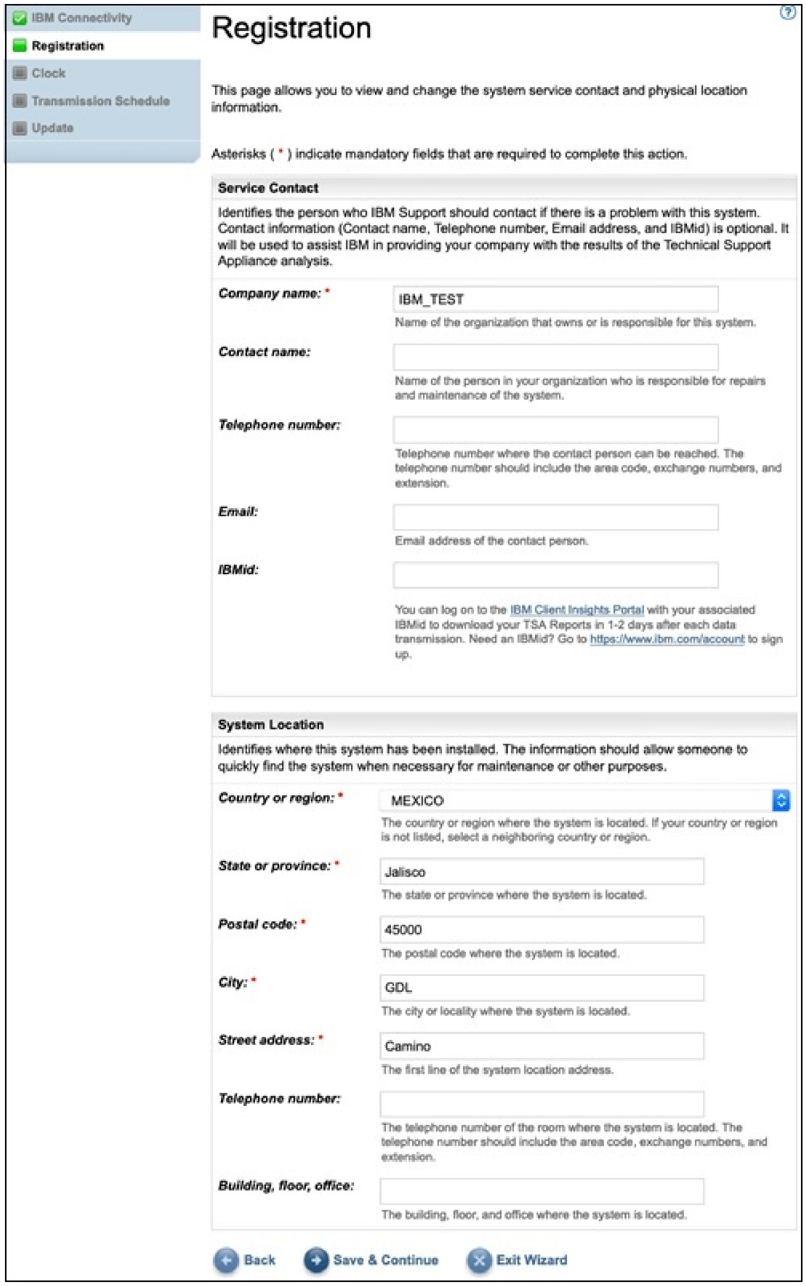
- Click **Save & Test Connection** to save and test the specified connection. If the connection is successful, the **Continue** button is displayed.
- Click **Continue** to go to the **Registration** page.

  -or-
- Click **Exit Wizard** to exit the **Setup Wizard** and go to the **Summary** page.

Registering the Technical Support Appliance

You can view and change the system service contact and physical location.

Procedure



Registration

This page allows you to view and change the system service contact and physical location information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Service Contact

Identifies the person who IBM Support should contact if there is a problem with this system. Contact information (Contact name, Telephone number, Email address, and IBMid) is optional. It will be used to assist IBM in providing your company with the results of the Technical Support Appliance analysis.

Company name: * IBM_TEST
Name of the organization that owns or is responsible for this system.

Contact name:
Name of the person in your organization who is responsible for repairs and maintenance of the system.

Telephone number:
Telephone number where the contact person can be reached. The telephone number should include the area code, exchange numbers, and extension.

Email:
Email address of the contact person.

IBMid:
You can log on to the IBM Client Insights Portal with your associated IBMid to download your TSA Reports in 1-2 days after each data transmission. Need an IBMid? Go to https://www.ibm.com/account to sign up.

System Location

Identifies where this system has been installed. The information should allow someone to quickly find the system when necessary for maintenance or other purposes.

Country or region: * MEXICO
The country or region where the system is located. If your country or region is not listed, select a neighboring country or region.

State or province: * Jalisco
The state or province where the system is located.

Postal code: * 45000
The postal code where the system is located.

City: * GDL
The city or locality where the system is located.

Street address: * Camino
The first line of the system location address.

Telephone number:
The telephone number of the room where the system is located. The telephone number should include the area code, exchange numbers, and extension.

Building, floor, office:
The building, floor, and office where the system is located.

Figure 24. Registration

1. Specify service contact information in the following fields:

   Company name
   The name of the organization that uses TSA.

   Contact name
   (Optional) The name of the person in the organization who is responsible for TSA.

   Telephone number
   (Optional) The telephone number where the contact person can be reached. The telephone number should include the area code, exchange numbers, and extension. Do not use parentheses in the telephone number.

Email
(Optional) The email address of the contact person.

IBMid
(Optional) The IBMid of the person you wish to authorize to view the reports on the IBM Client Insights Portal.

Note: You can log on to https://clientinsightsportal.ibm.com/ with your associated IBMid to download your TSA Reports in 1-2 days after each data transmission. To sign up for an IBMid, go to https://www.ibm.com/account.

Note: The service contact identifies the person who IBM Support should contact if there is a problem with the system. Contact information is used to assist IBM in providing your company with the results of the Technical Support Appliance analysis.

2. Specify TSA location information in the following fields:

Country or region
The country or region where TSA is located.

State or province
The state or province where TSA is located. If you are not sure of the state, type *Unknown*

Postal code
The postal code where the TSA is located.

City
The city or locality where TSA is located.

Street address
TSA location address.

Telephone number
(Optional) The telephone number of the room where TSA is located. The telephone number should include the area code, exchange numbers, and extension. Do not use parentheses in the telephone number.

Building, floor, office
(Optional) The building, floor, and office where TSA is located.

What to do next

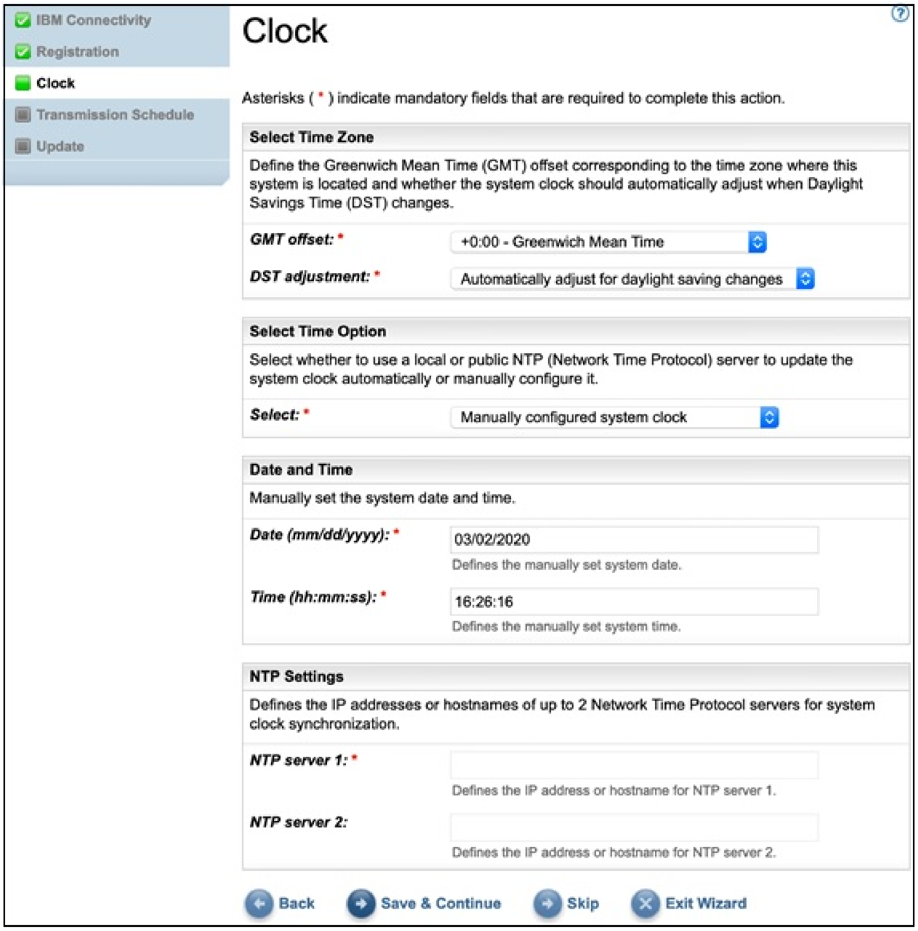
- Click **Save & Continue** to save registration information and continue to the **Clock** page.
- Click **Back** to go back to the **IBM Connectivity** page.

  -or-
- Click **Exit Wizard** to exit the **Setup Wizard** and go to the **Summary** page.

Setting the Clock

You can set the TSA system time, date, and local time zone during setup.

Procedure



Clock

Asterisks (*) indicate mandatory fields that are required to complete this action.

Select Time Zone

Define the Greenwich Mean Time (GMT) offset corresponding to the time zone where this system is located and whether the system clock should automatically adjust when Daylight Savings Time (DST) changes.

GMT offset: * +0:00 - Greenwich Mean Time

DST adjustment: * Automatically adjust for daylight saving changes

Select Time Option

Select whether to use a local or public NTP (Network Time Protocol) server to update the system clock automatically or manually configure it.

Select: * Manually configured system clock

Date and Time

Manually set the system date and time.

Date (mm/dd/yyyy): * 03/02/2020

Defines the manually set system date.

Time (hh:mm:ss): * 16:26:16

Defines the manually set system time.

NTP Settings

Defines the IP addresses or hostnames of up to 2 Network Time Protocol servers for system clock synchronization.

NTP server 1: *

Defines the IP address or hostname for NTP server 1.

NTP server 2:

Defines the IP address or hostname for NTP server 2.

Figure 25. Clock

1. Select your local time zone from the **GMT offset** drop-down list.
2. Select the daylight saving time (DST) adjustment from the **DST adjustment** drop-down list.

   Note: Not all time zones allow DST. If this option is selected for a time zone that does not allow DST, an error message is displayed.
3. Select a method for updating the system clock from the **Select Time Option** drop-down list.

   Options include synchronizing the system clock with a Network Time Protocol (NTP) server to update the system clock automatically or manually configuring the system clock.

   a) If you selected to manually configure the system clock, you must set the system date and time. Enter the date and time information into the **Date** and **Time** fields.

   b) If you selected to synchronize the system clock with a Network Time Protocol (NTP) server to update the system clock automatically, you must then specify the IP addresses and host names for the NTP servers. Type the IP address or host name information for up to two servers in the **NTP server** fields.

   Note: Make sure that the NTP server is accessible through the network to TSA.

What to do next

- Click **Save & Continue** to save clock information and continue to the **Transmission Schedule** page.

-or-

- Click **Skip** to skip to the **Transmission Schedule** page.

To modify settings on the previous step of the wizard

- Click **Back** to go back to the **Registration** page.

To exit the wizard

- Click **Exit Wizard** to exit the **Setup Wizard** and go to the **Summary** page.

Setting up the Transmission Schedule

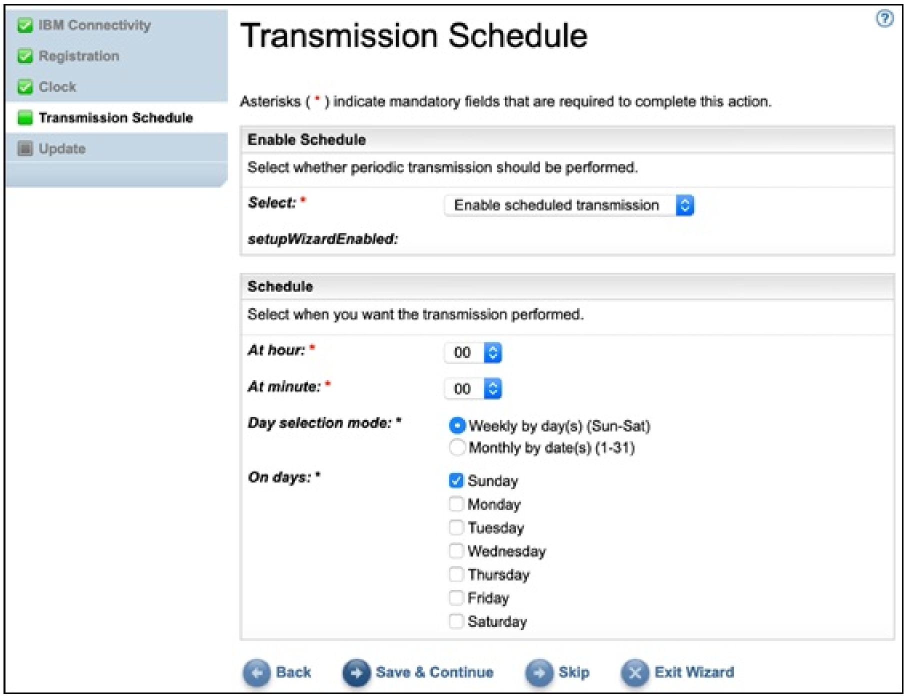
TSA provides a default schedule for the transmission process to run at specified times. You can modify this schedule according to your needs.

Procedure

1. Use the **At hour** and **At minute** drop-down lists to select a new time.
2. Select the **Day Selection mode**.

Weekly by day(s) (Sun - Sat)

To schedule the transmission on a particular day(s) of a week, select the **Weekly by day(s) (Sun - Sat)** option.



Transmission Schedule

Asterisks (*) indicate mandatory fields that are required to complete this action.

Enable Schedule

Select whether periodic transmission should be performed.

Select: * Enable scheduled transmission

setupWizardEnabled:

Schedule

Select when you want the transmission performed.

At hour: * 00

At minute: * 00

Day selection mode: * ● Weekly by day(s) (Sun-Sat) ○ Monthly by date(s) (1-31)

On days: *
☑ Sunday
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday

Figure 26. Weekly by day(s) (Sun - Sat)

For the **On days** field, select the appropriate checkbox to select one or more days of the week.

Monthly by date(s) (1-31)

To schedule the transmission on particular days of a month, select **Monthly by date(s) (1-31)** option.

For the **On days** field, select the appropriate checkbox to select one or more days of the month.

Note: If you select the days beyond the last day of a specific month, then the job is triggered on the last day of that particular month.

Note: Make sure that the discovery start time precedes the transmit time to avoid long delays in transmission of the newly collected data.

What to do next

- Click **Save & Continue** to save transmission schedule and continue to the **Update** page.

  -or-
- Click **Skip** to skip to the **Update** page.

To modify settings on the previous step of the wizard

- Click **Back** to go to back to the **Clock** page.

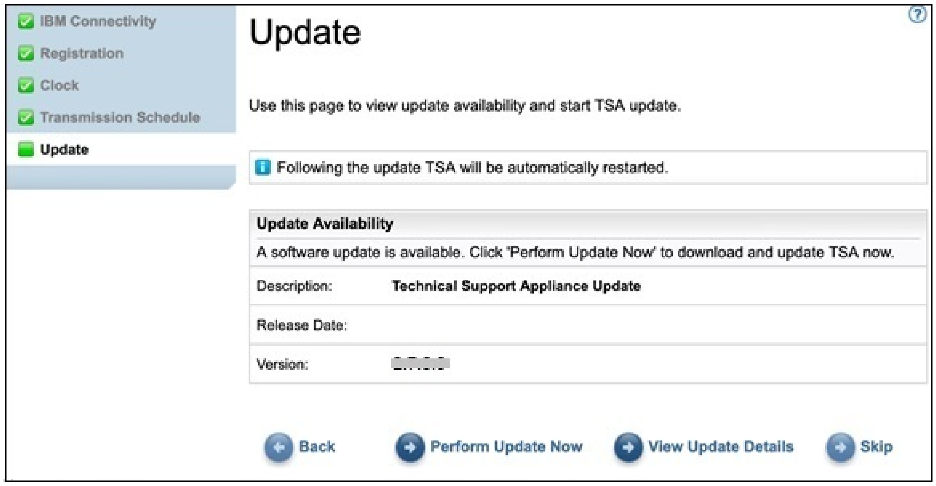
To exit the wizard

- Click **Exit wizard** to exit the **Setup Wizard** and go to the **Summary** page.

Updating the Technical Support Appliance

You can update TSA to the latest version that is available.

If an update is available, the following **Update** page is displayed.



Update

Use this page to view update availability and start TSA update.

Following the update TSA will be automatically restarted.

Update Availability

A software update is available. Click 'Perform Update Now' to download and update TSA now.

Description:	**Technical Support Appliance Update**
Release Date:	
Version:	[redacted]

Figure 27. Update availability

- Click **Perform Update Now** to install the update and complete the **Setup Wizard**.

  -or-
- Click **View Update Details** to view information about the contents of the update.

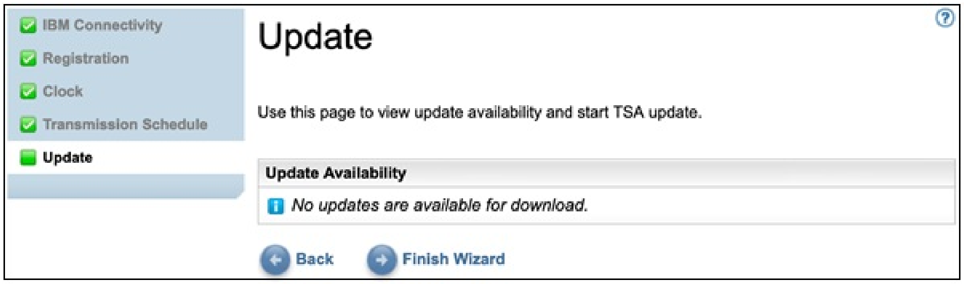
To modify settings on the previous step of the wizard

- Click **Back** to go back to the **Transmission Schedule** page.

To complete the wizard

- Click **Skip** to complete the **Setup Wizard** without applying the update.

If an update is not available, the following **Update** page is displayed.



Update

Use this page to view update availability and start TSA update.

Update Availability

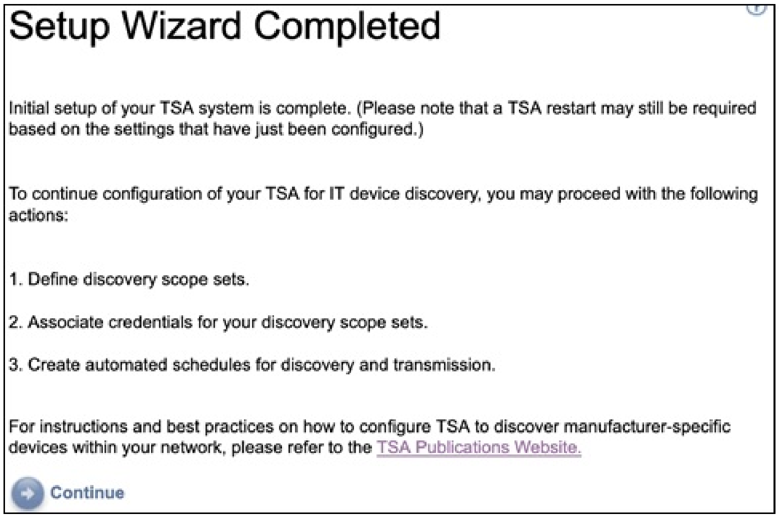
No updates are available for download.

Figure 28. No Updates available

- Click **Finish Wizard** to complete the **Setup Wizard**. The **Setup Wizard Completed** page is displayed.

  -or-

- Click **Back** to go back to the **Transmission Schedule** page.



Setup Wizard Completed

Initial setup of your TSA system is complete. (Please note that a TSA restart may still be required based on the settings that have just been configured.)

To continue configuration of your TSA for IT device discovery, you may proceed with the following actions:

1. Define discovery scope sets.
2. Associate credentials for your discovery scope sets.
3. Create automated schedules for discovery and transmission.

For instructions and best practices on how to configure TSA to discover manufacturer-specific devices within your network, please refer to the TSA Publications Website.

Figure 29. Setup Wizard Completed

- Click **Continue** to go to the **Summary** page.

  Note: Some changes in the **Clock** page might require a restart to take effect. For example, if you set the date or time, or changed from manual configuration to NTP server configuration, you are prompted to restart the system.

  – Click **OK** to finish the **Setup Wizard** and go back to the **Summary** page. The **Summary** page is displayed and the system restarts.

Note: If you exit or skip configuring any of the settings in the **Setup Wizard**, you can manually configure them from the navigation pane of TSA. For more information on configuring these settings, see Appendix A, "Configuring the Technical Support Appliance," on page 115.

Configuring network settings

Installing TSA requires configuration of basic network settings. If these settings are adequate for your IT network, then you can skip this section.

Before you begin

Use the **Network** page to do any of the following:

- Change the initial basic network settings
- Configure TSA to access multiple networks

To configure basic network settings through the console, follow the steps in the "Configuring the network details" on page 19 section.

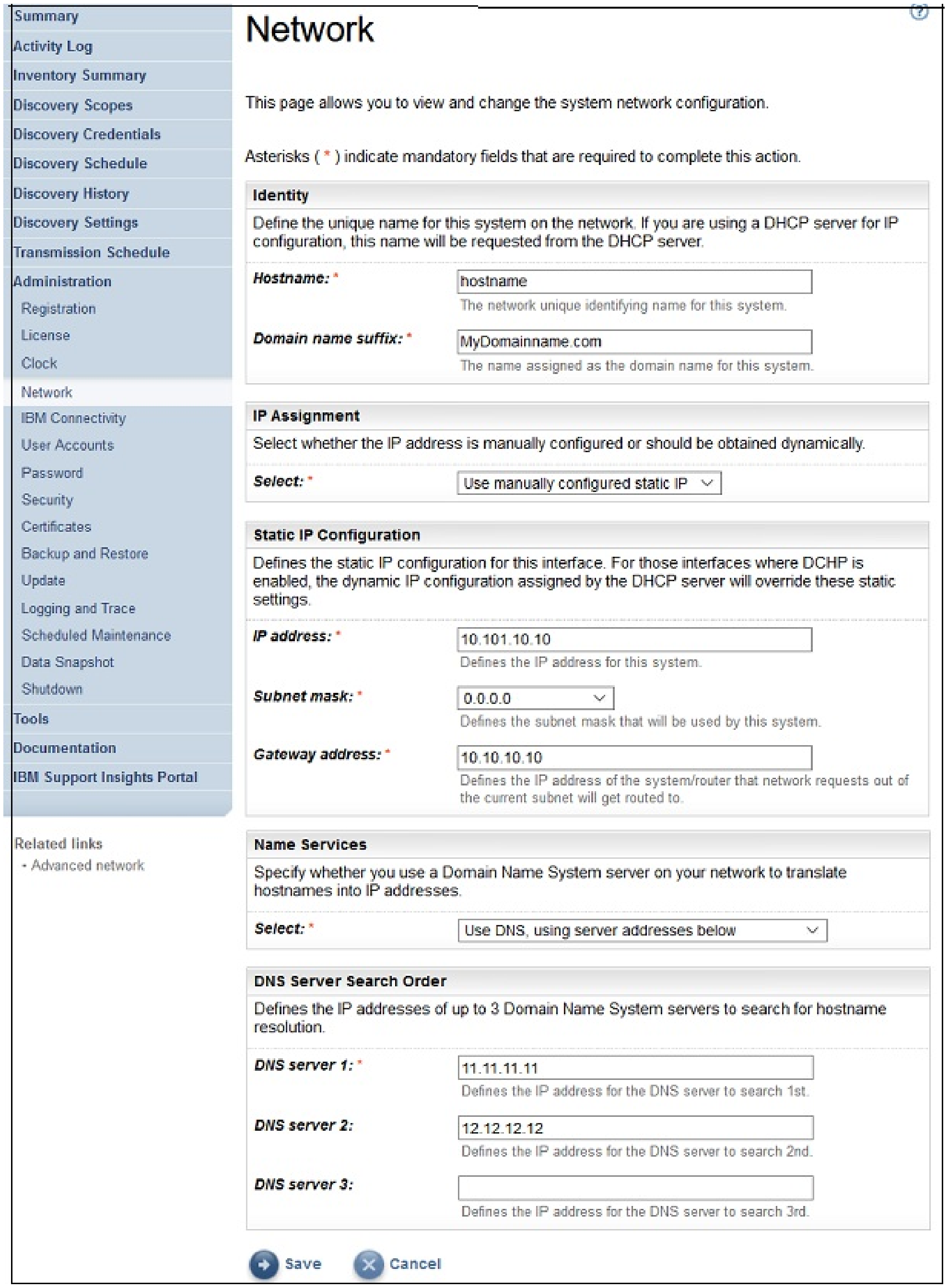
Configuring basic network settings

Use the **Network** page to alter any of the initial network settings.

Procedure

1. In the navigation pane, click **Administration** > **Network**.

   The **Network** page is displayed.



Network

This page allows you to view and change the system network configuration.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Identity

Define the unique name for this system on the network. If you are using a DHCP server for IP configuration, this name will be requested from the DHCP server.

Hostname: * hostname
The network unique identifying name for this system.

Domain name suffix: * MyDomainname.com
The name assigned as the domain name for this system.

IP Assignment

Select whether the IP address is manually configured or should be obtained dynamically.

Select: * Use manually configured static IP

Static IP Configuration

Defines the static IP configuration for this interface. For those interfaces where DCHP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

IP address: * 10.101.10.10
Defines the IP address for this system.

Subnet mask: * 0.0.0.0
Defines the subnet mask that will be used by this system.

Gateway address: * 10.10.10.10
Defines the IP address of the system/router that network requests out of the current subnet will get routed to.

Name Services

Specify whether you use a Domain Name System server on your network to translate hostnames into IP addresses.

Select: * Use DNS, using server addresses below

DNS Server Search Order

Defines the IP addresses of up to 3 Domain Name System servers to search for hostname resolution.

DNS server 1: * 11.11.11.11
Defines the IP address for the DNS server to search 1st.

DNS server 2: 12.12.12.12
Defines the IP address for the DNS server to search 2nd.

DNS server 3:
Defines the IP address for the DNS server to search 3rd.

Figure 30. Network

2. In the **Hostname** field, specify the unique name for this system on the local network.
3. In the **Domain name suffix** field, specify the name that is used as the domain name for this system on the local network.
4. Select **Use manually configured static IP** for *IP Assignment*. For DHCP address assignment, see section Appendix B, “Configuring the DHCP network details,” on page 125.
5. Configure the static IP address:
    a) In the **IP address** field, enter the IP address for this system.
    b) In the **Subnet mask** drop-down list, select the subnet mask to be used by this system.
    c) In the **Gateway address** field, enter the IP address of the system or router that handles requests outside of the current subnet.
6. Specify the **Name Services** according to the IP assignment.

a) For manually configured static IP, select the **Use DNS, using server addresses below** option.

b) For DHCP IP address assignment, select the **Use DNS, but obtain server addresses via DHCP** option.

7. Enter up to three IP addresses for Domain Name System (DNS) servers to use when you are resolving host names.

   TSA searches the servers in the order they are displayed.

8. Click **Save** to save the network settings.

   You are prompted to restart the system.

   ⚠ **CAUTION:** Be careful when you are changing the network settings. If a mistake is made with the network configuration the TSA UI may not be reachable. In that event, the TSA console must be used to repair the network configuration:

   - For VMware, use the VMware ESXi web interface or the VMware vSphere Client
   - For Microsoft Hyper-V, use the Hyper-V Manager

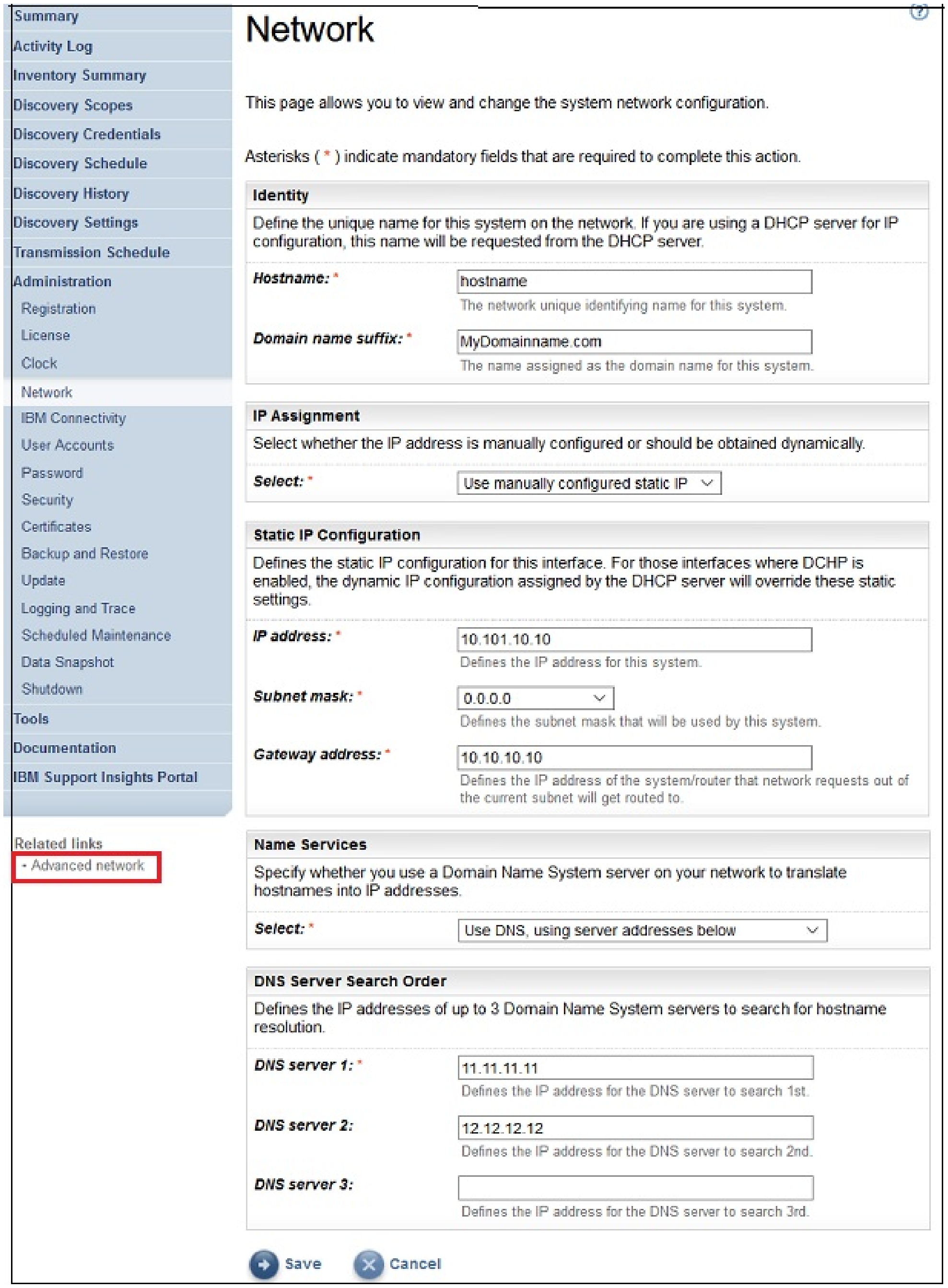
9. Click **Cancel** to exit the **Network** page without saving the settings.

Configuring advanced network settings

If you want to configure TSA to access multiple networks, use the **Network (advanced)** page to specify these network settings.

To configure advanced network settings, follow these steps:

1. In the navigation pane, click **Administration** > **Network**.
2. In the lower navigation pane, under **Related links**, click **Advanced network**.



Network

This page allows you to view and change the system network configuration.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Identity

Define the unique name for this system on the network. If you are using a DHCP server for IP configuration, this name will be requested from the DHCP server.

Hostname: * hostname
The network unique identifying name for this system.

Domain name suffix: * MyDomainname.com
The name assigned as the domain name for this system.

IP Assignment

Select whether the IP address is manually configured or should be obtained dynamically.

Select: * Use manually configured static IP

Static IP Configuration

Defines the static IP configuration for this interface. For those interfaces where DCHP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

IP address: * 10.101.10.10
Defines the IP address for this system.

Subnet mask: * 0.0.0.0
Defines the subnet mask that will be used by this system.

Gateway address: * 10.10.10.10
Defines the IP address of the system/router that network requests out of the current subnet will get routed to.

Name Services

Specify whether you use a Domain Name System server on your network to translate hostnames into IP addresses.

Select: * Use DNS, using server addresses below

DNS Server Search Order

Defines the IP addresses of up to 3 Domain Name System servers to search for hostname resolution.

DNS server 1: * 11.11.11.11
Defines the IP address for the DNS server to search 1st.

DNS server 2: 12.12.12.12
Defines the IP address for the DNS server to search 2nd.

DNS server 3:
Defines the IP address for the DNS server to search 3rd.

Figure 31. Access the Network (advanced) page

The **Network (advanced)** page is displayed.

The **Network (advanced)** page is divided into the following separate pages:

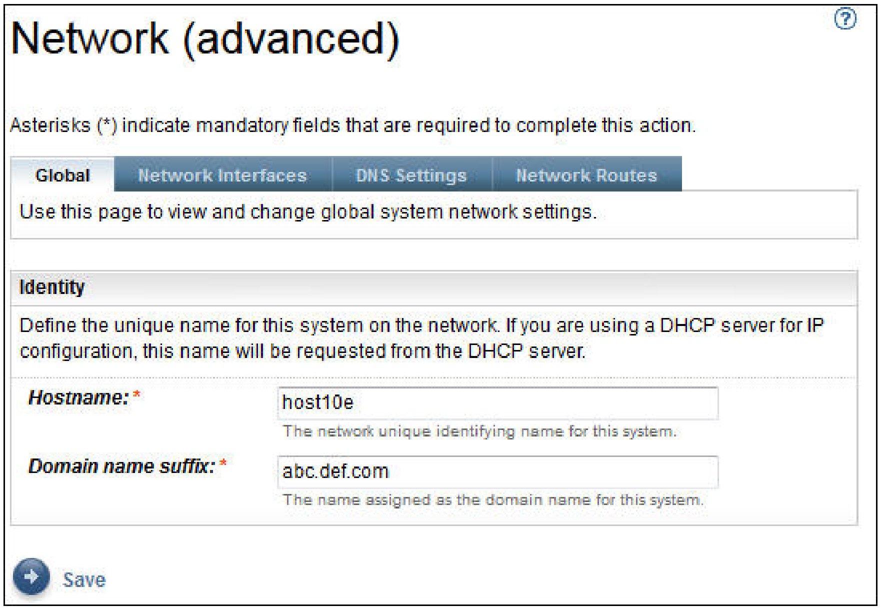
- Global
- Network Interfaces
- DNS Settings
- Network Routes

To access these individual pages, click the tab for the page you want to display.

Important: You must click **Save** before leaving a page to save the changes you made to fields on that page. You are prompted to restart the system for the changes to take effect.

Global

Use this page to view and change global network settings:



Network (advanced)

Asterisks (*) indicate mandatory fields that are required to complete this action.

Use this page to view and change global system network settings.

Identity

Define the unique name for this system on the network. If you are using a DHCP server for IP configuration, this name will be requested from the DHCP server.

Hostname:*	host10e The network unique identifying name for this system.
Domain name suffix:*	abc.def.com The name assigned as the domain name for this system.

Figure 32. Network (advanced) - Global

Identity

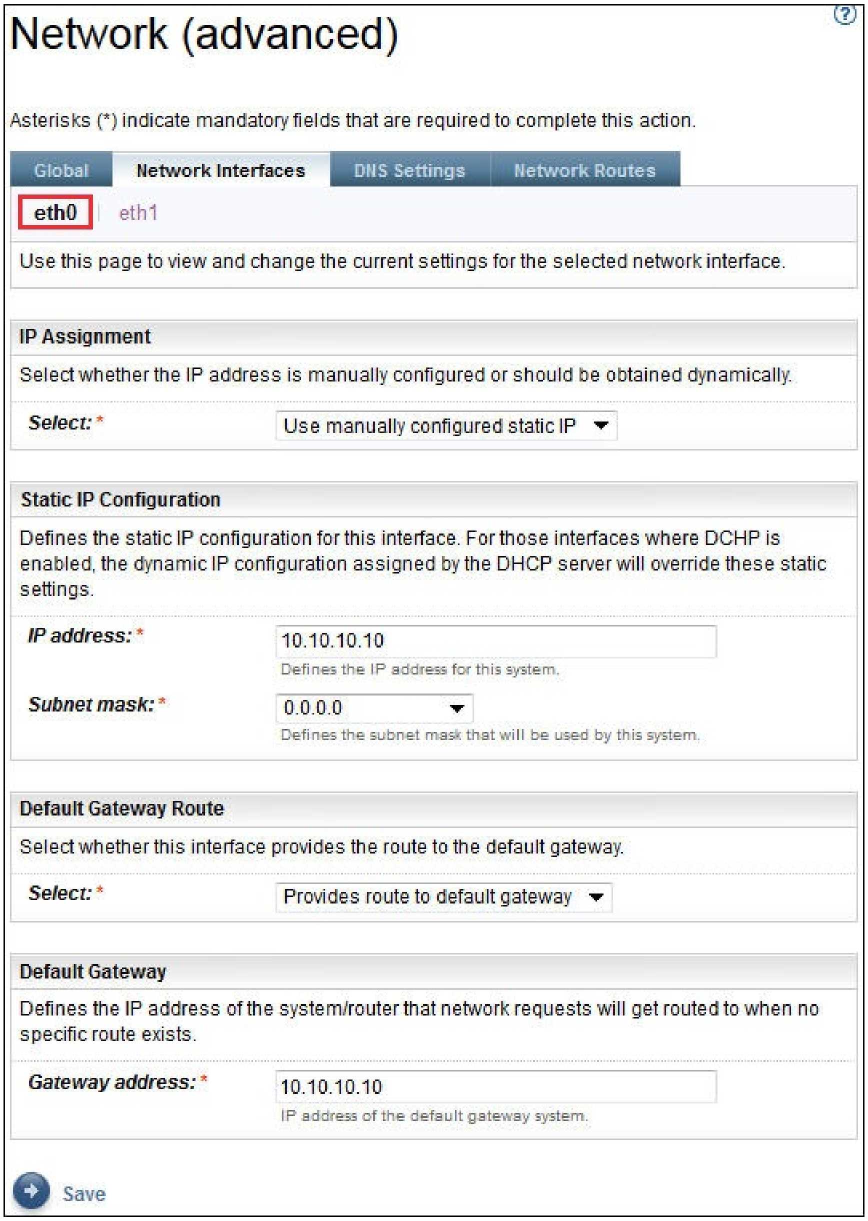
Define the identity of this system on the network.

1. In the **Hostname** field, specify the unique name for this system.
2. In the **Domain name suffix** field, specify the name used as the domain name for this system.

Network Interfaces

TSA is configured to have two Network Interface Controllers (NICs) - eth0 and eth1. Use this page to view and change the current settings for the selected network interface.

1. Click **eth0** to select the eth0 network interface.
2. Click **eth1** to select the eth1 network interface.


Network (advanced)

Asterisks (*) indicate mandatory fields that are required to complete this action.

Use this page to view and change the current settings for the selected network interface.

IP Assignment

Select whether the IP address is manually configured or should be obtained dynamically.

Select: * Use manually configured static IP

Static IP Configuration

Defines the static IP configuration for this interface. For those interfaces where DCHP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

IP address: * 10.10.10.10

Defines the IP address for this system.

Subnet mask: * 0.0.0.0

Defines the subnet mask that will be used by this system.

Default Gateway Route

Select whether this interface provides the route to the default gateway.

Select: * Provides route to default gateway

Default Gateway

Defines the IP address of the system/router that network requests will get routed to when no specific route exists.

Gateway address: * 10.10.10.10

IP address of the default gateway system.

Figure 33. Network (advanced) - Network Interfaces

IP Assignment

Select a method for assigning the IP address for this system. Options include dynamically obtaining the IP address from a DHCP server or using a manually configured static IP address. If you choose to use a manually configured static IP address, you must configure the system IP address on this page.

Static IP Configuration

If you selected to manually configure a static IP address, specify the IP information for this network interface as follows:

1. In the **IP address** field, specify the IP address for this system.
2. In the **Subnet mask** drop-down list, select the subnet mask to be used by this system.

Default Gateway Route

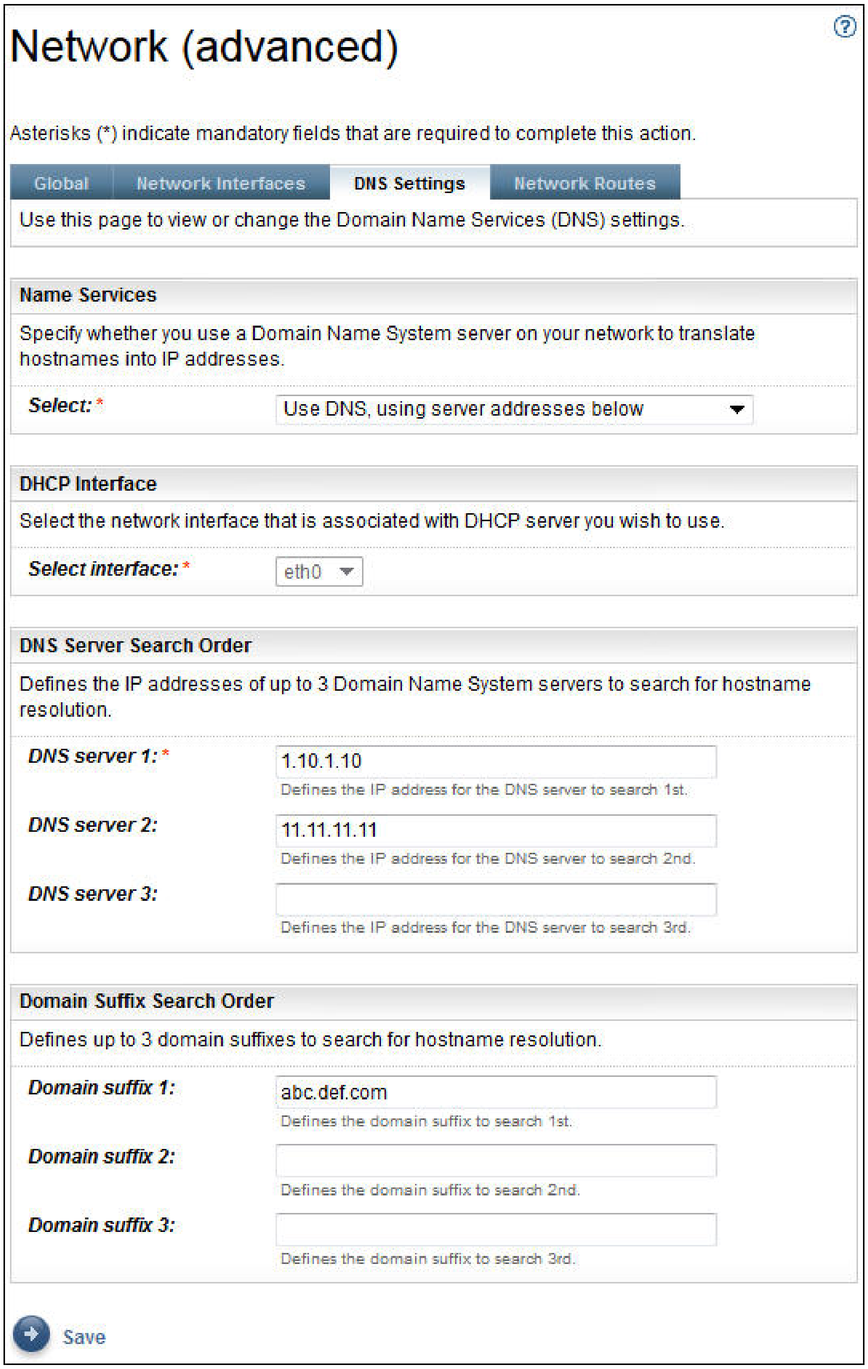
Specify whether this network interface provides a route to the default gateway.

Default Gateway

In the **Gateway address** field, specify the IP address of the default gateway for this system.

DNS Settings

Use this page to view and change the DNS settings.



