Technical Support Appliance
Setup Guide

Version 24.00
Technical Support Appliance
Setup Guide

Version 24.00
Note

Before using this information and the product it supports, read the information in "Notices" on page 133.

Twentieth edition (February 2019)

This edition applies to version 2, release 4, modification 0 of IBM Technical Support Appliance and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2011, 2019.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# Contents

**Figures** ........................................... v

## Chapter 1. Introduction ................................... 1
User accounts and user groups .................................... 1
Discovery Scopes and Scope Sets .................................. 2
Discovery credentials .................................................. 2
Discovery schedule ..................................................... 3
Transmission schedule ................................................ 3

## Chapter 2. Prerequisites ................................... 5
Downloading TSA image ............................................... 5
Requirements for TSA on VMWare ESXi ................................ 5
Required internet browsers .......................................... 5
Configuration requirements for connections to IBM Support ...................................................... 6
Credential and software requirements for the discovery environment .......................................... 6

## Chapter 3. Setting up the virtual Technical Support Appliance ................................... 9
Installing by using VMware vSphere Client .................................. 9
Installing using VMware ESXi web interface .......................... 15
Installing TSA on Hyper-V ............................................. 19
Changing $tsausr$ password (required) ............................... 24
Configuring the network details ...................................... 25

## Chapter 4. Setting up the Technical Support Appliance ................................... 29
Connecting and powering on the hardware Technical Support Appliance ............................................. 29
Logging in to the Technical Support Appliance ......................... 30
Accepting the License Agreement ..................................... 32
Registering the Technical Support Appliance ........................ 33
Setting the clock ....................................................... 35
Configuring network settings ........................................... 37
  Configuring basic network settings ................................ 37
  Configuring advanced network settings ............................ 39
Setting up IBM connectivity ........................................... 46
Updating the Technical Support Appliance .......................... 47
  Viewing Documentation ............................................. 49
  Installing an SSL server certificate (Optional) ...................... 49
Setting up user accounts and user groups .............................. 51
  Setting up a user group ............................................ 51
  Setting up a user account .......................................... 54
Setting up discovery scopes .......................................... 55
Setting up discovery credentials ...................................... 57
  Configuring key pair authentication ................................ 60
  Modifying the discovery schedule .................................. 61
Running the discovery .................................................. 62
  Running the discovery on specific scope sets ....................... 62
  Running discovery on specific scopes ................................ 63
Modifying the transmission schedule .................................. 64
Running the transmission .............................................. 66

## Chapter 5. Using the Technical Support Appliance ................................... 69
User accounts and user groups ........................................ 69
  Displaying user accounts and user groups ......................... 69
  Adding user accounts and user groups ............................. 69
  Modifying user accounts and user groups ........................ 74
  Deleting user accounts and user groups ........................... 75
Discovery scopes ...................................................... 76
  Displaying discovery scopes and scope sets ....................... 76
  Adding discovery Scopes ........................................... 76
  Modifying a discovery scope set .................................... 79
  Deleting discovery scopes .......................................... 80
  Importing a scope set .............................................. 81
HMC Dynamic Scopes .................................................. 82
  Displaying HMC Dynamic Scopes, Scope sets and Credentials ................................. 82
  Adding HMC Dynamic Scopes ....................................... 83
  Modifying HMC Dynamic Scopes .................................... 85
  Deleting HMC Dynamic Scopes ...................................... 86
Discovery credentials .................................................. 86
  Displaying credentials .............................................. 86
  Viewing credential details ......................................... 87
  Adding credentials .................................................. 88
  Modifying credentials .............................................. 91
  Deleting credentials ................................................ 92
Discovery schedule ................................................... 92
  Viewing the discovery schedule .................................... 93
  Adding discovery schedule ........................................ 93
  Modifying the discovery schedule ................................ 95
  Disabling the discovery schedule ................................... 95
  Deleting the discovery schedule ................................... 96
  Running the discovery .............................................. 96
Saving the discovered data collection ................................. 98
Discovery history ...................................................... 98
Discovery Settings .................................................... 99
  Configuring Connection Settings .................................. 99
Transmission schedule ................................................ 100
  Viewing the transmission schedule ................................. 100
  Modifying the transmission schedule .............................. 100
  Disabling the transmission schedule ............................... 102
  Running the transmission .......................................... 102
Status information .................................................... 103
  Viewing the activity log ............................................ 104
  Viewing the inventory summary .................................... 104
  Scheduling inventory data cleanup ................................ 106
  Viewing inventory cleanup archive ................................ 108
Passwords ........................................................... 109
  Changing your password ............................................ 109
Security .............................................................. 109
  Configuring key pair authentication ............................... 110
  Installing an SSL server certificate (Optional) ...................... 111
  Modifying session timeout settings ................................ 113
  Modifying the password age ........................................ 113
Backup and restore ................................................... 114
  Update .................................................................. 116
<table>
<thead>
<tr>
<th>Chapter 6. Contacting IBM Support for the Technical Support Appliance (TSA)</th>
<th>127</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating service request at the IBM Support Portal</td>
<td>127</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix. Configuring the dhcp network details</th>
<th>129</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating request through the IBM Call Center</td>
<td>127</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accessibility</th>
<th>131</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notices</td>
<td>133</td>
</tr>
<tr>
<td>Trademarks</td>
<td>134</td>
</tr>
</tbody>
</table>
Figures