Network (advanced)

Asterisks (*) indicate mandatory fields that are required to complete this action.

Use this page to view or change the Domain Name Services (DNS) settings.

Name Services

Specify whether you use a Domain Name System server on your network to translate hostnames into IP addresses.

Select: * Use DNS, using server addresses below

DHCP Interface

Select the network interface that is associated with DHCP server you wish to use.

Select interface: * eth0

DNS Server Search Order

Defines the IP addresses of up to 3 Domain Name System servers to search for hostname resolution.

DNS server 1: * 1.10.1.10
Defines the IP address for the DNS server to search 1st.

DNS server 2: 11.11.11.11
Defines the IP address for the DNS server to search 2nd.

DNS server 3:
Defines the IP address for the DNS server to search 3rd.

Domain Suffix Search Order

Defines up to 3 domain suffixes to search for hostname resolution.

Domain suffix 1: abc.def.com
Defines the domain suffix to search 1st.

Domain suffix 2:
Defines the domain suffix to search 2nd.

Domain suffix 3:
Defines the domain suffix to search 3rd.

Figure 34. Network (advanced) - DNS Settings

Name Services

Specify a Domain Name System (DNS) on your network for converting host names into IP addresses. You can choose from the following options:

- Use DNS, but obtain server addresses from a DHCP server.

  If you choose this option, you must select the network interface that is associated with the DHCP server that you want to use.
- Use DNS with server addresses that you specify.

If you choose this option, you must specify at least one DNS server on this page.

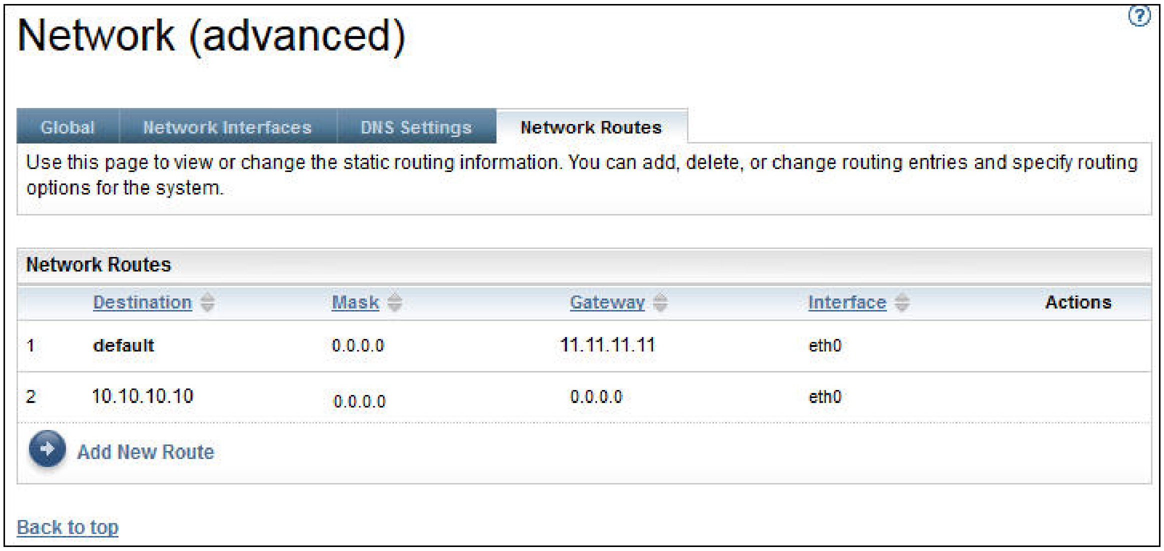
DHCP Interface
Select the network interface that is associated with the DHCP server that you want to use.

DNS Server Search Order
If you choose to use DNS with server addresses you specify, enter up to three IP addresses for Domain Name System (DNS) servers to use when resolving host names. TSA searches the servers in the order that they are displayed.

Domain Suffix Search Order
If you choose to use DNS with server addresses you specify, enter up to three domain name suffixes to use when resolving host names. TSA searches these domain name suffixes in the order they are displayed.

Network Routes

Use this page to view, add, change, or delete static routing entries.



Use this page to view or change the static routing information. You can add, delete, or change routing entries and specify routing options for the system.

Network Routes

	Destination	Mask	Gateway	Interface	Actions
1	default	0.0.0.0	11.11.11.11	eth0	
2	10.10.10.10	0.0.0.0	0.0.0.0	eth0	

Figure 35. Network (advanced) - Network Routes

The following information is displayed for each network route:

Destination

Specifies the TCP/IP destination network host or subnet address.

Mask
Specifies the subnet mask to use as the network mask when you add a route. This is the subnet address for the host portion of the IP address. Network interfaces can use different subnet masks, providing the capability of adding routes by selecting a subnet mask (variable subnet routes). You must select a subnet mask when you add a route, in 32-bit dotted decimal notation.

Gateway
Specifies the TCP/IP gateway address for routing the IP packets.

Interface
Select the adapter from the menu. This is the name of the network adapter that is associated with the table entry.

Actions
Click the **Delete** (🗑) icon to delete the route.

Note: The two routes that are shown in the figure cannot be modified or deleted.

Click **Add New Route** to define a new static network route. The **Network Route** page is displayed.

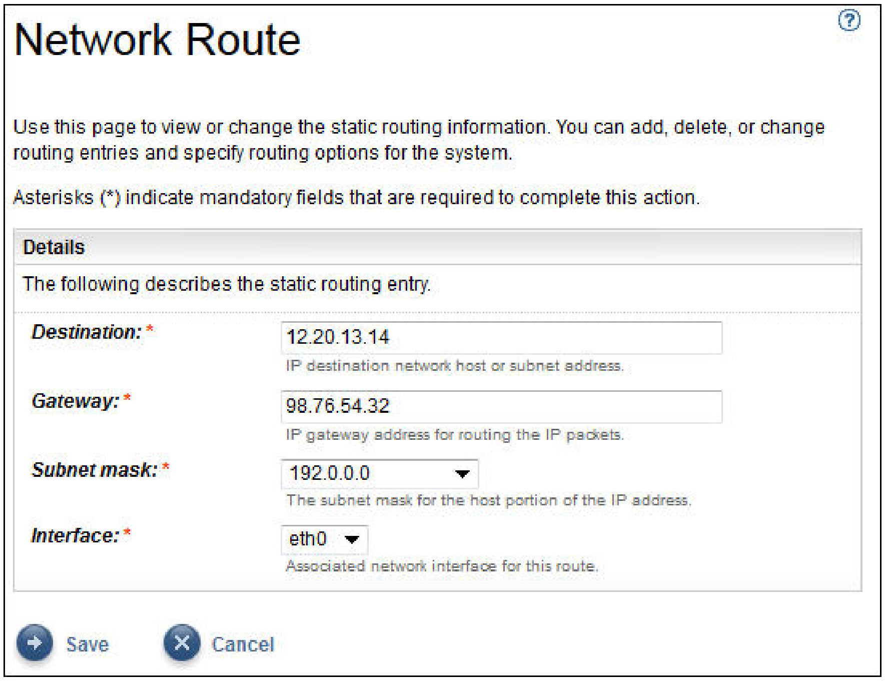
Adding network routes

You can add static network routes.

Procedure

To add a network route, follow these steps:

1. On the **Network (advanced) - Network Routes** page, click **Add New Route**. The **Network Route** page is displayed.

   Network Route

   Use this page to view or change the static routing information. You can add, delete, or change routing entries and specify routing options for the system.

   Asterisks (*) indicate mandatory fields that are required to complete this action.

   Details

   The following describes the static routing entry.

   Destination: * 12.20.13.14
   IP destination network host or subnet address.

   Gateway: * 98.76.54.32
   IP gateway address for routing the IP packets.

   Subnet mask: * 192.0.0.0
   The subnet mask for the host portion of the IP address.

   Interface: * eth0
   Associated network interface for this route.

   Figure 36. New Network Route

2. In the **Destination** field, enter the IP address for the TCP/IP destination network host or subnet.
3. In the **Gateway** field, enter the TCP/IP gateway address for routing the information. The address must be in 32-bit dotted decimal notation. For example: `xxx.xxx.xxx.xxx`.
4. In the **Subnet mask** drop-down list, select the subnet mask to use as the network mask for this route.
5. From the **Interface** drop-down list, select the network adapter to associate with this route.
6. Click **Save** to save this network route.

Setting up the certificates

The **Certificates** page allows you to view certificate signing information, generate and install certificates, or import certificates. These are the server certificates that TSA presents to a web server when the user interface is accessed.

The default configuration of TSA implements a generic self-signed SSL server certificate to facilitate setup. For added security, it is recommended that you replace the default certificate after the initial deployment and configuration steps are complete. You can use TSA to generate and install a self-signed SSL server certificate that is unique to this TSA, to generate and install a custom certificate that is signed by the certificate authority of your choice, or to upload your own Java keystore file that contains a custom SSL server certificate.

You can install a custom certificate using one of the following methods:

- "Installing a custom certificate (using signers)" on page 43
- "Installing a custom certificate (alternate method) " on page 44

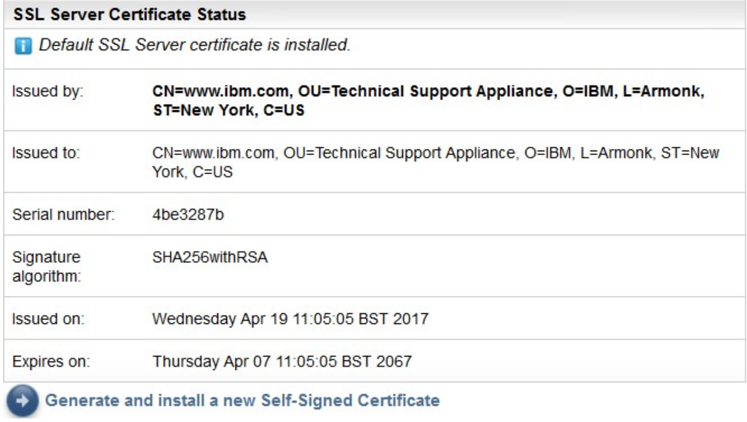
Viewing SSL server certificate status

Configuring TSA installs the default TSA certificate that is delivered with the Technical Support Appliance.

Procedure

1. In the navigation pane, click **Administration** > **Certificates**.

   The **Certificates** page is displayed.

   SSL Server Certificate Status

   Default SSL Server certificate is installed.

Issued by:	**CN=www.ibm.com, OU=Technical Support Appliance, O=IBM, L=Armonk, ST=New York, C=US**
Issued to:	CN=www.ibm.com, OU=Technical Support Appliance, O=IBM, L=Armonk, ST=New York, C=US
Serial number:	4be3287b
Signature algorithm:	SHA256withRSA
Issued on:	Wednesday Apr 19 11:05:05 BST 2017
Expires on:	Thursday Apr 07 11:05:05 BST 2067

   Figure 37. SSL Server Certificate Status

   The **SSL Server Certificate Status** section displays information about the SSL server certificate that is installed in TSA. The certificate information includes *Issued by*, *Issued to*, *Issued on*, *Expires on*, *Serial number*, and *Signature algorithm*.
2. Click **Generate and install a new Self-signed Certificate** to install a self-signed certificate that is unique to this TSA. A warning message is displayed that the appliance restarts automatically after you generate and install a Self-signed certificate.

   Note: The **Generate and install a new Self-signed Certificate** button is visible only if the default certificate is installed on TSA.

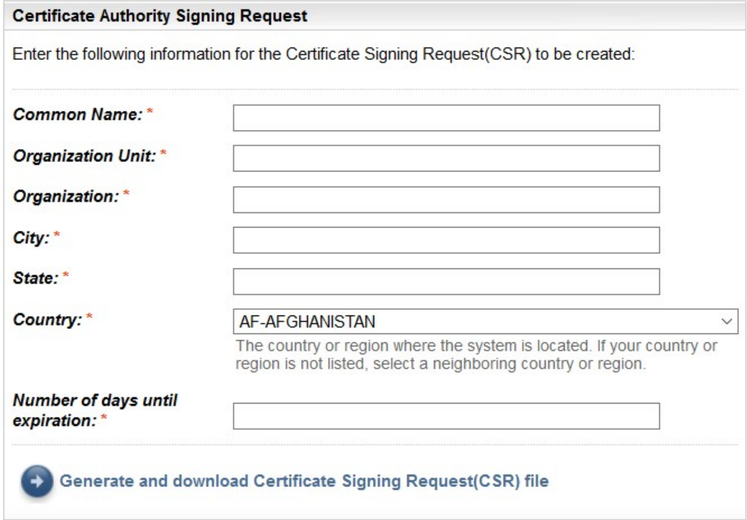
Generating and downloading CSR

To apply for an SSL certificate that is certified by a Certificate Authority, you need to provide the following information to generate and download the Certificate Signing Request (CSR) file.

Procedure

1. In the navigation pane, click **Administration** > **Certificates**.

   The **Certificates** page is displayed.



Certificate Authority Signing Request

Enter the following information for the Certificate Signing Request(CSR) to be created:

Common Name: *

Organization Unit: *

Organization: *

City: *

State: *

Country: * AF-AFGHANISTAN

The country or region where the system is located. If your country or region is not listed, select a neighboring country or region.

Number of days until expiration: *

Generate and download Certificate Signing Request(CSR) file

Figure 38. Certificate Signing Request

2. Enter the fully qualified host name (FQDN) of TSA in the **Common Name** field. The minimum character limit is 1 and the maximum character limit is 64.
3. Specify the organization name, which differentiates between divisions within an organization in the **Organization Unit** field.
4. Specify the name of the corporation, limited partnership, university, or government agency in the **Organization** field.
5. Specify the city or locality name where the TSA is operated in the **City** field.
6. Specify the state or province name where the TSA is operated in the **State** field. If you are not sure of the state, or if state does not apply for your country, type *Unknown*.
7. Select the country name where the TSA is operated in the **Country** drop-down.
8. Specify the number of days that the certificate is valid starting from the time the certificate is created, in the **Number of days until expiration** field.
9. Click **Generate and download Certificate Signing Request (CSR) file** to create and download the CSR file with the specified information.

   Note: To restore the default certificate that is packaged with TSA, see section "Restoring the default certificate" on page 45.

Installing a custom certificate (using signers)

Use this feature to install a custom certificate. You need the server certificate that is generated by a Certificate Authority, the root certificate for the Certificate Authority, and any intermediate certificates for the Certificate Authority.

Before you begin

Ensure that the certificate files (root, intermediate, and server certificate) are in any of the following formats:

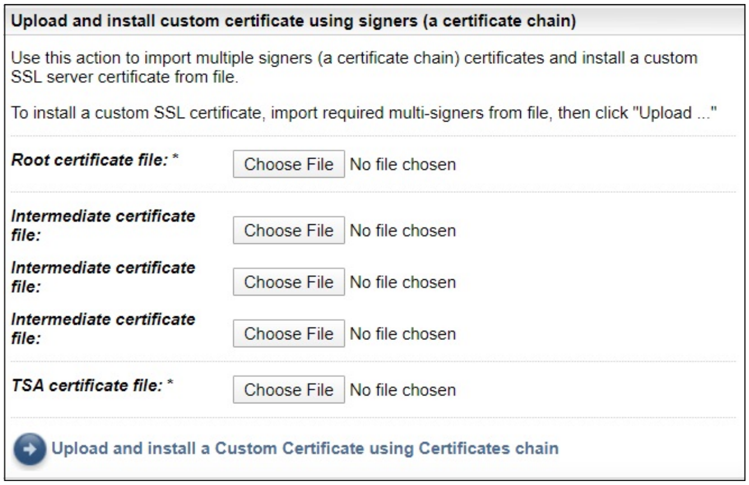
- *.crt*
- *.der*
- *.pem*

Procedure

Go through the following steps to upload and install the certificates on TSA:

1. In the navigation pane, click **Administration** > **Certificates**.

   The **Certificates** page is displayed.



Upload and install custom certificate using signers (a certificate chain)

Use this action to import multiple signers (a certificate chain) certificates and install a custom SSL server certificate from file.

To install a custom SSL certificate, import required multi-signers from file, then click "Upload ..."

Root certificate file: *	Choose File No file chosen
Intermediate certificate file:	Choose File No file chosen
Intermediate certificate file:	Choose File No file chosen
Intermediate certificate file:	Choose File No file chosen
TSA certificate file: *	Choose File No file chosen

Upload and install a Custom Certificate using Certificates chain

Figure 39. Install Custom Certificate

2. In the **Root Certificate file** field, specify the location of the root certificate file that you want to install on TSA.
3. In the **Intermediate Certificate file** field, specify the location of the intermediate certificate file that you want to install on TSA.

   Note: There can be multiple (maximum of 3) intermediate certificate files based on the multiple signers that are imported.
4. In the **TSA Certificate file** field, specify the location of the TSA Server Certificate file that you want to install on TSA.
5. Click **Upload and install a Custom Certificate using Certificates chain** to upload all the files (*Root Certificate file*, *Intermediate certificate files*, *TSA certificate file*) that you specified and install a custom certificate by using the chain of certificates.

   Note: To restore the default certificate that is packaged with TSA, see section "Restoring the default certificate" on page 45.

Installing a custom certificate (alternate method)

Use this feature to install a custom certificate. You can use this function to deploy an already built complete Java keystore file.

Before you begin

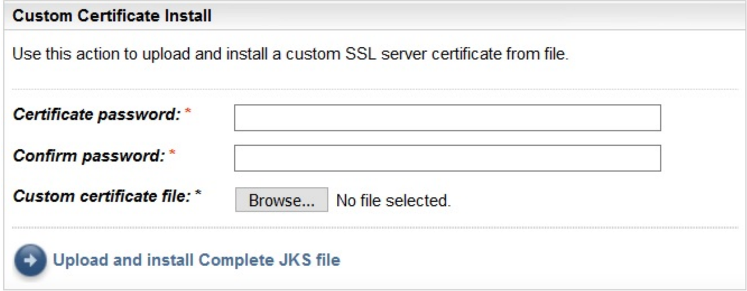
It is recommended that you use the **Certificate Authority Signing Request** and **Upload and install custom certificate using signers (a certificate chain)** functions from the **Certificates** page to deploy a custom certificate. However, if you have already built a complete Java keystore file independently (containing the keys, custom certificate and relevant CA certificates) you can use this function to deploy the keystore file. You must provide the location of the keystore file and the password for the file.

Note: When you create the keystore file, make sure that the key entry password and the keystore password are identical.

Procedure

1. In the navigation pane, click **Administration** > **Certificates**.

   The **Certificates** page is displayed.


Custom Certificate Install

Use this action to upload and install a custom SSL server certificate from file.

Certificate password: *

Confirm password: *

Custom certificate file: * Browse... No file selected.

Figure 40. Custom Certificate Install

2. To install a custom server certificate, follow these steps.
   a) Enter the password for the certificate in the **Certificate password** field.
   b) Enter the password again in the **Confirm password** field.

      The two passwords that you enter are compared to confirm that they match before the password is saved.
   c) Specify the location of the Java keystore file that contains the custom certificate in the **Custom certificate file** field.
   d) Click **Upload and install Complete JKS file** to upload the Java keystore file that you specified and install a custom certificate. The Java keystore file must include the custom certificate and any relevant certificate authority root and intermediate certificates. The appliance will restart to activate usage of the new certificate.

   Note: To restore the default certificate that is packaged with TSA, see section "Restoring the default certificate" on page 45.

Results

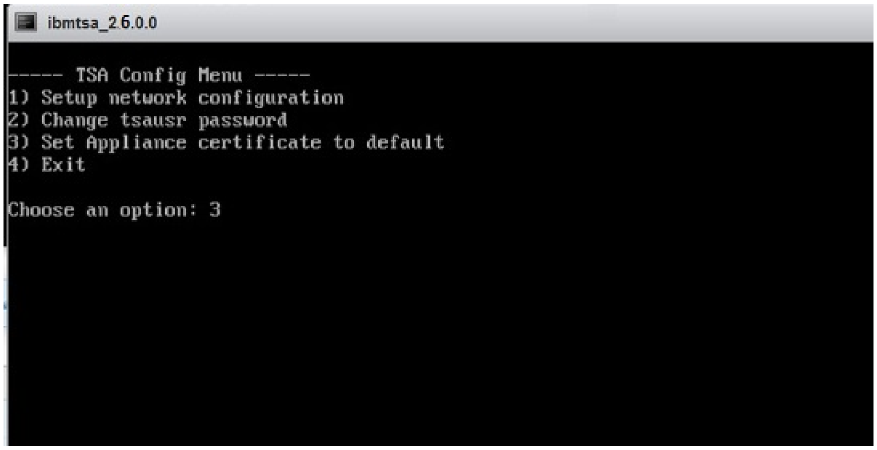
Once the new certificate is installed, TSA automatically restarts. When the restart completes, your browser may display a security prompt regarding whether to trust the new certificate.

Restoring the default certificate

To restore the default certificate that is packaged with TSA, use the TSA console and select the **Set Appliance certificate to default** option.

Procedure

1. Launch the TSA console.
2. Select option **3) Set Appliance certificate to default** from the **TSA Config Menu**.



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

Choose an option: 3
```

Figure 41. Set Appliance certificate to default

3. **Confirm setting appliance certificate to default certificate [y|n]:** Enter **y** to confirm setting the TSA certificate to the default certificate.

Results

Once the default certificate is installed, TSA automatically restarts in 5 seconds. When the restart completes, your browser may display a security prompt regarding whether to trust the default certificate.

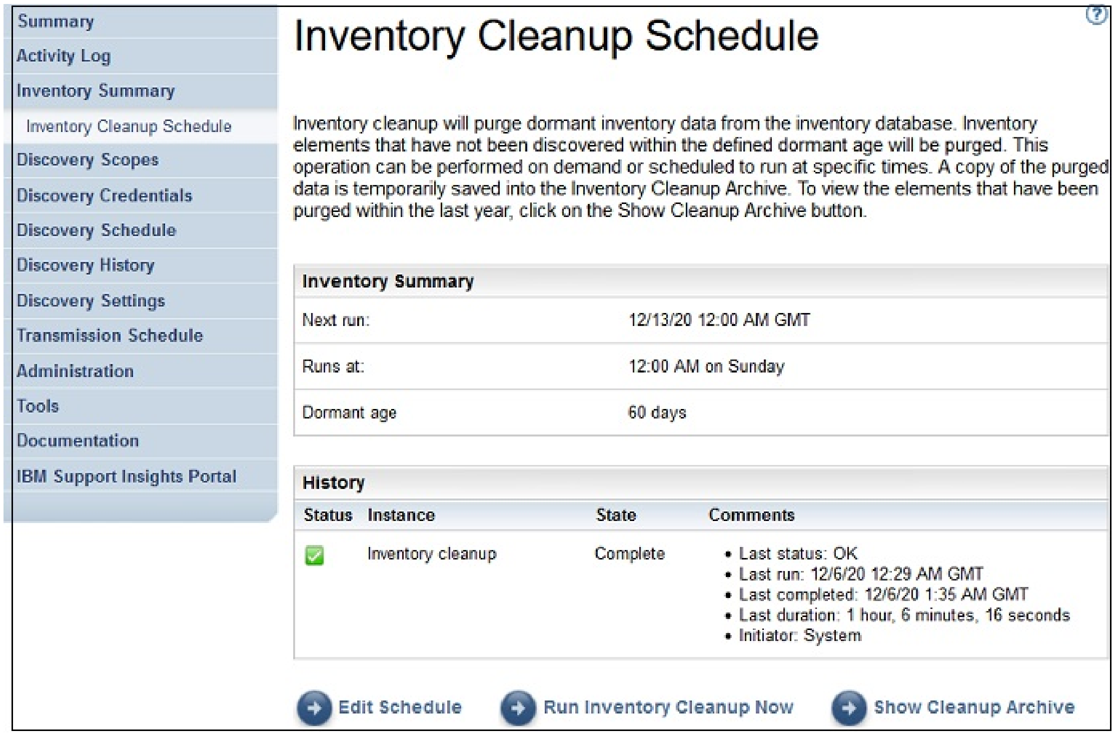
Scheduling inventory data cleanup

You can schedule or manually run a cleanup task for all the inventory data that is collected on the resources, from the time they are discovered.

About this task

Attention: It is recommended that you run the cleanup task once a week for most installations.

To view the current schedule for the inventory cleanup task, select **Inventory Summary** > **Inventory Cleanup Schedule**.



Inventory Cleanup Schedule

Inventory cleanup will purge dormant inventory data from the inventory database. Inventory elements that have not been discovered within the defined dormant age will be purged. This operation can be performed on demand or scheduled to run at specific times. A copy of the purged data is temporarily saved into the Inventory Cleanup Archive. To view the elements that have been purged within the last year, click on the Show Cleanup Archive button.

Inventory Summary	
Next run:	12/13/20 12:00 AM GMT
Runs at:	12:00 AM on Sunday
Dormant age	60 days

History

Status	Instance	State	Comments
✓	Inventory cleanup	Complete	• Last status: OK • Last run: 12/6/20 12:29 AM GMT • Last completed: 12/6/20 1:35 AM GMT • Last duration: 1 hour, 6 minutes, 16 seconds • Initiator: System

Figure 42. Inventory Cleanup Schedule

To run the inventory cleanup manually, click **Run Inventory Cleanup Now**.

To edit, enable, or disable the current inventory cleanup schedule, follow these steps:

Procedure

1. On the **Inventory Cleanup Schedule** page, click **Edit Schedule**.
2. On the **Inventory Settings** page, select **Enable scheduled inventory cleanup** to enable the inventory cleanup task or **Disable scheduled inventory cleanup** to disable the inventory cleanup task.
3. If you choose to enable the inventory cleanup task, complete the following steps:
    a) Select the **At hour** and **At minute** drop-down lists to select a new time.

b) Select the **Day Selection mode**. To schedule the inventory cleanup on a particular day(s) of a week, select the **Weekly by day(s) (Sun - Sat)** option or to schedule the inventory cleanup on particular days of a month, select **Monthly by date(s) (1-31)** option.

c) For the **On days** field, select the appropriate check box to select different or additional days of the week or month.

   Note: If you select the days beyond the last day of a specific month, then the job is triggered on the last day of that particular month.

4. Select the period for which you want to keep the inventory data from the **Dormant age** list.
5. Click **Save**.

Chapter 5. Setting up discovery and transmission to IBM

After TSA setup is complete, you can use various administration features to manage discovery, transmission, and jobs.

Discovery scopes

A discovery scope specifies the IP address or host name, range of IP addresses, or network to be used to discover IT elements. Discovery scopes are grouped into discovery scope sets.

TSA provides several types of discovery scopes:

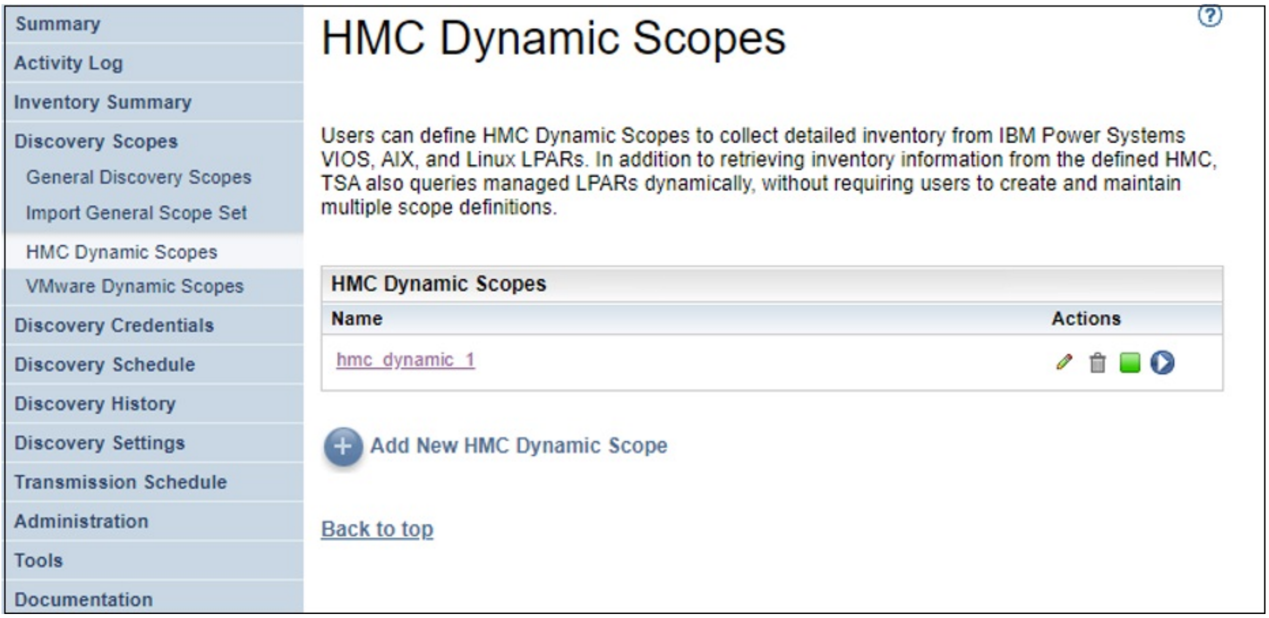
- HMC Dynamic Scope Sets - can be used to discover HMCs along with all partitions it manages.
- VMware Dynamic Scope Sets - can be used to discover VMware vCenter or ESXi hosts along with all virtual machines on the ESXi hosts.
- General Discovery Scopes - used to discover all other resources that are not discovered using a dynamic scope set. The IP addresses, range of IP addresses, or networks can be manually entered, or a list of IP addresses and host names can be imported from a file into TSA.

HMC Dynamic Scopes

You can define HMC dynamic scopes to collect detailed inventory from HMCs, the IBM Power Systems they manage, and also the VIOS, AIX, and Linux LPARs on those systems.

About this task

In addition to retrieving inventory information from the defined HMCs, TSA also queries the LPARs that are managed by these HMC dynamically, without requiring the creation and maintenance of multiple scope definitions. You must define a scope for the HMCs and select which types of LPARs (AIX, VIOS, and Linux) you would like to scan automatically when these HMCs are discovered. The advantage is that even if the LPARs change, you need not reconfigure TSA.



HMC Dynamic Scopes

Users can define HMC Dynamic Scopes to collect detailed inventory from IBM Power Systems VIOS, AIX, and Linux LPARs. In addition to retrieving inventory information from the defined HMC, TSA also queries managed LPARs dynamically, without requiring users to create and maintain multiple scope definitions.

HMC Dynamic Scopes

Name	Actions
hmc_dynamic_1	✎ 🗑 🟩 ➔

Figure 43. HMC Dynamic Scopes

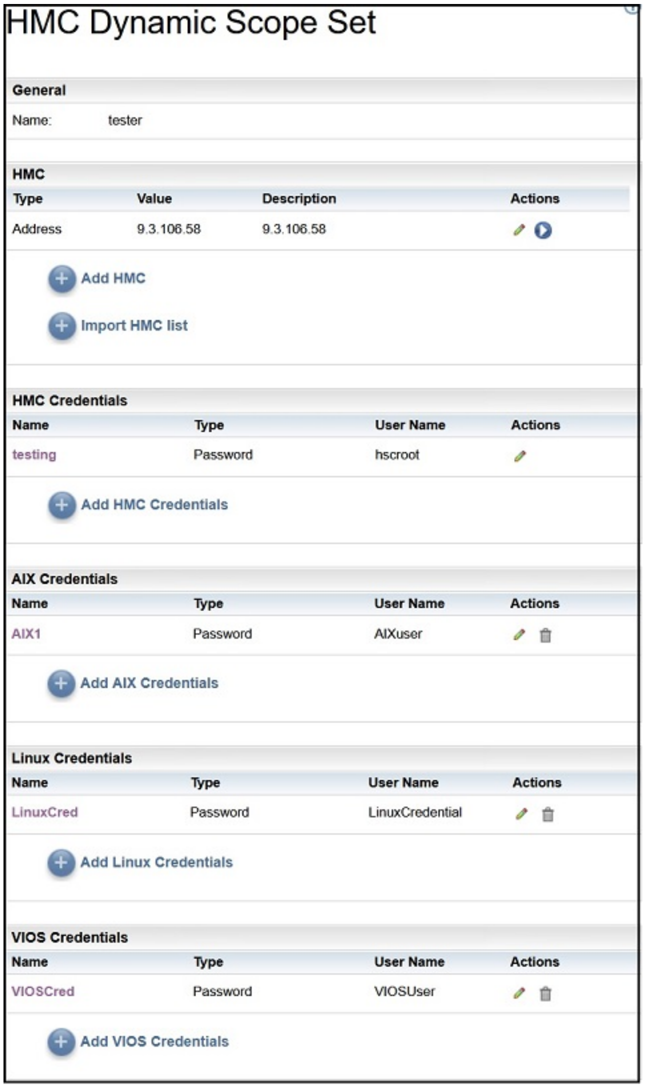
Displaying HMC Dynamic Scopes

You can display the existing HMC dynamic scopes.

About this task

To display the existing HMC dynamic scopes, click **Discovery scopes** > **HMC Dynamic Scopes** in the navigation pane. The **HMC Dynamic Scopes** page is displayed. The **HMC Dynamic Scopes** pane contains a list of the HMC dynamic scopes.

To display the scopes and credentials that are associated with a specific dynamic scope set, click the scope set name in the **Name** column. The **HMC Dynamic Scope Set** page is displayed.



HMC Dynamic Scope Set

General

Name: tester

HMC

Type	Value	Description	Actions
Address	9.3.106.58	9.3.106.58	✎ ▶

HMC Credentials

Name	Type	User Name	Actions
testing	Password	hscroot	✎

AIX Credentials

Name	Type	User Name	Actions
AIX1	Password	AIXuser	✎ 🗑

Linux Credentials

Name	Type	User Name	Actions
LinuxCred	Password	LinuxCredential	✎ 🗑

VIOS Credentials

Name	Type	User Name	Actions
VIOSCred	Password	VIOSUser	✎ 🗑

Figure 44. View HMC Dynamic Scope Set

The **HMC** pane displays the list of IP addresses of the HMCs that the dynamic scope set discovers. If the HMC was defined using a host name, that value is shown in the **Description** column of the HMC list. The various credentials panes, such as **AIX Credentials**, list the credentials that are configured in the scope set.

Adding HMC Dynamic Scopes

To add an HMC dynamic scope set, specify the IP address or host name of a single HMC along with a single credential for accessing the HMC. Optionally, you can specify the credentials for AIX, Linux, and VIOS to allow discovery of the LPARs of the IBM Power Systems the HMC manages. After the HMC dynamic scope set is created, it can be edited to define additional HMC IP addresses or host names. HMC dynamic scope sets can also be edited to support multiple credentials for accessing the HMCs as well as multiple credentials to access the LPARs.

About this task

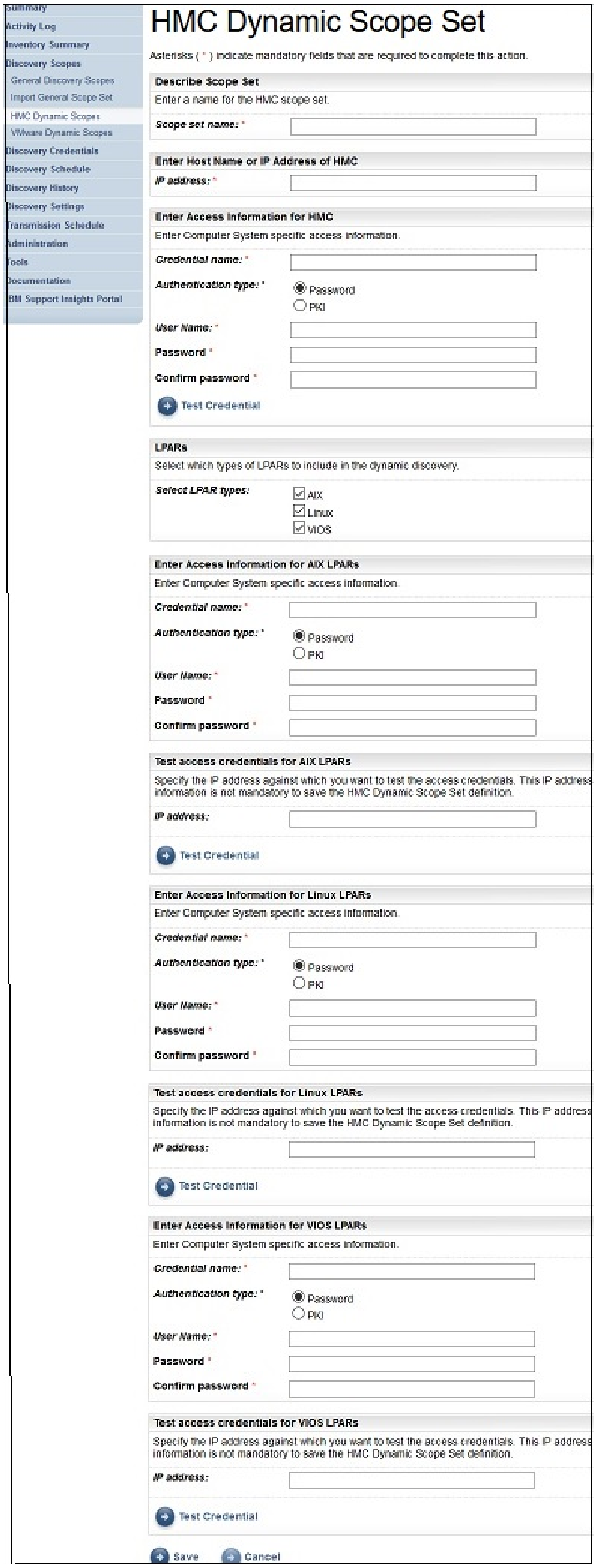
To add a scope set, follow these steps:

Procedure

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**.

   The **HMC Dynamic Scopes** page is displayed.
2. To define a new HMC dynamic scope set, click **Add New HMC Dynamic Scope**.

   The **HMC Dynamic Scope Set** page is displayed.



HMC Dynamic Scope Set

Asterisks (*) indicate mandatory fields that are required to complete this action.

Describe Scope Set

Enter a name for the HMC scope set.

Scope set name: *

Enter Host Name or IP Address of HMC

IP address: *

Enter Access Information for HMC

Enter Computer System specific access information.

Credential name: *

Authentication type: * ● Password ○ PKI

User Name: *

Password *

Confirm password *

Test Credential

LPARs

Select which types of LPARs to include in the dynamic discovery.

Select LPAR types: ☑ AIX ☑ Linux ☑ VIOS

Enter Access Information for AIX LPARs

Enter Computer System specific access information.

Credential name: *

Authentication type: * ● Password ○ PKI

User Name: *

Password *

Confirm password *

Test access credentials for AIX LPARs

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the HMC Dynamic Scope Set definition.

IP address:

Test Credential

Enter Access Information for Linux LPARs

Enter Computer System specific access information.

Credential name: *

Authentication type: * ● Password ○ PKI

User Name: *

Password *

Confirm password *

Test access credentials for Linux LPARs

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the HMC Dynamic Scope Set definition.

IP address:

Test Credential

Enter Access Information for VIOS LPARs

Enter Computer System specific access information.

Credential name: *

Authentication type: * ● Password ○ PKI

User Name: *

Password *

Confirm password *

Test access credentials for VIOS LPARs

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the HMC Dynamic Scope Set definition.

IP address:

Test Credential

Save Cancel

Figure 45. Add HMC Dynamic Scope Set

3. In the **Describe Scope Set** pane, enter a unique name in the **Scope set name** field.
4. In the **Enter Host Name or IP address of HMC** pane, enter the IP address or host name of the HMC.
5. In the **Enter Access Information for HMC** pane, enter the following details -

a) Enter the **Credential name**

b) Select the **Authentication type**

- **Password** - Uses the provided password.
- **PKI** - Uses SSH key that is associated with the specific scope set.

c) Enter the **User name** that is used to authenticate with the HMC.

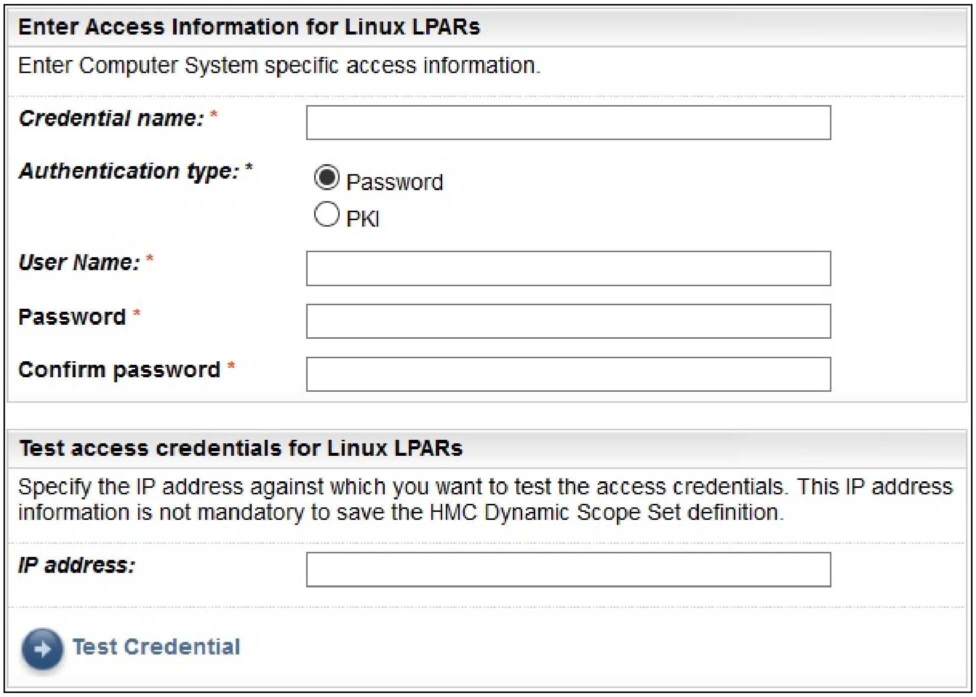
d) When **Authentication type** is **Password**, enter the **Password** and **Confirm Password**.

e) When **Authentication type** is **PKI**, enter the **Passphrase** and **Confirm Passphrase** if the SSH key is encrypted. If the SSH key is not encrypted, leave these two fields blank.

f) If **Authentication type** is **PKI**, click **Choose File** and upload the private key to TSA. You must externally deploy the public key on the HMC.

g) Optional: Click **Test Credential** to test the credentials of the target HMC.

6. In the **LPARs** pane, select which LPAR types (AIX, Linux, VIOS) to include in the dynamic discovery.
7. If you select any of the LPAR types (AIX, Linux, VIOS), enter the respective access information.



Enter Access Information for Linux LPARs

Enter Computer System specific access information.

Credential name: *

Authentication type: *

● Password
○ PKI

User Name: *

Password *

Confirm password *

Test access credentials for Linux LPARs

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the HMC Dynamic Scope Set definition.

IP address:

Figure 46. Example: Enter Access Information for Linux LPARs

a) Enter the **Credential name**.

b) Select the **Authentication type**

- **Password** - Uses the provided password.
- **PKI** - Uses SSH key that is associated with the specific scope set.

c) Enter the **User name** that is used to authenticate to the respective LPAR.

d) When **Authentication type** is **Password**, enter the **Password** and **Confirm Password**.

e) When **Authentication type** is **PKI**, enter the **Passphrase** and **Confirm Passphrase** if the SSH key is encrypted. If the SSH key is not encrypted, leave these two fields blank.

f) If **Authentication type** is **PKI**, click **Choose File** and upload the private key to TSA. You must externally deploy the public key on each LPAR.

g) Optional: Enter the **IP address** of an LPAR managed by this HMC and click **Test Credential** to test the credentials.

8. Click **Save** to save the HMC dynamic scope set.

Modifying HMC Dynamic Scopes - HMC IP Addresses

You can modify the list of HMC IP address associated with an existing HMC dynamic scope set.

About this task

To modify the list of HMC IP addresses, follow these steps.

Procedure

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**.
   The **HMC Dynamic Scopes** page is displayed.
2. To edit the scope set, click the **Edit** (✏) icon.
   The **HMC Dynamic Scope Set** page is displayed.
   - To add an HMC IP address or host name to the scope set, follow these steps:
     a. In the **HMC** pane, click **Add HMC**. The **HMC Dynamic Scopes** page is displayed.
     b. Enter the IP address or host name of the HMC in the **IP address** field.
     c. Click **Save** to add the HMC.
   - To edit an existing HMC IP address in the scope set, follow these steps:
     a. In the **HMC** pane, click the **Edit** (✏) icon. The **HMC Dynamic Scopes** page is displayed.
     b. Modify the **IP address** field with the IP address or host name of the HMC in the **Describe Address or Host** pane.
     c. Click **Save** to modify the HMC.
   - To delete an existing HMC IP address in the scope set, follow these steps:
     a. In the **HMC** pane, click the **Delete** (🗑) icon.
     b. In the dialog box, click **OK** to confirm the deletion.

       Note: An HMC dynamic scope set must always have at least one HMC IP address defined. TSA does not allow all HMC IP addresses to be deleted.

Importing HMC Dynamic Scope Set

You can import a list of IP addresses and hostnames to an existing HMC dynamic scope set.

About this task

A list of IP addresses or host names from an input file can be imported to an existing HMC dynamic scope set. TSA does the following validations when you import a scope set:

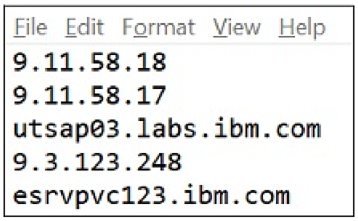
- Validates each line of the file to check whether it is a valid IP address or host name.
- Ignores trailing and leading blank spaces when validating the IP address or host name.
- Ignores duplicate IP addresses or host names.
- Ignores any entries that have the same IP address or host name as an existing HMC IP address.

Procedure

To import the IP addresses, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**.
   The **HMC Dynamic Scopes** page is displayed.
2. Click on an existing scope in the list. The **HMC Dynamic Scope Set** page is displayed.
3. In the HMC pane, click **Import HMC List**. The **Import HMC Dynamic Scope Set** page is displayed.

4. Click **Choose File** to select the text file.