1. Deploy OVF Template ........................................ 10
2. Source of OVF Template ................................... 11
3. Name and Location ........................................... 12
4. Storage .......................................................... 13
5. Disk Format ....................................................... 14
6. Ready to Complete ............................................. 15
7. Create / Register VM .......................................... 16
8. Select creation type .......................................... 16
9. Select OVF and VMDK files ................................. 17
10. Select storage ................................................ 17
11. Deployment options ......................................... 18
12. Review settings selection ................................. 18
13. Hyper-V Manager ............................................. 19
14. Virtual Machine Name ....................................... 20
15. Specify Generation .......................................... 20
16. Startup Memory ............................................... 21
17. Configure Networking ...................................... 22
18. Connect Virtual Hard Disk ................................. 23
19. Summary ........................................................ 23
20. Summary ........................................................ 24
21. Change Password ............................................. 24
22. New Password ................................................ 25
23. Setup network configuration ............................. 25
24. Network Configuration ...................................... 26
25. Login .................................................................. 30
26. Change Password ............................................. 31
27. License Agreement ............................................ 32
28. Registration ..................................................... 34
29. Clock .................................................................. 36
30. Network ........................................................... 38
31. Advanced network ............................................ 40
32. Global ............................................................... 41
33. Network Interfaces ........................................... 42
34. DNS Settings .................................................... 43
35. Network Routes ................................................ 44
36. New Network Route .......................................... 45
37. IBM Connectivity .............................................. 46
38. Update ............................................................ 48
39. Update ............................................................ 48
40. Security ........................................................... 50
41. Groups ............................................................. 52
42. Add User Group ............................................... 53
43. User Accounts and Groups ............................... 54
44. Add User Account ............................................. 54
45. Discovery Scope Set .......................................... 56
46. Discovery Scopes .............................................. 56
47. New Discovery Credentials ............................... 58
48. Run discovery on specific scopes ..................... 63
49. Discovery Scopes .............................................. 63
50. Run discovery on specific scopes ..................... 64
51. Edit transmission schedule .............................. 65
52. Weekly by day(s) (Sun - Sat) ............................ 65
53. Run Transmission Now .................................... 66
54. Groups ............................................................. 70
55. Add User Group ............................................... 71
56. User Accounts and Groups ............................... 72
57. Add User Account ............................................. 73
58. Discovery Scope Set .......................................... 77
59. Discovery Scopes .............................................. 77
60. Import Scope Set .............................................. 81
61. HMC Dynamic Scopes ....................................... 82
62. View HMC Dynamic Scope Set ....................... 83
63. Add HMC Dynamic Scope Set ......................... 84
64. Enter Access Information ................................. 85
65. New Discovery Credentials .............................. 87
66. Discovery Credentials details ......................... 88
67. New Discovery Credentials .............................. 89
68. Discovery Schedule .......................................... 93
69. Add Discovery Schedule .................................. 94
70. Weekly by day(s) (Sun - Sat) ............................ 95
71. Run discovery on specific scopes ..................... 97
72. Discovery Scopes .............................................. 97
73. Run discovery on specific scopes ..................... 98
74. Discovery History ............................................. 99
75. Edit transmission schedule .............................. 101
76. Weekly by day(s) (Sun - Sat) ............................ 101
77. Run Transmission Now .................................... 103
78. Activity Log .................................................... 104
79. Inventory Summary ......................................... 105
80. Inventory Summary Detail ............................... 106
81. Inventory Cleanup Schedule ............................ 107
82. Inventory Cleanup Archive .............................. 108
83. Security .......................................................... 112
84. Backup and Restore ........................................ 115
85. Update ............................................................ 117
86. Update ............................................................ 117
87. Logging and Trace .......................................... 119
88. Shutdown ......................................................... 121
89. Network Tools ................................................ 123
90. Authentication Status ..................................... 124
91. Documentation ............................................... 126
92. Setup network configuration ............................ 129
93. Network Configuration .................................... 129
94. DHCP IP Address ............................................ 130
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 is delivered as a virtual appliance that can be loaded onto your System x series, but can also be delivered as a hardware appliance.

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.

Note: 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.

Note: Throughout the document, TSA refers to the Technical Support Appliance.

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, 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, 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 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 IP addresses. For more information, see section “Importing a scope set” on page 81.

Note: For better performance, limit the cumulative number of IP addresses (after expanding any range or subnet scope elements) to 400 or less.

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.

Related tasks:

“Adding user accounts and user groups” on page 69
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 instance 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 for all the scope sets available. You can also create individual schedules to perform discovery on the selected scope sets. TSA has a default discovery schedule that you can modify for your needs. 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.

Note: All the prerequisites in the following sections are mandatory for both hardware and virtual TSA with an exception of requirements specified in the section “Requirements for TSA on VMWare ESXi.”

Downloading TSA image

TSA images can be downloaded from Fix Central at the following link.
[http://ibm.biz/TSAImageFixCentral](http://ibm.biz/TSAImageFixCentral)

Requirements for TSA on VMWare ESXi

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

**x86 64-bit hardware**

The virtual TSA must be loaded on x86 64-bit systems.

**Processor**

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

**CPU**

TSA requires four 64-bit CPUs.

**Memory**

TSA requires 8 GB memory.

**Direct access storage device (DASD)**

TSA requires 150 GB of DASD.

**Network**

TSA requires a 1-Gigabit Ethernet adapter.

Required internet browsers

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

TSA supports the following internet browsers:

- Mozilla Firefox V60.3.0 Extended Support Release (ESR)
- Microsoft Internet Explorer V9.0, V10.0 for Windows 7
- Microsoft Internet Explorer V11.0 for Windows 8
- Microsoft Edge browser for Windows 10
- Google Chrome V70.0.3538.77 (64-bit)

You can download these browsers from the following sites:

- [Microsoft Internet Explorer](http://www.microsoft.com/downloads/)
- [Mozilla Firefox](http://www.mozilla.org/products/firefox/)
- [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

<table>
<thead>
<tr>
<th>DNS name</th>
<th>IP address</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>esupport.ibm.com</td>
<td>129.42.54.189</td>
<td>443</td>
<td>HTTPS (to IBM)</td>
</tr>
<tr>
<td></td>
<td>129.42.56.189</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>129.42.60.189</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Type of credential</th>
<th>Access information</th>
</tr>
</thead>
</table>
| 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.  
  - **Default** - Use the appliance SSH Key if it exists, else use the provided password.  
  - **Password** - Use the provided password.  
  - **Public Key Infrastructure (PKI) using Scope Set specific SSH Key** - Use SSH key associated with the specific scope set.  
  - **PKI using Appliance SSH Server Key** - Use the appliance SSH Server Key that is installed through the Administration > Security pane. |
| Computer System (Windows)          | **User name:**  
User name to access the Windows computer system.  
**Password:**  
Password to access the Windows computer system.  
**Authentication type:**  
The type of authentication for the computer system (Windows) is **Password**. |
| 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 |
<table>
<thead>
<tr>
<th>Type of credential</th>
<th>Access information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other (Cisco Device)</td>
<td><strong>User name:</strong> The user name to access the Cisco device.</td>
</tr>
<tr>
<td></td>
<td><strong>Password:</strong> The password for the Cisco device.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable password:</strong> The enable password for the Cisco device.</td>
</tr>
<tr>
<td>Other (Cisco Works)</td>
<td><strong>User name:</strong> The user name to access the CiscoWorks server.</td>
</tr>
<tr>
<td></td>
<td><strong>Password:</strong> The password to access the CiscoWorks server.</td>
</tr>
</tbody>
</table>

**Note:** For more information about credentials and software requirements, refer to the Configuration Assistant Document.
Chapter 3. Setting up the virtual Technical Support Appliance

TSA 2.4 includes preinstalled software. It is packaged and distributed as an OVA image for VMware installations or as a VHDX image for Hyper-V installations. For VMware, TSA 2.4 can be installed by using either the VMware vSphere Client or the VMware web interface (for ESXi). For Hyper-V, TSA 2.4 can be installed by using Hyper-V Manager. This section provides the steps for installing TSA 2.4 using all of these methods.

Installing by using VMware vSphere Client

Before you begin

The virtual TSA requires VMware ESXi 6.x to be loaded to control the hardware.

About this task

Follow these steps to install the virtual TSA 2.4 image by using the VMware vSphere Client. For information on the requirements, see “Requirements for TSA on VMware ESXi” on page 5.

Note: The procedure (from step 1 to step 12) is an example / reference on how to deploy an OVA image. Some of these steps might vary based on your local procedures for deploying virtual machines.

Procedure

To install TSA 2.4, follow these steps:

1. Start the VMware vSphere Client.
2. Log in to connect to the ESXi system.
3. On the vSphere Client, click File > Deploy OVF Template. The Deploy OVF Template wizard is displayed.
4. Click **Browse** and select the OVA image that is saved on your system.
5. Click Next. The **OVF Template Details** are displayed.
6. Click Next. The **Name and Location** pane is displayed.
7. On the **Name and Location** pane, enter the **Name** for your virtual machine or you can use the default value and click **Next**.

8. On the **Storage** pane, select the data store (storage for the virtual machine files) and click **Next**.
9. On the Disk Format pane, select the **Thick Provision Eager Zeroed** option and click **Next**.

---

**Figure 4. Storage**

---

Chapter 3. Setting up the virtual Technical Support Appliance 13
10. If your ESXi has a single network connection, proceed to the next step. Otherwise, select the appropriate network on the Network Mapping pane and click Next.

11. Optional: Select **Power on after Deployment** option to automatically power on the virtual machine after deployment. You can also manually power on the virtual machine after the completion of deployment.
12. Click Finish. Deploying TSA might take around 30 minutes but varies based on the speed of the network connection between your system and the VMware ESXi system.

13. On successful deployment of the appliance, select the newly deployed virtual machine and click the Console tab of the vSphere Client.

14. Log in to the TSA console to set up the network configuration. Enter the ibm TSA login as tsau and Password as configTsa.

15. Required: To change the login password, continue with the steps that are listed in the section “Changing tsau password (required)” on page 24.

16. To complete the installation, continue with the steps that are listed in the section “Configuring the network details” on page 25.

Installing using VMware ESXi web interface

Before you begin

The virtual TSA requires VMware ESXi 6.x to be loaded to control the hardware.

About this task

Follow these steps to install the virtual TSA image by using the VMware ESXi web interface.
Procedure

1. Log in to connect to the ESXi system through the vSphere Web Client.
2. Click Create/Register VM. The New virtual machine wizard displays.

![Figure 7. Create / Register VM](image)

3. On the Select creation type screen, select the **Deploy a virtual machine from an OVF or OVA file** option to specify how you would like to create a virtual machine and click **Next**.

![Figure 8. Select creation type](image)

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

6. 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.

7. On the Deployment options screen, select network mappings from the VM Network drop-down list.
8. Select the **Thick** option for disk provisioning. Then, click **Next**.

9. 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.
   The TSA virtual machine is installed on your system.

10. In the TSA console, enter the `ibmtsa login` as **tsausr** and **Password** as `configTsa`.

11. Required: To change the login password, continue with the steps that are listed in the section "Changing **tsausr** password (required)" on page 24.
12. To complete the installation, continue with the steps that are listed in the section “Configuring the network details” on page 25.

Installing TSA on Hyper-V

Before you begin

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

- Hyper-V Server 2012
- Hyper-V Manager
- Virtual Network Switch has been created through Hyper-V Manager

About this task

Follow these steps to install TSA 2.4 on Hyper-V.

Procedure

To install TSA 2.4 on Hyper-V, follow these steps:

1. Download the ibmTSA_2400.zip file from Fix Central.
2. Extract ibmTSA_2400.zip file and move ibmTSA_2400.vhdx to a directory on Hyper-V server.
3. Start the Hyper-V Manager and connect to Hyper-V server from the client system.
4. Click Browse and select the OVA image that is saved on your system.

6. Enter the Name for the new virtual machine and click Next.
7. Select **Generation 1** as the generation of the virtual machine and click **Next**.
8. Enter **Startup memory** as 8192 MB and click **Next**.

![Assign Memory](image)

**Figure 16. Startup Memory**

9. Select a preconfigured virtual switch and click **Next**.
10. Select the **Use an existing virtual hard disk** option and browse for the `ibmtsa_2400.vhdx` file that you copied to Hyper-V server in **Step 2** and click **Next**.
11. In the Summary page, review the settings and click Finish.
12. The new virtual machine is added under the Hyper-V Manager. Select the virtual machine, go to Action menu and click Start.

![Hyper-V Manager](image)

*Figure 20. Summary*

13. Using Connect start a console session. In the TSA console, enter the `ibmtsa` login as `tsaur` and Password as `configTsa`.

14. Required: To change the login password, continue with the steps that are listed in the section “Changing `tsaur` password (required).”

15. To complete the installation, continue with the steps that are listed in the section "Configuring the network details” on page 25.

---

**Changing `tsaur` password (required)**

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

**Procedure**

1. Select option 2) Change `tsaur` password from the TSA Config Menu.

![TSA Config Menu](image)

*Figure 21. 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.

![Configuration Menu](image1.png)

**Figure 22. New Password**

### Configuring the network details

**Procedure**

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

![Setup Network Configuration](image2.png)

**Figure 23. Setup network configuration**

2. Enter the following network configuration details.
a. Enter IPTYPE = {static | dhcp}. Enter static or dhcp. If static, follow these steps, else go through the dhcp configuration steps in the section, “Configuring the dhcp network details,” on page 129

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 2a.

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 37. To configure the advanced network settings, follow the steps in “Configuring advanced network settings” on page 39.
3. Follow these steps to setup the virtual TSA, similar to that of hardware TSA from the Web UI:
   a. “Logging in to the Technical Support Appliance” on page 30
   b. “Accepting the License Agreement” on page 32
   c. “Registering the Technical Support Appliance” on page 33
   d. “Setting the clock” on page 35
   e. “Setting up IBM connectivity” on page 46
   f. “Updating the Technical Support Appliance” on page 47
   g. “Installing an SSL server certificate (Optional)” on page 49
   h. “Setting up user accounts and user groups” on page 51
   i. “Setting up discovery credentials” on page 57

Results

After you successfully set up TSA, see Chapter 5, “Using the Technical Support Appliance,” on page 69.
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. "Connecting and powering on the hardware Technical Support Appliance"
2. "Logging in to the Technical Support Appliance” on page 30
3. “Accepting the License Agreement” on page 32
4. “Registering the Technical Support Appliance” on page 33
5. “Setting the clock” on page 35
6. “Configuring network settings” on page 37
7. “Setting up IBM connectivity” on page 46
8. “Updating the Technical Support Appliance” on page 47
9. “Installing an SSL server certificate (Optional)” on page 49
10. “Setting up user accounts and user groups” on page 51
11. “Setting up discovery scopes” on page 55
12. “Setting up discovery credentials” on page 57
13. “Modifying the discovery schedule” on page 61
14. “Running the discovery” on page 62
15. “Viewing the inventory summary” on page 104
16. “Modifying the transmission schedule” on page 64
17. “Running the transmission” on page 66

What to do next

When you finish setting up TSA, see Chapter 5, “Using the Technical Support Appliance,” on page 69 for information about how to perform other tasks.