```
9.11.58.18
9.11.58.17
utsap03.labs.ibm.com
9.3.123.248
esrvpvc123.ibm.com
```

Figure 47. Import HMC Dynamic Scope Set

Note: The text file must be formatted as a single column where each row contains a single IP address or host name and no other data.

5. Click **Import file** to import the IP addresses and host names.
6. Click **OK** in the dialog box asking if you want to import the selected list. A status message is displayed when the import completes successfully - **`Successfully imported Scope "[n]" IP addresses / hostnames Set`**.

   Note: If the scope set file causes the HMC dynamic scope set to have more than 400 IP addresses, a warning message is displayed - **`This Scope Set resolves to over 400 IP addresses. To avoid potential performance issues keep the cumulative number of IP addresses in a Scope Set below this threshold.`**
7. After you import the IP addresses and host names, you can edit the HMC dynamic scope set in the **HMC Discovery Scopes** page of the user interface.

Modifying HMC Dynamic Scopes - Credentials

You can modify the list of credentials that are associated with an existing HMC dynamic scope set.

About this task

An HMC dynamic scope set must always have at least one HMC credential defined. TSA does not allow all HMC credentials to be deleted. If no credentials exist for AIX, Linux, or VIOS, then TSA does not collect detailed information for that LPAR type.

Procedure

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**.

   The **HMC Dynamic Scopes** page is displayed.
2. To edit the scope set, click the **Edit** (✎) icon.

   The **HMC Dynamic Scope Set** page is displayed.

   - To add a credential for HMC, AIX, Linux, or VIOS, follow these steps:
     a. In the appropriate **Credentials** pane, click **Add Credentials**. For example, to add an HMC credential, click **Add HMC Credentials** in the **HMC Credentials** pane. The **New HMC Discovery Credentials** page is displayed.
     b. Enter the **Credential name**
     c. Select the **Authentication type**
        – **Password** - Uses the provided password.
        – **PKI** - Uses SSH key that is associated with the specific scope set.
     d. Enter the **User name** that is used to authenticate to the HMC or respective LPAR.
     e. When **Authentication type** is **Password**, enter the **Password** and **Confirm Password**.
     f. When **Authentication type** is **PKI**, enter the **Passphrase** and **Confirm Passphrase** if the SSH key is encrypted. If the SSH key is not encrypted, leave these two fields blank.

    g. If **Authentication type** is **PKI**, click **Choose File** and upload the private key to TSA. You must externally deploy the public key on the HMCs or LPARs.
    h. **Optional:** Enter the IP address or host name of the HMC or LPAR in the **IP address** field and click **Test Credential** to test the credentials.
    i. Click **Save** to save the HMC dynamic scope set credential.

- To edit a credential for HMC, AIX, Linux, or VIOS, follow these steps:

    a. In the appropriate **Credentials** pane, click the **Edit** (✏) icon for the credential you wish to modify. For example, to edit an HMC credential, click the **Edit** (✏) icon in the **HMC Credentials** pane for the credential to be modified. The **Edit HMC Discovery Credentials** page is displayed.
    b. In the **Enter Access Information** pane, you can modify the following details -

        1) Enter the **User name** that is used to authenticate to the HMC or respective LPAR.
        2) Select the **Authentication type**

            – **Password** - Uses the provided password.
            – **PKI** - Uses SSH key that is associated with the specific scope set.

        3) When **Authentication type** is **Password**, enter the **Password** and **Confirm Password**.
        4) When **Authentication type** is **PKI**, enter the **Passphrase** and **Confirm Passphrase** if the SSH key is encrypted. If the SSH key is not encrypted, leave these two fields blank.
        5) If **Authentication type** is **PKI**, click **Choose File** and upload the private key to TSA. You must externally deploy the public key on each HMC or LPAR.

    c. **Optional:** Enter IP address or host name of the HMC or LPAR in the **IP address** field and click **Test Credential** to test the credentials.
    d. Click **Save** to update the credential.

- To delete a credential for HMC, AIX, Linux, or VIOS, follow these steps:

    a. In the appropriate **Credentials** pane, click the **Delete** (🗑) icon for the respective credential. For example, to delete an HMC credential, click the **Delete** (🗑) icon in the **HMC Credentials** pane for the credential to be deleted. A confirmation message is displayed.
    b. Click **OK** to delete the credential.

- To modify the order of a credential for HMC, AIX, Linux, or VIOS, follow these steps:

    a. If more than one credential exists for HMC, AIX, Linux, or VIOS, the order of the credentials for the HMCs or LPAR can be modified. When a single credential exists, the up and down arrows do not appear in the **Actions** column for the credentials pane.
    b. In the appropriate **Credentials** pane, click the **Up** (⬆) or **Down** (⬇) arrow icons to re-order the credential.

Enabling or Disabling Dynamic Scope Sets

You can enable or disable an HMC Dynamic Scope Set.

About this task

A disabled scope set is skipped during a scheduled discovery.

Note: A manual discovery can always be performed regardless of the state of the scope set.

Disabling Dynamic Scope Sets

Procedure

To disable an HMC dynamic scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**.

   The **HMC Dynamic Scopes** page is displayed.
2. Click the **Enable** (🟩) icon beside the scope set that you want to disable.

Enabling Dynamic Scope Sets

Procedure

To enable an HMC dynamic scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**.

   The **HMC Dynamic Scopes** page is displayed.
2. Click the **Disable** (⬛) icon beside the scope set that you want to enable.

Discovering an HMC

You can manually initiate a discovery of a single HMC within an HMC Dynamic Scope Set. The discovery collects information about the HMC along with its associated LPARs.

Procedure

To manually initiate a discovery an HMC, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**.

   The **HMC Dynamic Scopes** page is displayed.
2. Click the **Edit** (✏) icon for the required HMC Dynamic Scope Set. The **HMC Dynamic Scope Set** page is displayed.
3. Click the **Run** (▶) icon beside the HMC IP address that you want to discover.

Discovering Dynamic Scope Sets

You can manually initiate a discovery for an HMC Dynamic Scope Set. The discovery collects information about all of the HMCs defined to the scope set along with its associated LPARs.

Procedure

To manually initiate a discovery for an HMC Dynamic Scope Set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**.

   The **HMC Dynamic Scopes** page is displayed.
2. Click the **Run** (▶) icon beside the scope set that you want to discover.

Deleting HMC Dynamic Scopes

You can delete an existing HMC dynamic scope set.

Procedure

To delete an HMC dynamic scope set, follow these steps:

1. In the navigation pane, click **HMC Dynamic Scopes**.

   The **HMC Dynamic Scopes** page is displayed.
2. Click the **Delete** (🗑) icon beside the scope set that you want to delete.
3. Click **OK** to confirm that you want to delete the HMC dynamic scope set.

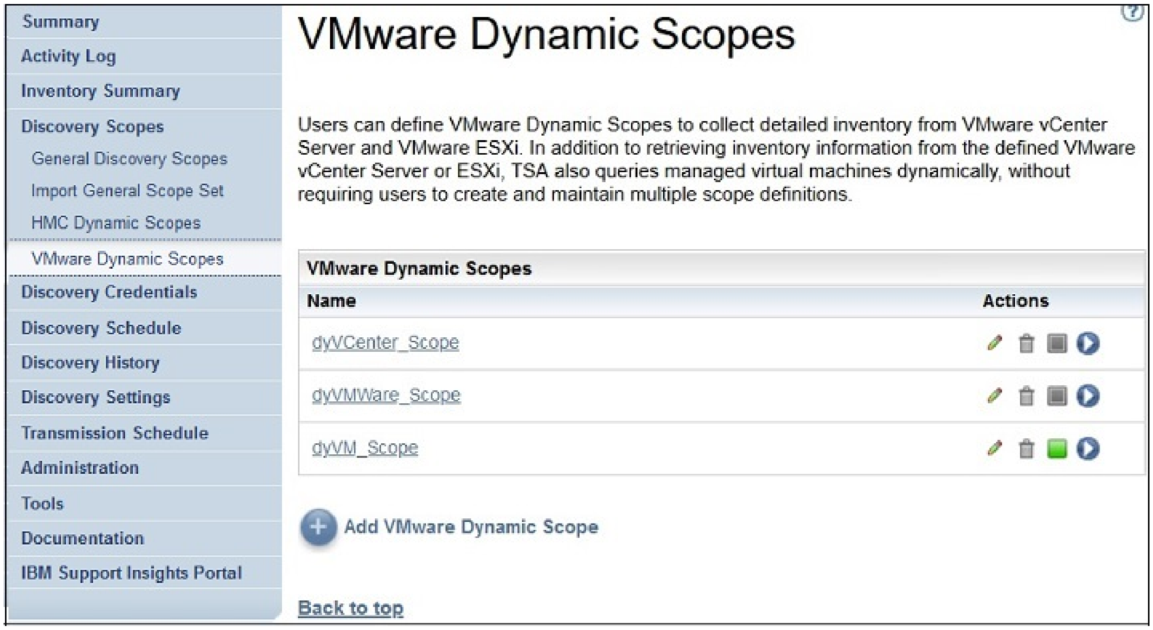
   Note: When you confirm deletion of the HMC dynamic scope set, the associated access information for AIX, Linux, or VIOS LPARs is also deleted.

VMware Dynamic Scopes

You can define VMware dynamic scopes to collect detailed inventory from VMware vCenter Servers and ESXi instances. VMware dynamic scopes also collect information about the x86 servers managed by the VMware vCenter Server or ESXi instance, and the Linux and Windows virtual machines on those systems.

TSA retrieves inventory information from the defined VMware vCenter Server and ESXi instances. TSA also queries virtual machines that are managed by the VMware instances dynamically, without the need of creating and maintaining multiple scope definitions. You must define a scope for the VMware instances and select which types of virtual machines (Linux and Windows) you would like to scan automatically when these VMware instances are discovered. The advantage is that even if the virtual machines change, you need not reconfigure TSA.

The VMware vCenter Server discovery finds all VMware ESXi instances that it manages, thus eliminating the need to discover the VMware ESXi instances directly. For any VMware ESXi instances that are not managed by a VMware vCenter Server, these can be directly discovered by TSA by defining the VMware ESXi in the VMware dynamic scope.



VMware Dynamic Scopes

Users can define VMware Dynamic Scopes to collect detailed inventory from VMware vCenter Server and VMware ESXi. In addition to retrieving inventory information from the defined VMware vCenter Server or ESXi, TSA also queries managed virtual machines dynamically, without requiring users to create and maintain multiple scope definitions.

VMware Dynamic Scopes

Name	Actions
dyVCenter_Scope	✎ 🗑 ■ ▶
dyVMWare_Scope	✎ 🗑 ■ ▶
dyVM_Scope	✎ 🗑 🟩 ▶

Figure 48. VMware Dynamic Scopes

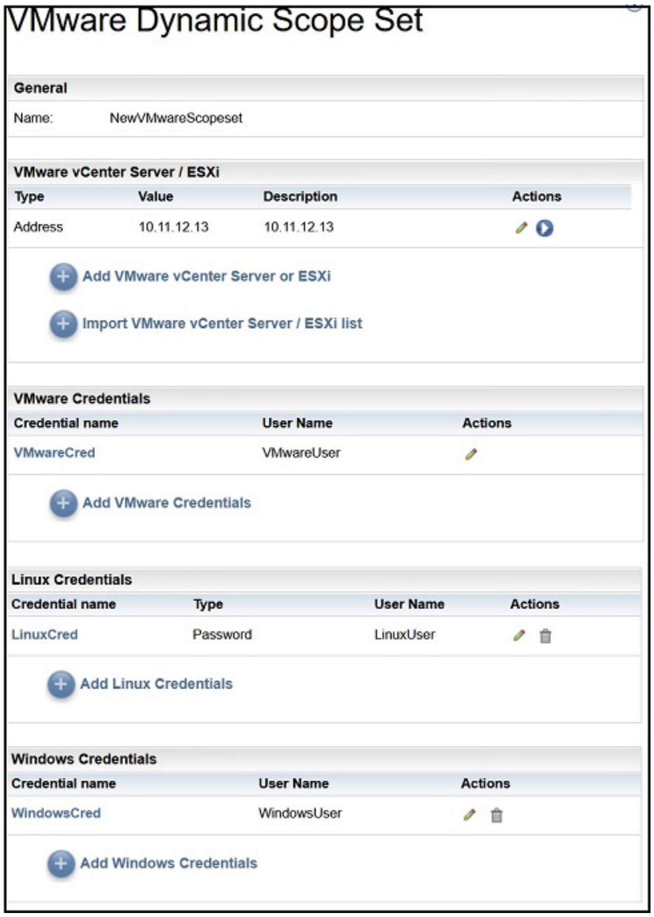
Displaying VMware Dynamic Scopes, Scope sets and Credentials

You can display the existing VMware dynamic scopes and scope sets.

About this task

To display the existing VMware dynamic scope sets, click **Discovery scopes** > **VMware Dynamic Scopes** in the navigation pane. The **VMware Dynamic Scopes** page is displayed. The **VMware Dynamic Scopes** pane contains a list of the VMware dynamic scopes.

To display the scopes and credentials that are associated with a specific dynamic scope set, click the scope set name in the **Name** column. The **VMware Dynamic Scope Set** page is displayed.



VMware Dynamic Scope Set

General

Name: NewVMwareScopeset

VMware vCenter Server / ESXi

Type	Value	Description	Actions
Address	10.11.12.13	10.11.12.13	✎ ➜

Add VMware vCenter Server or ESXi
Import VMware vCenter Server / ESXi list

VMware Credentials

Credential name	User Name	Actions
VMwareCred	VMwareUser	✎

Linux Credentials

Credential name	Type	User Name	Actions
LinuxCred	Password	LinuxUser	✎ 🗑

Windows Credentials

Credential name	User Name	Actions
WindowsCred	WindowsUser	✎ 🗑

Figure 49. View VMware Dynamic Scope Set

The **VMware vCenter Server / ESXi** pane displays the list of IP addresses of the VMware vCenter Server and ESXi instances that the dynamic scope set discovers. If the VMware vCenter Server or ESXi instance was defined using a host name, that value is shown in the **Description** column of the VMware vCenter Server / ESXi list. The various credentials panes, such as **Linux Credentials**, list the credentials that are configured in the scope set.

Adding VMware Dynamic Scopes

To add a VMware Dynamic Scope Set, specify the IP address or host name of a single VMware vCenter Server or ESXi instance along with a single credential for accessing the VMware instance. Optionally, you can specify the credentials for Linux and Windows to allow discovery of the virtual machines of the x86 servers the VMware instance manages. After the VMware Dynamic Scope Set is created, it can be edited to define additional VMware vCenter Server or ESXi IP addresses or host names. VMware Dynamic Scope Sets can also be edited to support multiple credentials for accessing the VMware instance and multiple credentials to access the virtual machines.

About this task

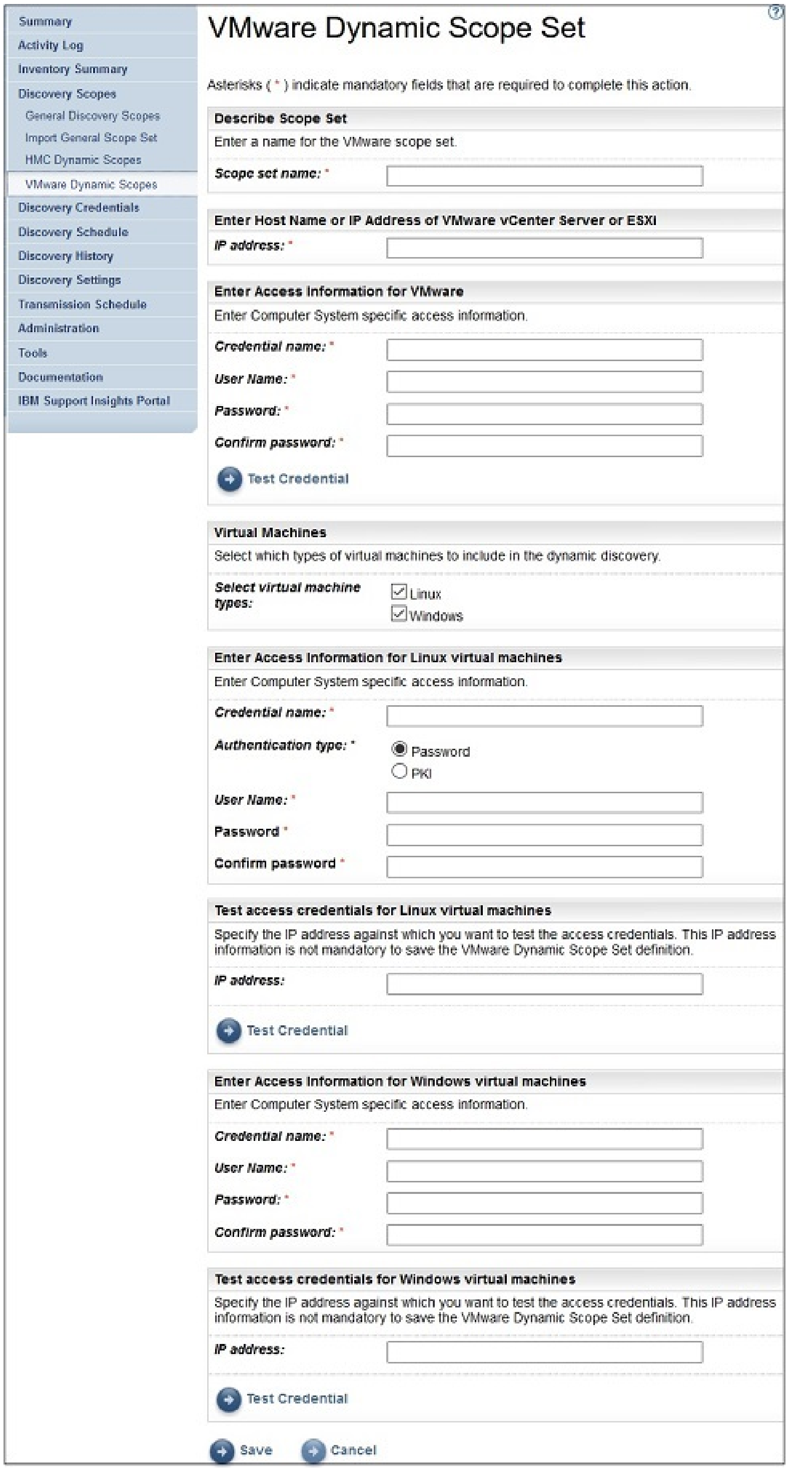
To add a VMware dynamic scope set, follow these steps:

Procedure

1. In the navigation pane, click **Discovery Scopes** > **VMware Dynamic Scopes**.

   The **VMware Dynamic Scopes** page is displayed.
2. To define a new VMware dynamic scope set, click **Add VMware Dynamic Scope**.

   The **VMware Dynamic Scope Set** page is displayed.



VMware Dynamic Scope Set

Asterisks (*) indicate mandatory fields that are required to complete this action.

Describe Scope Set

Enter a name for the VMware scope set.

Scope set name: *

Enter Host Name or IP Address of VMware vCenter Server or ESXi

IP address: *

Enter Access Information for VMware

Enter Computer System specific access information.

Credential name: *

User Name: *

Password: *

Confirm password: *

Virtual Machines

Select which types of virtual machines to include in the dynamic discovery.

Select virtual machine types: ☑ Linux ☑ Windows

Enter Access Information for Linux virtual machines

Enter Computer System specific access information.

Credential name: *

Authentication type: * ● Password ○ PKI

User Name: *

Password *

Confirm password *

Test access credentials for Linux virtual machines

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the VMware Dynamic Scope Set definition.

IP address:

Enter Access Information for Windows virtual machines

Enter Computer System specific access information.

Credential name: *

User Name: *

Password: *

Confirm password: *

Test access credentials for Windows virtual machines

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the VMware Dynamic Scope Set definition.

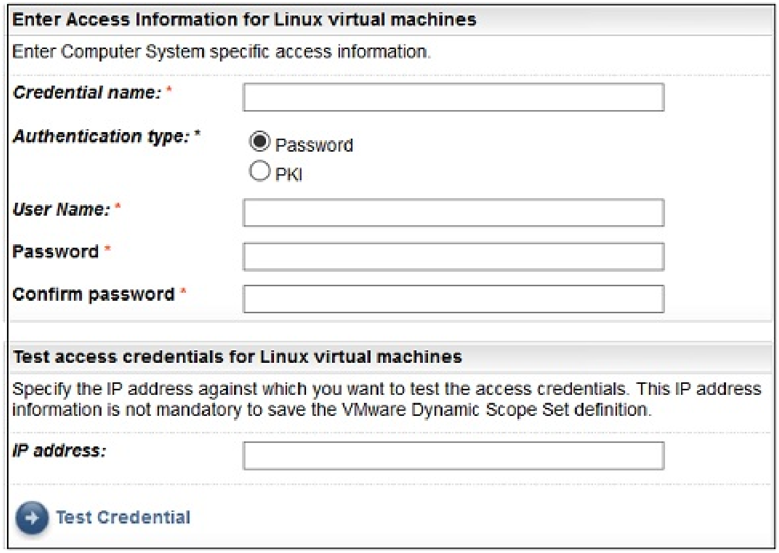
IP address:

Figure 50. Add VMware Dynamic Scope Set

3. In the **Describe Scope Set** pane, enter a unique name in the **Scope set name** field.
4. In the **Enter Host Name or IP address of VMware vCenter Server or ESXi** pane, enter the IP address or host name of the VMware vCenter Server or ESXi instance.
5. In the **Enter Access Information for VMware** pane, enter the following details -
   a) Enter the **Credential name**
   b) Enter the **User name** that is used to authenticate to the VMware vCenter Server or ESXi instance
   c) Enter the **Password** and **Confirm password**

d) Optional: Click **Test Credential** to test the credentials of the target VMware vCenter Server or ESXi instance.

6. In the **Virtual Machines** pane, select which virtual machines (Linux, Windows) to include in the dynamic discovery.
7. If you select Linux virtual machine, enter the respective access information.



Enter Access Information for Linux virtual machines

Enter Computer System specific access information.

Credential name: *

Authentication type: * ● Password ○ PKI

User Name: *

Password *

Confirm password *

Test access credentials for Linux virtual machines

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the VMware Dynamic Scope Set definition.

IP address:

Figure 51. Enter Access Information for Linux virtual machine

a) Enter the **Credential name**.

b) Select the **Authentication type**

- **Password** - Uses the provided password.
- **PKI** - Uses SSH key that is associated with the specific scope set.

c) Enter the **User name** that is used to authenticate to the respective virtual machine.

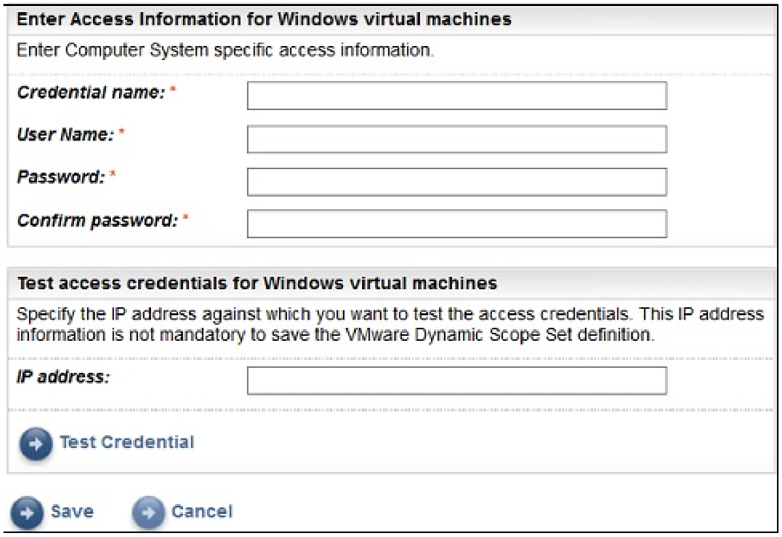
d) When **Authentication type** is **Password**, enter the **Password** and **Confirm Password**.

e) When **Authentication type** is **PKI**, enter the **Passphrase** and **Confirm Passphrase** if the SSH key is encrypted. If the SSH key is not encrypted, leave these two fields blank.

f) If **Authentication type** is **PKI**, click **Choose File** and upload the private key to TSA. You must externally deploy the public key on each virtual machine.

g) Optional: Enter the IP address or host name of the Linux virtual machine in the **IP address** field and click **Test Credential** to test the credentials.

8. If you select Windows virtual machine, enter the respective access information.



Enter Access Information for Windows virtual machines

Enter Computer System specific access information.

Credential name: *

User Name: *

Password: *

Confirm password: *

Test access credentials for Windows virtual machines

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the VMware Dynamic Scope Set definition.

IP address:

Figure 52. Enter Access Information for Windows virtual machine

a) Enter the **Credential name**.

b) Enter the **User name** that is used to authenticate to the respective virtual machine.

c) Enter the **Password** and **Confirm password**.

d) Optional: Enter the IP address or host name of the Windows virtual machine in the **IP address** field and click **Test Credential** to test the credentials.

9. Click **Save** to save the VMware dynamic scope set.

Modifying VMware Dynamic Scopes - VMware vCenter Server or ESXi IP Addresses

You can modify the list of VMware vCenter Server or ESXi IP addresses or host names associated with an existing VMware dynamic scope set.

About this task

To modify the list of VMware vCenter Server or ESXi IP addresses or host names, follow these steps.

Procedure

1. In the navigation pane, click **Discovery Scopes** > **VMware Dynamic Scopes**.
   The **VMware Dynamic Scopes** page is displayed.
2. To edit the scope set, click the icon.
   The **VMware Dynamic Scope Set** page is displayed.
   - To add a VMware vCenter Server or ESXi IP address or host name to the scope set, follow these steps:
     a. In the **VMware vCenter Server / ESXi** pane, click **Add VMware vCenter Server or ESXi**. The **VMware Dynamic Scopes** page is displayed.
     b. In the **Describe Address or Host** pane, enter the IP address or host name of the VMware vCenter Server or ESXi in the **IP address** field.
     c. Click **Save** to add the VMware vCenter Server or ESXi instance.
   - To edit an existing VMware vCenter Server or ESXi IP address in the scope set, follow these steps:
     a. In the **VMware vCenter Server/ESXi** pane, click the **Edit** (✎) icon. The **VMware Dynamic Scopes** page is displayed.

    b. In the **Describe Address or Host** pane, modify the IP address or host name of the VMware vCenter Server or ESXi instance in the **IP address** field.
    c. Click **Save**.

- To delete an existing VMware vCenter Server or ESXi IP address in the scope set, follow these steps:

    a. In the **VMware vCenter Server/ESXi** pane, click the **Delete** (🗑) icon.
    b. In the dialog box, click **OK** to confirm the deletion.

    Note: A VMware dynamic scope set must always have at least one VMware vCenter Server or ESXi IP address defined. TSA does not allow all VMware IP addresses to be deleted.

Importing VMware Dynamic Scope Set

You can import a list of IP addresses and hostnames to an existing VMware Dynamic Scope Set.

About this task

A list of IP addresses or host names from an input file can be imported to an existing VMware dynamic scope set. TSA does the following validations when you import a scope set:

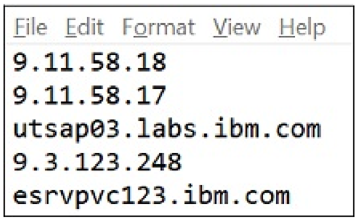
- Validates each line of the file to check whether it is a valid IP address or host name.
- Ignores trailing and leading blank spaces when validating the IP address or host name.
- Ignores duplicate IP addresses or host names.
- Ignores any entries that have the same IP address or host name as an existing an existing VMware vCenter Server or ESXi address.

Procedure

To import the IP addresses, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **VMware Dynamic Scopes**.

   The **VMware Dynamic Scopes** page is displayed.
2. Click on an existing scope in the list. The **VMware Dynamic Scope Set** page is displayed.
3. In the **VMware vCenter Server / ESXi** pane, click **Import VMware vCenter Server / ESXi List**. The **Import VMware Dynamic Scope Set** page is displayed.
4. Click **Choose File** to select the text file.

   ```
   9.11.58.18
   9.11.58.17
   utsap03.labs.ibm.com
   9.3.123.248
   esrvpvc123.ibm.com
   ```

   Figure 53. Import VMware Dynamic Scope Set

   Note: The text file must be formatted as a single column where each row contains a single IP address or host name and no other data.
5. Click **Import file** to import the IP addresses and host names.
6. Click **OK** in the dialog box asking if you want to import the selected list. A status message is displayed when the import completes successfully - **`Successfully imported Scope "[n]" IP addresses / hostnames Set`**.

   Note: If the scope set file causes the VMware dynamic scope set to have more than 400 IP addresses, a warning message is displayed - **`This Scope Set resolves to over 400 IP addresses.`**

```
To avoid potential performance issues keep the cumulative number of IP
addresses in a Scope Set below this threshold.
```

7. After you import the IP addresses and host names, you can edit the VMware dynamic scope set in the **VMware Discovery Scopes** page of the user interface.

Modifying VMware Dynamic Scopes - Credentials

You can modify the list of credentials that are associated with an existing VMware dynamic scope set.

About this task

A VMware dynamic scope set must always have at least one VMware credential defined. TSA does not allow all VMware credentials to be deleted. If no credentials exist for Linux or Windows, then TSA does not collect detailed information regarding that virtual machine type.

Procedure

1. In the navigation pane, click **Discovery Scopes** > **VMware Dynamic Scopes**.

   The **VMware Dynamic Scopes** page is displayed.

2. To edit the scope set, click the **Edit** ✏ icon.

   The **VMware Dynamic Scope Set** page is displayed.

   - To add a credential for VMware or Windows, follow these steps:

     a. In the appropriate **Credentials** pane, click **Add Credentials**. For example, to add a VMware credential, click **Add VMWare Credentials** in the **VMWare Credentials** pane. The **New VMware Discovery Credentials** page is displayed.

     b. Enter the **Credential name**

     c. Enter the **User name** that is used to authenticate to the VMware vCenter Server or ESXi instances or Windows virtual machines.

     d. Enter the **Password** and **Confirm password**.

     e. **Optional:** Enter the IP address or host name of the VMware vCenter Server or ESXi instance, or Windows virtual machine, in the **IP address** field, and click **Test Credential** to test the credentials.

     f. Click **Save** to save the credential.

   - To add a credential for Linux, follow these steps:

     a. In the **Linux Credentials** pane, click **Add Linux Credentials**. The **New VMware Discovery Credentials** page is displayed.

     b. Enter the **Credential name**

     c. Select the **Authentication type**

        – **Password** - Uses the provided password.

        – **PKI** - Uses SSH key that is associated with the specific scope set.

     d. Enter the **User name** that is used to authenticate to the Linux virtual machines.

     e. When **Authentication type** is **Password**, enter the **Password** and **Confirm Password**.

     f. When **Authentication type** is **PKI**, enter the **Passphrase** and **Confirm Passphrase** if the SSH key is encrypted. If the SSH key is not encrypted, leave these two fields blank.

     g. If **Authentication type** is **PKI**, click **Choose File** and upload the private key to TSA. You must externally deploy the public key on the Linux virtual machines.

     h. **Optional:** Enter the IP address or host name of the Linux virtual machine, in the **IP address** field, and click **Test Credential** to test the credentials.

     i. Click **Save** to save the Linux credential.

   - To edit a credential for VMware or Windows, follow these steps:

   a. In the appropriate **Credentials** pane, click the **Edit** (✏) icon for the credential you wish to modify. For example, to edit a VMware credential, click the **Edit** (✏) icon in the **VMware Credentials** pane for the credential to be modified. The **Edit VMware Discovery Credentials** page is displayed.
   b. In the **Enter Access Information** pane, you can modify the following details -
      1) Enter the **User name** that is used to authenticate when connecting to the VMware vCenter Server or ESXi instances, or Windows virtual machines.
      2) Enter the **Password** and **Confirm password**.
   c. **Optional:** Enter the IP address or host name of the VMware vCenter Server or ESXi instance, or Windows virtual machine, in the **IP address** field, and click **Test Credential** to test the credentials.
   d. Click **Save** to update the credential.

- To edit a credential for Linux, follow these steps:
   a. In the **Linux Credentials** pane, click the **Edit** (✏) icon for the credential you wish to modify. The **Edit VMware Discovery Credentials** page is displayed.
   b. In the **Enter Access Information** pane, you can modify the following details -
      1) Select the **Authentication type**
         – **Password** - Uses the provided password.
         – **PKI** - Uses SSH key that is associated with the specific scope set.
      2) Enter the **User name** that is used to authenticate to the Linux virtual machine.
      3) When **Authentication type** is **Password**, enter the **Password** and **Confirm Password**.
      4) When **Authentication type** is **PKI**, enter the **Passphrase** and **Confirm Passphrase** if the SSH key is encrypted. If the SSH key is not encrypted, leave these two fields blank.
      5) If **Authentication type** is **PKI**, click **Choose File** and upload the private key to TSA. You must externally deploy the public key on the Linux virtual machines.
      6) **Optional:** Enter the IP address or host name of a Linux virtual machine in the **IP address** field and click **Test Credential** to test the credentials.
   c. Click **Save** to update the credential.

- To delete a credential for VMware, Linux, or Windows, follow these steps:
   a. In the appropriate **Credentials** pane, click the **Delete** (🗑) icon for the respective credential. For example, to delete a VMware credential, click the **Delete** (🗑) icon in the **VMware Credentials** pane for the credential to be deleted. A confirmation message is displayed.
   b. Click **OK** to delete the credential.

- To modify the order of a credential for VMware, Linux, or Windows, follow these steps:
   a. If more than one credential exists for VMware, Linux, or Windows, the order of the credentials for the VMwares or virtual machines can be modified. When a single credential exists, the up and down arrows do not appear in the **Actions** column for the credentials pane.
   b. In the appropriate **Credentials** pane, click the **Up** (⬆) or **Down** (⬇) arrow icons to re-order the credential.

Enabling or Disabling Dynamic Scope Sets

You can enable or disable a VMware Dynamic Scope Set.

About this task

A disabled scope set is skipped during a scheduled discovery.

Note: A manual discovery can always be performed regardless of the state of the scope set.

Disabling Dynamic Scope Sets

Procedure

To disable a VMware dynamic scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **VMware Dynamic Scopes**.

   The **VMware Dynamic Scopes** page is displayed.
2. Click the **Enable** (🟩) icon beside the scope set that you want to disable.

Enabling Dynamic Scope Sets

Procedure

To enable an VMware dynamic scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **VMware Dynamic Scopes**.

   The **VMware Dynamic Scopes** page is displayed.
2. Click the **Disable** (▨) icon beside the scope set that you want to enable.

Discovering a VMware vCenter or ESXi

You can manually initiate a discovery of a single VMware vCenter Server or ESXi within a VMware dynamic scope set. The discovery collects information about the VMware instance along with its associated virtual machines.

Procedure

To manually initiate a discovery of a VMware vCenter Server or ESXi, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **VMware Dynamic Scopes**.

   The **VMware Dynamic Scopes** page is displayed.
2. Click the **Edit** (✎) icon for the required VMware Dynamic Scope Set. The **VMware Dynamic Scope Set** page is displayed.
3. Click the **Run** (▶) icon beside the VMware vCenter Server or ESXi IP address that you want to discover.

Discovering Dynamic Scope Sets

You can manually initiate a discovery for a VMware Dynamic Scope Set. The discovery collects information about all of the VMware vCenter Server or ESXi instances defined to the scope set along with its associated virtual machines.

Procedure

To manually initiate a discovery for a VMware Dynamic Scope Set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **VMware Dynamic Scopes**.

   The **VMware Dynamic Scopes** page is displayed.
2. Click the **Run** (▶) icon beside the scope set that you want to discover.

Deleting VMware Dynamic Scopes

You can delete an existing VMware dynamic scope set.

Procedure

To delete a VMware dynamic scope set, follow these steps:

1. In the navigation pane, click **VMware Dynamic Scopes**.

   The **VMware Dynamic Scopes** page is displayed.
2. Click the **Delete** (🗑) icon beside the scope set that you want to delete.
3. Click **OK** to confirm that you want to delete the VMware dynamic scope set.

   Note: When you confirm deletion of the VMware dynamic scope set, the associated access information for Linux or Windows virtual machines is also deleted.

General Discovery Scopes

The discovery process searches for IT elements within your infrastructure. A Discovery Scope defines a single IP address, range, or subnet that is discovered during the discovery process. Discovery scopes are grouped into user named Scope Sets.

Displaying discovery scopes and scope sets

You can display the existing discovery scopes and scope sets.

About this task

To display the existing discovery scope sets, click **Discovery Scopes** > **General Discovery Scopes** in the navigation pane. The **General Discovery Scopes** page is displayed. The **General Discovery Scopess** pane contains a list of scope sets.

To display the scopes that a scope set contains, click the scope set. The **Discovery Scope Set** page is displayed.

- The **General** pane displays the name of the scope set.
- The **IP Address Count** pane displays the total number of IP addresses in the scope set.
- The **Scopes** pane displays details about the scopes in the scope set.

Adding discovery Scopes

You can add a scope set and a new scope to that set, add a scope to an existing scope set or move scopes to other scope sets. To add a scope, specify a valid IP address or host name, a range of IP addresses, a network, or subnet.

About this task

Tips: There are some practical considerations for setting up discovery scopes and scope sets.

- The more IP addresses that are in the discovery scope, the longer the discovery takes. You can modify the discovery size by disabling or enabling scope sets or by excluding IP addresses, IP address ranges, networks, or subnets from a scope within a scope set.

  To minimize the time that a discovery takes, set up discovery scopes to target only those elements that you want to discover and disable scope sets or exclude IP addresses, IP address ranges, networks, or subnets that you do not want or need to discover.

  Note: For better performance, limit the cumulative number of IP addresses in a scope set to 400 or less. For information on importing a scope set, see section "Importing a scope set" on page 72

- Not all elements are equal. For example, a router with dozens of interfaces might take longer to fully discover than a single host.
- If you are using PKI authentication for device discovery, only one SSH key can be associated with each scope set.

For more information on best practices to setup discovery scopes, refer to the TSA Configuration Assistant Guide.

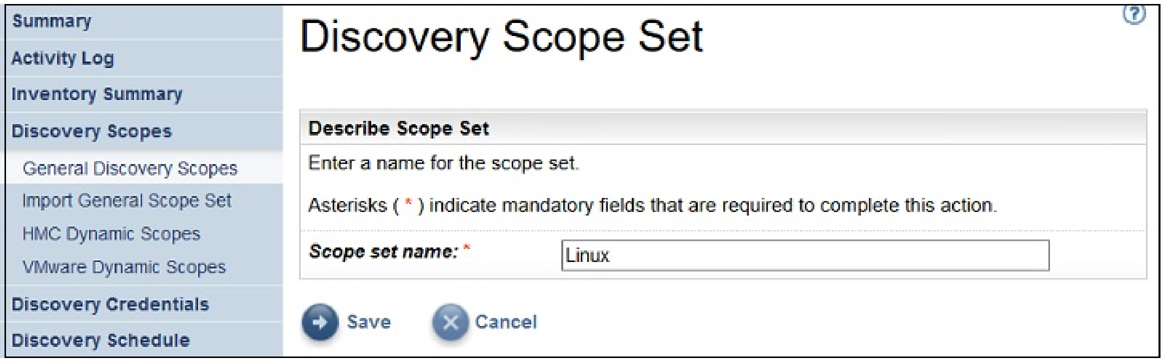
To add a scope set and scope, follow these steps:

Procedure

1. In the navigation pane, click **Discovery Scopes** > **General Discovery Scopes**.

   The **General Discovery Scopes** page is displayed.
2. To define a new discovery scope set, click **Add New Scope Set**.

   The **Discovery Scope Set** page is displayed.



Discovery Scope Set

Describe Scope Set

Enter a name for the scope set.

Asterisks (*) indicate mandatory fields that are required to complete this action.

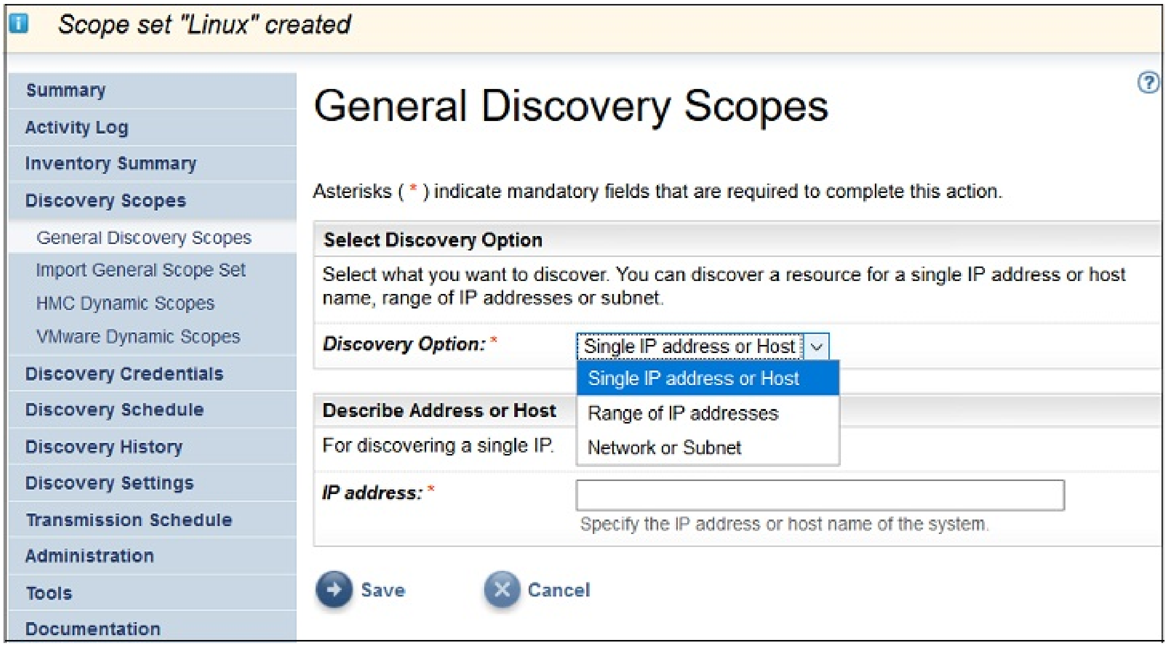
Scope set name: * Linux

Figure 54. Discovery Scope Set

   a) Enter a unique scope set name in the **Scope set** name field

   b) Click **Save**.

   The new scope set is created and the **General Discovery Scopes** page is displayed.



Scope set "Linux" created

General Discovery Scopes

Asterisks (*) indicate mandatory fields that are required to complete this action.

Select Discovery Option

Select what you want to discover. You can discover a resource for a single IP address or host name, range of IP addresses or subnet.

Discovery Option: * Single IP address or Host

Describe Address or Host

For discovering a single IP.

IP address: *

Specify the IP address or host name of the system.

Figure 55. General Discovery Scopes

3. Specify one of the following options in the **Select Discovery Option** pane:
   - `Single IP address or Host`

For **Describe Address or Host**, enter the IP address or host name.

- `Range of IP addresses`

  For **Describe Address Range**, enter the starting IP address, ending IP address, and optionally, a description in the fields provided.

- `Network or Subnet`

  For **Describe Network or Subnet**, enter the IP address, mask, and optionally, a description in the fields provided.

4. If you want to exclude IP addresses, range of IP addresses, or subnets from the discovery, click **Add Exclusion** and follow these steps:

   a) Select **Host**, **Range**, or **Subnet**.

   b) Specify the IP address, range of IP addresses, or subnet that you want to exclude from the discovery.

   c) Optional: Specify a description for the IP address, range of IP addresses or subnet that you are excluding from the discovery.

   Note: Exclusions are only applicable for a scope defined with a range of IP addresses or a subnet.

   Note: You cannot reuse an IP address, range of IP addresses, subnets, or description in any scopes or exclusions in a scope set.

   d) To add more exclusions, click **Add Exclusion** and follow the previous steps to define more exclusions.

5. Click **Save** to save the scope and exclusions. The **Discovery Scope Set** page is displayed with the new scope in the list.

6. To add more scopes to this scope set, click **Add New Scope** and follow the previous steps to define more scopes.

   Note: For better performance, limit the cumulative number of IP addresses in a scope set to 400 or less.

Adding a discovery scope to an existing scope set

You can add a scope to an existing scope set.

Procedure

To add a scope to an existing scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **General Discovery Scopes**.

   The **General Discovery Scopes** page is displayed.

2. In the **General Discovery Scopes** pane, click the scope set to which you want to add a scope.

   The **Discovery Scope Set** page is displayed.

3. Click **Add New Scope**.

   The **General Discovery Scopes** page is displayed.

4. In the **Select Discovery Option** pane, specify one of the following options.

   - `Single IP address or Host`

     For **Describe Address or Host**, enter the IP address or host name.

   - `Range of IP addresses`

     For **Describe Address Range**, enter the starting IP address, ending IP address, and optionally, a description in the fields provided.

   - `Network or Subnet`

     For **Describe Network or Subnet**, enter the IP address, mask, and optionally, a description in the fields provided.

5. If you want to exclude IP addresses, range of IP addresses, or subnets from the discovery, click **Add Exclusion** and follow these steps:

   a) Select **Host**, **Range**, or **Subnet**.

   b) Specify the IP address, range of IP addresses, or subnet that you want to exclude from the discovery.

   c) Optional: Specify a description for the IP address, range of IP addresses or subnet that you are excluding from the discovery.

      Note: Exclusions are only applicable for a scope defined with a range of IP addresses or a subnet.

      Note: You cannot reuse an IP address, range of IP addresses, subnets, or description in any scopes or exclusions in a scope set.

   d) To add more exclusions, click **Add Exclusion** and follow the previous steps to define more exclusions.

6. Click **Save** to save the scope and the exclusions.

   The **Discovery Scope Set** page is displayed with the new scope in the list.

Modifying a discovery scope set

You can modify an existing discovery scope set by changing the settings for the scope set.

About this task

To modify an existing discovery scope set, follow these steps.

Procedure

1. In the navigation pane, click **Discovery Scopes** > **General Discovery Scopes**.

   The **General Discovery Scopes** page is displayed.

2. To edit the scope set, click the **Edit** (✏) beside the scope set.

   The **Discovery Scope Set** page is displayed. You can edit the scope set by editing a scope, adding a scope, moving a scope to another scope set, or by deleting a scope.

   - To add a scope, follow these steps:

     a. Click **Add New Scope**.

     b. In the **Select Discovery Option** pane, specify one of the following options:

        – `Single IP address / host`

          For **Describe Address or Host**, type the IP address or host name.

        – `Range of IP addresses`

          For **Describe Address Range**, type the starting IP address, ending IP address, and optionally, a description in the fields provided.

        – `Network or Subnet`

          For **Describe Network or Subnet**, type the IP address, mask, and optionally, a description in the fields provided.

        Note: Provide a unique name for **Description**. If you specify a description that is already existing for any other scope within this scope set, TSA will not allow you to create the new scope. If the **Description** field is left blank, TSA automatically creates the description using the IP Address range / subnet mask.

     c. If you want to exclude IP addresses or subnets from the discovery, click **Add Exclusion** and follow these steps:

        1) Select **Host**, **Range**, or **Subnet**.

        2) Specify the IP address, range of IP addresses, or subnet that you want to exclude from the discovery.
        3) To add more exclusions, click **Add Exclusion** and follow the previous steps to define more exclusions.
    d. Click **Save** to save the scope and exclusions. The **Discovery Scope Set** page is displayed with the new scope in the list.

- To move a scope to another scope set, follow these steps:
    a. Click **Move Scopes**.
    b. On the **Move Scopes from one set to another** page, select the scopes that you want to move from the **Scopes** list.
    c. Select the scope set from the **Destination Scope Set** list to which you want to move the scopes.
    d. Click **Move**.
- To edit a scope, follow these steps:
    a. Click the **Edit** (✏) icon of a particular scope.
    b. You can modify the **Discovery Option**, **IP Addresses**, **Exclusions**, etc.
    c. Click **Save** to save the scope and exclusions. The **Discovery Scope Set** page is displayed with the new scope in the list.
- To delete a scope, follow these steps:
    a. Click the **Delete** (🗑) icon beside the scope that you want to delete.
    b. Click **OK** to confirm that you want to delete the discovery scope.

Deleting discovery scopes

You can delete existing discovery scopes within a scope set, or you can delete entire scope sets.

About this task

Procedure

To delete a discovery scope, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **General Discovery Scopes**.

   The **General Discovery Scopes** page is displayed.
2. Edit the scope set that contains the discovery scope that you want to delete by clicking the **Edit** (✏) icon beside the scope set.

   The **Discovery Scope Set** page is displayed.
3. Click the **Delete** (🗑) icon beside the scope that you want to delete.
4. Click **OK** to confirm that you want to delete the discovery scope.

Deleting discovery scope sets

You can delete existing discovery scope sets.

Procedure

Note: Before you can delete a scope set, you must delete all credentials associated with the scope set.

To delete a discovery scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **General Discovery Scopes**.

   The **General Discovery Scopes** page is displayed.
2. Click the **Delete** (🗑) icon beside the scope set that you want to delete.

3. Click **OK** to confirm that you want to delete the discovery scope set.

Importing a scope set

You can import a list of IP addresses or host names to define a new scope set.

About this task

A new scope set is created based on the specified name and the list of IP addresses or host names from the input file. TSA performs the following validations when you import a scope set:

- Checks if the scope set name already exists.
- Validates each line of the file to check whether it is a valid IP address / host name or not.
- Ignores trailing and leading blank spaces when validating the IP address or host name.
- Ignores duplicate IP addresses or host names.

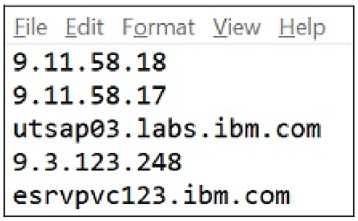
Procedure

To import the IP addresses or host names, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **Import General Scope Set**.

   The **Import General Scope Set** page is displayed.
2. Enter the **New scope set name**.

   Note: Enter a unique name that is not used by any existing scope sets. An error message is displayed if an existing scope set name is entered - `Scope set name already exists`.
3. Click **Choose File** to select the text file.

   ```
   9.11.58.18
   9.11.58.17
   utsap03.labs.ibm.com
   9.3.123.248
   esrvpvc123.ibm.com
   ```

   Figure 56. Import Scope Set

   Note: The text file must be formatted as a single column where each row contains a single IP address or host name and no other data.
4. Click **Import Scope set file** to import the scope set. A status message is displayed when the import completes successfully - **`Successfully imported Scope Set`**.

   Note: If the scope set file has more than 400 IP addresses, a warning message is displayed - **`Successfully imported Scope Set. But the number of scope elements is beyond the recommended guidelines, limit it to 400 for better performance.`**
5. After you import the scope set, you can edit the scope set in the **General Discovery Scopes** section of the user interface and associate credentials in the **Discovery Credentials** section.

Discovery Settings

Use the **Discovery Settings** page to adjust advanced discovery settings.

Configuring Connection Settings

Use the **Connection Settings** page to configure the SLP Discovery and discover EMC storage devices through EMC SMI-S Providers.

About this task

By default, a discovery job attempts to find EMC SMI-S Providers by running an SLP query to determine their IP address and port. If SLP is not available in your network (for example, if any security policies exist that block SLP messages), the discovery of EMC storage devices can still be done by disabling SLP Discovery and configuring the ports that the EMC SMI-S Provider listens for query requests.

Procedure

1. Select **Enable** or **Disable** options to enable or disable SLP Discovery.

   Note: By default, SLP discovery is enabled.
2. If you disable SLP discovery, you must set one or more EMC SMI-S Provider connection ports -
   a) **EMC SMI-S HTTPS Port(s):** 5989 is the default HTTPS port on which the EMC SMI-S Provider listens for query requests. If you specify multiple ports, separate them by commas. The EMC SMI-S listens on these ports for connection requests (such as from TSA). TSA needs to know that port to initiate the connection.

   b) **EMC SMI-S HTTP Port(s):** 5988 is the default HTTP port on which the EMC SMI-S Provider listens for query requests. TSA first tries an HTTPS connection (if configured) and if it fails, attempts to connect through HTTP ports that are defined. If you would like to avoid HTTP connections, do not define HTTP ports. If you specify multiple HTTP ports, separate them by commas. The EMC SMI-S listens on these ports for connection requests (such as from TSA). TSA needs to know that port to initiate the connection.
3. Click **Save** to save the connection settings. You get a message - *The discovery connection settings were successfully saved.*

Discovery credentials

Discovery credentials are the user names, passwords or SSH keys, and Simple Network Management Protocol (SNMP) community strings that TSA uses to access resources that are configured in **General Discovery Scopes** during discovery.

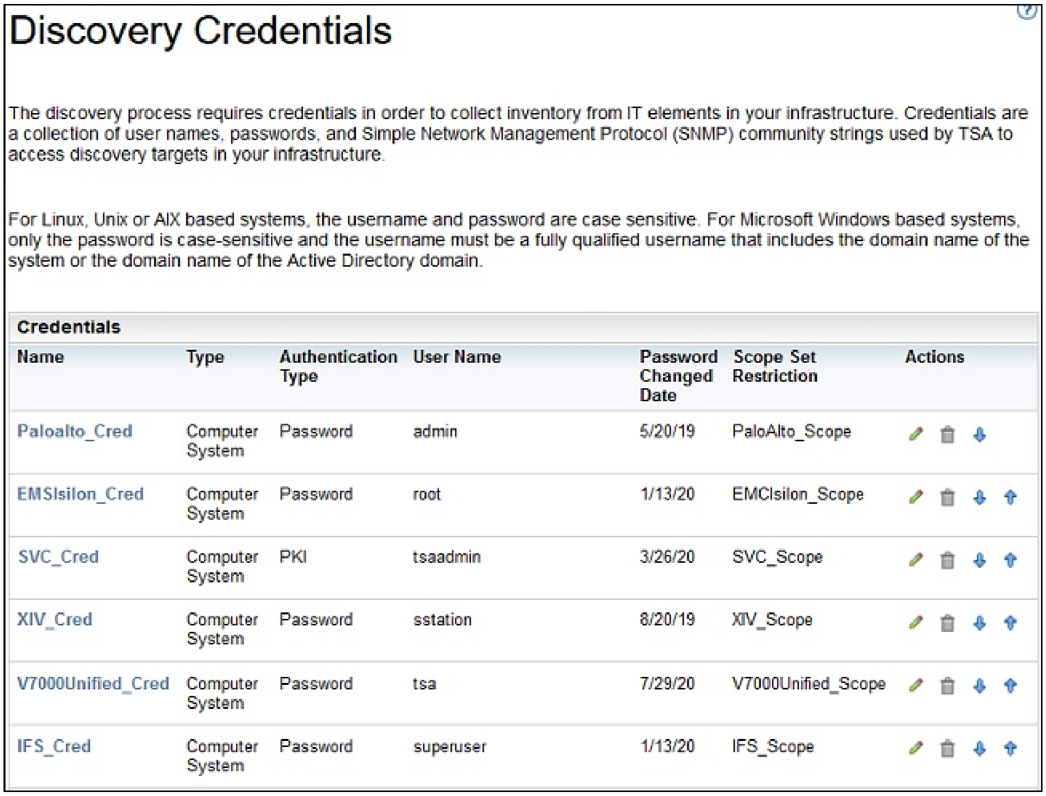
Displaying credentials

The discovery process requires credentials, such as user IDs and passwords, to access resources.

About this task

Important: The access information that you specify must match the access information for the discovery target resource. If you change access information, such as a password, on the target resource, be sure to also change the associated Technical Support Appliance access information.

You can display the existing credentials by clicking **Discovery Credentials** in the navigation pane. The **Discovery Credentials** page is displayed.



Discovery Credentials

The discovery process requires credentials in order to collect inventory from IT elements in your infrastructure. Credentials are a collection of user names, passwords, and Simple Network Management Protocol (SNMP) community strings used by TSA to access discovery targets in your infrastructure.

For Linux, Unix or AIX based systems, the username and password are case sensitive. For Microsoft Windows based systems, only the password is case-sensitive and the username must be a fully qualified username that includes the domain name of the system or the domain name of the Active Directory domain.

Credentials

Name	Type	Authentication Type	User Name	Password Changed Date	Scope Set Restriction	Actions
Paloalto_Cred	Computer System	Password	admin	5/20/19	PaloAlto_Scope	✎ 🗑 ↓
EMSIsilon_Cred	Computer System	Password	root	1/13/20	EMCIsilon_Scope	✎ 🗑 ↓ ↑
SVC_Cred	Computer System	PKI	tsaadmin	3/26/20	SVC_Scope	✎ 🗑 ↓ ↑
XIV_Cred	Computer System	Password	sstation	8/20/19	XIV_Scope	✎ 🗑 ↓ ↑
V7000Unified_Cred	Computer System	Password	tsa	7/29/20	V7000Unified_Scope	✎ 🗑 ↓ ↑
IFS_Cred	Computer System	Password	superuser	1/13/20	IFS_Scope	✎ 🗑 ↓ ↑

Figure 57. New Discovery Credentials

Viewing credential details

You can view detailed information about a specific discovery credential.

About this task

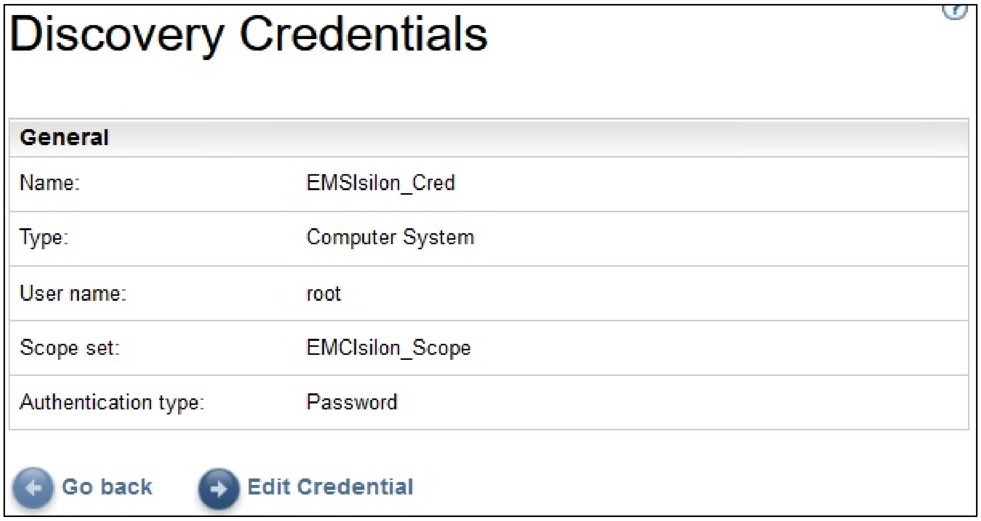
To view the credential details, follow these steps:

Procedure

1. In the navigation pane, click **Discovery Credentials**.

   The **Discovery Credentials** page is displayed with all the existing credentials listed.
2. To view details for a specific credential, click the name of the credential.

   The **Discovery Credentials** page is displayed with information for the selected credential.



Discovery Credentials

General	
Name:	EMSIsilon_Cred
Type:	Computer System
User name:	root
Scope set:	EMCIsilon_Scope
Authentication type:	Password

Figure 58. Discovery Credentials details

Related tasks

Modifying credentials
You can modify existing credentials to provide access control for the discovery process.

Adding credentials

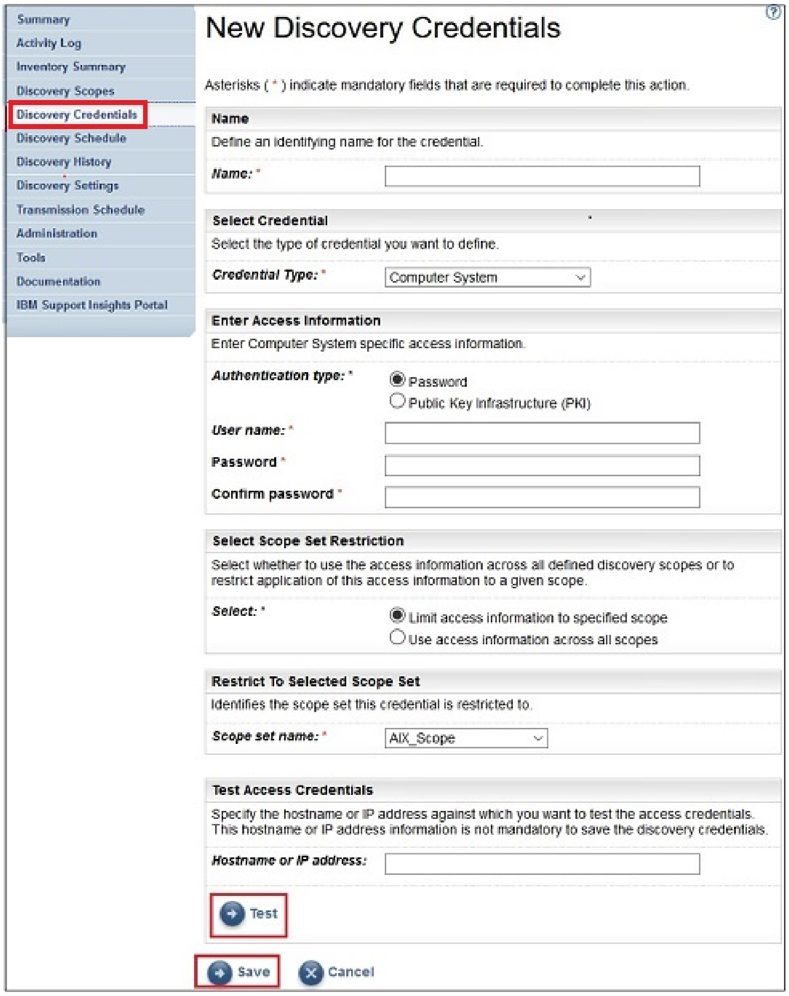
Add credentials to provide access control for the discovery process.

About this task

To add credentials, follow these steps:

Procedure

1. In the navigation pane, click **Discovery Credentials**.
   The **Discovery Credentials** page is displayed.
2. To create a credential, click **Add New Credentials**.
   The **New Discovery Credentials** page is displayed.



Summary
Activity Log
Inventory Summary
Discovery Scopes
Discovery Credentials
Discovery Schedule
Discovery History
Discovery Settings
Transmission Schedule
Administration
Tools
Documentation
IBM Support Insights Portal

New Discovery Credentials

Asterisks (*) indicate mandatory fields that are required to complete this action.

Name

Define an identifying name for the credential.

Name: *

Select Credential

Select the type of credential you want to define.

Credential Type: * Computer System

Enter Access Information

Enter Computer System specific access information.

Authentication type: *
● Password
○ Public Key Infrastructure (PKI)

User name: *

Password *

Confirm password *

Select Scope Set Restriction

Select whether to use the access information across all defined discovery scopes or to restrict application of this access information to a given scope.

Select: *
● Limit access information to specified scope
○ Use access information across all scopes

Restrict To Selected Scope Set

Identifies the scope set this credential is restricted to.

Scope set name: * AIX_Scope

Test Access Credentials

Specify the hostname or IP address against which you want to test the access credentials. This hostname or IP address information is not mandatory to save the discovery credentials.

Hostname or IP address:

Figure 59. New Discovery Credentials

a) In the **Name** field, type an identifying name for the credential.

b) In the **Credential Type** drop-down list, select the type of credential that you want to create.

c) In the **Enter Access Information** pane, specify the information for the credential type you selected:

The information that is required depends on the credential type. For information about the access information that is required for each type of credential, see "Credential and software requirements for the discovery environment " on page 6.

Important: The access information that you specify must match the access information for the discovery target resource. If you change access information about the target resource, be sure to also change the associated TSA access information. For more information, refer the IBM Technical Support Appliance Configuration Assistant Guide.