Connecting and powering on the hardware Technical Support Appliance

When you have received a physical hardware appliance from IBM, before signing on to TSA, you must ensure that it is connected and powered on.

About this task

Follow these steps to connect and power on TSA.

Procedure

1. Before powering the system on, connect an Ethernet cable from Ethernet Port 1 to your local Ethernet.
2. Connect a monitor, USB mouse, and USB keyboard to the system.
3. Power on the system. The monitor displays several messages at startup. After several minutes, the startup tasks complete and the VMware ESXi display is shown.

4. Press **F2** and enter `pw4ibmtsa` as the root password for ESXi.

   **Note:** After you connect, it is recommended that you change this default root password. To change the password, use **Configure Password** on the VMware ESXi console.

---

**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 internet 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.

   For virtual TSA, the initial password is `passw0rd`. For hardware TSA that is shipped from IBM, the initial password is `passw0rd1`. You must change this initial password after you log on to TSA.

---

![Login Page](image)

**Figure 25. Login**

The Change Password pane is displayed on your first login.
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 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 the appliance), contact IBM Support.

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

4. Click Accept.

   The Summary page is displayed.

Related concepts:

"Required internet browsers" on page 5
A web-based user interface is used to set up and monitor discovery and transmission.

Related tasks:
Accepting the License Agreement

Read and accept the License Agreement to proceed further.

The License Agreement includes the following items:

- IBM Base License Agreement
• IBM License and Statement of work

  Note: TSA is now GDPR compliant [EU/2016/679]. You can view the GDPR compliant information in the IBM License and Statement of work section.

• Terms and Conditions for Separately Licensed Code

  Click Accept to accept the agreement and start working with TSA.

  Note: The License Agreement displays only when you login to TSA for the first time. After you accept the agreement, the License Agreement page is not displayed.

Registering the Technical Support Appliance

Registering collects information required to identify TSA when it reports information to IBM for analysis.

Before you begin

Ensure that you use a system that is configured with the US International English keyboard layout when you are registering TSA.

About this task

To register, follow these steps:

Procedure

1. In the navigation pane, click Administration > Registration. The Registration page is displayed.
2. Specify service contact information in the following fields:

   **Company name**
   The name of the organization that uses TSA to monitor its systems.

   **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://clientinsightportal.ibm.com/](https://clientinsightportal.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](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.

   **Postal code**
   The postal code of the company.

   **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 or click **Cancel** to exit the Registration page.

### Setting the clock

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

**Procedure**

1. In the navigation pane, click **Administration > Clock**. The Clock page is displayed.
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 an 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.

---

### Configuring network settings

TSA setup includes configuring network information. Basic network configuration involves configuring the primary Ethernet adapter and other network information. As an alternative, you can configure TSA to access multiple networks.

**Before you begin**

To interact with the TSA user interface, you have to setup the basic network configuration initially by accessing the console. Later, you can configure the advanced settings or modify the basic settings through the user interface.

To configure basic network settings through the console, follow the steps in the **“Configuring the network details” on page 25** section.

**Configuring basic network settings**

To use basic network settings for TSA, you must configure the primary Ethernet adapter and other network information. Use the Network page if you want to alter the initial network configuration that was applied.

**Procedure**

1. In the navigation pane, click **Administration > Network**. The Network page is displayed.
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 “Configuring the dhcp network details,” on page 129.

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 a Domain Name System (DNS) server on your network for converting host names into IP addresses.

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 appliance UI may not be reachable. In that event, the VMware vSphere Client would be required to access the TSA console and repair the network configuration.

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**.
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:
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.
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.

Figure 34. DNS Settings
Name Services
Specify a domain name system server 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.

![Network (advanced) page](image)

Figure 35. 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. This must be in 32-bit dotted-decimal notation.

**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 do not have any actions that can be done on them.

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.

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 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](image)

*Figure 37. IBM Connectivity*

2. In the Access section, select from the following Internet access types:
Allow direct SSL connection
   The system connects to IBM by using a direct connection.

Use SSL proxy connection
   The system connects to IBM by using an SSL proxy connection.

Use authenticating SSL proxy connection
   The system connects to IBM by using an authenticating SSL proxy connection.

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

   IP address or host name
      The IP address or host name of the proxy server.

      Note: The host name must not contain an underscore (“_”).

   Port
      The port number of 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 enter 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” on page 6

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.

Updating the Technical Support Appliance

Update TSA to the latest level after you log in for the first time.
Procedure

1. In the navigation pane, click **Administration > Update**. The Update page is displayed.

![Update](image1.png)

*Figure 38. Update*

2. Click **Check for Update**. The Update Availability page lists any available updates.

![Update](image2.png)

*Figure 39. Update*

3. To install the updates, click **Perform Update Now**. Upon completion of the update, TSA is automatically restarted.
4. To view information about the contents of the update, click View Update Details.

Viewing Documentation

Procedure
1. In the navigation pane, click Administration > Update. The Update page is displayed.
2. Click View Documentation to open the Documentation page where you can download documentation for the currently installed release.

Note: If you do an update, then you must wait for the update process to complete to view the latest documentation that matches the updated appliance release version.

Installing an SSL server certificate (Optional)

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, or upload your own Java keystore file that contains a custom SSL server certificate signed by the certificate authority of your choice.

Before you begin

If you want to upload a custom certificate, you must acquire the certificate and package it in a Java 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 the key entry password and the keystore password identical.

Procedure
1. In the navigation pane, click Administration > Security. The Security page is displayed.
2. To install a self-signed server certificate, click Generate and install a new Self-signed Certificate. This certificate is unique to this TSA.
3. 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 a Custom Certificate** 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.

**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.

**Setting up user accounts and user groups**

**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.

**Setting up a user group**

**Procedure**

1. In the navigation pane, click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. Click the **Groups** tab.
3. Click Add User Group. The User Group page is displayed.

**Figure 41. Groups**
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 can optionally select which scope sets this user group has the authority to discover. For more information about scope sets, see "Discovery Scopes and Scope Sets" on page 2.

8. Click **Save** to save the user group. The User Accounts and Groups page is displayed with the new user group in the list.
Setting up a user account

Procedure

1. In the navigation pane, click Administration > User Accounts. The User Accounts and Groups page is displayed.

2. To define a new user account, click Add User Account. The User Account page is displayed.
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 **Maximum Password Age** 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 enter 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.
9. Select the user groups for this user account. 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.

---

**Setting up discovery scopes**

Set up discovery scopes to specify the IP address, range of IP addresses, network, or subnet to be used during discovery. Discovery scopes are grouped into discovery scope sets.

**Before you begin**

**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 (after expanding any range or subnet scope elements) to 400 or less.

   For information on importing a scope set, see section "Importing a scope set" on page 81

   • 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.

---

Chapter 4. Setting up the Technical Support Appliance  55
About this task

Procedure

1. In the navigation pane, click **Discovery Scopes**. The 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.

   a. For Describe Scope Set in the **Scope set name** field, enter a unique scope set name.
   b. Click **Save**. The new scope set is created and the Discovery Scopes page is displayed.

3. To add a scope to the new scope set, 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 hostname.
   - **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 hosts, 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:** You cannot reuse an IP address, range of IP addresses, subnet, 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.

---

**Setting up discovery credentials**

Set up discovery credentials to provide access control for the discovery process.

**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.
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. For information about configuring key pair authentication, see section “Configuring key pair authentication” on page 60.

**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.
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 86.

d. In the Select Scope Set Restriction pane, specify whether to use the access information across all scope sets or to limit the access information 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. For information about creating discovery scope sets, see “Setting up discovery scopes” on page 55.

e. If you choose to limit the access to a scope set that you specify, select the scope set from the **Scope set name** drop-down list in the Restrict To Selected Scope Set pane. 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 TS4500
- IBM TS7700
- IBM DS3000, DS4000, and DS5000 if password protected
- Windows

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.

### Configuring key pair authentication

You must configure discovery credentials on TSA to enable discovery on target devices. You can configure credentials that use user name and password authentication or OpenSSH Version 2 key-pair authentication. The advantage of using key-pair authentication is that you do not have to maintain passwords in TSA for service accounts that exist on the target devices.

#### Before you begin

Before you configure discovery credentials that use key-pair authentication, ensure the following:

- The service account is created on the target devices and has the necessary authorizations for the relevant platform
- No firewalls are blocking access from TSA to the target devices on port 22
- The private key must be uploaded through the UI when you select **PKI using Scope Set specific SSH Key** authentication and you must externally deploy the public key on the endpoint.

For more information about SSH, see the following sources:

- **OpenSSH**

- **SSH.com**

#### Procedure

1. **Generate the key pair**
   a. In the navigation pane, click **Administration** > **Security**. The Security page is displayed.
   b. Enter a passphrase in the **Passphrase** field.

   **Important:** The passphrase must be at least eight characters long and contain at least one numeric and one alphabetic character. A good passphrase is 10 - 30 characters long and consists of both numeric characters and random upper and lowercase alphabetic characters.
   c. Enter the passphrase again in the **Confirm Passphrase** field. The two passphrases that you enter are compared to confirm that they match before the passphrase is saved.
   d. Save the passphrase in a secure location for use in later configuration steps.
   e. Click **Generate SSH Server Public/Private Key Pair**. A message that the key pair has been generated along with a **Download SSH Server Public Key** button is displayed in the SSH Server Key Status pane.

2. **Download the generated public key**
a. Click **Download SSH Server Public Key** to download the public key on the system that you are using to sign on to TSA. This is the key that you deploy on the target devices.

3. **Deploy the public key to the target systems**
a. Use any available process or utility to deploy the public key to the target devices.

4. **Create the discovery credential**
a. In the navigation pane, click **Discovery Credentials**. The Discovery Credentials page is displayed.
b. Click **Add New Credentials**. The New Discovery Credentials page is displayed.
   1) In the **Name** field, type an identifying name for the credential.
   2) In the Credential Type drop-down list, select **Computer System**.
   3) In the **Enter Access Information** pane, specify the following information:
      - **User name**
         The user name for the service account on the target computer system.
      - **Password**
         The passphrase you specified when generating the public/private key pair.
      - **Confirm password**
         Enter the passphrase again. The two passphrases that you enter are compared to confirm that they match before the passphrase is saved.
      - **Authentication type**
         Select **PKI using Appliance SSH Server Key**.
   4) Click **Save**. The new credential is displayed in the Discovery Credentials page.

TSA can now run discoveries against the target that have this service account configured and the public key installed, and login using OpenSSH Version 2 key-based authentication.

---

**Modifying the discovery schedule**

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

**Procedure**

1. In the navigation pane, click **Discovery Schedule**. The Discovery Schedule page is displayed.
2. Click **Edit Schedule (계획)** 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.
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 screen.

3. To run a discovery on a specific schedule, click the Run icon for that schedule.
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 specific scope sets

Procedure

To run a discovery on a specific scope set, follow these steps:

1. In the navigation pane, click Discovery Scopes. The Discovery Scopes page is displayed. This page displays a list of all scope sets that are defined for this TSA.
2. To run a discovery on a specific scope set, click the Run icon for that scope set.

**Running discovery on specific scopes**

**Procedure**

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.

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.
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.

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.
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.

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.

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]

Figure 53. Run Transmission Now

2. Click Run Transmission Now. The History section is updated indicating that the transmission is running.

Tip: To save the results of the data collection on your system, click Download Last Collection and specify a location for the resultant file (collection.tar.xz). 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).

Depending on the amount of data, the download operation might take some time.

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.
Chapter 5. Using the Technical Support Appliance

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

User accounts and user groups

You can use user accounts and user groups to grant access to TSA functions.

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 section displays the user name, full name, and description that is associated with the selected user account. The Member Of section displays 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 section displays the name and authority level that is associated with the user group. The scope restrictions section displays the scope sets that the selected user group can discover. The Members section displays 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” on page 2

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.
3. Click **Add User Group**. The User Group page is displayed.

![User Accounts and Groups](image)

*Figure 54. Groups*
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 can optionally select which scope sets this user group has the authority to discover. For more information about scope sets, see "**Discovery Scopes and Scope Sets**" on page 2.

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.

2. To define a new user account, click Add User Account. The User Account page is displayed.
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 **Maximum Password Age** 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 enter 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.
9. Select the user groups for this user account. 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 75.

6. In the Member Of pane, you can change the user groups to which this user account belongs.

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 Administrator group and existing user groups.

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 Discovery authority level in the Restrict To Selected Scope Sets pane, you can change the scope sets that this user group has the authority to discover.

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 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: You can delete a user group even if there are users assigned to the group, but the users will no more be assigned to that group.
Discover scopes

A discovery scope specifies the IP address, range of IP addresses, or network to be used to discover resources. Discovery scopes are grouped into discovery 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 in the navigation pane. The Discovery Scopes page is displayed. The Scope Sets pane contains a list of the scope sets.

To display the scopes that a scope set contains, click the scope set. The Discovery Scope Set page is displayed. 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, 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 (after expanding any range or subnet scope elements) to 400 or less. For information on importing a scope set, see section “Importing a scope set” on page 81

- 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.

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

Procedure

1. In the navigation pane, click Discovery Scopes. The 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.
a. For Describe Scope Set in the **Scope set name** field, enter a unique scope set name.

b. Click **Save**. The new scope set is created and the **Discovery Scopes** page is displayed.

3. To add a scope to the new scope set, 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 hostname.
   - **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 hosts, 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:** You cannot reuse an IP address, range of IP addresses, subnet, 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.

**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**. The Discovery Scopes page is displayed.
2. In the Scope Sets 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 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 Hostname.
   - **Range of IP addresses**
     For **Describe Address Range**, enter the starting IP address, ending IP address, and a description in the fields provided.
   - **Network or Subnet**
     For **Describe Network or Subnet**, enter the IP address, mask, and a description in the fields provided.
5. If you want to exclude hosts, 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:** You cannot reuse an IP address, range of IP addresses, subnet, 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.
Moving scopes from one scope set to another scope set
You can move one or more scopes from one scope set to another scope set.

Procedure

To move scopes from one scope set to another scope set, follow these steps:
1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. In the **Scope Sets** pane, click to select a scope set from which you want to move scopes. The Discovery Scope Set page is displayed.
3. Click **Move Scopes**. The Move Scopes from one set to another page is displayed.
4. Select the scopes that you want to move from the **Scopes** list. You can select one or more scopes here.
5. Select the scope set from the **Destination Scope Set** list to which you want to move the scopes.
6. Click **Move**.

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**. The Discovery Scopes page is displayed.
2. To edit the scope set, click the **Edit** icon 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 hostname.
        - **Range of IP addresses**
          For Describe Address Range, type the starting IP address, ending IP address, and a description in the fields provided.
        - **Network or Subnet**
          For Describe Network or Subnet, type the IP address, mask, and a description in the fields provided.

   **Note:** Provide a unique name for **Description**. If you specify the description that is already existing for any other scope, TSA will not allow you to create a 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 hosts, 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 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. The 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**. The 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 to define a new scope set.

**About this task**

A new scope set is created based on the specified name and the list of the IP addresses from the input file. TSA performs the following validations when you import 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 or not.
- Ignores trailing and leading blank spaces when validating IP address.
- Ignores duplicate IP addresses.

**Procedure**

To import the IP addresses, follow these steps:

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

   ![Image of text file](image)

   **Figure 60. Import Scope Set**

   **Note:** The text file must be formatted to a single column where each row contains a single IP address 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 Discovery Scopes section of the user interface and associate credentials in the Discovery Credentials section.
HMC Dynamic Scopes

You can define HMC Dynamic Scopes to collect detailed inventory from IBM Power Systems for VIOS, AIX, and Linux partitions.

About this task

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

Displaying HMC Dynamic Scopes, Scope sets and Credentials

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

About this task

To display the existing HMC dynamic scope sets, 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, HMC partition scope sets, and credentials that a scope set contains, click the scope set. The HMC Dynamic Scope Set page is displayed.
The Scopes pane displays details about the scopes in the scope set. The Credentials pane lists the credentials that are configured in the scope set. The HMC Partition Scope Set displays the scope sets of the selected HMC partitions.

### Adding HMC Dynamic Scopes

To add an HMC Dynamic Scope, specify the IP address of the HMC. Each scope defines a single HMC. Additional information is required to indicate how LPARs of each supported operating system are to be accessed.

#### 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.
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 **LPARs** pane, select the type of LPARs (AIX, LINUX, or VIOS) to include in the dynamic discovery.

6. In the **Enter Access Information for HMC** pane, enter the following details -
   a. Enter the **Credential name**
   b. Enter the **User name** that is used to authenticate when connecting to the HMC.
   c. Enter the **Password** and **Confirm password**
   d. Select the **Authentication type**
      - **Default** - Uses the appliance SSH Key if it exists, else uses the provided password.
      - **Password** - Uses the provided password.
      - **Public Key Infrastructure (PKI) using Scope Set specific SSH Key** - Uses SSH key that is associated with the specific scope set.
      - **PKI using Appliance SSH Server Key** - Uses the appliance SSH Server Key that is installed through the **Administration > Security** pane.

7. Optional: Click **Test Credential** to test the credentials of the target HMC.
8. If you select any of the LPAR types (AIX, Linux, or VIOS), enter the respective access information.

![Enter Access Information for LINUX LPARs](image)

**Figure 64. Enter Access Information**

- a. Enter the Credential name.
- b. Enter the User name that is used to authenticate to the respective LPAR.
- c. Enter the Password and Confirm password.
- d. Optional: Enter the IP address of the LPAR and click Test Credential to test the credentials of the target LPAR.

9. Click Save to save the HMC dynamic scope set.

**Modifying HMC Dynamic Scopes**

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

**About this task**

To modify an existing HMC dynamic 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 edit the scope set, click the Edit icon beside the scope set. The HMC Dynamic Scope Set page is displayed. You can edit the scope set by editing the Scopes, editing the credentials, or by deleting the credentials.
   - To edit a scope, follow these steps:
     - a. In the Scopes pane, click the Edit icon beside the scope. The Discovery Scopes page is displayed.
     - b. You can edit the IP address and click Save to save the modifications.
To run a discovery on the HMC dynamic scope, click the Run icon for that scope.

To edit the credentials, follow these steps:

a. In the Credentials pane, click the Edit icon beside the credential. The Edit Discovery Credentials page is displayed.

b. Select the Scope set name, if it is HMC or the LPAR partition.

c. 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 HMC.
2) Enter the Password and Confirm password.
3) Select the Authentication type.

Note:

Only one SSH key per Scope Set is allowed. If a new SSH key is assigned to the scope set when the scope set is modified, the new SSH key replaces the existing SSH key.

d. Click Save to update the modifications for the respective credential.

Deleting HMC Dynamic Scopes

You can delete an existing HMC dynamic scope set.

About this task

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 to delete the HMC dynamic scope set, the respective access information for AIX, Linux, or VIOS partitions is also deleted.

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 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 this appliance 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, the username and password are not case sensitive and the username should be a fully qualified username that includes the domain name of the system or the domain name of the Active Directory domain.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>User Name</th>
<th>Password Changed Date</th>
<th>Scope Set Restriction</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFS 040</td>
<td>Computer System</td>
<td>J/vlc</td>
<td>6/15/15</td>
<td>IFS 040</td>
<td></td>
</tr>
<tr>
<td>IFS 820</td>
<td>Computer System</td>
<td>user</td>
<td>6/15/15</td>
<td>IFS 820</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 65. 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. The General section displays the name and type of credential. The Properties section displays the name and value of various properties of the credential.
Related tasks:

“Modifying credentials” on page 91

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.
In the Name field, type an identifying name for the credential. In the Credential Type drop-down list, select the type of credential that you want to create. 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. For information about configuring key pair authentication, see section “Configuring key pair authentication” on page 60.

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.
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 86.

d. In the Select Scope Set Restriction pane, specify whether to use the access information across all scope sets or to limit the access information 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. For information about creating discovery scope sets, see “Setting up discovery scopes” on page 55.

e. If you choose to limit the access to a scope set that you specify, select the scope set from the Scope set name drop-down list in the Restrict To Selected Scope Set pane. 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 TS4500
   • IBM TS7700
   • IBM DS3000, DS4000, and DS5000 if password protected
   • Windows

   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.

   **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 86](#).

   b. In the Select Scope Set Restriction pane, specify whether to use the access information across all components of the entire discovery scope or to limit the access information 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. If you choose to limit the access to a scope set that you specify, select the scope set from the **Scope set name** drop-down list in the Restrict To Selected Scope Set pane. The credential is used only when discovering using 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 a 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” on page 2

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” on page 6

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**

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 Summary 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 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](image)

Figure 68. 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 that is created with the default date (2:15 AM on Tuesday). 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.

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

4. Select the **Show only unassigned Scope Sets** option to view only those scope sets that are not assigned to any discovery schedule.

5. Select the desired scope sets from **Select Scope Sets** list. Alternatively, 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.
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 this schedule according to your needs.

**Procedure**
1. In the navigation pane, click **Discovery Schedule**. The Discovery Schedule page is displayed.
2. Click **Edit Schedule** (كرة) 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.
Procedure

To disable scheduled discoveries, follow these steps:
1. In the navigation pane, click Discovery Schedule. The Discovery Schedule page is displayed.
2. Click 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 icon for the respective schedule to be deleted.

Note: You cannot delete the default full discovery schedule, but the default full discovery 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 screen.
3. To run a discovery on a specific schedule, click the Run icon for that schedule.
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 specific scope sets

Procedure

To run a discovery on a specific scope set, follow these steps:
1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed. This page displays a list of all scope sets that are defined for this TSA.

![Discovery Scopes](image1.png)

**Figure 71. Run discovery on specific scopes**

2. To run a discovery on a specific scope set, click the **Run** icon for that scope set.

**Running discovery on specific scopes**

**Procedure**

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.

![Discovery Scopes](image2.png)

**Figure 72. 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](image)

*Figure 73. 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.

**Saving the discovered data collection**

You can save the last discovered data collection.

**About this task**

To save the last discovered data collection, follow these steps:

**Procedure**

1. In the navigation pane, click Transmission Schedule. The Transmission Schedule page is displayed.

2. Click Download Last Collection. Specify where you want to save the data.

   *Note:* Depending on the amount of data, the save operation might take some time.

**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](image)

**Figure 74. 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. The Discovery scopes pane displays the scopes that were used for 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.

**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.*

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](image)

**Figure 75. Edit transmission schedule**

- Use the **At hour** and **At minute** drop-down lists to select a new time.
- 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.

![Weekly by day(s) (Sun - Sat)](image)

**Figure 76. 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 **Do not perform 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 **Perform 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.
2. Click **Run Transmission Now**. The History section is updated indicating that the transmission is running.

   **Tip:** To save the results of the data collection on your system, click **Download Last Collection** and specify a location for the resultant file (collection.tar.xz). 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).

   Depending on the amount of data, the download operation might take some time.

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.

---

**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](image)

**Figure 78. 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 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.

The Inventory Summary page shows six different groups of IT elements:

- **Hypervisors**: Includes hypervisors such as HMC, IBM Flex System Manager, VM, 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](#) panel (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 is completed.

**Note:** The data on this pane is populated shortly after TSA is started. If you view the page in this time frame, 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 this display, click **Refresh** 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](image)

**Figure 80. 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 discovered by Level 1 Discovery through Nmap, but that do not have credentials to allow a Level 3 Discovery, no values are provided in the **Element information** pane.

Click **Download Inventory Summary** to download a file containing a summary of the devices that are discovered.

**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**

To view the current schedule for the inventory cleanup task, select **Inventory Summary > 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 transmission on a particular day(s) of a week, select the **Weekly by day(s) (Sun - Sat)** option or 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 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**.

### 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](image)

**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.

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 the appliance), contact IBM Support. For more information, see section [“Logging in to the Technical Support Appliance” on page 30](#).

---

### 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 configure SSH key pair authentication, generate or upload and install a server certificate, or modify session timeout settings.
Configuring key pair authentication

You must configure discovery credentials on TSA to enable discovery on target devices. You can configure credentials that use user name and password authentication or OpenSSH Version 2 key-pair authentication. The advantage of using key-pair authentication is that you do not have to maintain passwords in TSA for service accounts that exist on the target devices.

Before you begin

Before you configure discovery credentials that use key-pair authentication, ensure the following:

- The service account is created on the target devices and has the necessary authorizations for the relevant platform.
- No firewalls are blocking access from TSA to the target devices on port 22.
- The private key must be uploaded through the UI when you select **PKI** using **Scope Set** specific **SSH Key** authentication and you must externally deploy the public key on the endpoint.

For more information about SSH, see the following sources:

**OpenSSH**


**SSH.com**


Procedure

1. Generate the key pair
   a. In the navigation pane, click **Administration** > **Security**. The Security page is displayed.
   b. Enter a passphrase in the **Passphrase** field.

   **Important:** The passphrase must be at least eight characters long and contain at least one numeric and one alphabetic character. A good passphrase is 10 - 30 characters long and consists of both numeric characters and random upper and lowercase alphabetic characters.

   c. Enter the passphrase again in the **Confirm Passphrase** field. The two passphrases that you enter are compared to confirm that they match before the passphrase is saved.

   d. Save the passphrase in a secure location for use in later configuration steps.

   e. Click **Generate SSH Server Public/Private Key Pair**. A message that the key pair has been generated along with a **Download SSH Server Public Key** button is displayed in the SSH Server Key Status pane.

2. Download the generated public key
   a. Click **Download SSH Server Public Key** to download the public key on the system that you are using to sign on to TSA. This is the key that you deploy on the target devices.

3. Deploy the public key to the target systems
   a. Use any available process or utility to deploy the public key to the target devices.

4. Create the discovery credential
a. In the navigation pane, click **Discovery Credentials**. The Discovery Credentials page is displayed.

b. Click **Add New Credentials**. The New Discovery Credentials page is displayed.

1) In the **Name** field, type an identifying name for the credential.
2) In the Credential Type drop-down list, select **Computer System**.
3) In the Enter Access Information pane, specify the following information:

   **User name**
   The user name for the service account on the target computer system.

   **Password**
   The passphrase you specified when generating the public/private key pair.

   **Confirm password**
   Enter the passphrase again. The two passphrases that you enter are compared to confirm that they match before the passphrase is saved.

   **Authentication type**
   Select **PKI using Appliance SSH Server Key**.

4) Click **Save**. The new credential is displayed in the Discovery Credentials page.

TSA can now run discoveries against the target that have this service account configured and the public key installed, and login using OpenSSH Version 2 key-based authentication.

### Installing an SSL server certificate (Optional)

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, or upload your own Java keystore file that contains a custom SSL server certificate signed by the certificate authority of your choice.

**Before you begin**

If you want to upload a custom certificate, you must acquire the certificate and package it in a Java 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 the key entry password and the keystore password identical.

**Procedure**

1. In the navigation pane, click **Administration > Security**. The Security page is displayed.
2. To install a self-signed server certificate, click **Generate and install a new Self-signed Certificate**. This certificate is unique to this TSA.

3. 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 a Custom Certificate** 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.

**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.

**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 1,200 seconds or 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 1,200 seconds.
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 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** section.

3. In the **Maximum Password Age** section, 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 Technical Support Appliance configuration.

**Backup date**

Displays the date and time at which the latest backup is started.

**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 current TSA configuration summary. The displayed information shows the configurations that the 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.
2. Enter a password 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**.
5. You can optionally specify a name and location for the backup configuration file.
6. Click **Save** to save the backup configuration compressed file on the system that you are using to sign on to TSA.

   **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 Browse 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 to perform a successful backup and restore operation. 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 and also you can view the TSA documentation.

**Procedure**

1. In the navigation pane, click Administration > Update. The Update page is displayed.
2. Click **Check for Update**. The Update Availability page lists any available updates.

3. To install the updates, click **Perform Update Now**. Upon completion of the update, TSA is automatically restarted.

4. To view information about the contents of the update, click **View Update Details**.
Viewing Documentation

Procedure
1. In the navigation pane, click Administration > Update. The Update page is displayed.
2. Click View Documentation to open the Documentation page where you can download documentation for the currently installed release.

Note: If you do an update, then you must wait for the update process to complete to view the latest documentation that matches the updated appliance release version.

Enabling scheduled maintenance

To maintain TSA running at optimal performance, it is recommended to enable the scheduled maintenance feature.

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, the appliance cannot run these jobs. You must relogin to the appliance after the completion of Scheduled Maintenance.

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.
   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 Appliance Trace Level section shows the current trace setting (Error, Warning, Information, Debug, or Trace).

2. If needed, you can change the trace setting in the Appliance Trace Level section, by clicking the radio button beside the trace setting that you want.

3. Click Save.

Note: By default the trace level for the Technical Support Appliance & its Discovery Manager 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 Trace Level page is displayed indicating the current trace setting in the Discovery Manager Trace Level section.

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**.

The Summary page is displayed.

---

**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.
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.

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 vSphere client or web interface.

---

**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 the appliance’s network protocols.

<table>
<thead>
<tr>
<th>Ping</th>
<th>Traceroute</th>
<th>Test SSH</th>
<th>Interfaces</th>
<th>Ethernet</th>
<th>Address</th>
<th>Routes</th>
<th>ARP</th>
<th>Sockets</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the TCP/IP Address or Hostname to ping.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 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 (“_”).

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.

**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](image)

*Figure 90. 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.

**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 check box 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 check box in the Recreate inventory database section to maintain all the discovery credentials. If you do not select, the credentials are lost and you will need to set up all the credentials again. For more information about discovery credentials, see the "Discovery credentials" on page 86 section.

   Note: The credentials can be preserved only if the Discovery Manager is running (green status).
3. Click Recreate inventory database link. 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. You get the following message - Recreate Database Started. It might take approximately 6 hours to recreate the database, in the mean time you get a status - 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 link. The following warning message is displayed - Are you sure you want to perform RUNSTATS on the inventory database tables?
3. Click OK. You get the following message - RUNSTATS Started. After approximately 30 minutes, you can check the activity log. When the job is complete you get a message as - 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 link. The following confirmation message is displayed - Are you sure you want to perform REORG on the inventory database tables?
3. Click OK. You get the following message - REORG Started. After approximately 30 minutes, you can check the activity log. When the job is complete you get a message as - REORG inventory database successful.

Documentation

Use the Documentation page to download and view the TSA documentation for the current release.
Procedure

To view the documentation, follow these steps:

1. Click **Documentation** from the left navigation menu.

2. To download **TSADocumentation.zip** file, click Download documentation link.

3. Extract the **TSADocumentation.zip** file to view the documentation files. The **TSADocumentation** folder contains the following files:
   
   • **Technical Support Appliance Connectivity Security white paper**: Describes the connectivity, security, and service information that is transmitted by TSA to communicate with IBM Service Delivery Center (SDC).
   
   • **Technical Support Appliance Setup guide**: Describes the prerequisites, steps to set up and work with virtual and hardware TSA.
   
   • **Technical Support Appliance Configuration Assistant guide**: Assists you with installation planning and the configuration of TSA.
   
   • **Technical Support Appliance Update History**: Lists all the new features / enhancements that are included in the current release.
Chapter 6. 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 in any of the following two options:
1. Create your service request at the IBM Support Portal.
2. Create your service request through the IBM Call Center.

Creating service request at the IBM Support Portal

Procedure
1. Log on to https://www.ibm.com/support/servicerequest/
   
   Note: You must first be registered in the Service Request Tool.
2. Select New Service Request.
3. Select I’m having a problem with Software.
4. To route your request directly to the Technical Support Appliance team, search for product ID 5621IZX01.
5. 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

Creating 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. 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.

![Figure 92. Setup network configuration](image)

2. Enter the following network configuration details.

![Figure 93. Network Configuration](image)

   a. Enter `IPTYPE = {static | dhcp}`. Enter `dhcp`.

   **IPTYPE: dhcp**

   Enter Hostname (default=ibmtsa). You can change the default host name. Ensure that the hostname 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 2a on page 129.

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

d. After system reboot, login to the VMware vSphere Client / VMware vSphere Web Client and make a note of the **IP Address** on the Summary tab.

![Figure 94. DHCP IP Address](image)

e. Access TSA from the browser with the URL that you obtained from the previous step. For example, https://newhost1.new.abclabs.klm.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.
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 internet 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:

icfeebk@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](http://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.