Tip: The **Discovery Credentials** page displays the last time that the password was changed. If you regularly change the password on the target resource, you can use this information to make sure that you also change the password on TSA to match the new password for the target resource. For information about displaying the discovery credentials, see "Displaying credentials" on page 73.

d) The **Select Scope Set Restriction** pane is used to specify whether a credential is limited to a single scope set or if it applies to all scope sets. If **Credential Type** is **Computer System** and the **Authentication type** is **PKI**, then this pane is not displayed. PKI credentials must always be scoped to a single scope set.

Tip: Creating discovery credentials that are restricted to a specific scope set can improve performance by reducing the number of credentials that are attempted for resources that are being discovered.

   e) The **Restrict To Selected Scope Set** pane is used to limit a credential to a single scope set. This pane is visible under one of these two conditions.

      - The **Select Scope Set Restriction** pane has **Limit access information to specified scope** selected, or
      - The **Credential type** is **Computer System** and the **Authentication type** is **PKI**.

      The credential is used only to discover the selected scope set. When discovering with a different scope set, the credential is not used. This method prevents invalid login attempts that can cause you to be locked out of the account.

   f) If your credential type is **Computer System**, **Computer System (Windows)**, **SNMP**, or **SNMPV3**, you can verify whether the credentials are correct. The **Test** function for the **Computer System** credential type supports the following devices:

      - Devices that use SSH or Telnet based authentication
      - XIV®
      - DS6000™ & DS8000®
      - VMware ESXi
      - VMware vCenter Server
      - EMC CLARiiON / VNX / VMAX via EMC SMI-S
      - IBM TS3100 / TS3200
      - IBM TS3310
      - IBM TS3500
      - IBM TS4300
      - IBM TS4500
      - IBM TS7700
      - IBM DS3000, DS4000, and DS5000 if password protected
      - Windows
      - Palo Alto Networks (PAN-OS)

      To test the credentials, enter an IP address or a host name for the target device against which you want to test the credentials and click **Test**.

      Note:

      - The host name you enter must not contain an underscore ("_").
      - To run discovery or test credential on systems that run Linux, AIX, IBM i, or HP-UX operating systems, enable SSH.

   g) Click **Save**.

      The new credential is displayed in the **Discovery Credentials** page.

      Note: It is a best practice to backup TSA configuration when you create or modify discovery credentials.

3. To change the order in which a credential is used by TSA to access a resource, click either the **Up arrow** icon ⇧ or the **Down arrow** icon ⇩ beside the credential to move it up or down in the list.

   For information about how the order is used, see "Discovery credentials" on page 2.

   The **Discovery Credentials** page list is displayed again with the new order.

Modifying credentials

You can modify existing credentials to provide access control for the discovery process.

About this task

To modify credentials, follow these steps:

Procedure

1. In the navigation pane, click **Discovery Credentials**.

   The **Discovery Credentials** page is displayed with all the existing credentials listed.

2. Edit the credential by clicking the **Edit** (✎) icon beside the credential.

   The **Edit Discovery Credentials** page is displayed.

   a) In the **Modify Access Information** pane, you can change the access information for this credential.

      Important: The access information that you specify must match the access information for the discovery target resource. If you change access information about the target resource, be sure to also change the associated TSA access information. For more information, refer the IBM Technical Support Appliance Configuration Assistant Guide.

      Tip: The **Discovery Credentials** page displays the last time that the password was changed. If you regularly change the password on the target resource, you can use this information to make sure that you also change the password on TSA to match the new password for the target resource. For information about displaying the discovery credentials, see "Displaying credentials" on page 73.

   b) The **Select Scope Set Restriction** pane is used to specify whether a credential is limited to a single scope set or if it applies to all scope sets. If the **Credential Type** is **Computer System** and the **Authentication type** is **PKI**, then this pane is not displayed. PKI credentials must always be scoped to a single scope set.

      Tip: Creating discovery credentials that are restricted to a specific scope set can improve performance by reducing the number of credentials that are attempted for resources being discovered.

   c) The **Restrict To Selected Scope Set** pane is used to limit a credential to a single scope set. This pane is visible under one of these two conditions:

      - The **Select Scope Set Restriction** pane has **Limit access information to specified scope** selected, or
      - The **Credential type** is **Computer System** and the **Authentication type** is **PKI**.

      The credential is used only when discovering the selected scope set. This credential is not used with any other scope set. This method prevents invalid login attempts that can cause the user to be locked out of the account.

   d) If your credential type is **Computer System**, **Computer System (Windows)**, **SNMP**, or **SNMPV3** you can verify whether the credentials are correct. To test these credentials, enter an IP address or host name for the target you want to test the credentials with and click **Test**.

      Note: The host name you enter must not contain an underscore ("_").

   e) Click **Save**.

      The changed credential is displayed in the **Discovery Credentials** page.

3. To change the priority order in which a credential is used by TSA to access a resource, click either the **Up arrow** (↑) icon or the **Down arrow** (↓) icon beside the credential to move it up or down in the list. For information about how the order is used, see "Discovery credentials" on page 2.

   The **Discovery Credentials** page list is displayed again with the new order.

Related concepts

Discovery credentials

Discovery credentials are a collection of user names, passwords or SSH keys, and Simple Network Management Protocol (SNMP) community strings that TSA uses to access resources during the discovery.

Credential and software requirements for the discovery environment
In order to discover endpoints or resources in your environment, TSA must have access to those resources. It is recommended that you create a service account on each resource that is specifically for TSA to use when accessing that resource.

Deleting credentials

You can delete credentials that TSA uses when accessing your resources.

About this task

To delete a credential, follow these steps:

Procedure

1. In the navigation pane, click **Discovery Credentials**.

   The **Discovery Credentials** page is displayed.
2. Click the **Delete** (🗑) icon beside the credential that you want to delete.
3. Click **OK** to confirm that you want to delete the credential.

Discovery schedule

Discoveries are scheduled to ensure that discovered data is always current and accurate. You can view the discovery schedule and details of the last discoveries, modify the discovery schedules, and disable scheduled discoveries. You can also run a discovery whenever you choose.

Before you begin

By default, TSA uses the Full Discovery schedule to discover all IT elements defined in HMC and VMware Dynamic Scopes as well as General Discovery Scopes. TSA automatically spreads out the detection of IT elements during the discovery process in order to minimize the impact.

An alternative is to create several user-defined schedules. This allows discovery of specific discovery scopes to be spread out to different dates and times when the impact to your network and IT elements is minimal (or ideal). In this case, the full discovery schedule should be disabled in favor of the user-defined schedules.

At the beginning of any scheduled discoveries, the appliance runs the pre-discovery maintenance job during which a few functions such as the Inventory Summary, Discovery Scopes, Discovery Schedules, and Credentials are not available. During the pre-discovery maintenance job the **Discovery Manager** status on the **Sumary** screen is set to the warning symbol (⚠). In addition, a warning message is displayed on TSA screens indicating that some functions are temporarily unavailable: `As part of Pre-Discovery Maintenance, the Discovery Manager is temporarily offline. Some UI functions related to discovery or inventory could display partial or no information during this time (typically up to 10 minutes).`

After the successful pre-discovery maintenance, the **Discovery Manager** status turns to *OK*(✅) state in the **Summary** page and resumes the full discovery activity (within 10 minutes).

Viewing the discovery schedule

You can view the summary information about a discovery schedule.

About this task

To view the discovery schedule, follow these steps:

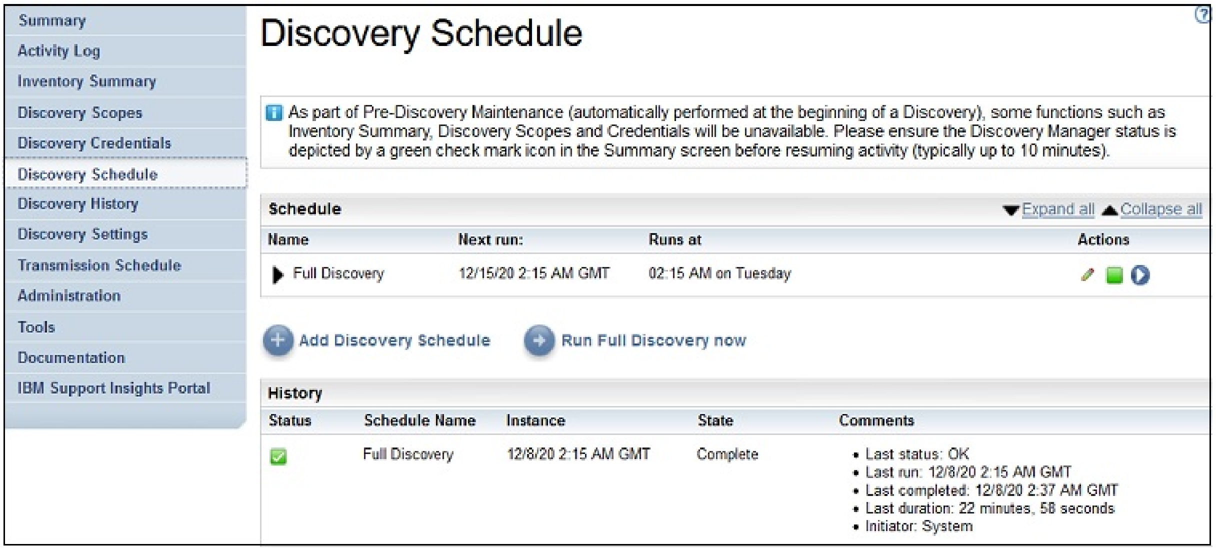
Procedure

In the navigation pane, click **Discovery Schedule**.

The **Discovery Schedule** page is displayed.

The **Schedule** pane displays the name of the schedule, the next scheduled run, the run schedule, and the actions (Edit (✎), Delete (🗑), Enable / Disable (🟩 / ▨), Run (▶)) for each schedule.

Click the **Expand** (▶) icon to view all the scope sets that are assigned for the schedule. For the full discovery schedule, the icon lists all the scope sets that are defined in TSA and are assigned to the schedule by default.



Discovery Schedule

As part of Pre-Discovery Maintenance (automatically performed at the beginning of a Discovery), some functions such as Inventory Summary, Discovery Scopes and Credentials will be unavailable. Please ensure the Discovery Manager status is depicted by a green check mark icon in the Summary screen before resuming activity (typically up to 10 minutes).

Schedule

Name	Next run:	Runs at	Actions
▶ Full Discovery	12/15/20 2:15 AM GMT	02:15 AM on Tuesday	✎ 🟩 ▶

History

Status	Schedule Name	Instance	State	Comments
✓	Full Discovery	12/8/20 2:15 AM GMT	Complete	• Last status: OK • Last run: 12/8/20 2:15 AM GMT • Last completed: 12/8/20 2:37 AM GMT • Last duration: 22 minutes, 58 seconds • Initiator: System

Figure 60. Discovery Schedule

Note: If you have a TSA which is a fresh install, migrated, or upgraded to the latest version, the new TSA has a discovery schedule named **Full Discovery** that is created with the default date (2:15 AM on Tuesday). The Full Discovery schedule can be edited or disabled, but it cannot be deleted. If you have any pre-defined discovery schedules (enabled / disabled), the same values are restored after migration.

The **History** pane displays the status, schedule name, and more details of the currently running and previously discovered jobs.

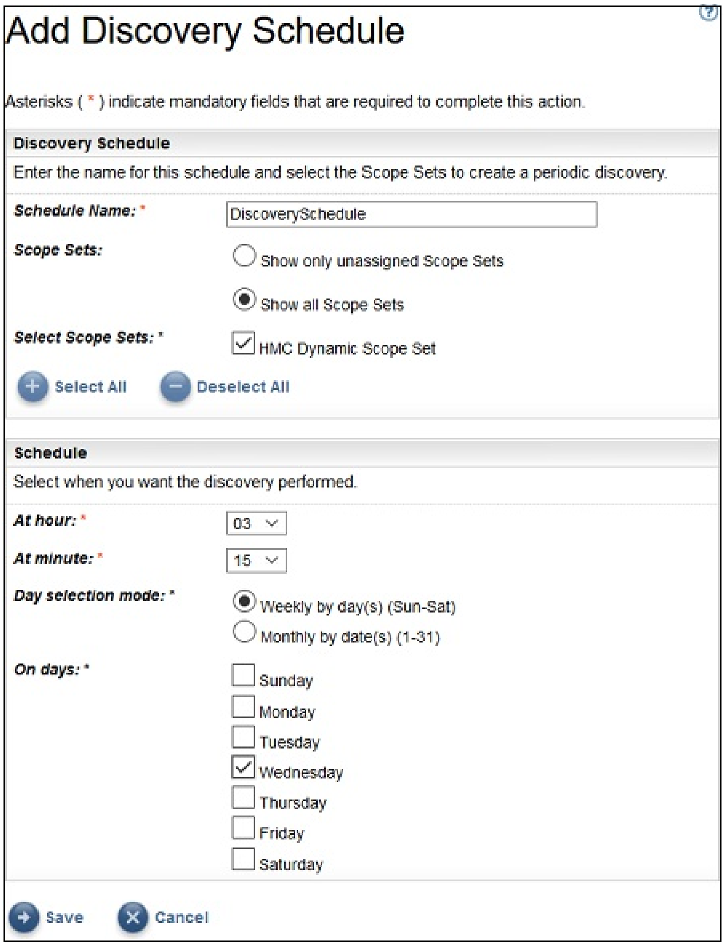
Adding discovery schedule

You can add new schedules for the discovery process to run at a specified time. The new schedules allow TSA to discover a subset of your IT elements at the scheduled date and time.

Procedure

1. In the navigation pane, click **Discovery Schedule**.

   The **Discovery Schedule** page is displayed.
2. Click **Add Discovery Schedule**. The **Add Discovery Schedule** page is displayed.



Add Discovery Schedule

Asterisks (*) indicate mandatory fields that are required to complete this action.

Discovery Schedule

Enter the name for this schedule and select the Scope Sets to create a periodic discovery.

Schedule Name: *	DiscoverySchedule
Scope Sets:	○ Show only unassigned Scope Sets ● Show all Scope Sets
Select Scope Sets: *	☑ HMC Dynamic Scope Set

Schedule

Select when you want the discovery performed.

At hour: *	03
At minute: *	15
Day selection mode: *	● Weekly by day(s) (Sun-Sat) ○ Monthly by date(s) (1-31)
On days: *	□ Sunday □ Monday □ Tuesday ☑ Wednesday □ Thursday □ Friday □ Saturday

Figure 61. Add Discovery Schedule

3. In the **Schedule Name** field, type an identifying name for the schedule.
4. **Scope Sets**

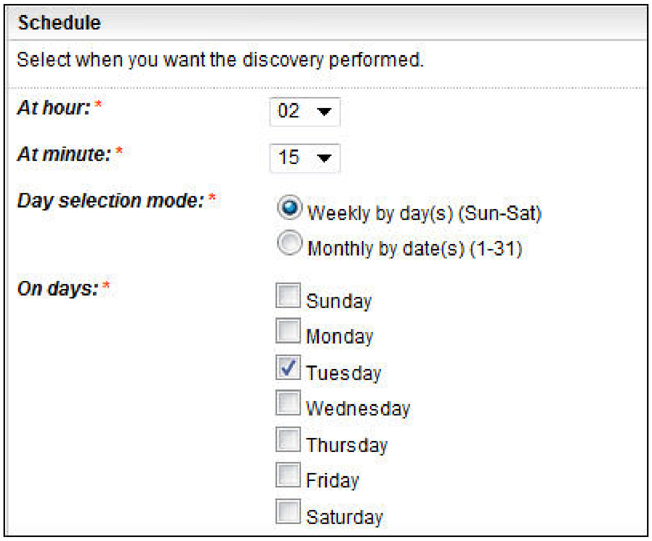
   a) Select the **Show only unassigned Scope Sets** option to view only those scope sets that are not assigned to any other user-defined discovery schedule.

   b) Select the **Show all Scope Sets** option to view all the scope sets.
5. Select the desired scope sets from **Select Scope Sets** list.

   You can use **Select All** / **Deselect All** to select all or none of the scope sets.
6. Use the **At hour** and **At minute** lists to select a new time.
7. Select the **Day Selection mode**.

   Weekly by day(s) (Sun - Sat)

   To schedule the discovery on a particular day(s) of a week, select the **Weekly by day(s) (Sun - Sat)** option.



Schedule

Select when you want the discovery performed.

At hour: * 02

At minute: * 15

Day selection mode: *
● Weekly by day(s) (Sun-Sat)
○ Monthly by date(s) (1-31)

On days: *
□ Sunday
□ Monday
☑ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday

Figure 62. Weekly by day(s) (Sun - Sat)

For the **On days** field, select the appropriate check box to select one or more days of the week.

Monthly by date(s) (1-31)

To schedule the discovery on particular days of a month, select **Monthly by date(s) (1-31)** option.

For the **On days** field, select the appropriate check box to select one or more days of the month.

Note: If you select the days beyond the last day of a specific month, then the job is triggered on the last day of that particular month.

8. Click **Save**.

   The **Discovery Schedule** page is displayed again with the new schedule shown.

Modifying the discovery schedule

TSA provides a default schedule for the discovery process to run at specified times. You can modify the default schedule or use custom schedules according to your needs.

Procedure

1. In the navigation pane, click **Discovery Schedule**.

   The **Discovery Schedule** page is displayed.

2. Click the **Edit Schedule** (✏) icon.

   The **Edit Discovery Schedule** page is displayed.

   a) Edit the **Schedule Name**, **Scope Sets**, and **Select Scope Sets** as needed in the **Discovery Schedule** pane.

      Note: You cannot edit these fields for the default Full Discovery.

   b) Edit the **At hour**, **At minute**, **Day Selection mode**, and **On days** as needed in the **Schedule** pane.

3. Click **Save**.

   The **Discovery Schedule** page is displayed again with the modified schedule shown.

Disabling the discovery schedule

You can disable scheduled discoveries.

Before you begin

Note: If user-defined discovery schedules have been configured, it is recommended that the **Full Discovery** schedule is disabled so that duplicate discoveries of the same IT elements does not occur.

Procedure

To disable scheduled discoveries, follow these steps:

1. In the navigation pane, click **Discovery Schedule**.

   The **Discovery Schedule** page is displayed.

2. Click the **Enable / Disable** (🟩 / ⬛) icon for the respective schedule to disable / enable the discovery schedule.

Deleting the discovery schedule

You can delete scheduled discoveries.

Procedure

To delete scheduled discoveries, follow these steps:

1. In the navigation pane, click **Discovery Schedule**.

   The **Discovery Schedule** page is displayed.

2. Click the Delete (🗑) icon for the respective schedule to be deleted.

   Note: You cannot delete the **Full Discovery** schedule, but this schedule can be disabled if desired.

   A confirmation message is displayed to delete the selected discovery schedule.
3. Click **OK** to the delete the schedule.

Running the discovery

You can run a discovery on demand rather than wait for the next scheduled discovery. You can run a discovery on all defined discovery scopes, a specific discovery schedule, or on specific discovery scope sets or scopes."

Procedure

To run a discovery on all defined scopes, follow these steps:

1. In the navigation pane, click **Discovery Schedule**. The **Discovery Schedule** page is displayed.
2. Click **Run Full Discovery Now**. The History section is updated indicating that the discovery is running.

   Note: TSA attempts to minimize impacts to the network environment. As a result, the discovery process uses an iterative and measured approach which may cause a full discovery to take up to 72 hours. You can monitor the discovery process in the **Job Summary** section on the **Summary** page.

3. To run a discovery on a specific scope, click the **Run** (▶) for that scope.
4. Check the **Summary** page (click **Summary** in the navigation pane). The discovery is shown in the **Job Summary** pane. The **Summary** page periodically refreshes to show the current state of TSA. Once the job is no longer listed in the **Job Summary** pane, check the **Activity Log** (click **Activity Log** in the navigation pane). The discovery should complete without errors.

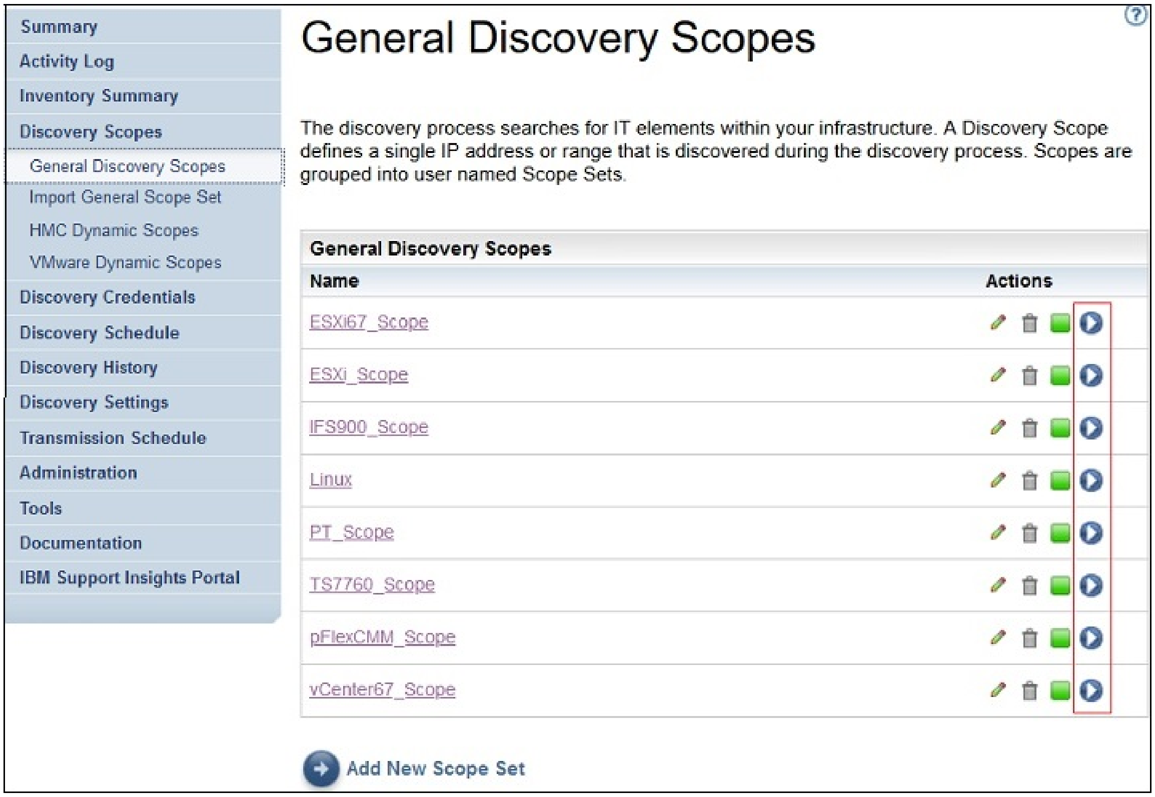
Running the discovery on General Scope Sets

Procedure

To run a discovery on a specific scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **General Discovery Scopes**.

   The **General Discovery Scopes** page is displayed. This page displays a list of all scope sets that are defined for this TSA.



General Discovery Scopes

The discovery process searches for IT elements within your infrastructure. A Discovery Scope defines a single IP address or range that is discovered during the discovery process. Scopes are grouped into user named Scope Sets.

General Discovery Scopes

Name	Actions
ESXi67_Scope	✎ 🗑 🟩 ▶
ESXi_Scope	✎ 🗑 🟩 ▶
IFS900_Scope	✎ 🗑 🟩 ▶
Linux	✎ 🗑 🟩 ▶
PT_Scope	✎ 🗑 🟩 ▶
TS7760_Scope	✎ 🗑 🟩 ▶
pFlexCMM_Scope	✎ 🗑 🟩 ▶
vCenter67_Scope	✎ 🗑 🟩 ▶

Figure 63. Run discovery on specific scopes

2. To run a discovery on a specific scope set, click the **Run** (▶) icon for that scope set.
3. Check the **Summary** page (click **Summary** in the navigation pane). The discovery is shown in the **Job Summary** pane. The **Summary** page periodically refreshes to show the current state of TSA. Once the job is no longer listed in the **Job Summary** pane, check the **Activity Log** (click **Activity Log** in the navigation pane). The discovery should complete without errors.

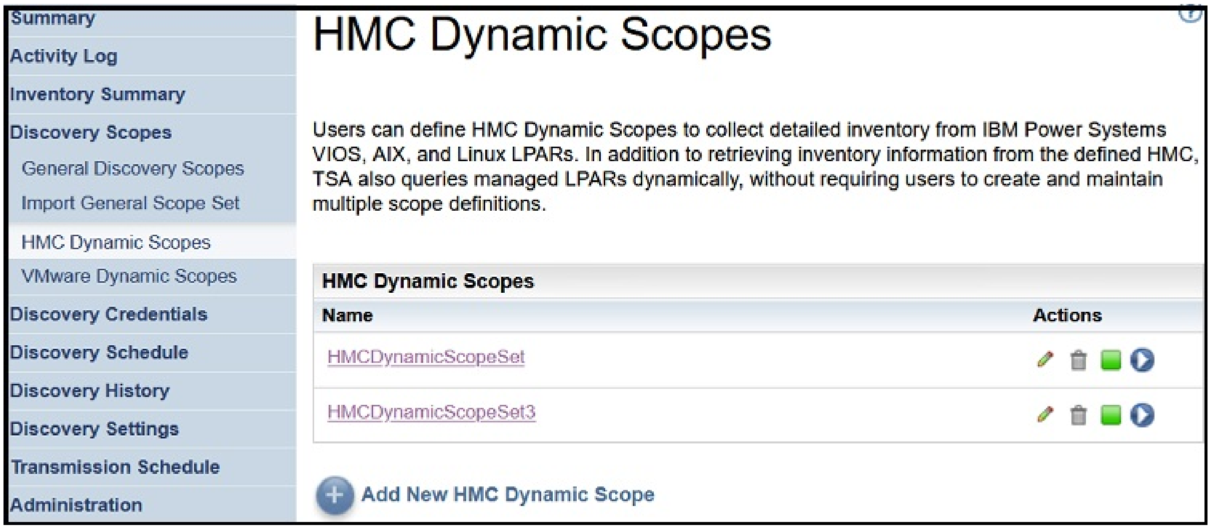
Running the discovery on HMC Dynamic Scope Sets

Procedure

To run a discovery on a specific scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**.

   The **HMC Dynamic Scopes** page is displayed. This page displays a list of all scope sets that are defined for this TSA.



HMC Dynamic Scopes

Users can define HMC Dynamic Scopes to collect detailed inventory from IBM Power Systems VIOS, AIX, and Linux LPARs. In addition to retrieving inventory information from the defined HMC, TSA also queries managed LPARs dynamically, without requiring users to create and maintain multiple scope definitions.

HMC Dynamic Scopes

Name	Actions
HMCDynamicScopeSet	✎ 🗑 🟩 ▶
HMCDynamicScopeSet3	✎ 🗑 🟩 ▶

Figure 64. HMC Dynamic Scopes

2. To run a discovery on a specific scope set, click the **Run** (▶) icon for that scope set.
3. Check the **Summary** page (click **Summary** in the navigation pane). The discovery is shown in the **Job Summary** pane. The **Summary** page periodically refreshes to show the current state of TSA. Once the job is no longer listed in the **Job Summary** pane, check the **Activity Log** (click **Activity Log** in the navigation pane). The discovery should complete without errors.

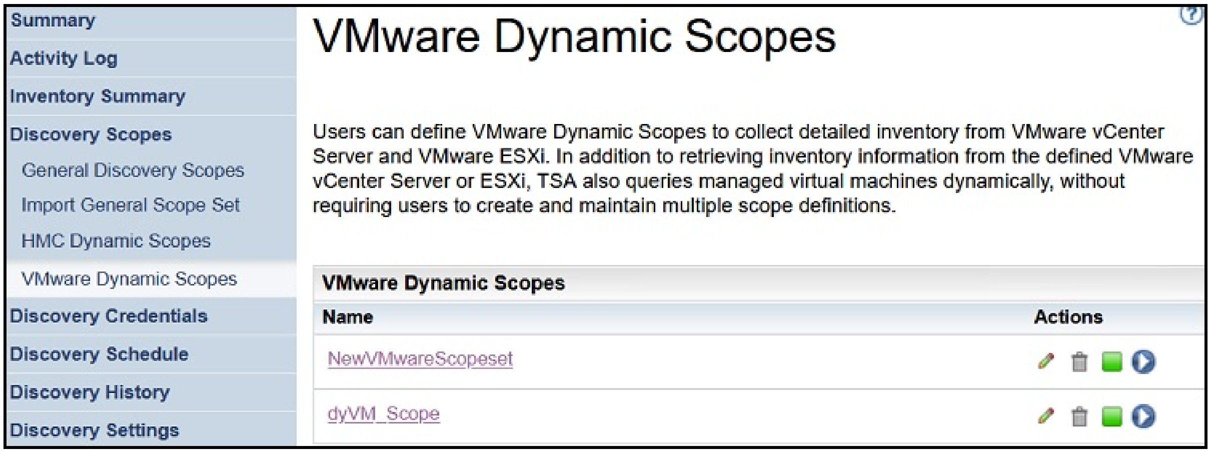
Running the discovery on VMWare Scope Sets

Procedure

To run a discovery on a specific scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes** > **VMWare Dynamic Scope Set**.

   The **VMWare Dynamic Scopes** page is displayed. This page displays a list of all scope sets that are defined for this TSA.



VMware Dynamic Scopes

Users can define VMware Dynamic Scopes to collect detailed inventory from VMware vCenter Server and VMware ESXi. In addition to retrieving inventory information from the defined VMware vCenter Server or ESXi, TSA also queries managed virtual machines dynamically, without requiring users to create and maintain multiple scope definitions.

VMware Dynamic Scopes

Name	Actions
NewVMwareScopeset	✎ 🗑 🟩 ▶
dyVM_Scope	✎ 🗑 🟩 ▶

Figure 65. Run discovery on VMware Dynamic Scopes

2. To run a discovery on a specific scope set, click the **Run** (▶) for that scope set.
3. Check the **Summary** page (click **Summary** in the navigation pane). The discovery is shown in the **Job Summary** pane. The **Summary** page periodically refreshes to show the current state of TSA. Once the job is no longer listed in the **Job Summary** pane, check the **Activity Log** (click **Activity Log** in the navigation pane). The discovery should complete without errors.

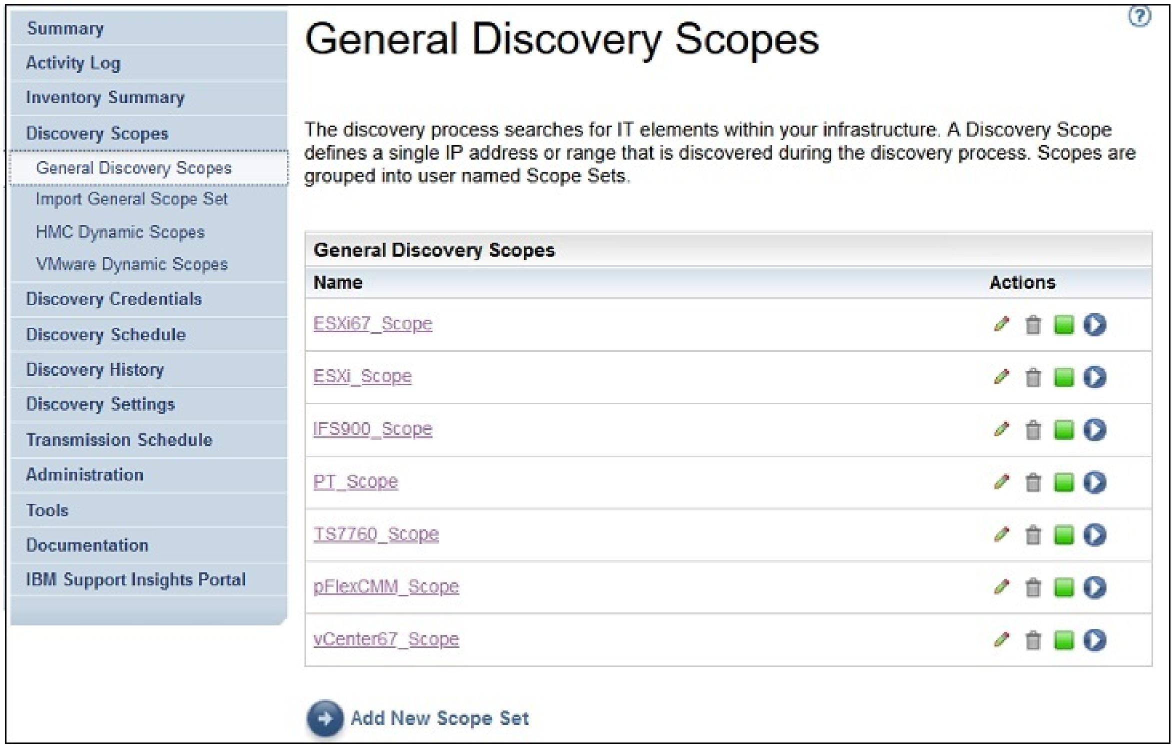
Running the discovery on Scopes

You can run a discovery on demand rather than wait for the next scheduled discovery. You can run a discovery on all defined discovery scopes, a specific discovery schedule, or on specific discovery scope sets or scopes."

Running the discovery on General Scopes

Procedure

1. In the navigation pane, click **Discovery Scopes** > **General Discovery Scopes**. The **General Discovery Scopes** page is displayed.



General Discovery Scopes

The discovery process searches for IT elements within your infrastructure. A Discovery Scope defines a single IP address or range that is discovered during the discovery process. Scopes are grouped into user named Scope Sets.

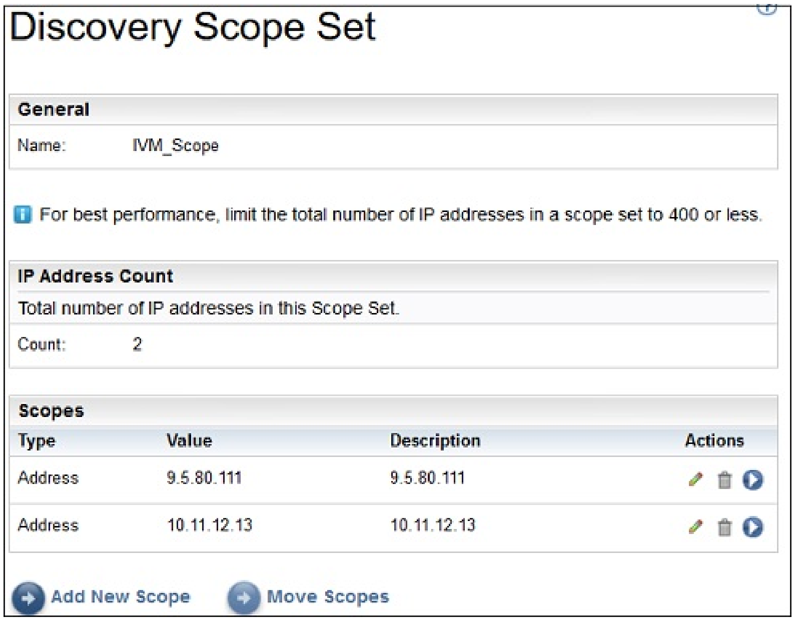
General Discovery Scopes

Name	Actions
ESXi67_Scope	✎ 🗑 🟩 ▶
ESXi_Scope	✎ 🗑 🟩 ▶
IFS900_Scope	✎ 🗑 🟩 ▶
PT_Scope	✎ 🗑 🟩 ▶
TS7760_Scope	✎ 🗑 🟩 ▶
pFlexCMM_Scope	✎ 🗑 🟩 ▶
vCenter67_Scope	✎ 🗑 🟩 ▶

Figure 66. Discovery Scopes

2. Click the scope set that contains the scope to be discovered.

   The **Discovery Scope Set** page is displayed. This page displays all the scopes that are defined for that scope set.



Discovery Scope Set

General

Name: IVM_Scope

For best performance, limit the total number of IP addresses in a scope set to 400 or less.

IP Address Count

Total number of IP addresses in this Scope Set.

Count: 2

Scopes

Type	Value	Description	Actions
Address	9.5.80.111	9.5.80.111	✎ 🗑 ▶
Address	10.11.12.13	10.11.12.13	✎ 🗑 ▶

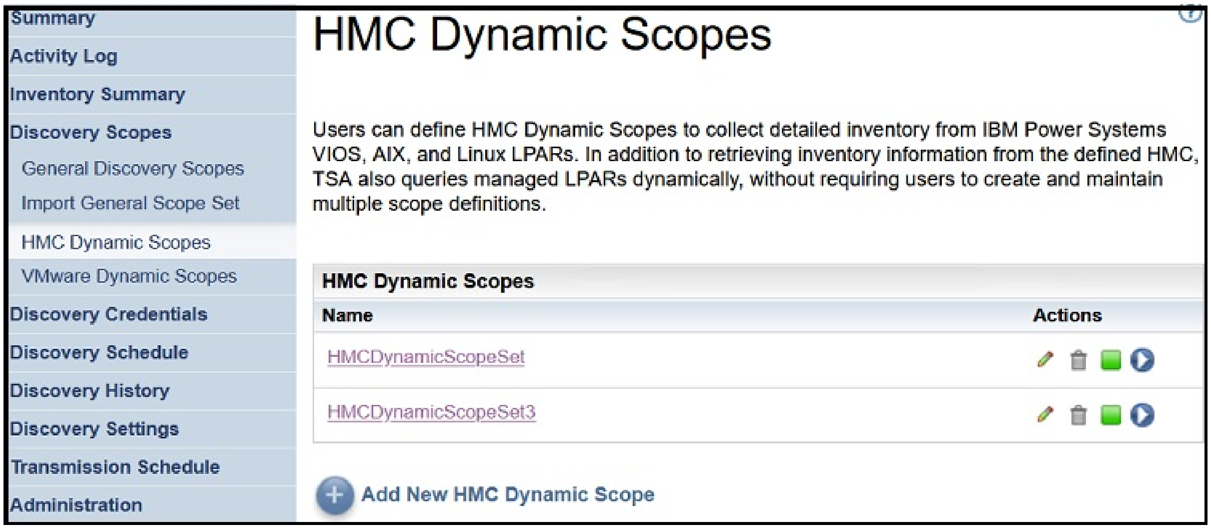
Figure 67. Run discovery on specific scopes

3. To run a discovery on a specific scope, click the **Run** (▶) icon for that scope.
4. Check the **Summary** page (click **Summary** in the navigation pane). The discovery is shown in the **Job Summary** pane. The **Summary** page periodically refreshes to show the current state of TSA. Once the job is no longer listed in the **Job Summary** pane, check the **Activity Log** (click **Activity Log** in the navigation pane). The discovery should complete without errors.

Running the discovery on HMC Dynamic Scopes

Procedure

1. In the navigation pane, click **Discovery Scopes** > **HMC Dynamic Scopes**. The **HMC Dynamic Scopes** page is displayed.



HMC Dynamic Scopes

Users can define HMC Dynamic Scopes to collect detailed inventory from IBM Power Systems VIOS, AIX, and Linux LPARs. In addition to retrieving inventory information from the defined HMC, TSA also queries managed LPARs dynamically, without requiring users to create and maintain multiple scope definitions.

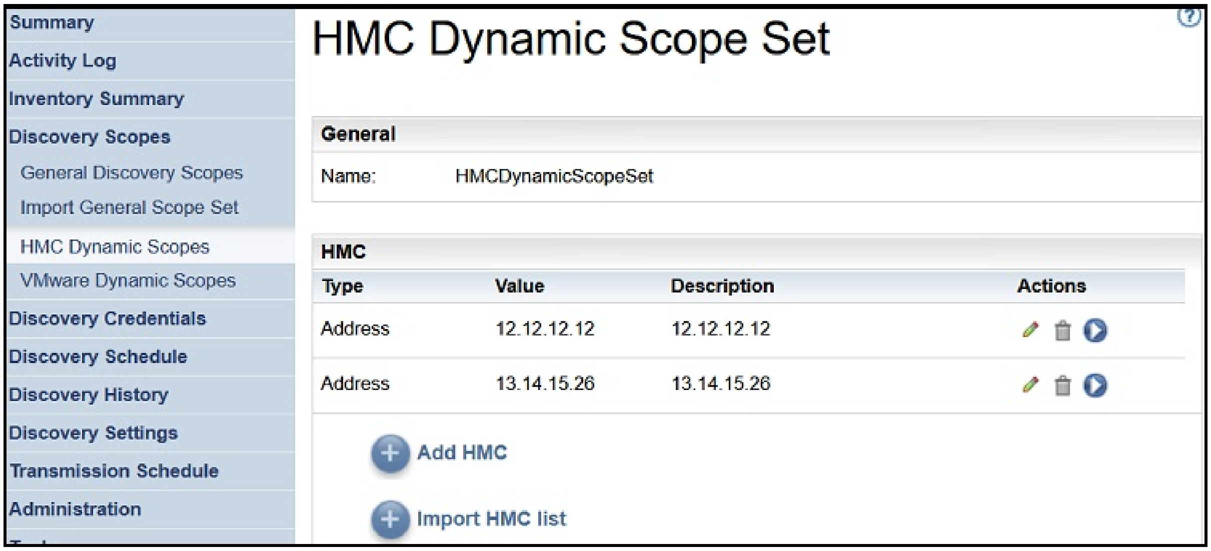
HMC Dynamic Scopes

Name	Actions
HMCDynamicScopeSet	✎ 🗑 🟩 ▶
HMCDynamicScopeSet3	✎ 🗑 🟩 ▶

Figure 68. HMC Dynamic Scopes

2. Click the scope set that contains the scope to be discovered.

   The **HMC Dynamic Scope Set** page is displayed. This page displays all the scopes that are defined for that scope set.



HMC Dynamic Scope Set

General

Name: HMCDynamicScopeSet

HMC

Type	Value	Description	Actions
Address	12.12.12.12	12.12.12.12	✎ 🗑 ▶
Address	13.14.15.26	13.14.15.26	✎ 🗑 ▶

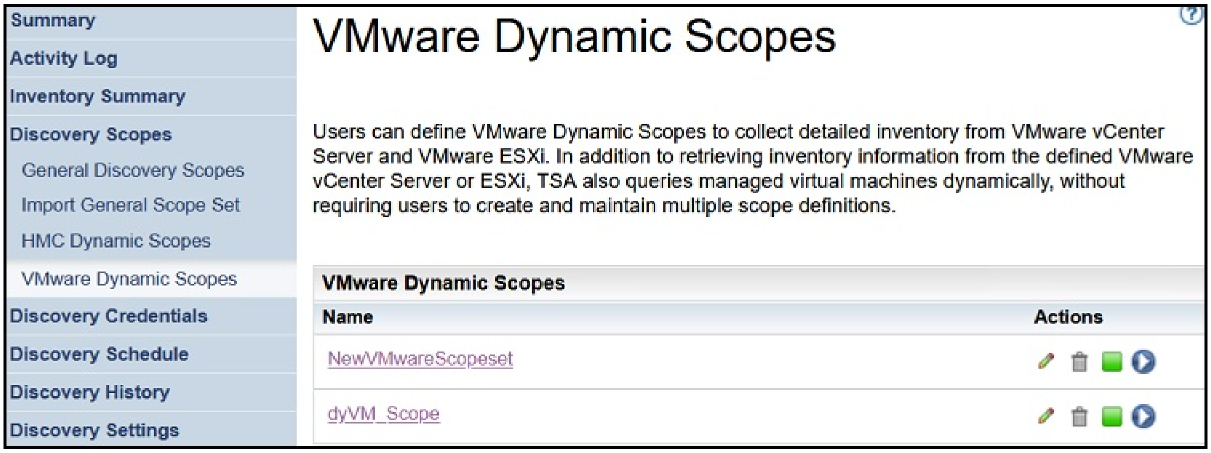
Figure 69. Run discovery on specific scopes

3. To run a discovery on a specific scope, click the **Run** (▶) for that scope.
4. Check the **Summary** page (click **Summary** in the navigation pane). The discovery is shown in the **Job Summary** pane. The **Summary** page periodically refreshes to show the current state of TSA. Once the job is no longer listed in the **Job Summary** pane, check the **Activity Log** (click **Activity Log** in the navigation pane). The discovery should complete without errors.

Running the discovery on VMWare Dynamic Scopes

Procedure

1. In the navigation pane, click **Discovery Scopes** > **VMWare Dynamic Scopes**. The **VMWare Dynamic Scopes** page is displayed.



VMware Dynamic Scopes

Users can define VMware Dynamic Scopes to collect detailed inventory from VMware vCenter Server and VMware ESXi. In addition to retrieving inventory information from the defined VMware vCenter Server or ESXi, TSA also queries managed virtual machines dynamically, without requiring users to create and maintain multiple scope definitions.

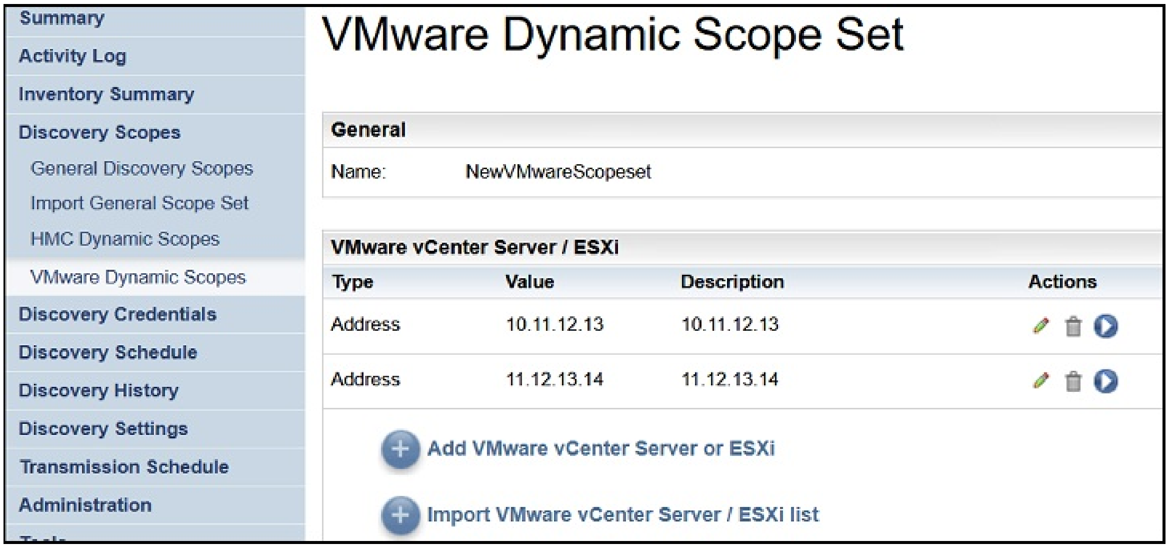
VMware Dynamic Scopes

Name	Actions
NewVMwareScopeset	✎ 🗑 🟩 ▶
dyVM_Scope	✎ 🗑 🟩 ▶

Figure 70. VMWare Dynamic Scopes

2. Click the scope set that contains the scope to be discovered.

   The **VMWare Dynamic Scope Set** page is displayed. This page displays all the scopes that are defined for that scope set.



VMware Dynamic Scope Set

General

Name: NewVMwareScopeset

VMware vCenter Server / ESXi

Type	Value	Description	Actions
Address	10.11.12.13	10.11.12.13	✎ 🗑 ▶
Address	11.12.13.14	11.12.13.14	✎ 🗑 ▶

Figure 71. Run discovery on VMware dynamic scopes

3. To run a discovery on a specific scope, click the **Run** (▶) icon for that scope.
4. Check the **Summary** page (click **Summary** in the navigation pane). The discovery is shown in the **Job Summary** pane. The **Summary** page periodically refreshes to show the current state of TSA. Once the job is no longer listed in the **Job Summary** pane, check the **Activity Log** (click **Activity Log** in the navigation pane). The discovery should complete without errors.

Discovery history

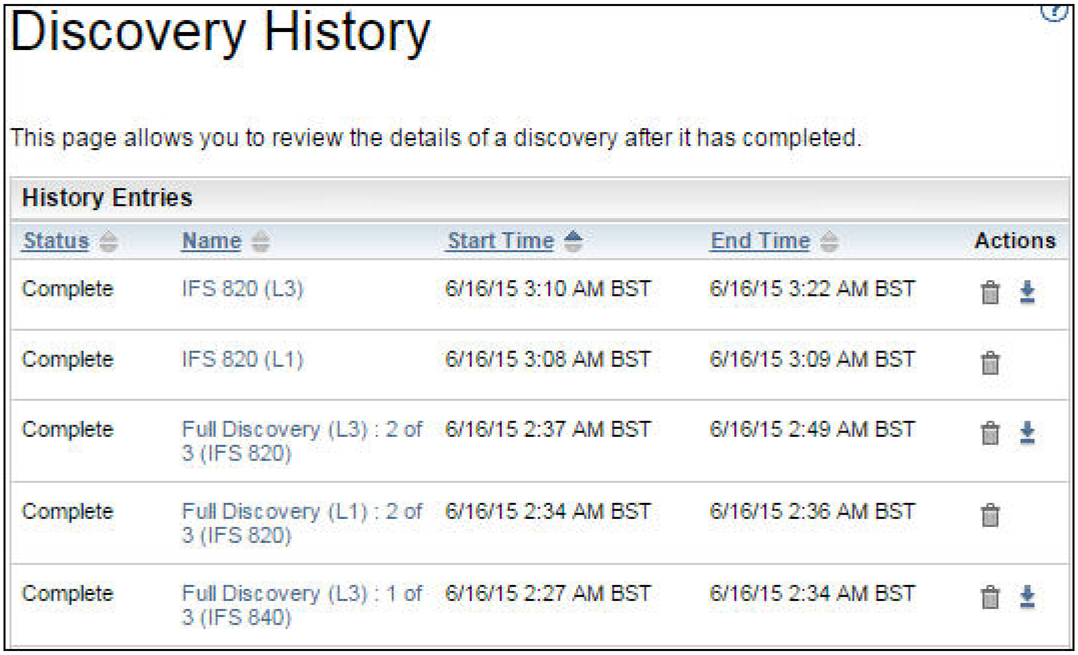
You can view the details of a discovery after it completes and download a diagnostics log file for the discovery.

Procedure

To view the discovery history or download a diagnostics log file, follow these steps:

1. In the navigation pane, click **Discovery History**.

   The **Discovery History** page is displayed. A list of discovery entries is displayed. Each entry displays the status, name, and the start and end times for a discovery.



Discovery History

This page allows you to review the details of a discovery after it has completed.

History Entries

Status	Name	Start Time	End Time	Actions
Complete	IFS 820 (L3)	6/16/15 3:10 AM BST	6/16/15 3:22 AM BST	🗑 ⬇
Complete	IFS 820 (L1)	6/16/15 3:08 AM BST	6/16/15 3:09 AM BST	🗑
Complete	Full Discovery (L3) : 2 of 3 (IFS 820)	6/16/15 2:37 AM BST	6/16/15 2:49 AM BST	🗑 ⬇
Complete	Full Discovery (L1) : 2 of 3 (IFS 820)	6/16/15 2:34 AM BST	6/16/15 2:36 AM BST	🗑
Complete	Full Discovery (L3) : 1 of 3 (IFS 840)	6/16/15 2:27 AM BST	6/16/15 2:34 AM BST	🗑 ⬇

Figure 72. Discovery History

2. To display more information about an entry in the **History Entries** list, click the name of the history entry.

   The **Entry information** pane displays information about the selected discovery.

3. To download a diagnostics log file for a discovery, click the **Download** (⬇) icon for the discovery.
4. To delete a diagnostics log file for a discovery, click the **Delete** (🗑) icon for the discovery.

Transmission schedule

Transmission of data is scheduled to ensure that discovered data is regularly sent to IBM Support. You can view the transmission schedule and the details of the last transmissions, modify the transmission schedule, and disable scheduled transmissions. You can also send the data to IBM whenever you choose.

Viewing the transmission schedule

You can view the summary information about a transmission schedule.

About this task

To view the transmission schedule, follow these steps:

Procedure

In the navigation pane, click **Transmission Schedule**.

The **Transmission Schedule** page is displayed.

The **Schedule** pane displays the next scheduled run and the scheduled run times. The **History** pane displays the status and additional details of the currently running and previous transmission jobs.

Modifying the transmission schedule

TSA provides a default schedule for the transmission process to run at specified times. You can modify this schedule according to your needs.

Procedure

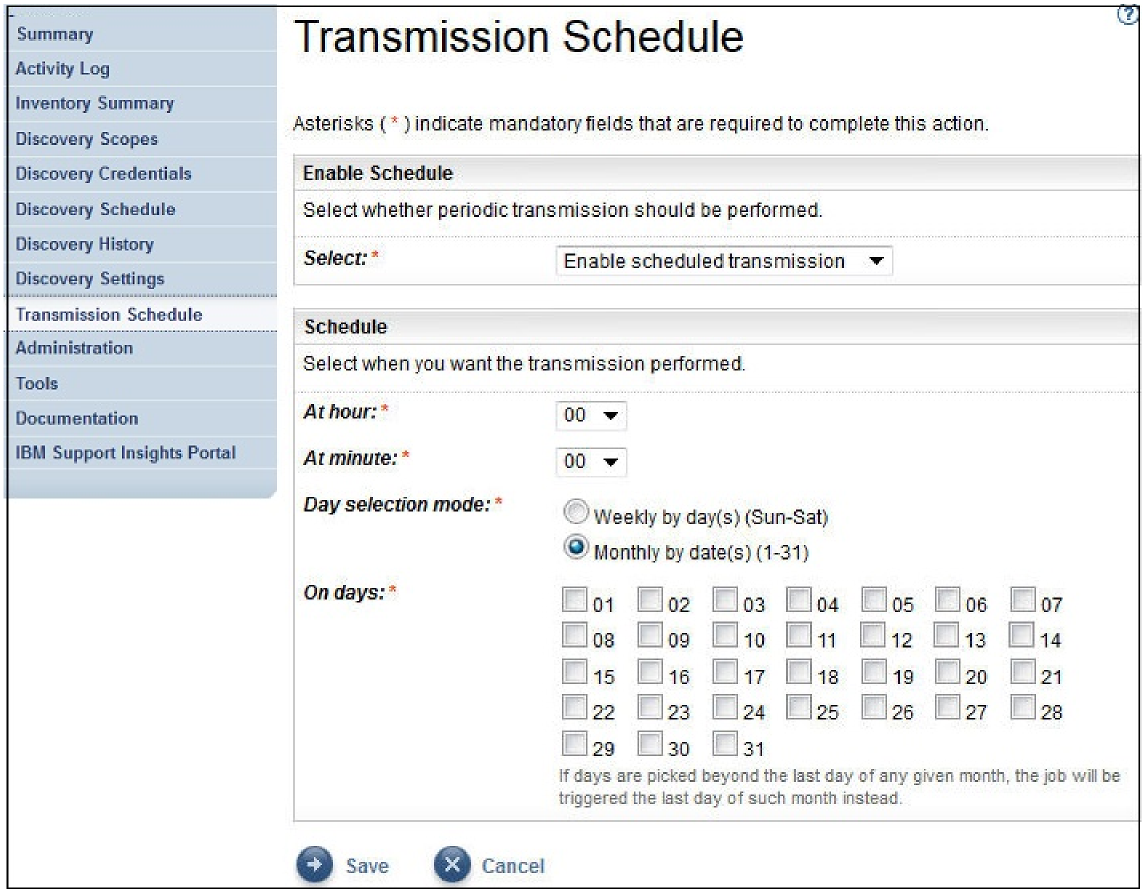
1. In the navigation pane, click **Transmission Schedule**.

   The **Transmission Schedule** page is displayed.

   The **Schedule** pane displays the next scheduled run and the scheduled run times. The **History** pane displays the status and additional details of the currently running and previous transmission jobs.

2. Click **Edit Schedule**.

   The **Transmission Schedule** page is displayed.



Transmission Schedule

Asterisks (*) indicate mandatory fields that are required to complete this action.

Enable Schedule

Select whether periodic transmission should be performed.

Select: * Enable scheduled transmission

Schedule

Select when you want the transmission performed.

At hour: * 00

At minute: * 00

Day selection mode: *
○ Weekly by day(s) (Sun-Sat)
● Monthly by date(s) (1-31)

On days: *
□ 01 □ 02 □ 03 □ 04 □ 05 □ 06 □ 07
□ 08 □ 09 □ 10 □ 11 □ 12 □ 13 □ 14
□ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21
□ 22 □ 23 □ 24 □ 25 □ 26 □ 27 □ 28
□ 29 □ 30 □ 31

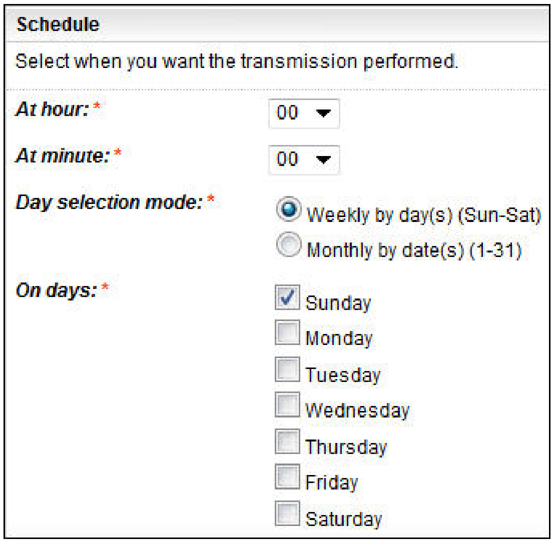
If days are picked beyond the last day of any given month, the job will be triggered the last day of such month instead.

Figure 73. Edit transmission schedule

   a) Use the **At hour** and **At minute** drop-down lists to select a new time.

   b) Select the **Day Selection mode**.

   Weekly by day(s) (Sun - Sat)
   To schedule the transmission on a particular day(s) of a week, select the **Weekly by day(s) (Sun - Sat)** option.



Schedule

Select when you want the transmission performed.

At hour: *	00 ▾
At minute: *	00 ▾
Day selection mode: *	● Weekly by day(s) (Sun-Sat) ○ Monthly by date(s) (1-31)
On days: *	☑ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Figure 74. Weekly by day(s) (Sun - Sat)

For the **On days** field, select the appropriate check box to select one or more days of the week.

Monthly by date(s) (1-31)

To schedule the transmission on particular days of a month, select **Monthly by date(s) (1-31)** option.

For the **On days** field, select the appropriate check box to select one or more days of the month.

Note: If you select the days beyond the last day of a specific month, then the job is triggered on the last day of that particular month.

3. Click **Save**.

   The **Transmission Schedule** page is displayed again, with the new schedule shown.

Disabling the transmission schedule

You can disable scheduled data transmissions.

Procedure

To disable scheduled transmissions, follow these steps:

1. In the navigation pane, click **Transmission Schedule**.

   The **Transmission Schedule** page is displayed.
2. Click **Edit Schedule**.

   The **Transmission Schedule** page is displayed.
3. In the **Enable Schedule** pane, select **Disable scheduled transmission**.
4. Click **Save**.

   The **Discovery Schedule** page is displayed and the **Schedule** pane shows that the scheduled discovery is disabled. You can enable scheduled transmissions by clicking **Enable scheduled transmission**.

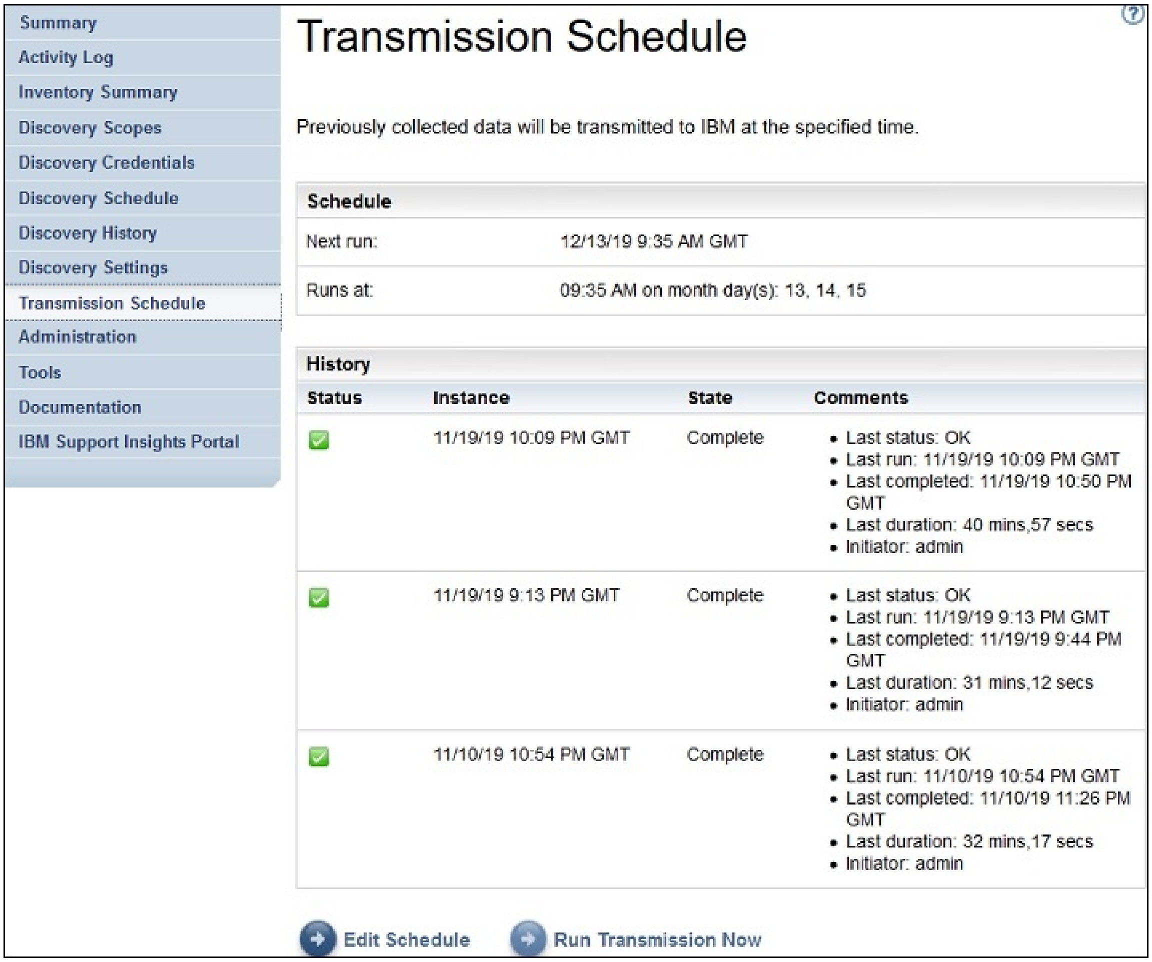
Running the transmission

You can run a transmission on demand, rather than wait for the next scheduled transmission.

Procedure

1. In the navigation pane, click **Transmission Schedule**.

   The **Transmission Schedule** page is displayed.



Transmission Schedule

Previously collected data will be transmitted to IBM at the specified time.

Schedule

Next run:	12/13/19 9:35 AM GMT
Runs at:	09:35 AM on month day(s): 13, 14, 15

History

Status	Instance	State	Comments
✓	11/19/19 10:09 PM GMT	Complete	• Last status: OK • Last run: 11/19/19 10:09 PM GMT • Last completed: 11/19/19 10:50 PM GMT • Last duration: 40 mins,57 secs • Initiator: admin
✓	11/19/19 9:13 PM GMT	Complete	• Last status: OK • Last run: 11/19/19 9:13 PM GMT • Last completed: 11/19/19 9:44 PM GMT • Last duration: 31 mins,12 secs • Initiator: admin
✓	11/10/19 10:54 PM GMT	Complete	• Last status: OK • Last run: 11/10/19 10:54 PM GMT • Last completed: 11/10/19 11:26 PM GMT • Last duration: 32 mins,17 secs • Initiator: admin

Figure 75. Run Transmission Now

2. Click **Run Transmission Now**.

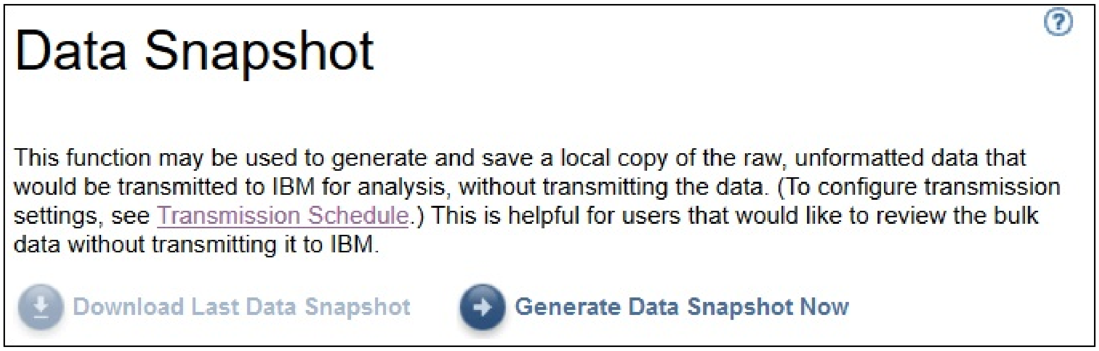
   The **History** pane is updated indicating that the transmission is running.

3. Check the **Summary** page (click **Summary** in the navigation pane). The transmission is shown in the **Job Summary** pane. The **Summary** page periodically refreshes to show the current state of TSA. Once the job is no longer listed in the **Job Summary** pane, check the **Activity Log** (click **Activity Log** in the navigation pane). The transmission should complete without errors.

Data Snapshot

You can generate and save a local copy of the raw, unformatted data that is collected by TSA without transmitting the data to IBM. You can also view the last data that was transmitted to IBM.

1. In the navigation pane, click **Administration** > **Data Snapshot**. The **Data Snapshot** page is displayed.



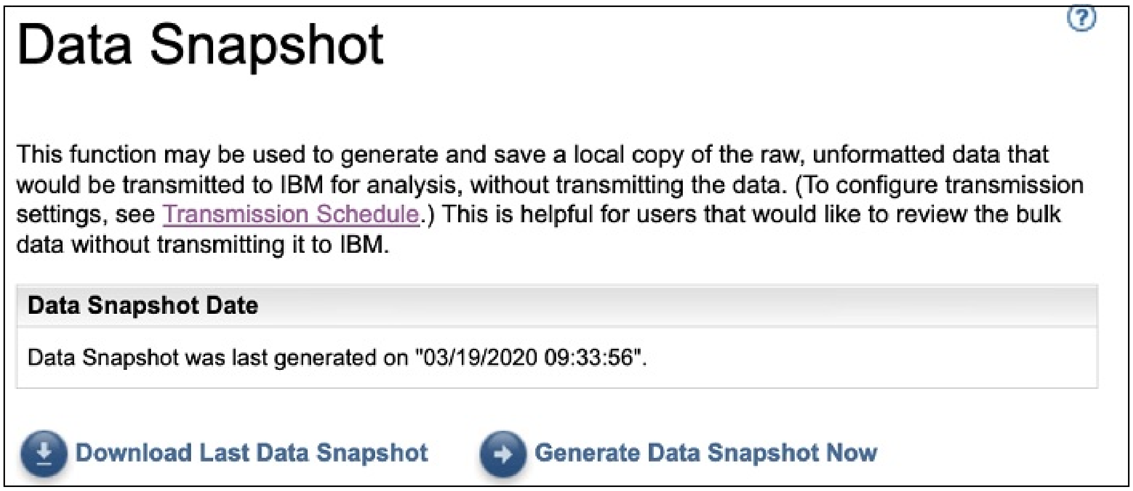
Data Snapshot

This function may be used to generate and save a local copy of the raw, unformatted data that would be transmitted to IBM for analysis, without transmitting the data. (To configure transmission settings, see Transmission Schedule.) This is helpful for users that would like to review the bulk data without transmitting it to IBM.

Figure 76. Data Snapshot

Note: The **Download Last Data Snapshot** button is only enabled when a completed transmission or data snapshot exists.

2. Click **Generate Data Snapshot Now** to collect the latest discovered data by TSA and generate a new data snapshot. The following message is displayed - `Data Snapshot in progress. This could take up to 2 hours. View Activity log or Summary page for status.` Click **Summary** in the navigation menu to view the **Summary** page. The **Job Summary** pane shows the status of the data snapshot collection until it completes. Click **Activity Log** in the navigation menu to view the completion status of the data snapshot request.
3. If the transmission or data snapshot service is completed, then the **Data Snapshot Date** is displayed.



Data Snapshot

This function may be used to generate and save a local copy of the raw, unformatted data that would be transmitted to IBM for analysis, without transmitting the data. (To configure transmission settings, see Transmission Schedule.) This is helpful for users that would like to review the bulk data without transmitting it to IBM.

Data Snapshot Date

Data Snapshot was last generated on "03/19/2020 09:33:56".

Figure 77. Data Snapshot Date

4. Click **Download Last Data Snapshot** to download the latest data snapshot. Specify a location for the resultant file (*collection.tar.xz*). Depending on the amount of data, the download operation might take some time. For extracting the contents of the *.tar.xz* archive, use either the *tar* utility (for Linux) or the *7-Zip* utility (available both for Linux and Windows).

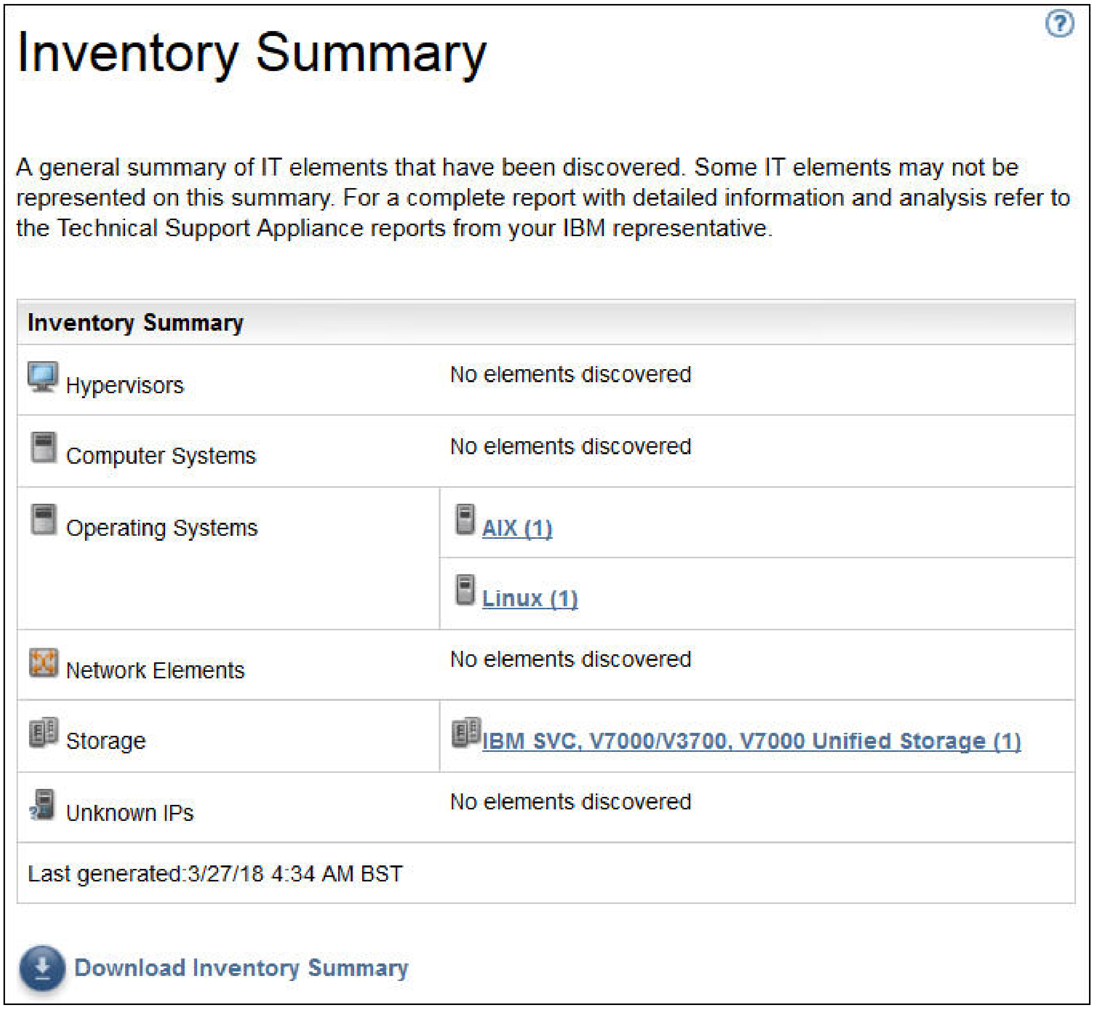
   Note:

   - If a transmission or collection job is in progress, then the following message is displayed - `A collection job is currently running. The latest data snapshot was generated on <<timestamp>>. Are you sure you want to download the collection?`.
     - Click **OK** to proceed with the download.
     - Click **Cancel** to cancel the download and wait for the currently running collection job to complete.
   - If a transmission or collection job is not in progress, then the following message is displayed - `The latest data snapshot was generated on <<timestamp>>. Are you sure you want to download the collection?`. Click **OK** to proceed with the download.

Viewing the inventory summary

Use the **Inventory Summary** page to view the summary of IT elements, such as computer systems, operating systems, and storage subsystems that are discovered.

Click the **Inventory Summary** in the navigation pane to display the **Inventory Summary** page.



Inventory Summary

A general summary of IT elements that have been discovered. Some IT elements may not be represented on this summary. For a complete report with detailed information and analysis refer to the Technical Support Appliance reports from your IBM representative.

Inventory Summary	
Hypervisors	No elements discovered
Computer Systems	No elements discovered
Operating Systems	AIX (1)
	Linux (1)
Network Elements	No elements discovered
Storage	IBM SVC, V7000/V3700, V7000 Unified Storage (1)
Unknown IPs	No elements discovered
Last generated:3/27/18 4:34 AM BST	

Download Inventory Summary

Figure 78. Inventory Summary

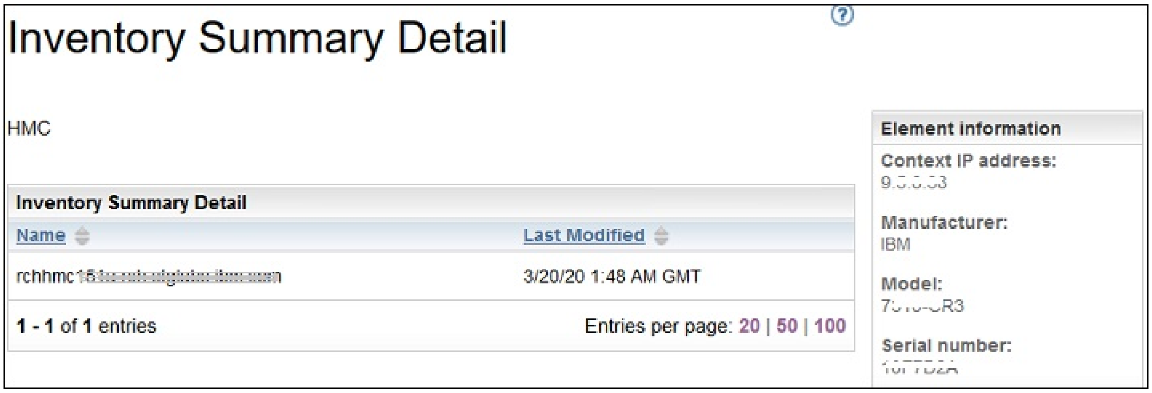
The Inventory Summary page shows six different groups of IT elements:

- **Hypervisors**: Includes hypervisors such as HMC, IBM Flex System Manager, VMware, VIOS, etc.
- **Computer Systems**: Includes physical computer systems.
- **Operating Systems**: Includes operating systems such as AIX, Linux, etc. running on bare metal or in a virtualized environment.
- **Network Elements**: Includes switches and routers.
- **Storage**: Includes storage subsystems such as IBM XIV, IBM FlashSystem, EMC, and HP storage devices. In addition, it also includes tape devices.
- **Unknown IPs**: Devices that might not be classified for reasons including the following:
  - Firewall blocking access to the device.
  - No credentials defined for the device. View the **Authentication Status** page (**Tools** → **Authentication Status**) for information about IP addresses and associated credentials.
  - No sensor exists for the device type.
- The **Last generated** row indicates the last time when the inventory summary job completed.

Note: The data on this pane is displayed shortly after TSA is started. If you view the page in this time gap, an informational message is displayed: `Inventory summary generation in progress`. After the summary information is initially populated, it is refreshed approximately every 30 minutes. To refresh manually, click the **Refresh** icon of the browser.

Each group displays the list of device types and the count for each of the device type.

1. Click any of the device type hyperlinks to view the **Inventory Summary Detail** page.



Inventory Summary Detail

HMC

Inventory Summary Detail

Name	Last Modified
rchhmc1[redacted]	3/20/20 1:48 AM GMT

1 - 1 of 1 entries

Entries per page: 20 | 50 | 100

Element information

Context IP address:
9.[redacted]3

Manufacturer:
IBM

Model:
7[redacted]R3

Serial number:
[redacted]

Figure 79. Inventory Summary Detail

2. Select any of the devices in the list to view the **Element information** such as *Context IP address*, *Manufacturer*, *Model*, and *Serial number*.

   Note: For devices that are detected by TSA but for which no valid credentials were defined, the **Element information** is not filled in. TSA requires a successful login to the device in order to provide these details.

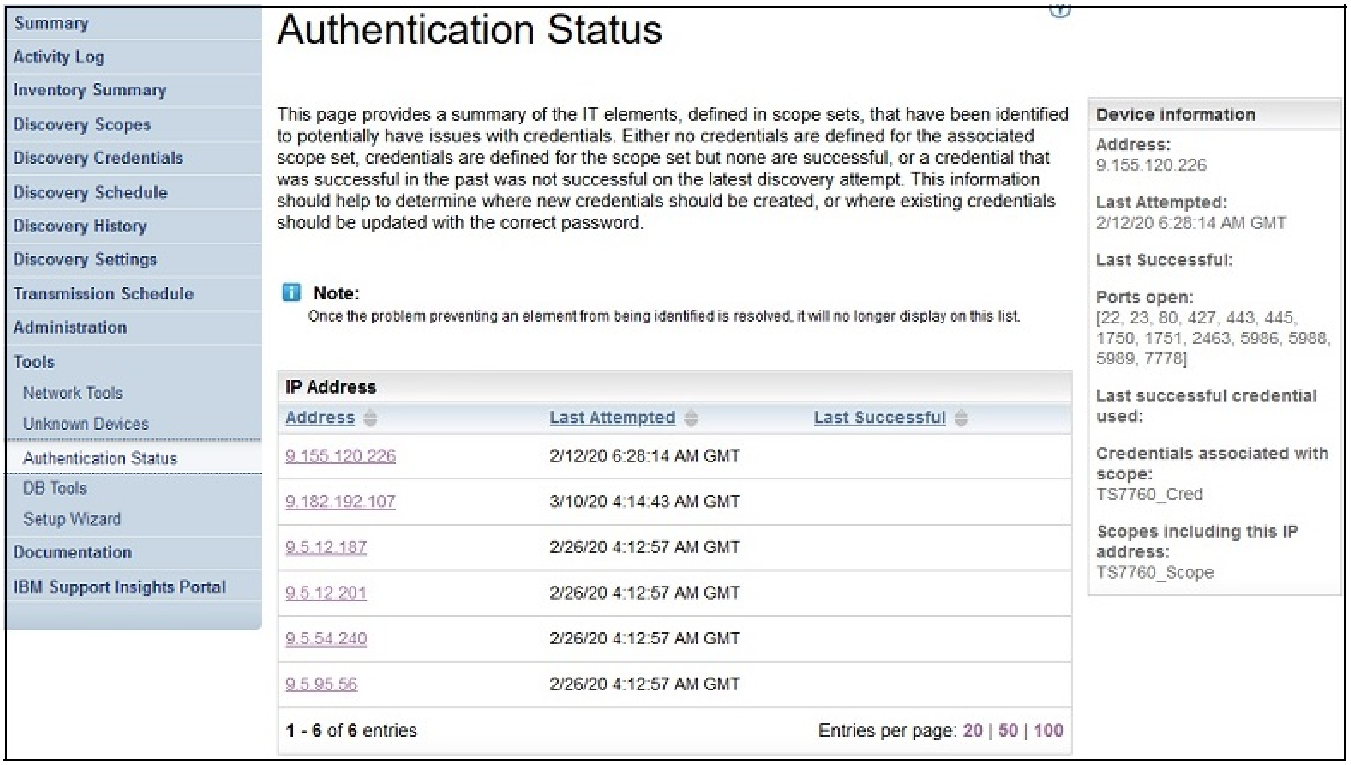
Click **Download Inventory Summary** to download a file containing a summary of the devices that are discovered.

Debug of discovery problems

Authentication Status

Use the **Authentication Status** page to view a summary of the IT elements which are defined in scope sets and are having issues with credentials.

To view the authentication status, click **Tools** > **Authentication Status** in the navigation pane. The **Authentication Status** page is displayed.



Authentication Status

This page provides a summary of the IT elements, defined in scope sets, that have been identified to potentially have issues with credentials. Either no credentials are defined for the associated scope set, credentials are defined for the scope set but none are successful, or a credential that was successful in the past was not successful on the latest discovery attempt. This information should help to determine where new credentials should be created, or where existing credentials should be updated with the correct password.

Note:
Once the problem preventing an element from being identified is resolved, it will no longer display on this list.

IP Address

Address	Last Attempted	Last Successful
9.155.120.226	2/12/20 6:28:14 AM GMT	
9.182.192.107	3/10/20 4:14:43 AM GMT	
9.5.12.187	2/26/20 4:12:57 AM GMT	
9.5.12.201	2/26/20 4:12:57 AM GMT	
9.5.54.240	2/26/20 4:12:57 AM GMT	
9.5.95.56	2/26/20 4:12:57 AM GMT	

1 - 6 of **6** entries Entries per page: 20 | 50 | 100

Device information

Address:
9.155.120.226

Last Attempted:
2/12/20 6:28:14 AM GMT

Last Successful:

Ports open:
[22, 23, 80, 427, 443, 445, 1750, 1751, 2463, 5986, 5988, 5989, 7778]

Last successful credential used:

Credentials associated with scope:
TS7760_Cred

Scopes including this IP address:
TS7760_Scope

Figure 80. Authentication Status

The status displays all the device IPs that reported issues with credentials. The issues might be due to any of the following reasons:

- Credentials are not defined for the associated scope set.
- Credentials are defined for the scope set but are not successful.
- Credentials that were successful in the past are not successful on the most recent discovery attempt.

Click the respective IP address link to view the device information such as *Last Attempted*, *Last successful*, *Ports Open*, *Last successful credential used*, *Date credential was last changed*, *Credential associated with scope*, and *Scopes including this IP address*. This information is helpful in determining where new credentials are to be created, or where existing credentials need to be updated with the correct password.

Note: When the credential issue is resolved for a device, the respective device IP is not displayed in the list.

Unknown Devices

You can display information about devices that TSA has discovered, but is not able to fully identify.

To display these unknown devices, click **Tools** > **Unknown Devices** in the navigation pane. The **Unknown Devices** page is displayed.

You can click any entry in the Unknown IPs list to display additional information about that device.

Chapter 6. Setting up administrative tasks

Status information

TSA provides summary information, logs, and reports to enable you to quickly find information about jobs, discovered inventory, and product information.

You can display the high level summary information about jobs, inventory, and product information by clicking **Summary** in the navigation pane. The **Summary** page refreshes frequently to show the most up-to-date summary information. The **Summary** page includes the following information:

- **System Status**

  The **System Status** pane displays the status of current services and tasks being performed. You can display the pages for the services displayed by clicking the name of the service in the **System Status** pane.

- **Job Summary**

  The **Job Summary** pane displays a summary of current jobs.

- **Inventory Summary**

  The **Inventory Summary** pane displays a list of discovered inventory.

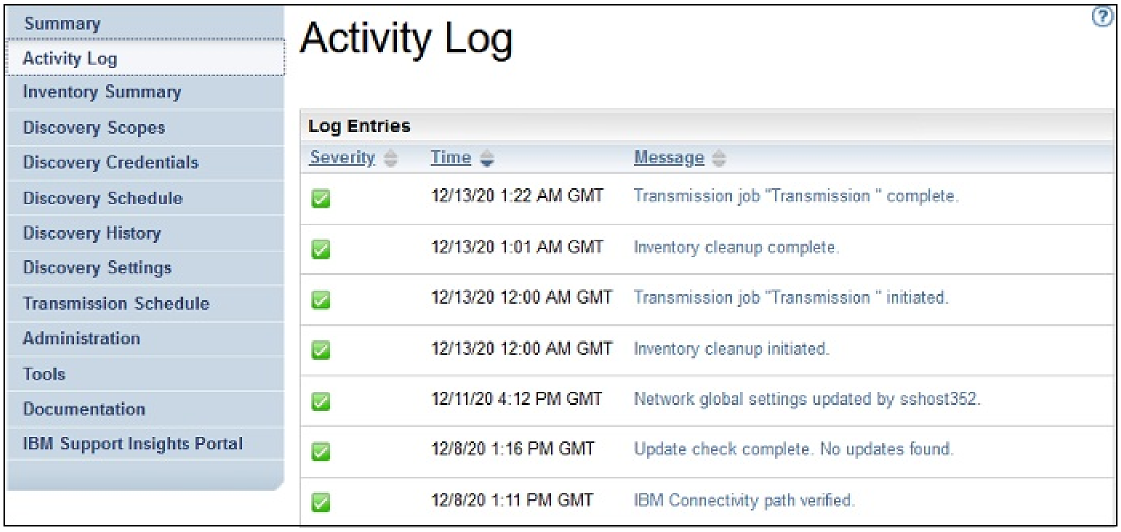
- **Product Information**

  The **Product Information** pane displays the host name and ID of TSA.

Viewing the activity log

The activity log displays log messages for the discovery and transmission processes. You can click the entries in the activity log to view more information.

You can display the activity log by clicking **Activity Log** in the navigation pane. A list of log entries is displayed. Each entry displays the message, the severity, and the time the activity occurred.



Activity Log

Log Entries

Severity	Time	Message
✓	12/13/20 1:22 AM GMT	Transmission job "Transmission " complete.
✓	12/13/20 1:01 AM GMT	Inventory cleanup complete.
✓	12/13/20 12:00 AM GMT	Transmission job "Transmission " initiated.
✓	12/13/20 12:00 AM GMT	Inventory cleanup initiated.
✓	12/11/20 4:12 PM GMT	Network global settings updated by sshost352.
✓	12/8/20 1:16 PM GMT	Update check complete. No updates found.
✓	12/8/20 1:11 PM GMT	IBM Connectivity path verified.

Figure 81. Activity Log

Note: Because discoveries are run on individual scope sets, there might be multiple log entries for a full discovery.

To display extended details about any activity log entry, click the message for that entry.

To save the log files to your computer, click **Download All Logs**.

To clear the log, click **Clear Log**.

Viewing inventory cleanup archive

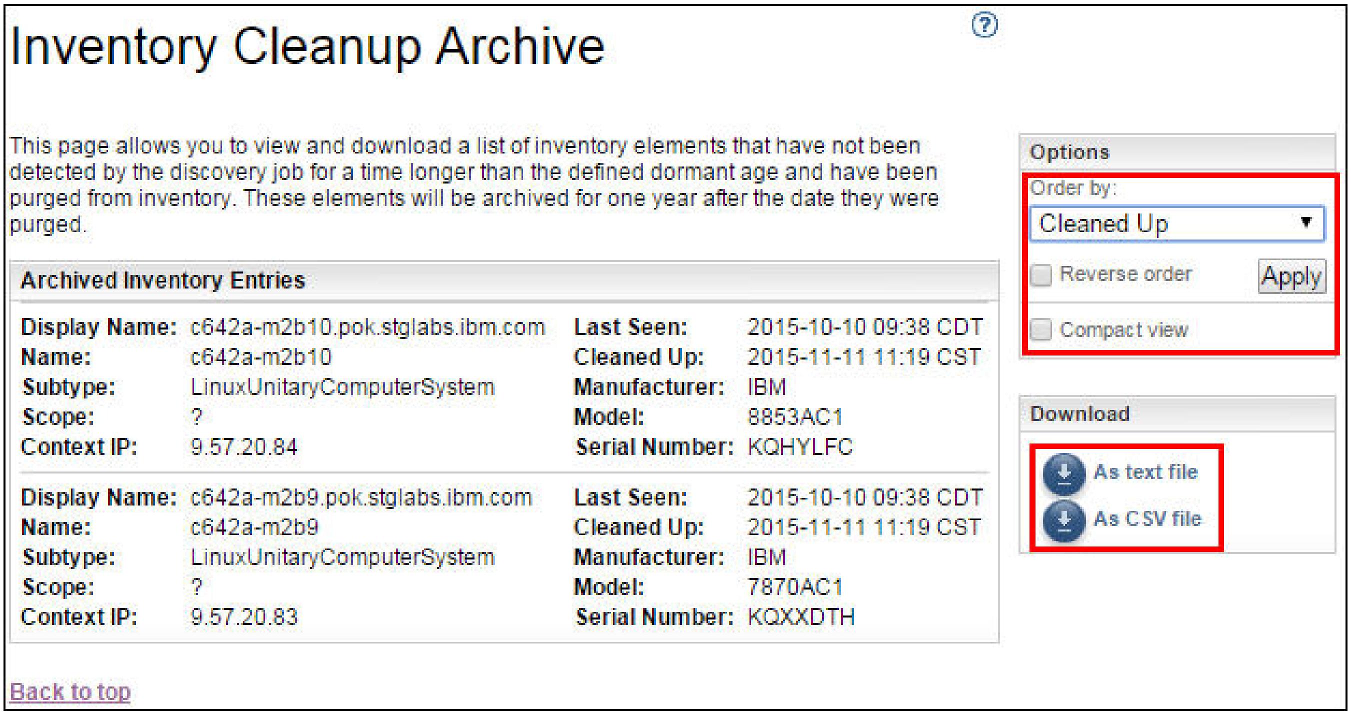
You can view the inventory that is cleaned up according to the dormant age that you specified in the **Inventory Cleanup Schedule**

About this task

To view the deleted inventory, follow these steps:

Procedure

1. On the **Inventory Cleanup Schedule** page, click **Show Cleanup Archive**. The **Inventory Cleanup Archive** page displays.



Inventory Cleanup Archive

This page allows you to view and download a list of inventory elements that have not been detected by the discovery job for a time longer than the defined dormant age and have been purged from inventory. These elements will be archived for one year after the date they were purged.

Archived Inventory Entries

Display Name:	c642a-m2b10.pok.stglabs.ibm.com	**Last Seen:**	2015-10-10 09:38 CDT
Name:	c642a-m2b10	**Cleaned Up:**	2015-11-11 11:19 CST
Subtype:	LinuxUnitaryComputerSystem	**Manufacturer:**	IBM
Scope:	?	**Model:**	8853AC1
Context IP:	9.57.20.84	**Serial Number:**	KQHYLFC
Display Name:	c642a-m2b9.pok.stglabs.ibm.com	**Last Seen:**	2015-10-10 09:38 CDT
Name:	c642a-m2b9	**Cleaned Up:**	2015-11-11 11:19 CST
Subtype:	LinuxUnitaryComputerSystem	**Manufacturer:**	IBM
Scope:	?	**Model:**	7870AC1
Context IP:	9.57.20.83	**Serial Number:**	KQXXDTH

Back to top

Options

Order by: Cleaned Up ▾

□ Reverse order Apply

□ Compact view

Download

As text file

As CSV file

Figure 82. Inventory Cleanup Archive

2. On the **Inventory Cleanup Archive** page, you can view the elements that are purged from the inventory as part of a cleanup process.

   Note:

   - You can see the inventory information in this archive only for one year. After a year, the archive information is purged.
   - The archive will be empty (that is no objects are cleaned up), if all the defined targets are being actively discovered within the last year.

3. Use the **Options** pane to reorder the inventory details.

   a) Select the **Order by** property in the **Options** pane and click **Apply** to order the view of the inventory details.

   b) Select the **Reverse order** option to view the details in the reverse order of the selected property.

   c) Select the **Compact view** option to view a summary of the inventory.

4. Click **As text file** or **As CSV file** to download the inventory details. Save the inventory details to handle the data locally and also preserve the data on your computer for a longer period (more than a year). The data that is preserved in this archive is maintained only for a year and then it is purged.

Passwords

You use passwords to secure TSA user accounts.

Changing your password

Change TSA user password.

Procedure

1. In the navigation pane, click **Administration** > **Password**.
   The **Password** page is displayed.
2. Enter your current password in the **Current password** field.
3. Enter the new password in the **New password** field.

   The password must adhere to the following rules:

   - Must be at least 8 characters long
   - Must contain at least one alphabetic and one non-alphabetic character
   - Must not contain the user name
   - Must not be the same as any of the previous eight passwords
   - Must be changed at least once every 90 days, but must not be changed more than once each day
4. Enter the new password again in the **Confirm password** field.
   The two passwords that you enter are compared to confirm that they match before the password is saved.
5. Click **Save**.

What to do next

Important: It is not possible to recover a password, so if the password is lost or forgotten, you cannot log in to TSA to change credentials. If you lose or forget your password for a user account or an administrator account (if you have multiple accounts), contact your TSA administrator. If you lose or forget your password for the default administrator account (shipped with TSA), contact IBM Support. For more information, see section "Logging in to the Technical Support Appliance" on page 21.

Security

You can access and modify security functions and utilities for TSA.

The **Security** page lists the available security utilities. On this page, you can modify session timeout settings or modify the maximum password age for all user accounts.

Modifying session timeout settings

For security, the user is logged out of TSA after a period of inactivity. You can prevent TSA from automatically logging out the user or change the amount of time before the user is logged out.

Disabling session timeout

You can prevent TSA from automatically logging the user out after a period of inactivity by disabling session timeout.

Procedure

1. Check the **Disable Session Timeout** check box.
2. Click **Change Session Timeout Settings**.

Modifying the session timeout value

By default, the user is logged out after 20 minutes of inactivity. You can increase the amount of time before the user is logged out by modifying the session timeout value.

Procedure

1. Clear the **Disable Session Timeout** check box.
2. In the **Session timeout** field, enter the time in seconds before TSA logs out the user.

   Note: This session timeout value cannot be less than 20 minutes.
3. Click **Change Session Timeout Settings**.

Modifying the password age

As a security measure, every user is forced to change their TSA login password after a specified number of days. By default, the maximum age of a password is 90 days, but you can change the maximum age for the password to 30 days or 60 days instead.

Procedure

1. In the navigation pane, click **Administration** > **Security**. The **Security** page is displayed.
2. On the **Security** page, scroll down to view the **Maximum Password Age** pane.
3. In the **Maximum Password Age** pane, select the age (30 days, 60 days, or 90 days) from the **Maximum age** drop-down list.
4. Click **Change Maximum Password Age** to update. The confirmation message - *Maximum password age updated.* is displayed.

Backup and restore

You can back up and restore the TSA configuration.

Important: It is highly recommended that you perform a backup on a regular basis. Also, a backup should be performed after changes are made to scope sets or credentials.

Backup date

Displays the date and time at which the most recent backup occurred.

Configuration summary

Use this option to view a summary of the current TSA configuration before you save it.

To display the TSA configuration summary, follow these steps:

1. In the navigation pane, click **Administration** > **Backup and Restore**. The **Backup and Restore** page is displayed.
2. Click **View Summary** to view the current TSA configuration summary. The displayed information shows the configurations that TSA saves if a backup is performed.

   Note: This information is shown via a pop-up window. If your web browser blocks pop-up windows, you might need to allow the browser to display pop-ups from TSA.

   In the **Summary** page, the **Backup** section displays the information related to backup status with the following messages:

   - An *OK* (✅) icon, if the backup last done is within 60 days.
   - A *Warning* (⚠) icon, if backup isn’t done for more than 60 days and less than or equal to 90 days.

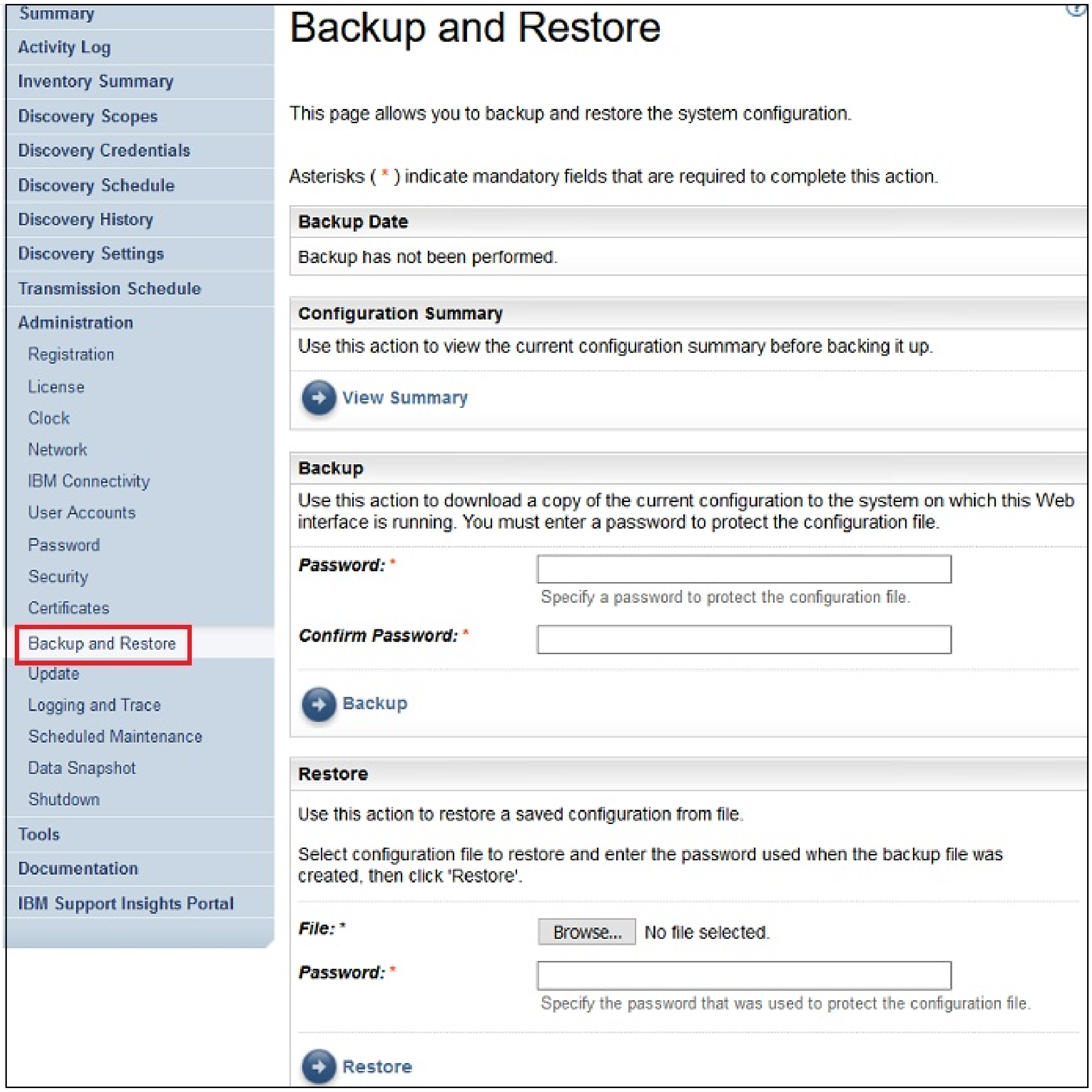
- An *Error* (✖) icon, if backup isn't performed for more than 90 days.

Backup

Use this option to save a copy of the TSA configuration.

To back up the TSA configuration, follow these steps:

1. In the navigation pane, click **Administration** > **Backup and Restore**. The **Backup and Restore** page is displayed.



Backup and Restore

This page allows you to backup and restore the system configuration.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Backup Date

Backup has not been performed.

Configuration Summary

Use this action to view the current configuration summary before backing it up.

View Summary

Backup

Use this action to download a copy of the current configuration to the system on which this Web interface is running. You must enter a password to protect the configuration file.

Password: *
Specify a password to protect the configuration file.

Confirm Password: *

Backup

Restore

Use this action to restore a saved configuration from file.

Select configuration file to restore and enter the password used when the backup file was created, then click 'Restore'.

File: * Browse... No file selected.

Password: *
Specify the password that was used to protect the configuration file.

Restore

Figure 83. Backup and Restore

2. Enter a password in the **Backup** pane to protect the configuration file.
3. Enter the password again in the **Confirm password** field. The two passwords that you enter are compared to confirm that they match before the password is saved.

   Note: You need to save the password securely as it is needed during restore.
4. Click **Backup** and save the backup configuration compressed file on the system.

   Note: The backup configuration file that is generated can be opened only by TSA.

   Note: If you have changed your admin password recently, take a backup after changing the password and use the latest backup file to restore.

Restore

Use this option to restore a previously saved copy of the configuration.

To restore a TSA configuration, follow these steps:

1. In the navigation pane, click **Administration** > **Backup and Restore**. The **Backup and Restore** page is displayed.
2. Click **Choose File** to locate and select the configuration file that you want to restore.
3. Enter the password that is used to backup the configuration file.
4. Click **Restore**.

   The restore job is displayed in the Job Summary pane of the **Summary** page. When the restoration is complete, you are prompted to restart the system.

   Note: Restoring from a backup deletes the existing configurations. All the configurations including scope definitions and credentials are replaced with those from the backup file.

Note: Make sure that the Discovery Manager status is in OK(✅) state in the **Summary** page when performing backup or restore operations. If the Discovery Manager isn't running, you'll get a message - `"Discovery Manager is not running. Please ensure the Discovery Manager status is depicted by the green check mark icon in the Summary screen before resuming activity (typically up to 10 minutes)."` After 10 minutes, if the Discovery Manager isn't running, contact IBM Support.

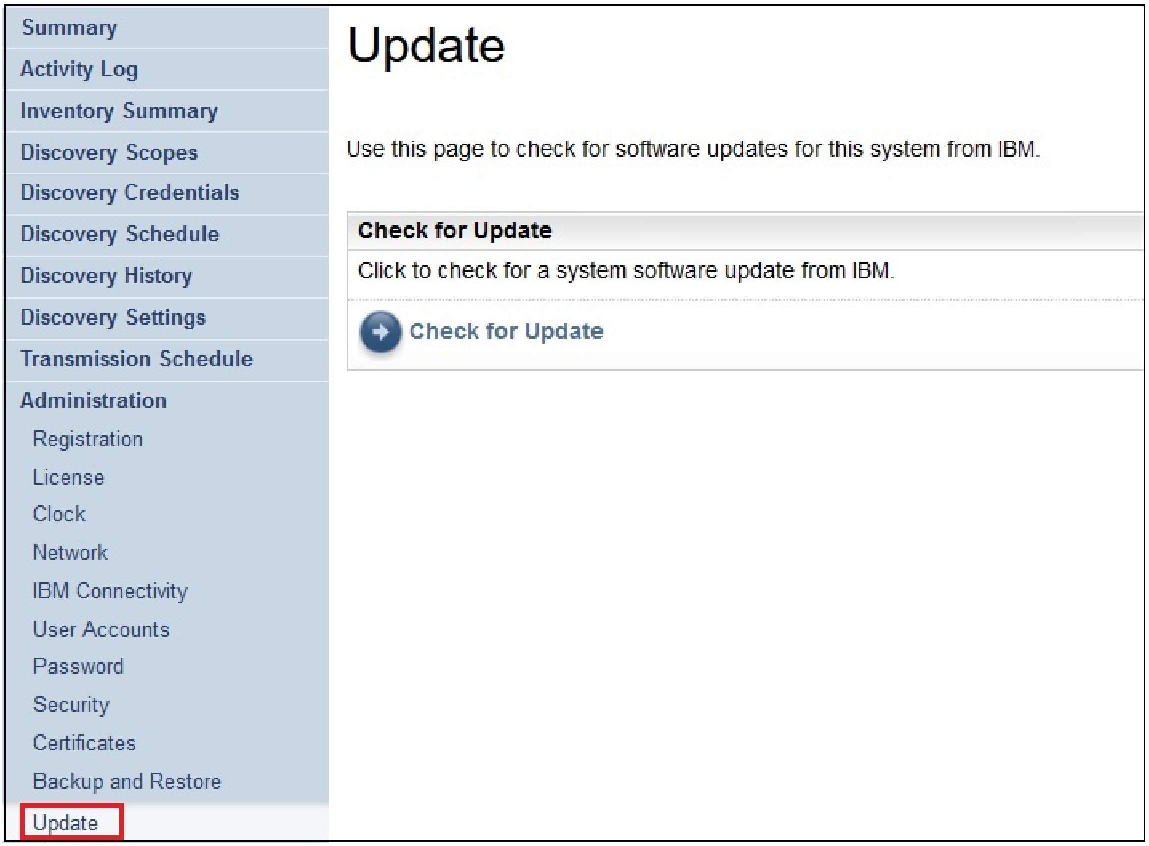
Update

You can check and download updates for TSA.

Procedure

1. In the navigation pane, click **Administration** > **Update**.

   The **Update** page is displayed.



Update

Use this page to check for software updates for this system from IBM.

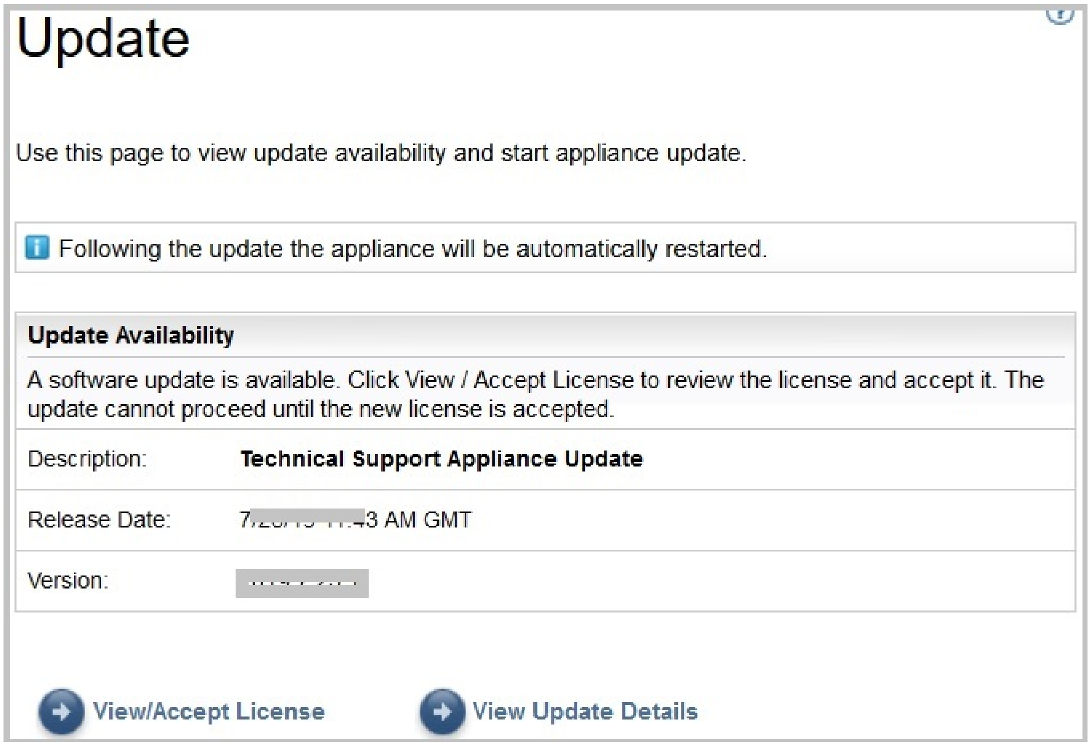
Check for Update

Click to check for a system software update from IBM.

Figure 84. Update

2. Click **Check for Update**.

   The **Update Availability** page lists any available updates.



Update

Use this page to view update availability and start appliance update.

Following the update the appliance will be automatically restarted.

Update Availability

A software update is available. Click View / Accept License to review the license and accept it. The update cannot proceed until the new license is accepted.

Description:	Technical Support Appliance Update
Release Date:	7[redacted]3 AM GMT
Version:	[redacted]

Figure 85. Update availability

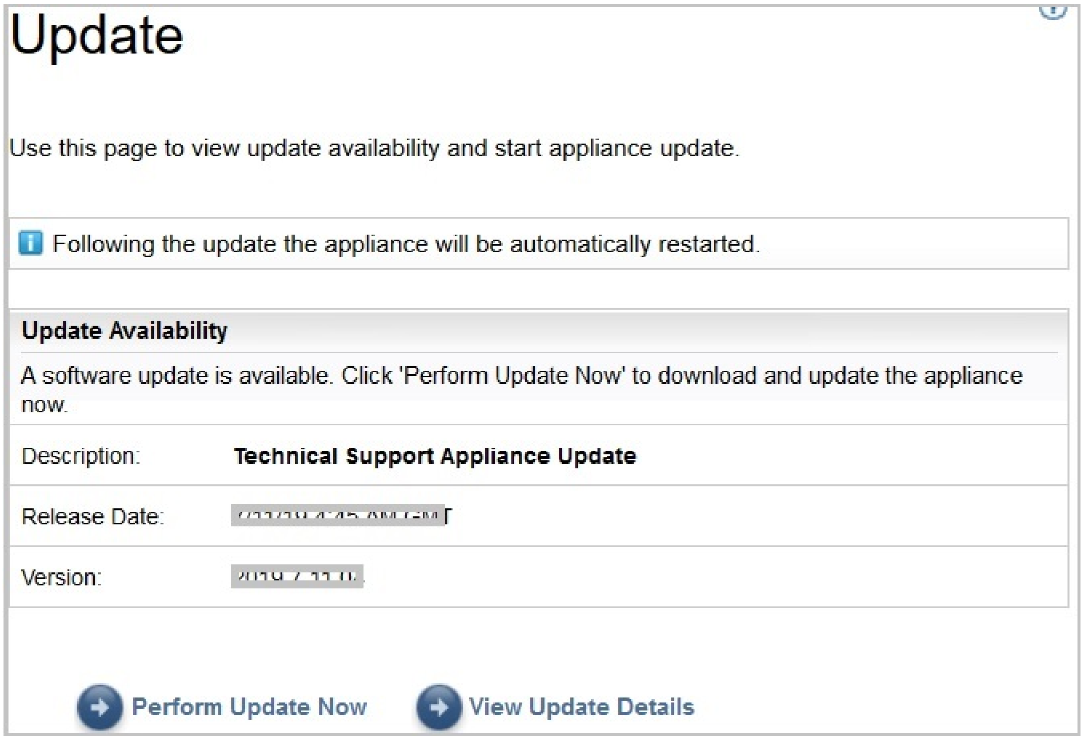
a) For some new releases of TSA, you must accept a new license agreement before proceeding with the update. If there is a new license, click **View/Accept License**, the **License Agreement** page is displayed.

b) Click the **Accept** button on the **License Agreement** page to accept the new license agreement. The **Update** page is displayed again with the **Perform Update Now** button. If there is no requirement to accept a new license agreement, the **View/Accept License** button is not displayed, click **Perform Update Now** to proceed.

Note:

- Once you accept the license, the **View/Accept License** button is no longer displayed.
- In the navigation pane, click **Administration** > **License** to view the latest License Agreement that you have accepted.

c) To install the updates, click **Perform Update Now**.



Update

Use this page to view update availability and start appliance update.

Following the update the appliance will be automatically restarted.

Update Availability

A software update is available. Click 'Perform Update Now' to download and update the appliance now.

Description:	**Technical Support Appliance Update**
Release Date:	[redacted]
Version:	[redacted]

Figure 86. Perform Update Now

Upon completion of the update, TSA is automatically restarted.

d) To view information about the contents of the update, click **View Update Details**.

Enabling scheduled maintenance

To maintain TSA running at optimal performance, it is recommended that the scheduled maintenance feature be enabled.

About this task

The scheduled maintenance job ensures optimal performance of TSA. You can always enable or disable this feature. If you enable scheduled maintenance, you can set the day and time to automatically run the maintenance. The status of the scheduled maintenance is displayed in the **System Status** section of **Summary** page.

If you schedule the maintenance job, the system restarts automatically after the maintenance and you are notified about the system restart an hour before it occurs. For example, `Due to scheduled maintenance, a system restart job will be queued in 59 minute(s).`

Important: Do not schedule the appliance maintenance within 30 minutes of other scheduled jobs, such as Discovery, Transmission, or Inventory Cleanup. If you schedule maintenance within 30 minutes of other scheduled jobs, TSA cannot run these jobs.

Procedure

To edit the maintenance schedule, complete the following steps:

1. In the navigation pane, click **Scheduled Maintenance**.

   The **Scheduled Maintenance** page displays the **Schedule** for next scheduled run and the scheduled run time. The **History** section displays the status and more details of the currently running and previous maintenance jobs.
2. On the **Scheduled Maintenance** page, click **Edit Schedule**.
   a) In the **Enable Schedule** pane, select whether you want to enable or disable scheduled maintenance.
   b) If you choose to enable the scheduled maintenance task, select the **At hour** and **At minute** drop-down lists to select a new time.
   c) Select the **Day Selection mode**. To schedule the maintenance on a particular days of a week, select the **Weekly by day(s) (Sun - Sat)** option or to schedule the maintenance on particular days of a month, select **Monthly by date(s) (1-31)** option.
   d) Select the appropriate check box for the **On days** field, to select different, or additional days of the week or month.

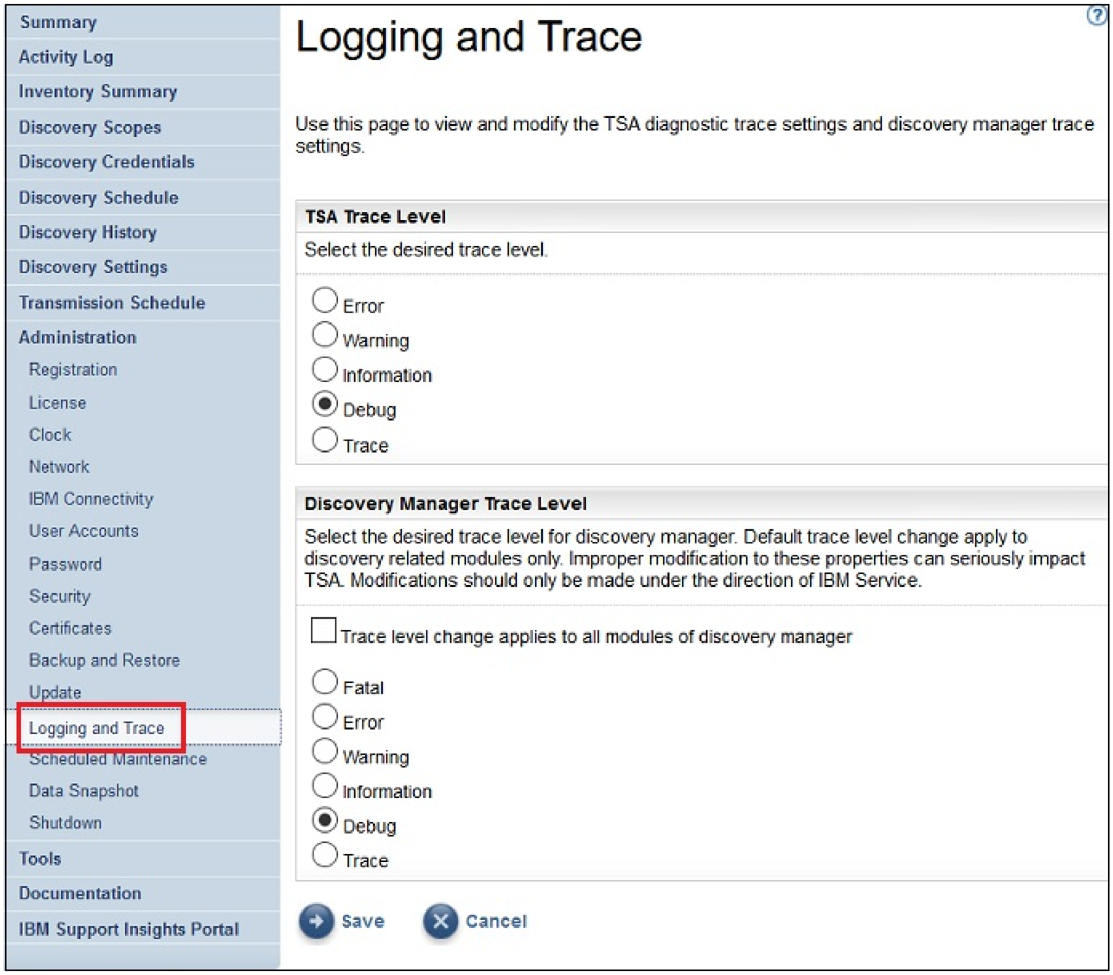
      Note: If you select the days beyond the last day of a specific month, then the job is triggered on the last day of that particular month.
3. Click **Save**.

   The **Scheduled Maintenance** page is displayed again, with the new schedule.

Logging and trace

You can view and modify the TSA diagnostic trace settings. You can also modify settings for the Discovery Manager trace levels. Modifying these settings can affect performance so do this only if directed by IBM Support.

1. In the navigation pane, click **Administration** > **Logging and Trace**. The **Logging and Trace** page is displayed. The **TSA Trace Level** pane shows the current trace setting (Error, Warning, Information, Debug, or Trace).



Logging and Trace

Use this page to view and modify the TSA diagnostic trace settings and discovery manager trace settings.

TSA Trace Level

Select the desired trace level.

○ Error
○ Warning
○ Information
● Debug
○ Trace

Discovery Manager Trace Level

Select the desired trace level for discovery manager. Default trace level change apply to discovery related modules only. Improper modification to these properties can seriously impact TSA. Modifications should only be made under the direction of IBM Service.

□ Trace level change applies to all modules of discovery manager

○ Fatal
○ Error
○ Warning
○ Information
● Debug
○ Trace

Figure 87. Logging and Trace

2. If needed, you can change the trace setting in the **TSA Trace Level** pane, by clicking the radio button beside the trace setting that you want.
3. Click **Save**.

Note: By default the trace level for the *TSA Trace Level* & its *Discovery Manager Trace Level* panes are set to **Debug** level.

To view and modify the **Discovery Manager Trace Level** settings, follow these steps:

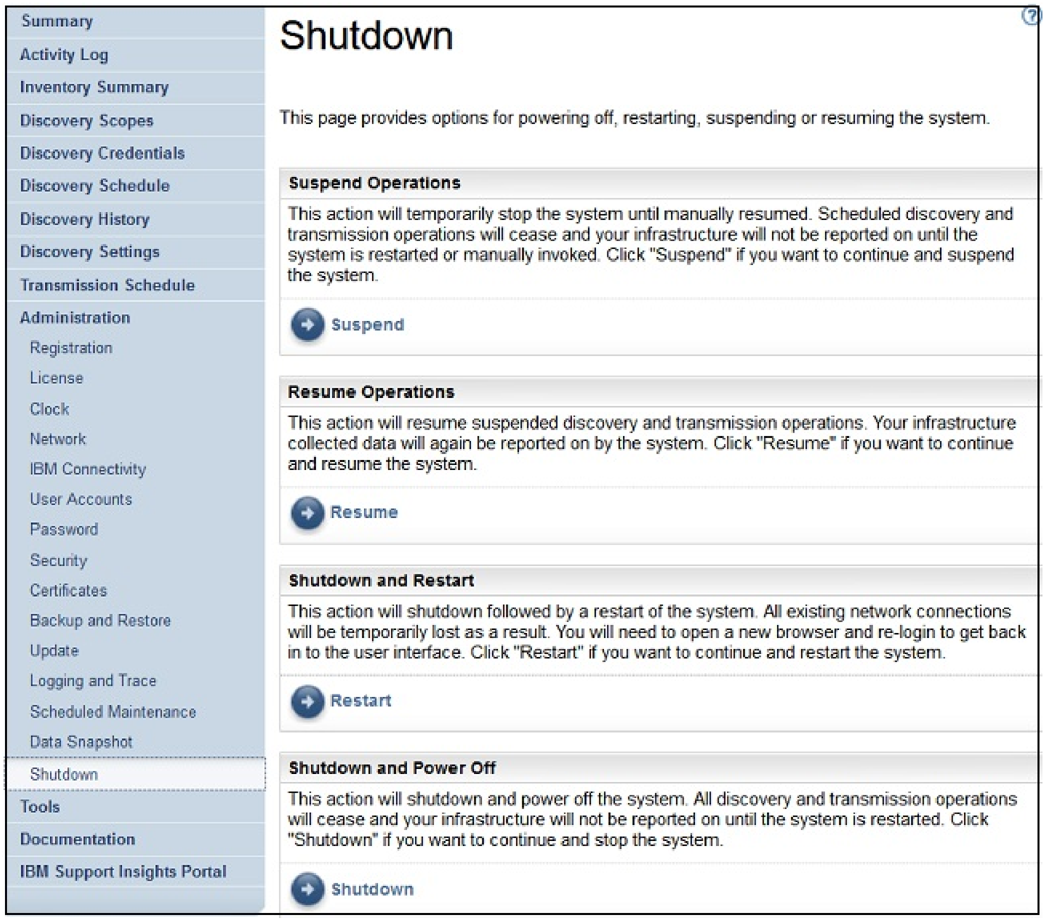
Important: Make modifications to this section only if directed by IBM Service.

1. In the navigation pane, click **Administration** > **Logging and Trace**. The **Logging and Trace** page is displayed indicating the current trace setting.
2. Check **Trace level change applies to all modules of discovery manager** if you want the trace level to be applied to all modules of the Discovery Manager.
3. Select the radio button beside the trace setting that you want.
4. Click **Save**.

Shutdown

You can suspend or resume TSA operations, or shut down and then restart or power off the TSA.

Shutdown takes several minutes to complete.



Shutdown

This page provides options for powering off, restarting, suspending or resuming the system.

Suspend Operations

This action will temporarily stop the system until manually resumed. Scheduled discovery and transmission operations will cease and your infrastructure will not be reported on until the system is restarted or manually invoked. Click "Suspend" if you want to continue and suspend the system.

Resume Operations

This action will resume suspended discovery and transmission operations. Your infrastructure collected data will again be reported on by the system. Click "Resume" if you want to continue and resume the system.

Shutdown and Restart

This action will shutdown followed by a restart of the system. All existing network connections will be temporarily lost as a result. You will need to open a new browser and re-login to get back in to the user interface. Click "Restart" if you want to continue and restart the system.

Shutdown and Power Off

This action will shutdown and power off the system. All discovery and transmission operations will cease and your infrastructure will not be reported on until the system is restarted. Click "Shutdown" if you want to continue and stop the system.

Figure 88. Shutdown

Suspend Operations

This action temporarily stops TSA. All discovery and transmission operations are stopped, and no information is reported to IBM until operations are resumed.

To suspend TSA operations, follow these steps:

1. In the navigation pane, click **Administration** > **Shutdown**. The **Shutdown** page is displayed.
2. Click **Suspend**.

   Note: You can check the status of TSA in the **Summary** page. When TSA is suspended, the **System Status** pane shows that TSA has been suspended.

Resume Operations

This action resumes the temporarily stopped TSA. All discovery and transmission operations are resumed, and information is reported to IBM as scheduled.

To resume TSA operations, follow these steps:

1. In the navigation pane, click **Administration** > **Shutdown**. The **Shutdown** page is displayed.
2. Click **Resume**.

Shutdown and Restart

This action shuts down and then restarts TSA. All existing network connections are temporarily lost. You must open a new browser and login again.

To shut down and restart TSA, follow these steps:

1. In the navigation pane, click **Administration** > **Shutdown**. The **Shutdown** page is displayed.
2. Click **Restart**.

Shutdown and Power Off

This action shuts down and powers off TSA. All discovery and transmission operations cease and your infrastructure is not reported until TSA is restarted.

To shut down and power off the TSA, follow these steps:

1. In the navigation pane, click **Administration** > **Shutdown**. The **Shutdown** page is displayed.
2. Click **Shutdown**.

Note: After you shutdown the appliance, you must power on TSA using the VMware ESXi web interface or Hyper-V Manager.

Tools

TSA provides tools to help you when setting up the TSA environment.

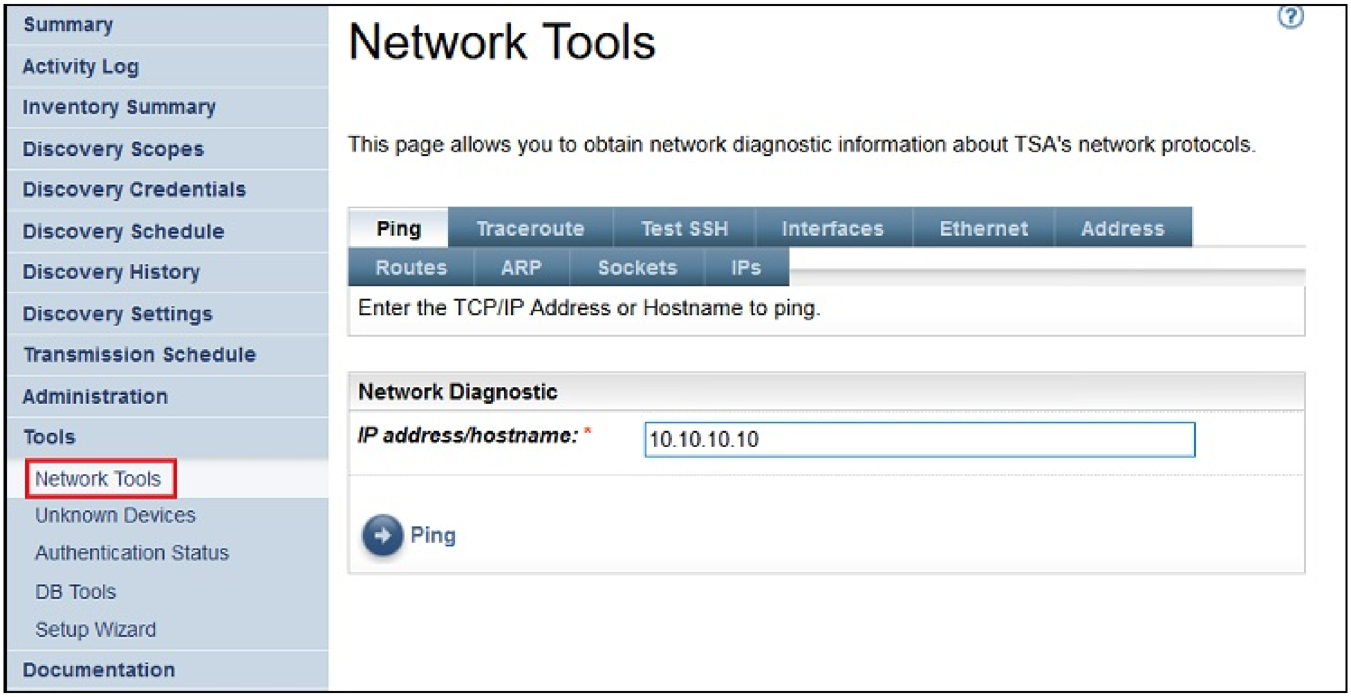
You can access these tools by clicking **Tools** in the navigation pane.

Network Tools

Use the **Network Tools** page to obtain diagnostic tools and information for the network protocols that TSA uses.

To access these diagnostic tools, click **Tools** > **Network Tools** in the navigation pane. The **Network Tools** page is displayed.

The Network Tools page is divided into tabbed pages. Click any tab to display the page that corresponds to that tab.



Network Tools

This page allows you to obtain network diagnostic information about TSA's network protocols.

Enter the TCP/IP Address or Hostname to ping.

Network Diagnostic

IP address/hostname: * 10.10.10.10

Figure 89. Network Tools

Ping
Use this page to send an echo request to a remote host to check if the host is accessible and to receive information about the host name or IP address.

Traceroute
Use this page to display the path that packets take to a remote host.

Test SSH
Use this page to test whether a remote host is accessible with SSH using the discovery credentials defined for the host.

Interfaces
Use this page to display the statistics for the network interfaces that are currently configured.

Ethernet
Use this page to display settings for the Ethernet cards that are currently configured.

Address
Use this page to display the IP addresses for the network interfaces that are currently configured.

Routes
Use this page to display the Kernel IP routing tables and corresponding network interfaces.

ARP
Use this page to display the contents of the Address Resolution Protocol (ARP) connections.

Sockets
Use this page to display information about the TCP/IP sockets.

IPs
Use this page to display information about the IP packet filter rules.

Note: The host name you enter must not contain an underscore ("_").

Database Tools

Use the **Database Tools** page to run data maintenance operations. It is recommended that you use these functions only when directed to do so by IBM Support.

You can run the following operations on the database:

Recreating the inventory database

When you re-create the inventory database, all the inventory data is lost. In addition, the credentials are lost if the **Preserve Credentials** checkbox is cleared or the Discovery Manager is not available.

To re-create the database, complete the following steps:

1. In the navigation pane, click **Tools** > **DB Tools**.
2. Select the **Preserve Credentials and Scopes** checkbox in the **Recreate inventory database** section to maintain all the discovery credentials. If you do not select the **Preserve Credentials and Scopes** option, the credentials and scopes are lost and you need to set up all the credentials and scopes again. For more information about discovery credentials, see "Discovery credentials" on page 73.

   Note: The credentials and scopes can be preserved only if the Discovery Manager is running (green status).
3. Click **Recreate inventory database**. The following warning message is displayed - `Taking this action will temporarily shutdown the Discovery Manager. Are you sure you want to recreate the inventory database?`
4. Click **OK** to re-create the inventory database. The following message is displayed - `Recreate Database Started`. It might take approximately 6 hours to recreate the database, in the meantime, the following message is displayed - `dbinit starting` in the Summary page. After 6 hours, you can check the **Activity Log** to view the status as `Recreate inventory database successful`.

   Note: When re-creating the inventory database, the Discovery Manager shuts down temporarily and the *Inventory Clean-up Archive* is cleared.

Performing RUNSTATS

To run the **RUNSTATS** command, complete the following steps:

1. In the navigation pane, click **Tools** > **DB Tools**.
2. Click **Perform RUNSTATS**. The following warning message is displayed - `Are you sure you want to perform RUNSTATS on the inventory database tables?`
3. Click **OK**. The following message is displayed - `RUNSTATS Started`. After approximately 30 minutes, you can check the activity log. When the job is complete, the following message is added to the activity log - `RUNSTATS for inventory database successful`.

Performing REORG

To run the **REORG** command, complete the following steps:

1. In the navigation pane, click **Tools** > **DB Tools**.
2. Click **Perform REORG**. The following confirmation message is displayed - `Are you sure you want to perform REORG on the inventory database tables?`
3. Click **OK**. The following message is added to the activity log - `REORG Started`. After approximately 30 minutes, you can check the activity log. When the job is complete, the following message is added to the activity log - `REORG inventory database successful`.

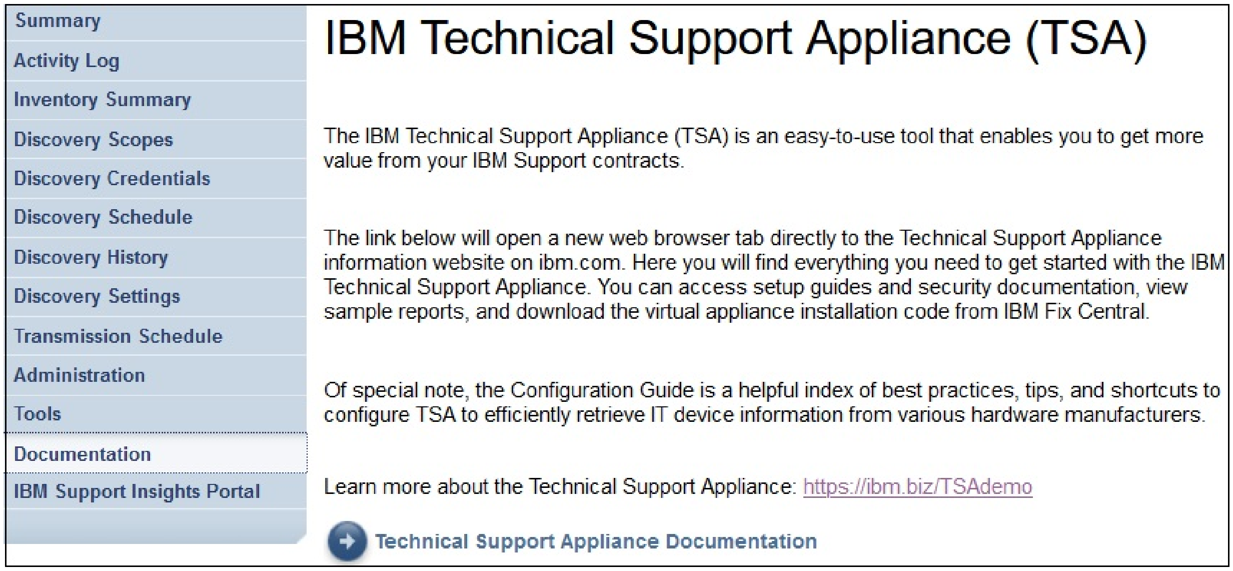
Documentation

Use the **Documentation** page to get started with IBM Technical Support Appliance. You can access setup guides and security documentation, view sample reports, and download the TSA installation code from the TSA website at: https://ibm.biz/TSAdemo.

Procedure

To view the documentation and learn more about the Technical Support Appliance, follow these steps:

1. Click **Documentation** from the left navigation menu.



IBM Technical Support Appliance (TSA)

The IBM Technical Support Appliance (TSA) is an easy-to-use tool that enables you to get more value from your IBM Support contracts.

The link below will open a new web browser tab directly to the Technical Support Appliance information website on ibm.com. Here you will find everything you need to get started with the IBM Technical Support Appliance. You can access setup guides and security documentation, view sample reports, and download the virtual appliance installation code from IBM Fix Central.

Of special note, the Configuration Guide is a helpful index of best practices, tips, and shortcuts to configure TSA to efficiently retrieve IT device information from various hardware manufacturers.

Learn more about the Technical Support Appliance: https://ibm.biz/TSAdemo

Technical Support Appliance Documentation

Figure 90. Documentation

2. To learn more about the Technical Support Appliance, click the link: https://ibm.biz/TSAdemo
3. On the **Install TSA** page, you will find links to the TSA image, setup guide, configuration guide, and relevant tutorials.

Chapter 7. Contacting IBM Support for the Technical Support Appliance (TSA)

IBM Support is available from Monday to Friday during business hours of your time zone.

About this task

You can contact IBM Support with any of the following two options:

1. Open a case at the IBM Support Portal
2. Creating a service request through the IBM Call Center

Opening a case at the IBM Support Portal

Procedure

1. Log on to https://www.ibm.com/mysupport/s/

   Note: You must first create an account to access the IBM Support Portal.
2. Click **Open a case** on the upper right of the portal. The **Open a case** page is displayed.
3. Select the **Type of support**.
4. Enter the **Title**, **Product manufacturer**, and **Product**.

   Note: To route your request directly to the Technical Support Appliance team, enter `Technical Support Appliance` in the **Product** field.
5. Select the **Severity**
6. Enter the **Description**, and select your preferred language.
7. If an agent who speaks your language is not available and you are interested to communicate in English, then select **Yes**.
8. Click **Submit case**.

Creating a service request through the IBM Call Center

Procedure

1. Dial the correct phone number for the country of origin: https://www.ibm.com/planetwide
2. Select language.
3. Select 1 (IBM products).
4. Select 2 (Software support).
5. Use the product ID *5621IZX01* or use the product name *Technical Support Appliance*.
6. You are prompted for:
   - Company number/geography
   - Customer/company name
   - Address/City/State/Postal code
   - Building/Floor Room
   - Phone number where TSA is located.
   - Contact name/email/phone number
   - Problem description

- Severity level

Appendix A. Configuring the Technical Support Appliance

If you exit or skip configuring any of the settings in the **Setup Wizard**, you can manually configure them from the left navigation menu of TSA.

Registering the Technical Support Appliance

Registering collects information required to identify TSA when it reports information to IBM for analysis.

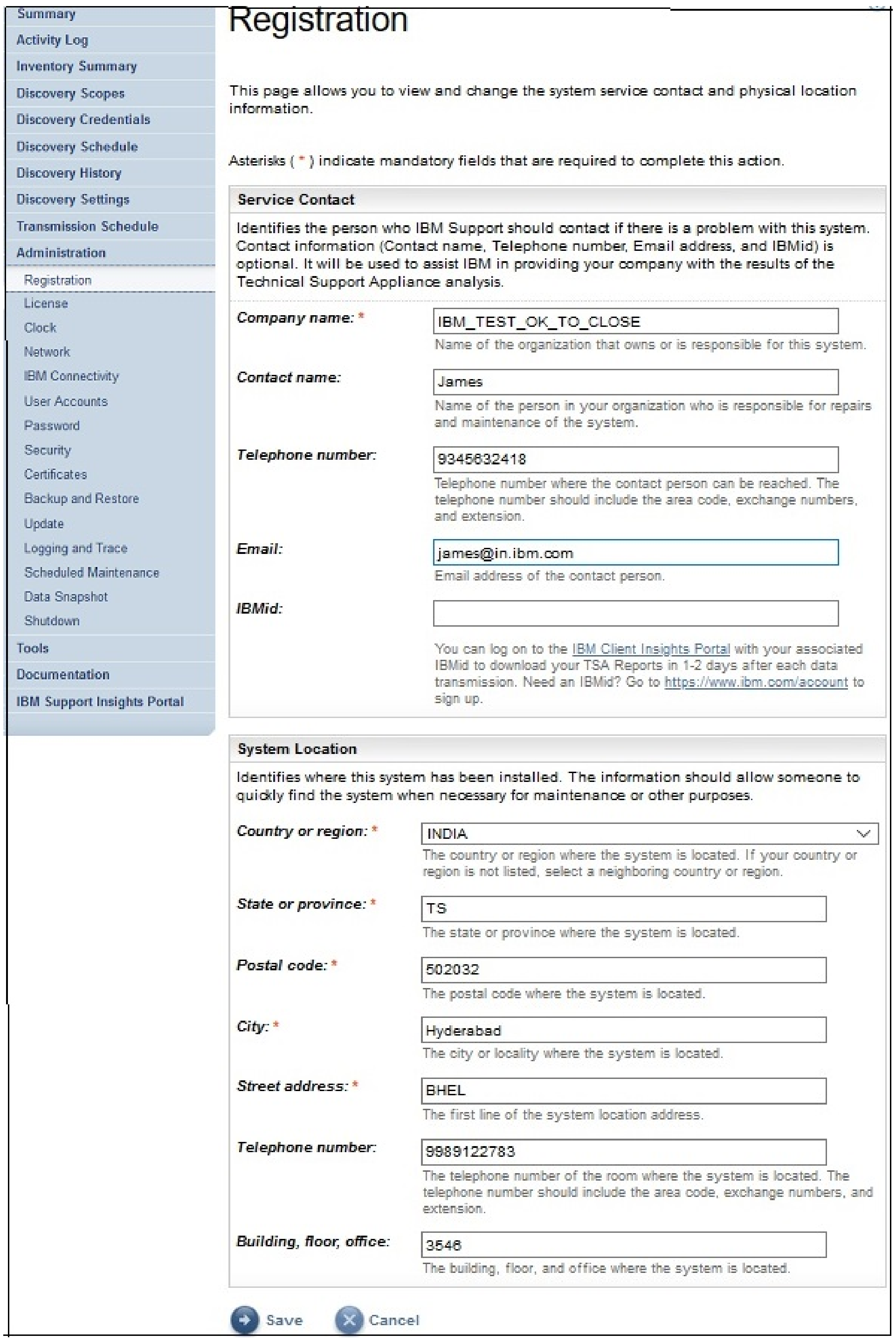
About this task

To register, follow these steps:

Procedure

1. In the navigation pane, click **Administration** > **Registration**.

   The **Registration** page is displayed.



Registration

This page allows you to view and change the system service contact and physical location information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Service Contact

Identifies the person who IBM Support should contact if there is a problem with this system. Contact information (Contact name, Telephone number, Email address, and IBMid) is optional. It will be used to assist IBM in providing your company with the results of the Technical Support Appliance analysis.

Company name: * IBM_TEST_OK_TO_CLOSE
Name of the organization that owns or is responsible for this system.

Contact name: James
Name of the person in your organization who is responsible for repairs and maintenance of the system.

Telephone number: 9345632418
Telephone number where the contact person can be reached. The telephone number should include the area code, exchange numbers, and extension.

Email: james@in.ibm.com
Email address of the contact person.

IBMid:
You can log on to the IBM Client Insights Portal with your associated IBMid to download your TSA Reports in 1-2 days after each data transmission. Need an IBMid? Go to https://www.ibm.com/account to sign up.

System Location

Identifies where this system has been installed. The information should allow someone to quickly find the system when necessary for maintenance or other purposes.

Country or region: * INDIA
The country or region where the system is located. If your country or region is not listed, select a neighboring country or region.

State or province: * TS
The state or province where the system is located.

Postal code: * 502032
The postal code where the system is located.

City: * Hyderabad
The city or locality where the system is located.

Street address: * BHEL
The first line of the system location address.

Telephone number: 9989122783
The telephone number of the room where the system is located. The telephone number should include the area code, exchange numbers, and extension.

Building, floor, office: 3546
The building, floor, and office where the system is located.

Figure 91. Registration

2. Specify service contact information in the following fields:

Company name
The name of the organization that uses TSA.

Contact name
(Optional) The name of the person in the organization who is responsible for TSA.

Telephone number
(Optional) The telephone number where the contact person can be reached. The telephone number should include the area code, exchange numbers, and extension. Do not use parentheses in the telephone number.

Email
(Optional) The email address of the contact person.

IBMid
(Optional) The IBMid of the person you wish to authorize to view the reports on the IBM Client Insights Portal.

Note: You can log on to https://clientinsightsportal.ibm.com/ with your associated IBMid to download your TSA Reports in 1-2 days after each data transmission. To sign up for an IBMid, go to https://www.ibm.com/account.

Note: The service contact identifies the person who IBM Support should contact if there is a problem with the system. Contact information is used to assist IBM in providing your company with the results of the Technical Support Appliance analysis.

3. Specify TSA location information in the following fields:

   Country or region
   The country or region where TSA is located.

   State or province
   The state or province where TSA is located. If you are not sure of the state, type *Unknown*

   Postal code
   The postal code where the TSA is located.

   City
   The city or locality where TSA is located.

   Street address
   TSA location address.

   Telephone number
   (Optional) The telephone number of the room where TSA is located. The telephone number should include the area code, exchange numbers, and extension. Do not use parentheses in the telephone number.

   Building, floor, office
   (Optional) The building, floor, and office where TSA is located.

4. Click **Save** to save the registration information.

Setting up IBM connectivity

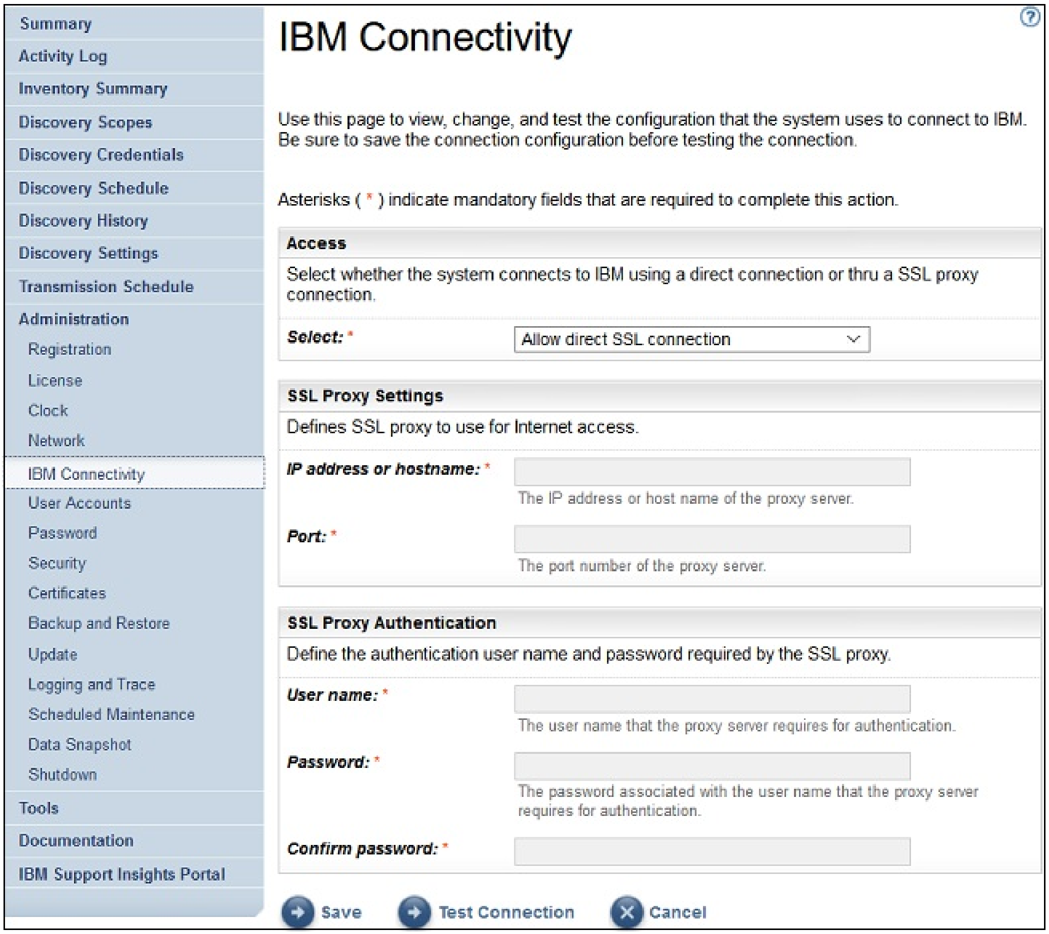
Specify the Internet connection information to use when connecting to IBM.

Before you begin

Ensure that your firewall allows connections to the IBM server host name and IP addresses as explained in Table 1 on page 6. If your network does not allow access to the IBM servers, TSA transactions to IBM Support will fail.

Procedure

1. In the navigation pane, click **Administration** > **IBM Connectivity**.



IBM Connectivity

Use this page to view, change, and test the configuration that the system uses to connect to IBM. Be sure to save the connection configuration before testing the connection.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Access

Select whether the system connects to IBM using a direct connection or thru a SSL proxy connection.

Select: * Allow direct SSL connection

SSL Proxy Settings

Defines SSL proxy to use for Internet access.

IP address or hostname: *

The IP address or host name of the proxy server.

Port: *

The port number of the proxy server.

SSL Proxy Authentication

Define the authentication user name and password required by the SSL proxy.

User name: *

The user name that the proxy server requires for authentication.

Password: *

The password associated with the user name that the proxy server requires for authentication.

Confirm password: *

Figure 92. IBM Connectivity

2. In the **Access** pane, select from the following Internet access types:

Allow direct SSL connection
TSA connects to IBM by using a direct connection.

Use SSL proxy connection
TSA connects to IBM by using an SSL proxy connection.

Use authenticating SSL proxy connection
TSA connects to IBM by using an authenticating SSL proxy connection.

3. If you have selected **Use SSL proxy connection** or **Use authenticating SSL proxy connection**, specify the following information for the proxy server.

IP address or hostname
The IP address or host name of the proxy server.

Note: The host name you enter must not contain an underscore ("_").

Port
The port number of the proxy server.

4. If you have selected **Use authenticating SSL proxy connection**, specify the following information for the proxy server:

User name
The user name that the proxy server requires for authentication.

Password
The password that is associated with the user name that the proxy server requires for authentication.

Confirm password

Enter the password again. The two passwords that you entered are compared to confirm that they match before the password is saved.

5. Click **Save** to save the IBM connection information.
6. Click **Test Connection** to test the specified connection.

   Important:

   - Save the connection settings before testing the connection.
   - You must have a working connection to IBM or TSA functions will not work.

Related concepts

Configuration requirements for connections to IBM Support
TSA can connect to IBM Support through a direct connection or through a user-supplied proxy that you must configure to allow communication with IBM. If you are using a proxy, TLS/SSL inspection is not supported. Any requests through a proxy must be allowed to flow directly to IBM without TLS/SSL termination.

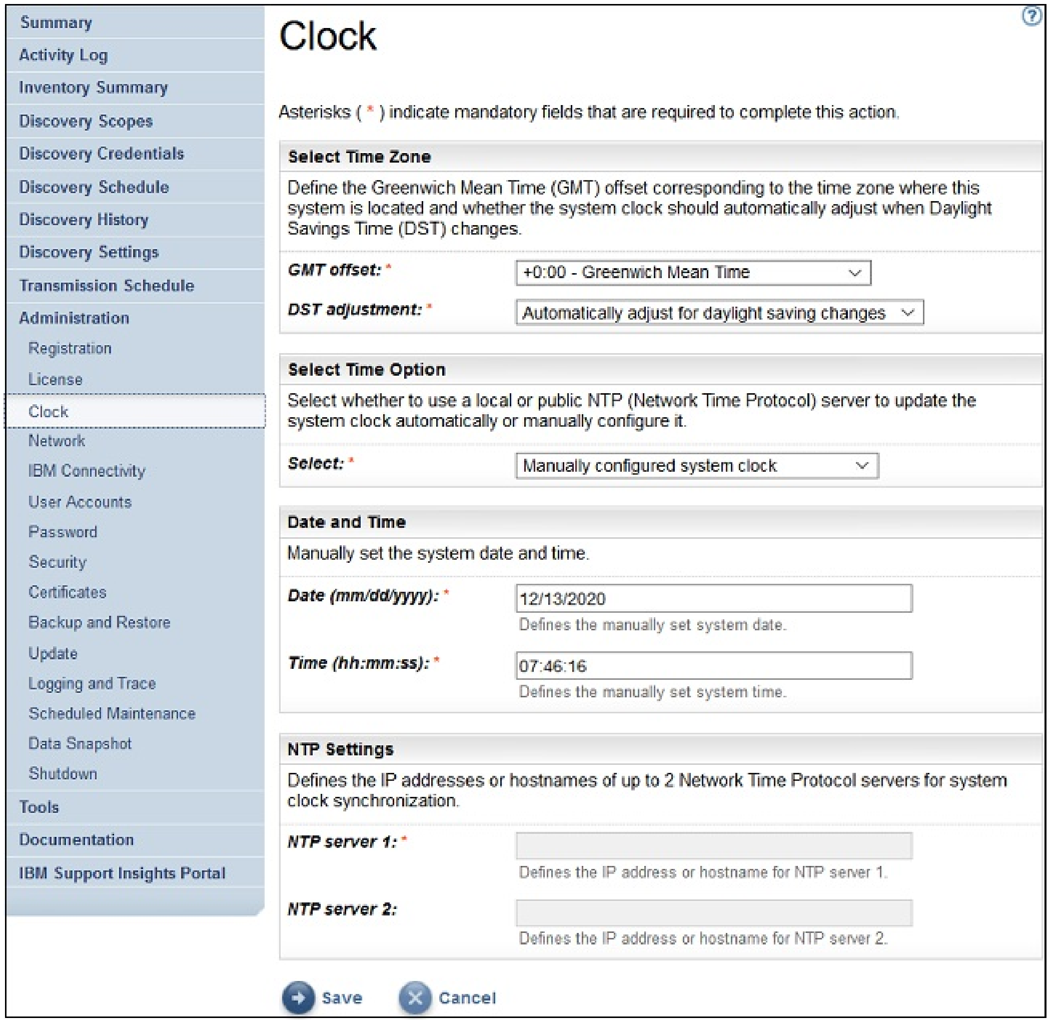
Setting the clock

You must set the TSA system time, date, and local time zone during setup.

Procedure

1. In the navigation pane, click **Administration** > **Clock**.

   The **Clock** page is displayed.



Clock

Asterisks (*) indicate mandatory fields that are required to complete this action.

Select Time Zone

Define the Greenwich Mean Time (GMT) offset corresponding to the time zone where this system is located and whether the system clock should automatically adjust when Daylight Savings Time (DST) changes.

GMT offset: * +0:00 - Greenwich Mean Time

DST adjustment: * Automatically adjust for daylight saving changes

Select Time Option

Select whether to use a local or public NTP (Network Time Protocol) server to update the system clock automatically or manually configure it.

Select: * Manually configured system clock

Date and Time

Manually set the system date and time.

Date (mm/dd/yyyy): * 12/13/2020

Defines the manually set system date.

Time (hh:mm:ss): * 07:46:16

Defines the manually set system time.

NTP Settings

Defines the IP addresses or hostnames of up to 2 Network Time Protocol servers for system clock synchronization.

NTP server 1: *

Defines the IP address or hostname for NTP server 1.

NTP server 2:

Defines the IP address or hostname for NTP server 2.

Figure 93. Clock

2. Select your local time zone from the **GMT offset** drop-down list.
3. Select the daylight saving time (DST) adjustment from the **DST adjustment** drop-down list.

   Note: Not all time zones allow DST. If this option is selected for a time zone that does not allow DST, an error message is displayed.
4. Select a method for updating the system clock from the **Select Time Option** drop-down list.

   Options include synchronizing the system clock with a Network Time Protocol (NTP) server to update the system clock automatically or manually configuring the system clock.

   a) If you selected to manually configure the system clock, you must set the system date and time. Enter the date and time information into the **Date** and **Time** fields.

   b) If you selected to synchronize the system clock with a Network Time Protocol (NTP) server to update the system clock automatically, you must then specify the IP addresses and host names for the NTP servers. Type the IP address or host name information for up to two servers in the **NTP server** fields.

   Note: Make sure that the NTP server is accessible through the network to TSA.
5. Click **Save** to save the clock information.

Results

Note: Some changes require a restart to take effect. For example, if you set the date or time, or changed from manual configuration to NTP server configuration, you are prompted to restart the system.

Setting up the transmission schedule

TSA provides a default schedule for the transmission process to run at specified times. You can modify this schedule according to your needs.

Procedure

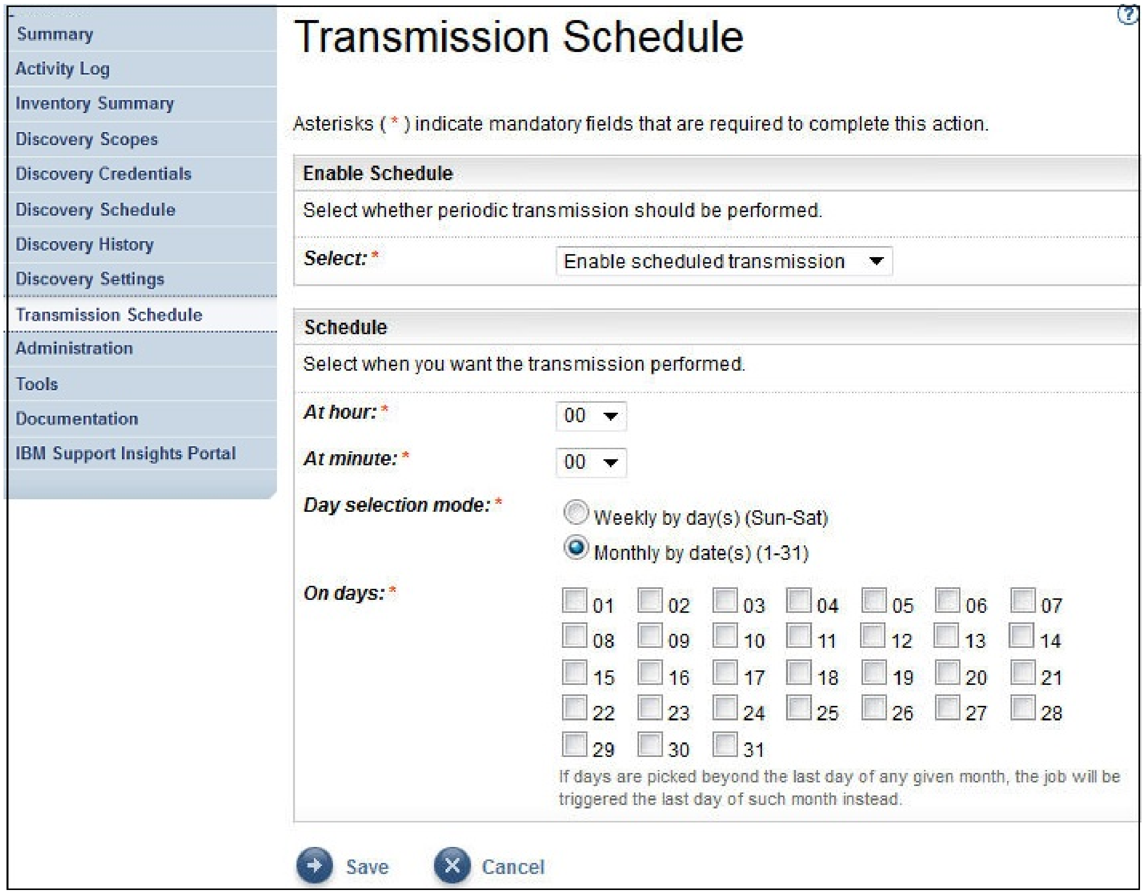
1. In the navigation pane, click **Transmission Schedule**.

   The **Transmission Schedule** page is displayed.

   The **Schedule** pane displays the next scheduled run and the scheduled run times. The **History** pane displays the status and additional details of the currently running and previous transmission jobs.

2. Click **Edit Schedule**.

   The **Transmission Schedule** page is displayed.



Transmission Schedule

Asterisks (*) indicate mandatory fields that are required to complete this action.

Enable Schedule

Select whether periodic transmission should be performed.

Select: * Enable scheduled transmission

Schedule

Select when you want the transmission performed.

At hour: * 00

At minute: * 00

Day selection mode: *
○ Weekly by day(s) (Sun-Sat)
● Monthly by date(s) (1-31)

On days: *
□ 01 □ 02 □ 03 □ 04 □ 05 □ 06 □ 07
□ 08 □ 09 □ 10 □ 11 □ 12 □ 13 □ 14
□ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21
□ 22 □ 23 □ 24 □ 25 □ 26 □ 27 □ 28
□ 29 □ 30 □ 31

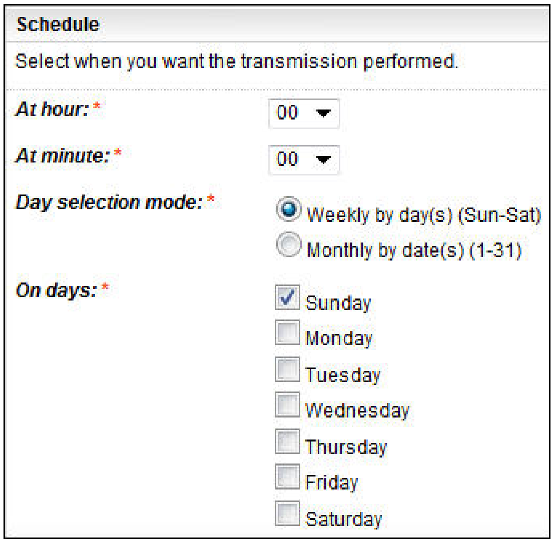
If days are picked beyond the last day of any given month, the job will be triggered the last day of such month instead.

Figure 94. Edit transmission schedule

   a) Use the **At hour** and **At minute** drop-down lists to select a new time.

   b) Select the **Day Selection mode**.

   Weekly by day(s) (Sun - Sat)
   To schedule the transmission on a particular day(s) of a week, select the **Weekly by day(s) (Sun - Sat)** option.



Schedule

Select when you want the transmission performed.

At hour: * 00

At minute: * 00

Day selection mode: *

● Weekly by day(s) (Sun-Sat)

○ Monthly by date(s) (1-31)

On days: *

☑ Sunday

□ Monday

□ Tuesday

□ Wednesday

□ Thursday

□ Friday

□ Saturday

Figure 95. Weekly by day(s) (Sun - Sat)

For the **On days** field, select the appropriate check box to select one or more days of the week.

Monthly by date(s) (1-31)

To schedule the transmission on particular days of a month, select **Monthly by date(s) (1-31)** option.

For the **On days** field, select the appropriate check box to select one or more days of the month.

Note: If you select the days beyond the last day of a specific month, then the job is triggered on the last day of that particular month.

3. Click **Save**.

   The **Transmission Schedule** page is displayed again, with the new schedule shown.

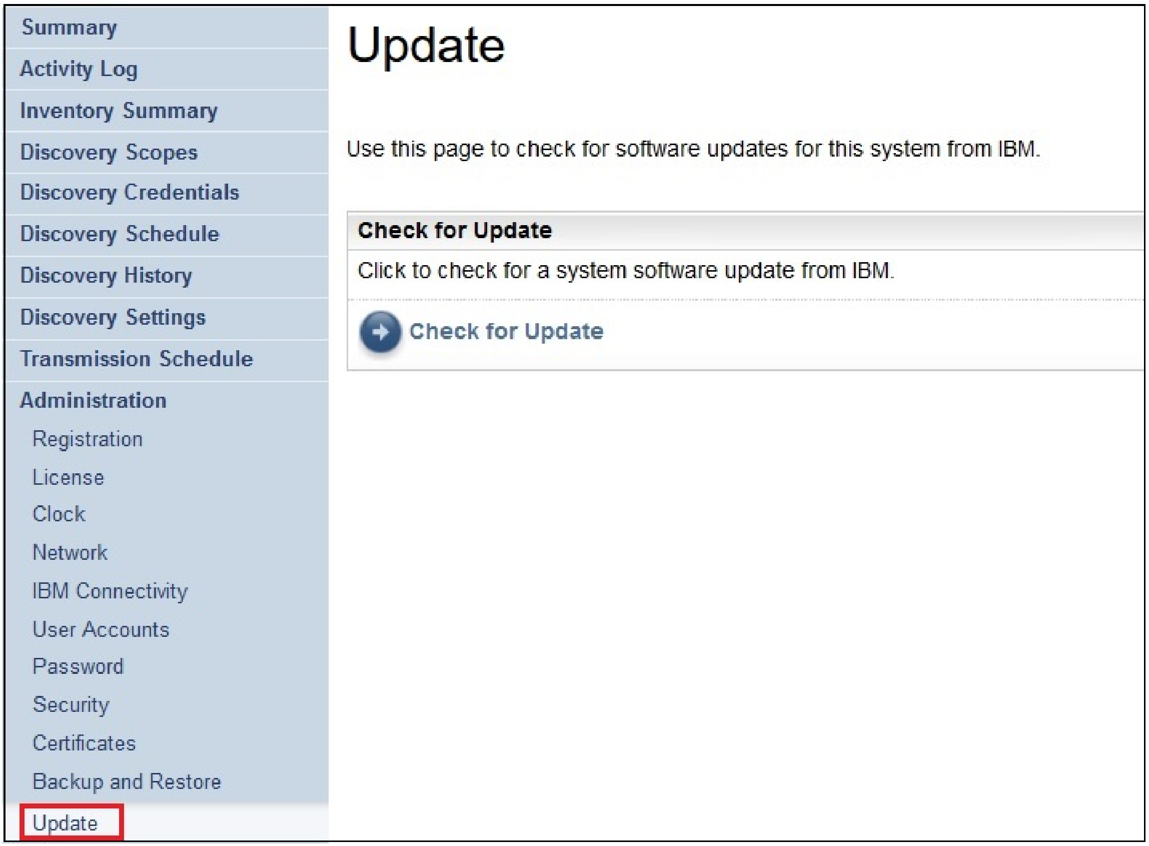
Update

You can check and download updates for TSA.

Procedure

1. In the navigation pane, click **Administration** > **Update**.

   The **Update** page is displayed.



Update

Use this page to check for software updates for this system from IBM.

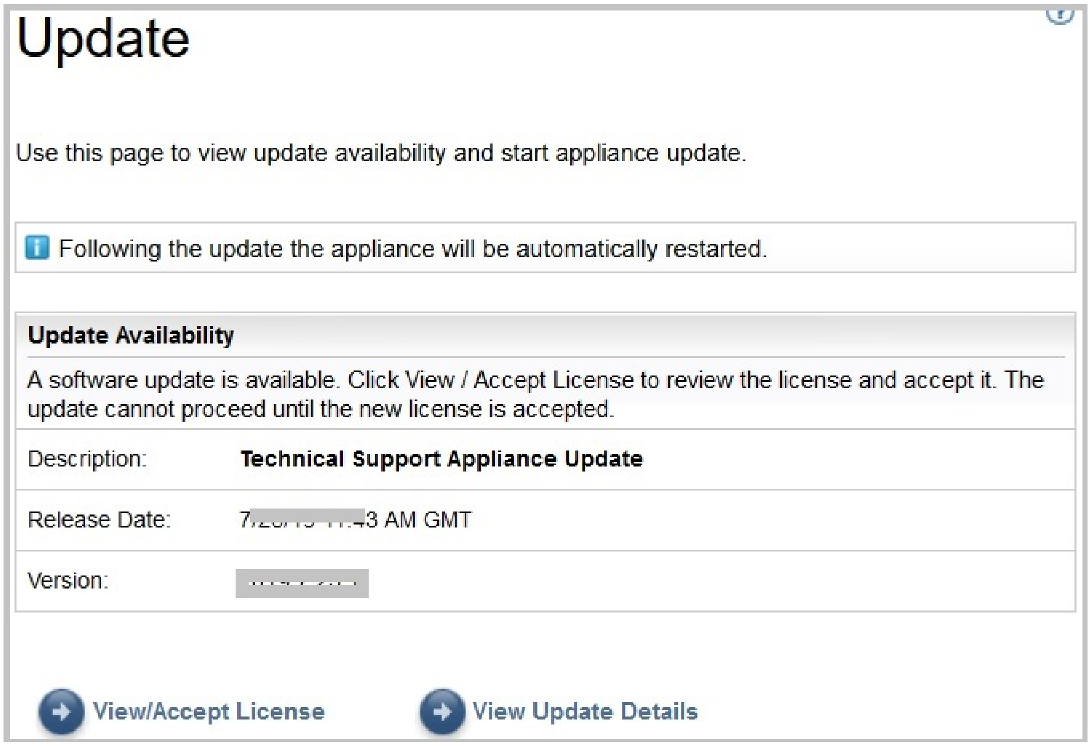
Check for Update

Click to check for a system software update from IBM.

Figure 96. Update

2. Click **Check for Update**.

   The **Update Availability** page lists any available updates.



Update

Use this page to view update availability and start appliance update.

Following the update the appliance will be automatically restarted.

Update Availability

A software update is available. Click View / Accept License to review the license and accept it. The update cannot proceed until the new license is accepted.

Description:	**Technical Support Appliance Update**
Release Date:	7[redacted]3 AM GMT
Version:	[redacted]

Figure 97. Update availability

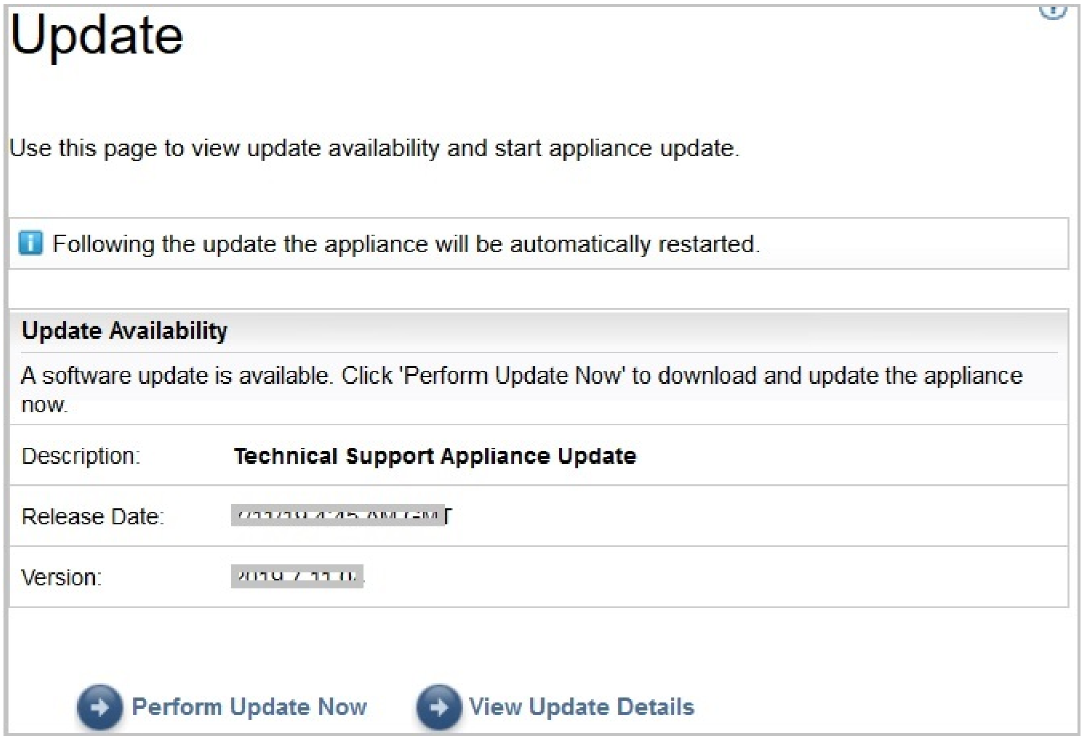
a) For some new releases of TSA, you must accept a new license agreement before proceeding with the update. If there is a new license, click **View/Accept License**, the **License Agreement** page is displayed.

b) Click the **Accept** button on the **License Agreement** page to accept the new license agreement. The **Update** page is displayed again with the **Perform Update Now** button. If there is no requirement to accept a new license agreement, the **View/Accept License** button is not displayed, click **Perform Update Now** to proceed.

Note:

- Once you accept the license, the **View/Accept License** button is no longer displayed.
- In the navigation pane, click **Administration** > **License** to view the latest License Agreement that you have accepted.

c) To install the updates, click **Perform Update Now**.



Update

Use this page to view update availability and start appliance update.

Following the update the appliance will be automatically restarted.

Update Availability

A software update is available. Click 'Perform Update Now' to download and update the appliance now.

Description:	**Technical Support Appliance Update**
Release Date:	[redacted]
Version:	[redacted]

Figure 98. Perform Update Now

Upon completion of the update, TSA is automatically restarted.

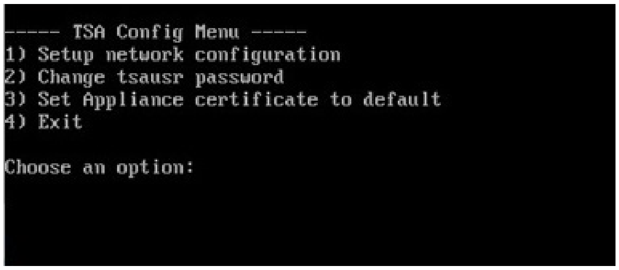
d) To view information about the contents of the update, click **View Update Details**.

Appendix B. Configuring the DHCP network details

Follow these steps to configure the DHCP network details:

Procedure

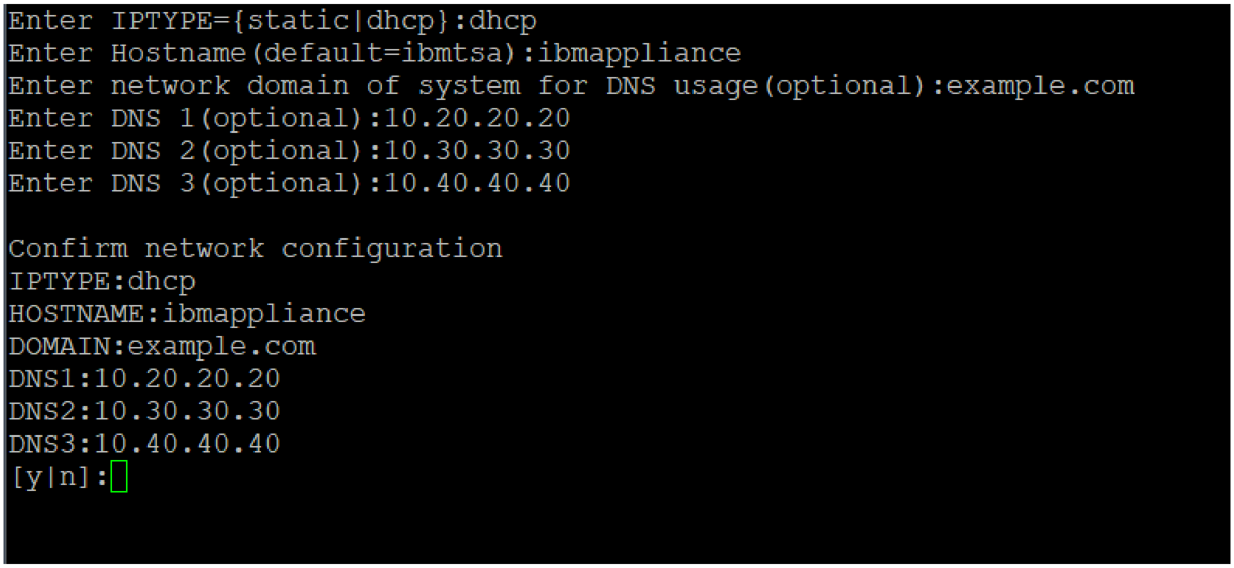
1. Select option **1) Setup network configuration** from the **TSA Config Menu**.



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

Choose an option:
```

Figure 99. Setup network configuration

2. Enter the following network configuration details.



```
Enter IPTYPE={static|dhcp}:dhcp
Enter Hostname(default=ibmtsa):ibmappliance
Enter network domain of system for DNS usage(optional):example.com
Enter DNS 1(optional):10.20.20.20
Enter DNS 2(optional):10.30.30.30
Enter DNS 3(optional):10.40.40.40

Confirm network configuration
IPTYPE:dhcp
HOSTNAME:ibmappliance
DOMAIN:example.com
DNS1:10.20.20.20
DNS2:10.30.30.30
DNS3:10.40.40.40
[y|n]:
```

Figure 100. Network Configuration

a) **Enter IPTYPE = {static|dhcp}**. Enter `dhcp`.

IPTYPE: dhcp

`Enter Hostname(default=ibmtsa)`. You can change the default host name. Ensure that the host name you use is unique.

`Enter network domain of system for DNS usage (optional)`.

`Enter DNS 1(optional)`, **`Enter DNS 2(optional)`**, and **`Enter DNS 3(optional)`**.

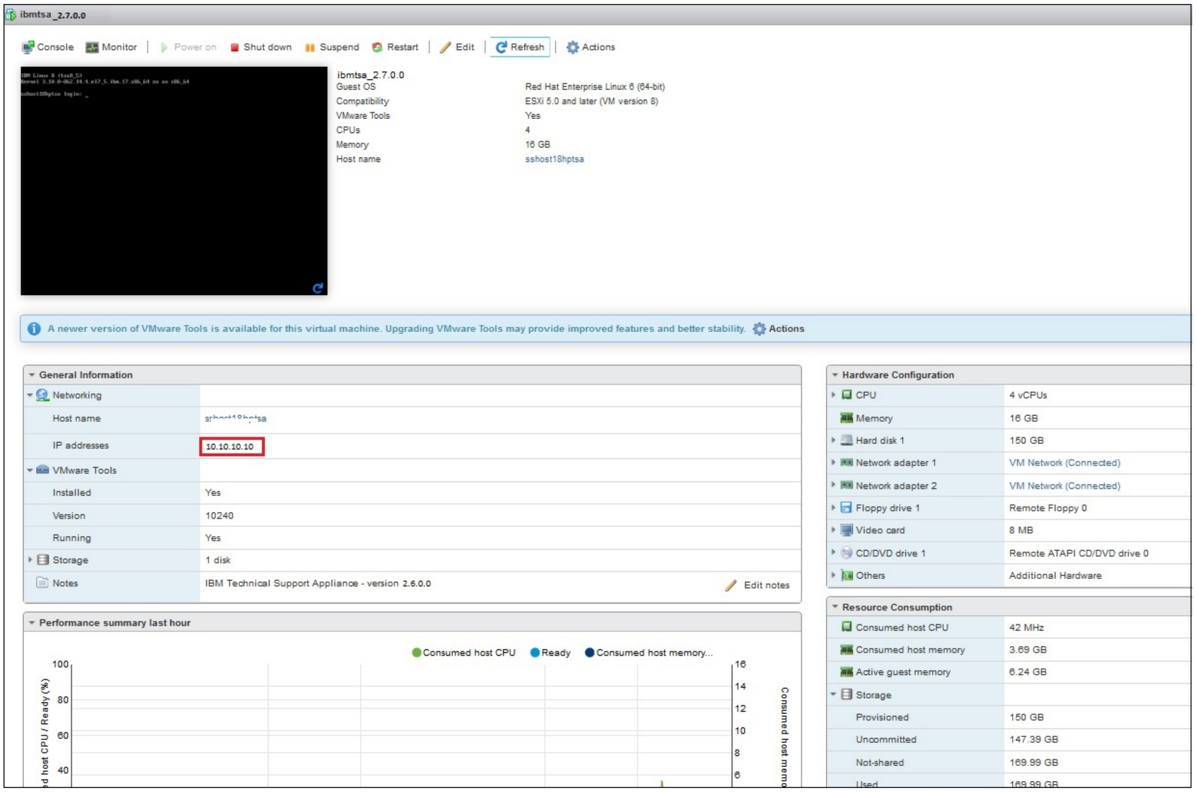
The specified network configuration details are displayed for confirmation.

b) Enter **[y|n]** to confirm or discard the network configuration. Entering **y** saves the network configuration and restarts the system automatically.

Note: For any incorrect configuration, you can change the details. Enter **n** to ignore the current settings and restart the configuration from step "2.a" on page 125

c) The system reboots in 15 seconds for the new network configuration to take effect.

d) After system reboot, login to the virtualization manager and make a note of the **IP Address** on the **Summary** tab.



ibmtsa_2.7.0.0

Console | Monitor | Power on | Shut down | Suspend | Restart | Edit | Refresh | Actions

```
IBM Linux 8 (tsa8_5)
Kernel 3.10.0-862.14.4.el7_5.ibm.17.x86_64 on an x86_64

sshost18hptsa login: _
```

ibmtsa_2.7.0.0

Guest OS	Red Hat Enterprise Linux 6 (64-bit)
Compatibility	ESXi 5.0 and later (VM version 8)
VMware Tools	Yes
CPUs	4
Memory	16 GB
Host name	sshost18hptsa

A newer version of VMware Tools is available for this virtual machine. Upgrading VMware Tools may provide improved features and better stability. Actions

General Information

Networking	
Host name	sshost18hptsa
IP addresses	10.10.10.10
VMware Tools	
Installed	Yes
Version	10240
Running	Yes
Storage	1 disk
Notes	IBM Technical Support Appliance - version 2.6.0.0 Edit notes

Performance summary last hour

Hardware Configuration

CPU	4 vCPUs
Memory	16 GB
Hard disk 1	150 GB
Network adapter 1	VM Network (Connected)
Network adapter 2	VM Network (Connected)
Floppy drive 1	Remote Floppy 0
Video card	8 MB
CD/DVD drive 1	Remote ATAPI CD/DVD drive 0
Others	Additional Hardware

Resource Consumption

Consumed host CPU	42 MHz
Consumed host memory	3.69 GB
Active guest memory	6.24 GB
Storage	
Provisioned	150 GB
Uncommitted	147.39 GB
Not-shared	169.99 GB
Used	169.99 GB

Figure 101. DHCP IP Address

e) Access TSA from the browser with the URL that you obtained from the previous step. For example, `https://newhost1.new.abclabs.example.com`

Note: On the first connection, your browser may display a security exception. You must accept the security certificate and continue to log on to TSA.

Appendix C. User accounts and user groups

You can use user accounts and user groups to grant access to TSA functions.

Before you begin

TSA is installed with a user account named **admin**. This account has authority to perform any TSA function. You may want to add user accounts for the following reasons:

- Allow another user to act as a backup for the **admin** user.
- Allow some users to access a limited amount of function on TSA.

About this task

Executing any TSA function requires a certain authority level. If an authenticated user attempts to perform a function without the appropriate authority level, an error is displayed and the function is not executed.

In TSA, authority levels are associated with user groups. Users are assigned membership in one or more user groups, and through those group memberships, users have the authority level to perform particular functions.

TSA comes with an **Administrator** user group and an **admin** user account. The **Administrator** user group has unrestricted access to all system functions. The **admin** user account is assigned to the **Administrator** user group.

Displaying user accounts and user groups

You can display the existing user accounts and user groups.

Procedure

1. In the navigation pane, click **Administration** > **User Accounts**.

   The **User Accounts and Groups** page is displayed.
2. To display the existing user accounts, click the **Accounts** tab.

   The User Accounts table displays the user accounts.

   Tip: To view details for a specific user account, click the name of the user account. The **General** pane on the right side displays the user name, full name, and description that is associated with the selected user account. Click the **Member Of** pane on the right to view the user groups to which this user account belongs.
3. To display the existing user groups, click the **Groups** tab.

   The User Groups table displays the user groups.

   Tip: To view details for a specific user group, click the name of the user group. The **General** pane on the right side displays the name and authority level that is associated with the user group. Click the **Scope restrictions** pane on the right side, to view the scope sets that the selected user group can discover. Click the **Members** pane to view the user accounts that are associated with this user group.

Adding user accounts and user groups

You can add user accounts and groups to control access to TSA functions.
Related concepts

Discovery Scopes and Scope Sets

Discovery scopes identify the resources that you want TSA to discover. Discovery scopes are grouped into discovery scope sets.

Adding a user group

You can add user groups to control access to TSA functions.

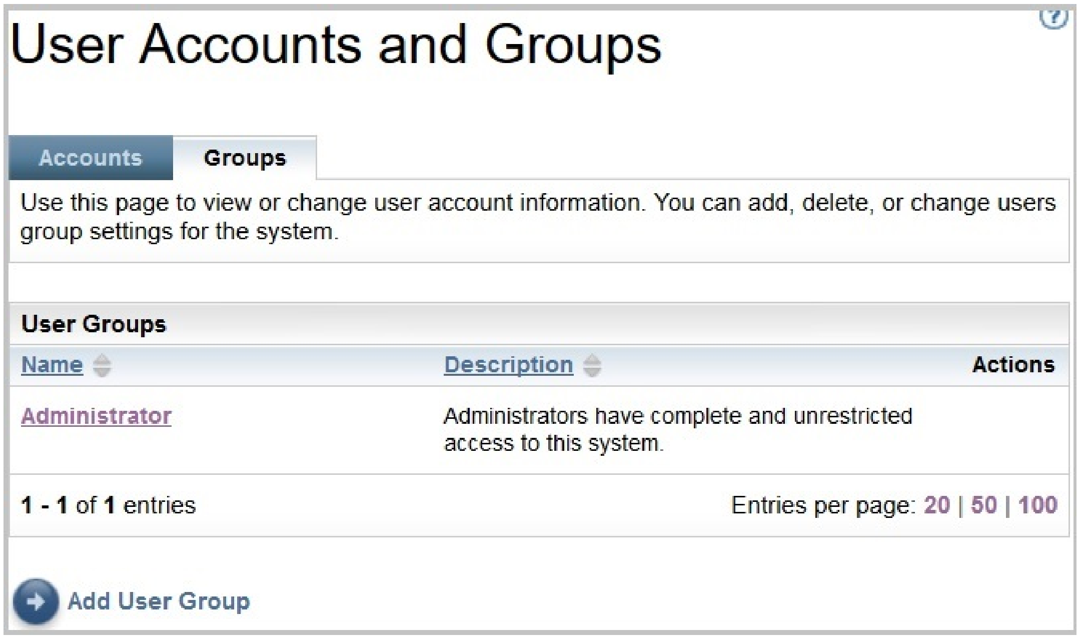
About this task

To add a user group, follow these steps:

Procedure

1. In the navigation pane, click **Administration** > **User Accounts**.

   The **User Accounts and Groups** page is displayed.
2. Click the **Groups** tab.



User Accounts and Groups

Use this page to view or change user account information. You can add, delete, or change users group settings for the system.

User Groups

Name	Description	Actions
Administrator	Administrators have complete and unrestricted access to this system.	

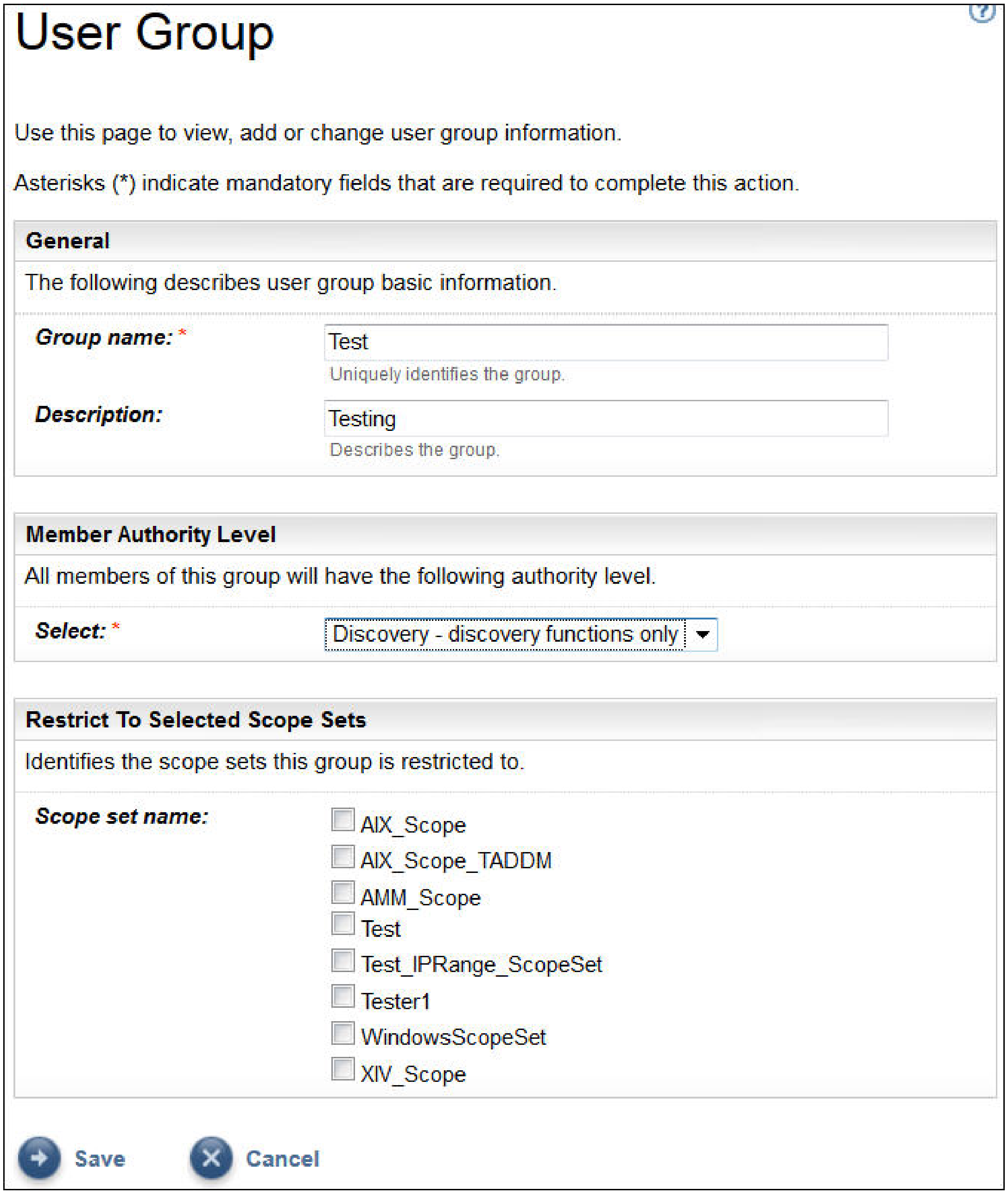
1 - 1 of 1 entries

Entries per page: 20 | 50 | 100

Figure 102. Groups

3. Click **Add User Group**.

   The **User Group** page is displayed.



User Group

Use this page to view, add or change user group information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

General

The following describes user group basic information.

Group name: * Test

Uniquely identifies the group.

Description: Testing

Describes the group.

Member Authority Level

All members of this group will have the following authority level.

Select: * Discovery - discovery functions only

Restrict To Selected Scope Sets

Identifies the scope sets this group is restricted to.

Scope set name:

- □ AIX_Scope
- □ AIX_Scope_TADDM
- □ AMM_Scope
- □ Test
- □ Test_IPRange_ScopeSet
- □ Tester1
- □ WindowsScopeSet
- □ XIV_Scope

Figure 103. Add User Group

4. In the **Group name** field, enter a unique name for this user group.
5. Optional: In the **Description** field, enter a description for this user group.
6. Select the authority level that you want the members of this user group to have.

   TSA defines the following group authority levels:

   - **Administrator** – no restrictions
   - **Discovery** – discovery functions only
   - **Visitor** – read access only
7. If you specify the *Discovery* authority level for this user group, you must select at least one scope set that is restricted to this user group.

   For more information about scope sets, see “Discovery Scopes and Scope Sets” on page 1.
8. Click **Save** to save the user group.

   The **User Accounts and Groups** page is displayed with the new user group in the list.

Adding a user account

You can add user accounts to control access to TSA functions.

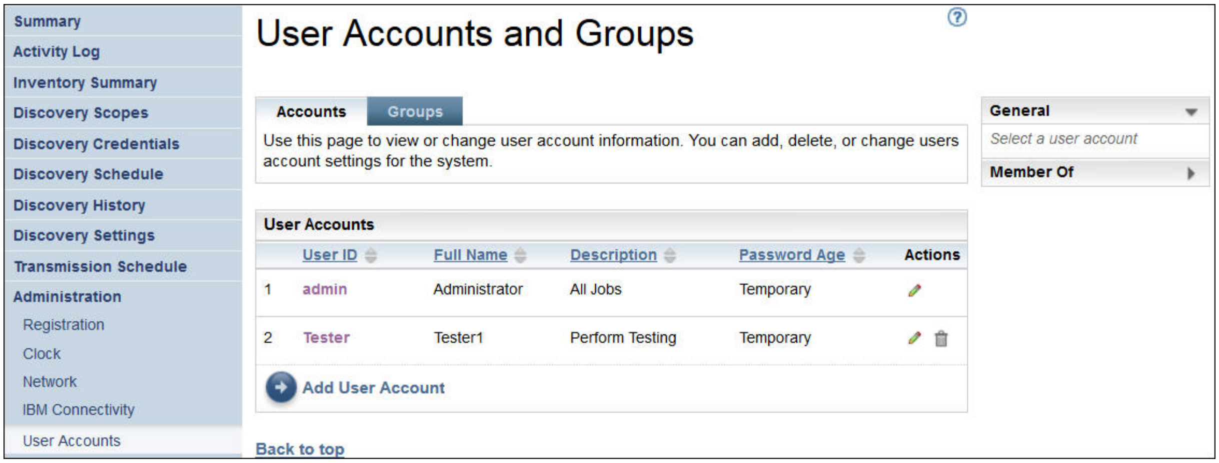
About this task

To add a user account, follow these steps:

Procedure

1. In the navigation pane, click **Administration** > **User Accounts**.

   The **User Accounts and Groups** page is displayed.



User Accounts and Groups

Use this page to view or change user account information. You can add, delete, or change users account settings for the system.

User Accounts

	User ID	Full Name	Description	Password Age	Actions
1	admin	Administrator	All Jobs	Temporary	✎
2	Tester	Tester1	Perform Testing	Temporary	✎ 🗑

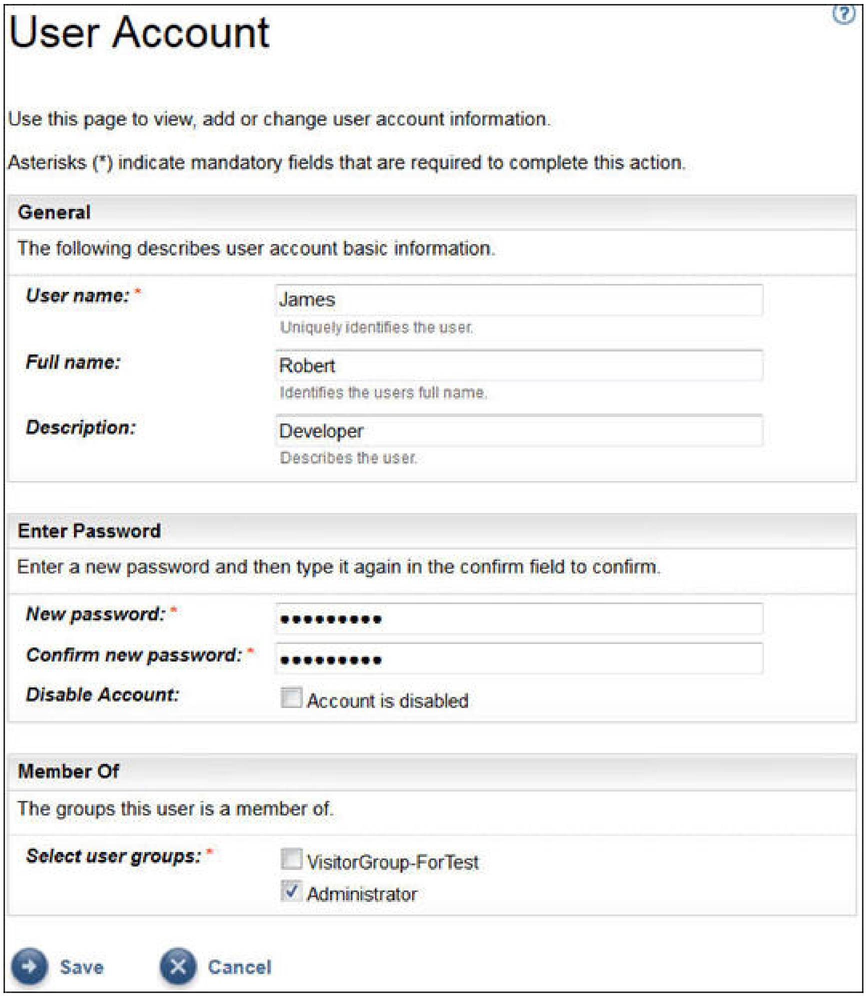
Add User Account

Back to top

Figure 104. User Accounts and Groups

2. To define a new user account, click **Add User Account**.

   The **User Account** page is displayed.



User Account

Use this page to view, add or change user account information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

General

The following describes user account basic information.

User name: * James
Uniquely identifies the user.

Full name: Robert
Identifies the users full name.

Description: Developer
Describes the user.

Enter Password

Enter a new password and then type it again in the confirm field to confirm.

New password: * ••••••••••

Confirm new password: * ••••••••••

Disable Account: □ Account is disabled

Member Of

The groups this user is a member of.

Select user groups: * □ VisitorGroup-ForTest
☑ Administrator

Figure 105. Add User Account

3. In the **User name** field, enter a name for this user account.
4. Optional: In the **Full name** field, enter a full name for the user of this account.
5. Optional: In the **Description** field, enter a description for this user account.
6. In the **New password** field, enter a password for this user account.

   The password must adhere to the following rules:

   - Must be at least 8 characters long
   - Must contain at least one alphabetic and one non-alphabetic character
   - Must not contain the user name
   - Must not be the same as any of the previous eight passwords
   - Must be changed at least once every 30 days (by default) or as specified in the "Modifying the password age" on page 102 section, but must not be changed more than once each day.
7. In the **Confirm password** field, enter the password for this user account again.

   The two passwords that you entered are compared to confirm that they match before the password is saved.

   Note: The password must be changed at the first login to this user account.
8. If you want to disable this user account, select the **Account is disabled** check box.

   Disabling the account enables you to prevent the account from being used without deleting the account.

   Note: You can neither disable the **admin** account nor change the group of the **admin** account.

9. Select the user groups for this user account. At least one user group must be selected. The user will have the authority level defined for any groups that you select.
10. Click **Save** to save the user account.

    The **User Accounts and Groups** page is displayed with the new user account in the list.

Modifying user accounts and user groups

You can modify existing user accounts and user groups.

Modifying user accounts

You can modify existing user accounts.

About this task

To modify a user account, follow these steps:

Procedure

1. In the navigation pane, click **Administration** > **User Accounts**.

   The **User Accounts and Groups** page is displayed.
2. Click the **Accounts** tab, and then click the **Edit** (✏) icon beside the user account.

   The **User Account** page is displayed.
3. In the **General** pane, you can change the basic information for this user account.
4. In the **Enter Password** pane, you can change the password and password administration information. You can also disable this user account.

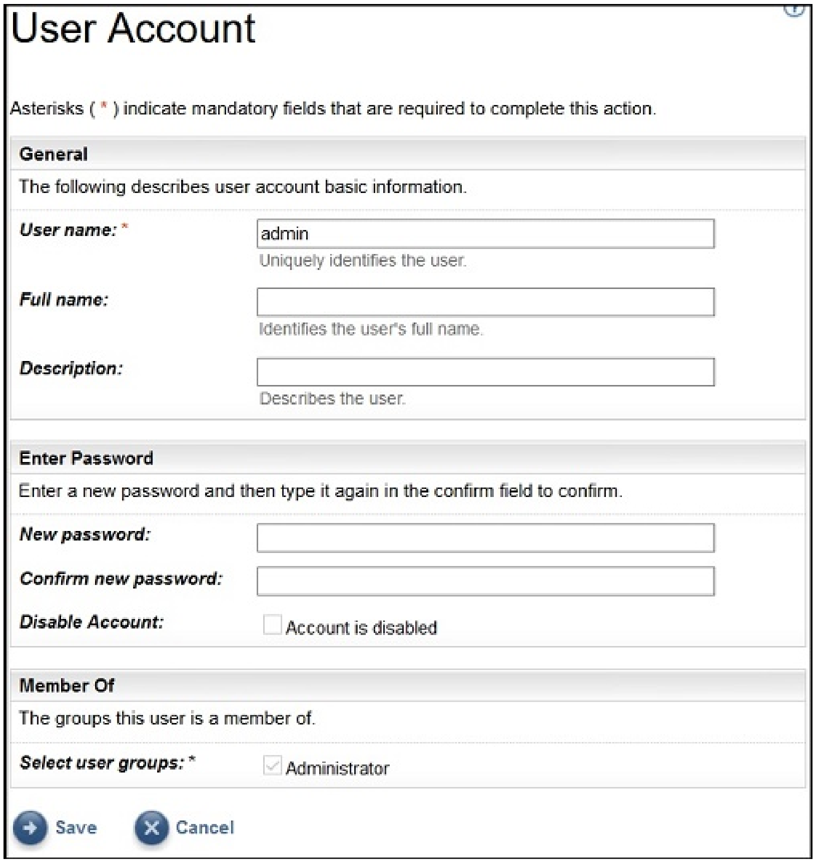
   The password must adhere to the following rules:

   - Must be at least 8 characters long
   - Must contain at least one alphabetic and one non-alphabetic character
   - Must not contain the user name
   - Must not be the same as any of the previous eight passwords
   - Must be changed at least once every 90 days, but must not be changed more than once each day

   Note: The password must be changed at the first login to this user account.
5. If you want to disable this user account, select **Account is disabled**.

   Disabling the account enables you to prevent the account from being used without deleting the account. For information about deleting a user account, see "Deleting user accounts and user groups" on page 134.

   Note: You can neither disable the **admin** account nor change the group of the **admin** account.



User Account

Asterisks (*) indicate mandatory fields that are required to complete this action.

General

The following describes user account basic information.

User name: * admin
Uniquely identifies the user.

Full name:
Identifies the user's full name.

Description:
Describes the user.

Enter Password

Enter a new password and then type it again in the confirm field to confirm.

New password:

Confirm new password:

Disable Account: □ Account is disabled

Member Of

The groups this user is a member of.

Select user groups: * ☑ Administrator

Figure 106. Modify Admin User Account

6. In the **Member Of** pane, you can change the user groups to which this user account belongs. The user account must be a member of at least one user group.
7. Click **Save** to save your changes.

   The changed information is displayed in the **User Accounts and Groups** page.

Modifying user groups

You can modify the existing user groups.

Before you begin

Note: You cannot change the **Administrator** group.

About this task

To modify a user group, follow these steps:

Procedure

1. In the navigation pane, click **Administration** > **User Accounts**.

   The **User Accounts and Groups** page is displayed.

2. Click the **Groups** tab, and then click the **Edit** (✎) icon beside the user group.

   The **User Group** page is displayed.
3. In the **General** pane, you can change the basic information for this user group.
4. In the **Member Authority Level** pane, you can change whether this user group has *Administrator*, *Discovery*, or *Read* authority.

5. If you specified the *Discovery* authority level in the **Member Authority Level**, then you can change the scope sets that this user group has the authority to discover in the **Restrict To Selected Scope Sets** pane.
6. Click **Save** to save your changes.

   The changed information is displayed in the **User Accounts and Groups** page.

Deleting user accounts and user groups

You can delete existing user accounts and user groups.

Deleting user accounts

You can delete existing user accounts.

About this task

Note: The **admin** user account cannot be deleted.

To delete a user account, follow these steps:

Procedure

1. In the navigation pane, click **Administration** > **User Accounts**.

   The **User Accounts and Groups** page is displayed.
2. Click the **Accounts** tab, and then click the **Delete** (🗑) icon next to the user account that you want to delete.
3. Click **OK** to confirm that you want to delete the user account.

Deleting user groups

You can delete existing user groups.

About this task

Note: The **Administrator** user group cannot be deleted.

To delete a user group, follow these steps:

Procedure

1. Click **Administration** > **User Accounts**.

   The **User Accounts and Groups** page is displayed.
2. Click the **Groups** tab, and then click the **Delete** (🗑) icon next to the user group that you want to delete.
3. Click **OK** to confirm that you want to delete the user group.

   Note: A user group can be deleted only if there are no users assigned to it.

Accessibility

The Technical Support Appliance does not interfere with the accessibility features for supported browsers. For a comprehensive list of accessibility features please visit the accessibility support page for the supported browser that you are using. For a list of supported browsers, see “Required web browsers” on page 5.

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties using the PDF files and want to request a web-based format for a publication, email a request to the following address:

icfeedbk@us.ibm.com

Or, you can mail a request to the following address:

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

In the request, be sure to include the publication title, "IBM Technical Support Appliance Setup Guide"in the subject line of your note.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Hyper-V, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Part Number:

(1P) P/N: