

IBM[®] Technical Support Appliance Configuration Assistant Guide

Version 2.10.1.0

June 2022

Table of Contents

Introduction	3
Pre-Discovery Network Considerations	3
Useful Documentation	3
Overview.....	4
Defining scope sets	4
Factors to Consider When Creating Scopes.....	5
Discovery Credentials.....	6
Factors to consider to set up Discovery Credentials.....	7
Getting Started	8
Initial Setup and Configuration of TSA.....	8
Preparing for Discoveries.....	8
Discovery Steps.....	8
Device Discovery Configuration.....	10
Operating Systems and Hosts	10
IBM Power Systems	11
Hardware Management Console (HMC)	11
Integrated Virtualization Manager (IVM)	13
Virtual I/O Server (VIOS) Partitions	13
AIX.....	13
Linux on Power	15
IBM i.....	16
UNIX Systems.....	17
Solaris.....	17
Solaris via Oracle iLOM.....	18
Linux	18
HP-UX	19
VMware vCenter Server and VMware ESXi.....	19
Windows.....	21
Windows via WINRM.....	21
Windows via SMB1	23
ATM Devices.....	25
Management Module.....	25
Flex System Manager (FSM) Devices	25
Chassis Management Module (CMM) Devices	26
Advanced Management Module (AMM) Devices	26
HP Proliant Blade Server via HP OnBoard Administrator	26
Integrated Management Module (IMM) & Integrated Management Module II (IMM2) Devices	26

HP Integrity & HP9000 Servers via iLO.....	27
Dell Server via Integrated Dell Remote Access Controller (iDRAC)	27
Network Devices.....	27
BNT Switches.....	28
Brocade.....	28
Check Point.....	28
Cisco.....	29
F5 Big-IP (TMOS).....	29
Fortinet (FortiOS).....	29
IBM b-type Storage Area Network (SAN) switches	30
Juniper.....	30
Palo Alto Networks (PAN-OS).....	30
QLogic Switches	30
Storage Devices	31
EMC Corporation Storage	31
HP StorageWorks P2000 Modular Smart Array	32
IBM DS3xxx, DS4xxx or DS5xxx Storage.....	32
IBM DS6xxx / DS8xxx Storage.....	33
IBM FlashSystem, v9000	33
IBM ProtecTIER	33
IBM SVC, V7000/V3700 storage	34
IBM TS3100 Tape Library	34
IBM TS3200 Tape Library	34
IBM TS3310 Tape Library	34
IBM TS3494, TS3953 Tape Libraries	34
IBM TS3500, TS3584 Tape Libraries	34
IBM TS4300 Tape Library	35
IBM TS4500 Tape Library	35
IBM TS7700 Tape Library	36
IBM V7000 Unified Storage.....	36
IBM XIV Storage.....	36
nSeries or NetApp Storage.....	36
Firewall Considerations	38
Discovery Issues.....	41
Ongoing Considerations.....	42
Troubleshooting.....	43
Active Session for AMM Discovery.....	43
Appendix A: Terms and Definitions.....	44
Appendix B: Miscellaneous Items.....	45
User Interface Download Functions	45

Appendix C: CIM Provider for VMware ESXi	46
Appendix D: Windows using WINRM	48




Introduction

The IBM 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 securely transmits the data to IBM Support for analysis. This data provides IBM Support with insight into the complex relationships between the servers and network components in your data center.

The intent of this document is to provide information and guidance to assist with installation, planning, and the configuration of TSA.

Pre-Discovery Network Considerations

Before configuring TSA for the initial discovery and transmission, ensure that the following items have been addressed. It is assumed that TSA has already been installed, the web interface is accessible, and TSA has been updated to the most current level, if not, see the Technical Support Appliance Setup Guide (referred to as the Setup Guide in the remainder of this document).

TSA Pre-Discovery Network Considerations		
Networking		
	Open firewall access from TSA to IBM. See section, Configuration requirements for connections to IBM Support in the Setup Guide.	
	If an SSL proxy is used to connect back to IBM, ensure that it is configured in TSA. See section, Setting up IBM connectivity in the Setup Guide. <table border="1" data-bbox="402 1268 1466 1367"><tr><td> SSL inspection is not supported. If utilizing SSL inspection on the proxy, disable it for these flows.</td></tr></table>	 SSL inspection is not supported. If utilizing SSL inspection on the proxy, disable it for these flows.
 SSL inspection is not supported. If utilizing SSL inspection on the proxy, disable it for these flows.		
	If any firewalls exist between TSA and the target devices, ensure that the required ports are open. For more information, see section <u>“Firewall Considerations”</u> on page 38.	

Useful Documentation

The link below will point you directly to the Technical Support Appliance information website. Here you will find everything that you need to get started with the IBM Technical Support Appliance. You can access setup guides and security documentation, view sample reports, and download the Technical Support Appliance installation code from ibm.com.

To learn more about the Technical Support Appliance: <https://ibm.biz/TSAdemo>

Overview

TSA can discover information about your IT infrastructure, including deployed Operating System components, firmware components, physical servers, network devices, virtual LAN, etc. To optimize the breadth and depth of information that is collected, configuration tasks are required within TSA to identify the discovery devices.

TSA attempts to minimize impacts to the customer's network environment. The discovery process uses an iterative and measured approach which may cause a full discovery to take up to 72 hours. The status of the discovery job can be monitored by viewing the **Job Summary** section of the **Summary** panel.

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


For TSA to collect information about your IT infrastructure, provide it with the following:

- Scopes
- Access Credentials

Defining scope sets

A scope set is a logical grouping of individual scopes. Scopes use IP addresses to tell TSA where to begin discovering the environment. A scope set is composed of one or more scopes. There are three types of scope entries:

- Subnet - Defined by an IP address and a subnet mask. Subnets are limited to class C subnets.
- IP Range - Includes all IP addresses between the start and end.
- IP Address / Host - An individual IP address or Host name.

 Host name is resolved at entry time, not discovery time. See section “[Factors to Consider When Creating Scopes](#),” on page 5 for details.

If desired, scope exclusions can be defined for a scope by specifying a host, range, or subnet definition. The resulting IP addresses will not be considered part of the scope and will not be scanned.

TSA supports three types of scope sets:

1. **General Scope Sets:** Allows you to discover individual IT network elements. The scope set contains one or more scopes that identify the location of these network elements using an IP address, a range of IP addresses, or a network or subnet.

2. **HMC Dynamic Scope Sets:** Allows you to specify the IP address of one or more IBM POWER Systems HMCs along with associated credentials. In addition, information regarding all LPARs that the HMCs manage can also be collected without the need to identify the IP addresses for the LPARs. The dynamic scope set uses credential information that you provide to successfully access these LPARs.
3. **VMware Dynamic Scope Sets:** Allows you to specify the IP address of one or more VMware vCenter Server or ESXi instances along with their associated credentials. In addition, information regarding all virtual machines that VMware manages can also be collected without the need to identify the IP addresses for the virtual machines. The dynamic scope set uses credential information that you provide to successfully access these virtual machines.

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


For detailed instructions regarding how to define discovery scopes on TSA, see the **Setting up discovery scopes** section in the Setup Guide.

Factors to Consider When Creating Scopes

While there are not any defined standards for setting up scopes, there are some practical considerations that can save time and effort:

- Where practical, use dynamic scope sets to define discoveries of HMCs and their managed LPARs, or VMware vCenter Server / ESXi and their managed virtual machines. When dynamic scope sets are used, there is no need to define scopes for the LPARs or virtual machines.
- HMC Dynamic Scope Sets allow the import of one or more IP addresses / hostnames for the HMCs you want to discover. For more information, see section **HMC Dynamic Scopes** in the Setup Guide.
- VMware Dynamic Scope Sets allow the import of one or more IP addresses / hostnames for the VMware vCenter Servers and ESXi instances you want to discover. For more information, see section **VMware Dynamic Scopes** in Setup Guide.
- Use IP Range or Subnet scopes to discover multiple devices as opposed to individual IP addresses or host names. This will limit the number of scope definitions and make administration easier.

- If using subnet scope definitions, only include one per scope set. Ensure the subnet scope definition resolves to a Class C network (256 IP addresses) or less.
- Use the **Import General Scope Set** feature to create a new scope set based on the specified name and the list of the IP addresses from an input text file. For more information, see section **Discovery Scopes → Import General Scope Set** in the Setup Guide for instructions.
- TSA resolves host names once at entry time. If the IP address for a system change while retaining the same hostname, the scope for this system should be deleted and recreated to resolve to the new IP address.
- The more IP addresses that are in the scope set, the longer the discovery will take. To minimize the time a discovery takes, set up scopes to target only the elements that you want to discover.

 When using General Scope Sets, limit the cumulative number of IP addresses that a scope set resolves to (after expanding any range or subnet scope definitions) to 400 or less. Performance, server, or network issues may be encountered during the discovery process if more than 400 IP addresses are scanned for a single scope set. Displaying the scope set will show how many IP addresses a given scope set will attempt to discover.

- TSA does not prevent IP addresses from being defined in multiple scope sets. In general, this practice should be avoided since it increases the discovery time without collecting any additional information.
- Group scopes into scope sets that make up a logical grouping of devices:
 - Group the same device type within a scope set. For example, create a scope set for IBM FlashSystem storage subsystems.
 - Group devices that are in the same geography.
 - Group devices based on business applications or services.

Discovery Credentials

With a few exceptions, discoveries require some level of access to acquire the detailed information that is needed for a complete understanding of your environment.

Normally service accounts should be created on the discovery devices for use by TSA. See the sections below for the specific access rights required by each platform type. To simplify administration of these service accounts, use the same username for all devices of a given product family.

The task of maintaining the service accounts that TSA uses to connect to the devices can be simplified by using one of the following strategies:

- Create service accounts with non-expiring passwords
- Use SSH keys for device product families that support their use

For detailed instructions regarding how to define access credentials on the appliance, see section **Setting up discovery credentials** in the Setup Guide.

Factors to consider to set up Discovery Credentials

The appliance attempts to use credentials in the order that they appear in the access list. To speed up discovery, make sure you have the credentials in the order that best suits your environment. Some considerations are as follows:

- Restrict credentials to specific scope sets where appropriate. This will limit unnecessary login attempts and improve discovery performance.
- SSH keys can be used for these device discoveries:
 - AIX
 - Check Point
 - Cisco
 - Dell iDRAC
 - F5 Big IP
 - Fortinet
 - HMC
 - HP-UX
 - IBM FlashSystem
 - IBM i
 - IVM
 - Linux
 - Sun SPARC (Solaris)
 - SVC / V7000
 - VIOS

 Only one SSH key credential can be linked to a scope set.

- It is a best practice to create separate service accounts that are used exclusively by TSA with the lowest level of authority required.

Getting Started

This section covers some best practices and recommendations for configuring TSA.


Initial Setup and Configuration of TSA

Go through the instructions specified in the following sections of the Setup Guide:

- Installing the Technical Support Appliance
- Logging in to the Technical Support Appliance
- Accepting the License Agreement
- Setting up the Technical Support Appliance using the setup wizard

Preparing for Discoveries


An iterative process is recommended whereby a small portion of the network is initially configured for discovery and more sections of the network are added with each iteration until all of the desired network is covered.

 It is a best practice to save a backup of your TSA configuration after significant additions/modifications made to scopes and/or credentials. For more information, see section “Backup and restore” in the IBM Technical Support Appliance Setup Guide.

Discovery Steps


For each discovery iteration perform the following steps:

1. Prepare the devices for discovery. For any necessary device and credential configuration requirements, see section “[Device Discovery Configuration](#)” on page 10.
2. For HMC Dynamic Scope Sets, perform the following steps:
 - a. Add the IP addresses of the HMCs in the **HMC Dynamic Scope Set** page.
 - b. Add the credentials for the HMCs in the **HMC Dynamic Scope Set** page.
 - c. Select which LPAR types you wish to discover. Provide credentials for each type.

 You may select the LPAR types to discover when the dynamic scope set is created, or you can add the LPAR types in a later iteration by editing the dynamic scope set.

- d. (Optional) Use the Test function on the **HMC Dynamic Scope Set** page to verify that the credentials are defined properly and can be used to establish a connection to the HMCs or its LPARs.
3. For VMWare Dynamic Scope Sets, perform the following steps:
 - a. Add the IP addresses of the VMware vCenter Servers.

- b. Add the IP addresses of any VMware ESXi hosts that are not managed by a VMware vCenter Server.
- c. Add the credentials for the VMware vCenter Servers and ESXi instances in the **VMware Dynamic Scope Set** page.
- d. Select which virtual machine types you wish to discover. Provide credentials for each type.

 You may select the virtual machine types to discover when the dynamic scope set is created, or you can add the virtual machine types in a later iteration by editing the dynamic scope set.

- e. (Optional) Use the Test function on the **VMware Dynamic Scope Set** page to verify that the credentials are defined properly and can be used to establish a connection to the VMware vCenter Servers and ESXi instances, as well as its virtual machines.
4. For General Discovery Scopes, perform the following steps:
 - a. Add the desired IP addresses into the appropriate scope sets / scopes. If firewalls exist between the TSA instance and the discovery devices, ensure that the appropriate ports are opened in the firewall to allow the discovery to succeed. For information on which ports must be accessible for each platform type, see section “[Firewall Considerations](#)” on page 38.
 - b. Create the necessary credentials.
 - c. (Optional) Use the Test function on the **New Discovery Credentials** panel to verify that the credential is defined properly and can be used to establish a connection with a target device.
 5. Run a full discovery to scan the IP addresses added for this iteration.
 6. Run a transmission to upload the data to IBM.

Device Discovery Configuration

In addition to providing credentials, there may be specific discovery device configuration prerequisites required in order for TSA to effectively discover and collect useful component information. This section allows you to identify discovery devices in your environment that will require specific configurations. It is recommended that you create service accounts with the minimum authorities required, also refer to section [“Firewall Considerations”](#) for port and protocol information.

✚ For devices for which both the SSH & Telnet ports are open, TSA will first attempt a connection using SSH (for security reasons). If this SSH connection fails, TSA will then attempt the connection using Telnet.

Operating Systems and Hosts

Platform
<u>IBM Power Systems</u> <ul style="list-style-type: none">• <u>Hardware Management Console (HMC)</u>• <u>Integrated Virtualization Manager (IVM)</u>• <u>Virtual I/O Server (VIOS) Partitions</u>• <u>AIX</u>• <u>Linux on Power</u>
<u>IBM i</u>
<u>UNIX Systems</u> <ul style="list-style-type: none">• <u>Solaris</u>• <u>Solaris via iLOM</u>• <u>Linux</u>• <u>HP-UX</u>
<u>VMware vCenter Server and VMware ESXi</u>
<u>Windows</u>
<u>ATM devices</u>

Management Module

- [Flex System Manager \(FSM\)](#)
- [Chassis Management Module \(CMM\)](#)
- [Advanced Management Module \(AMM\)](#)
- [HP ProLiant Blade Server via HP OnBoard Administrator](#)
- [Integrated Management Module \(IMM & IMM2\)](#)
- [HP Integrity & HP9000 Servers via iLO](#)
- [Dell Server via Integrated Dell Remote Access Controller \(iDRAC\)](#)



Click each of the above links for detailed information.

IBM Power Systems


For IBM Power systems, where the configuration of LPARs is managed by an HMC or IVM, use HMC Dynamic Scope Sets. With HMC Dynamic Scope Sets you create a scope definition for the HMCs and provide the associated HMC and LPAR credentials, but do not need to create scopes for each managed LPAR. When the HMC is discovered, TSA determines which LPARs are in existence at that point in time and automatically scans each LPAR.

For IBM Power Systems where the configuration of LPARs is generally static, an alternative method to HMC Dynamic Scope Sets is to iterate by adding scopes and credentials for entities in the following order:

1. **The HMC or IVM instances:** The HMC returns high level information about all the Power Systems it manages, and the logical partitions contained therein. The IVM returns similar information for the single system that it manages.
2. **The VIOS partitions:** This returns information about the physical adapters and resources that are owned by these partitions.
3. **Individual partitions:** In some cases, a non-VIOS partition owns physical adapters.

Hardware Management Console (HMC)

Using HMC Dynamic Scope Sets allows TSA to collect detailed OS information from each LPAR that can be analyzed by ProWeb.

 For information on adding scopes and credentials for HMC environments, see section **HMC Dynamic Scopes** in the IBM Technical Support Appliance Setup Guide.

Level of data collected for the report by scanning various Power Systems entities:

- By scanning only HMCs, you will get all essential information on the Identified tab, HMC Topology, Power Systems Firmware, IBM i Recommendations, Linux Recommendations, HMC/VIOS/AIX and Contract tabs and some Adapter information.
- By scanning VIOS partitions directly you will get additional information on adapter firmware and connected storage.
- By scanning LPARs directly you will get more information about the LPAR, including OS details and instances of specific software such as PowerHA, GPFS, and PowerSC.

To discover HMC instances, complete the following steps:

Preparing the environment:

- For TSA to gather information about managing LPARs through the HMC, the HMC must be able to communicate with the LPARs using RMC tools. Ensure that the HMC and the LPARs are configured to allow this communication. For more information on RMC tools for Linux, see <https://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/yum.html>
- To enable secure data collection, remote command execution must be enabled on the HMC. For information, see “Enabling and disabling HMC remote commands” at the following address:
<https://www.ibm.com/support/knowledgecenter/POWER7/p7ha1/enablinganddisablinghmcremotecommands.htm>

Credentials for access list:

- For HMC Dynamic Scope Sets - Username / password or Username / SSH key authentication for the HMC service account.
- For General Discovery Scope Sets - Computer System: Username / password or Username / SSH key authentication for the HMC service account.
- The HMC user must have the following roles:
 - Resource role: AllSystemResources
 - Task role (based on **hmcoperator** with command line tasks):

- ManagedSystem (lshwres, lssyscfg)
- Logical Partition (lshwres, lssyscfg, viosvrcmd)
- HMC Configuration (lshmc)
- A user (service account) with **hmcviewer** authority can be used if necessary, however, this will result in partial data collection.

✚ When running with **hmcviewer** authority, information about adapters owned by VIOS partitions cannot be obtained. To get this information, ensure the service account has a minimum of **hmcoperator** authority. If that is not possible, then add scopes and credentials to discover the VIOS partitions directly in addition to the HMC.

Integrated Virtualization Manager (IVM)

To discover IVM instances, complete the following steps:

Credentials for access list:

- Computer System: Username / password or Username / SSH key authentication for the IVM service account.
- The service account must have view only permission.

Virtual I/O Server (VIOS) Partitions

To discover VIOS instances, complete the following steps:

Credentials for access list:

- For HMC Dynamic Scope Sets - Username / password or Username / SSH key authentication for the VIOS partition service account.
- For General Discovery Scope Sets - Computer System: Username / password or Username / SSH key authentication for the VIOS partition service account.
- The service account must be an administrator account (such as **padmin**).
- The service account must have a user attribute of **rlogin=true**. You can set this attribute using SMIT or by editing the `/etc/security/user` file.
- The parameter **PermitUserEnvironment** in the `/etc/ssh/sshd_config` file must be set to **yes**.

AIX

To discover AIX instances, complete the following steps:

Preparing the environment:

- Ensure that the packages `bos.perf.tools` and `openSSH/openSSL` are installed.

- Disable invalid login attempt fail for the service account.

Credentials for access list:


- For HMC Dynamic Scope Sets - Username / password or Username / SSH key authentication for the AIX partition service account.
- For General Discovery Scope Sets - Computer System: Username / password or Username / SSH key authentication for the AIX service account.
- The service account can be root or an account with sudo authority.
- The service account must have a user attribute of **rlogin=true**. You can set this attribute using SMIT or by editing the **/etc/security/user** file.
- To enable a non-root service account for sudo authority for AIX:
 - Install the sudo RPM (sudo-1.6.9p15-2noldap) and ssh filesets (openssh.base.server, openssh.base.client on the AIX instance).
 - Create a non-root user ID on the target AIX instance that can be used by TSA to access the system.
 - Modify **/etc/sudoers** on each AIX instance to allow TSA to run the specified commands using sudo authority.

Cmnd alias specification

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

User privilege specification


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

 <User Name> is the non-root service account that TSA uses to collect AIX information. This <User Name> is a user on each AIX instance. The **/etc/sudoers** file on each AIX instance must be updated with the above specification.

Or

An alternative to the above modifications to `/etc/sudoers` is to use the following user privilege specification:

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

 `<User Name>` is the non-root service account that TSA uses to collect AIX information. This user specification allows the service account to use sudo authority on any AIX command.

If you use the IBM Proweb portal for AIX as part of your support offering with IBM, it is recommended that you configure TSA using HMC Dynamic Scope Sets. As an alternative, you can configure TSA to discover the HMCs and the logical partitions (including VIOS) on the power systems.

Linux on Power

To discover Linux on Power instances, complete the following steps:

Preparing the environment:

- Disable invalid login attempt fail for the service account

Credentials for access list:


- For HMC Dynamic Scope Sets - Username / password or Username / SSH key authentication for the Linux partition service account.
- For General Discovery Scope Sets - Computer System: Username / password or Username / SSH key authentication for the Linux service account.
- To enable a non-root service account for sudo authority for Linux:
 - Create a non-root user ID on the target Linux instance that can be used by TSA to access the system.
 - Modify `/etc/sudoers` on each Linux instance to allow TSA to run the specified commands using sudo authority.

Cmnd alias specification

```
Cmnd_Alias TSA_CMDS = /usr/sbin/lsvpd, /sbin/lsvpd,  
/usr/sbin/lscfg, /sbin/lscfg, /usr/sbin/lsmcode,  
/sbin/lsmcode, /usr/sbin/lvmdiskscan, /sbin/lvmdiskscan,  
/usr/sbin/dmidecode, /usr/bin/mtlib, /usr/bin/tapeutil,  
/usr/bin/crontab, /sbin/fdisk, /bin/ls -aLR /boot/*,  
/bin/cat /proc/irq/*, /bin/cat /proc/net/vlan/config,  
/bin/cat /proc/ppc64/rtas/*, /bin/cat /proc/sys/kernel/cap-  
bound, /bin/cat /proc/sys/kernel/random/entropy_avail
```

User privilege specification


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

 <User Name> is the non-root service account that TSA uses to collect Linux information. This <User Name> is a user on each Linux instance. The **/etc/sudoers** file on each Linux instance must be updated with the above specification.

Or

An alternative to the above modifications to **/etc/sudoers** is to use the following user privilege specification:

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

 <User Name> is the non-root service account that TSA uses to collect Linux information. This user specification allows the service account to use sudo authority on any Linux command.

IBM i

IBM i instances are discovered using an SSH connection. If the IBM i instance does not have SSH installed and configured, complete the following steps:

Preparing the environment:

Ensure that the following products/options are installed and configured for IBM i 7.2:

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

Ensure that the following products/options are installed and configured for IBM i 7.3:

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

Ensure that the following products/options are installed and configured for IBM i 7.4:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, option 30
- Portable App Solutions Environment, 5770-SS1, option 33
- IBM Developer Kit for Java, 5770-JV1 option 16

- Java SE 8 32 bit

To start the SSH daemon, execute the following command:

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

To start the SSHD service on IBM i, execute the following command:

```
STRTCPSVR SERVER(*SSHD)
```

 For additional information on how to configure SSH on IBM i, see chapters 21-23 in this Redbook - <http://www.redbooks.ibm.com/redpapers/pdfs/redp4163.pdf>

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account can have any user class including ***USER**, though additional object authority requirements are needed to collect PTF information (which is done using the **DSPPTF** command).
- **DSPPTF** is shipped with the following object authority restrictions:
 - The command is shipped with ***EXCLUDE** public authority
 - **QPGMR**, **QSYSOPR**, **QSRV**, and **QSRVBAS** user profiles are shipped with private authorities to use this command
 - As always, the **QSECOFR** user profile or any user profile with a user class of ***SECOFR** can run this command
- The **QSYS/DSPPTF** object of object type ***CMD** can have its authorities edited to allow any other user to run this command.
- If a new service account is created for TSA, the following recommendations apply:
 - Create the user profile with user class ***USER**
 - Use the **GRTOBJAUT** command to allow this user profile to run the **DSPPTF** command; object is **QSYS/DSPPTF** of object type ***CMD**.

UNIX Systems

Solaris

To discover Solaris devices, complete the following steps:

Preparing the environment:

- On Solaris systems, ensure that the SUNWscpu (Source Compatibility) package is installed.
- On some Solaris systems, SNEEP needs to be installed and configured to obtain serial numbers.

Credentials for access list:

- Computer System: Username / password or Username / SSH key authentication for the service account.
- The service account can be non-root.

Solaris via Oracle iLOM

To discover Solaris devices via Oracle iLOM, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account can have either **Operator** or **Administrator** privileges.

Linux

If the Linux instance is running on an IBM Power System, refer to the [Linux on Power](#) section on page 15, under IBM Power Systems for instructions.

To discover Linux on x86 devices, complete the following steps:

Preparing the environment:

- Ensure the `pciutils` package is installed. The `lspci` command contained therein is used to collect information about adapters and connections to external storage devices.

Credentials for access list:


- For VMware Dynamic Scope Sets - Username / password or Username / SSH key authentication for the Linux virtual machine service account.
- For General Discovery Scope Sets – Computer System: Username / password or Username / SSH key authentication for the Linux service account.
- Set `/bin/sh` as the shell for this account.
- For Linux (x86), the service account can be root or an account with `sudo` authority.
- To discover using a non-root service account, add the following to the `/etc/sudoers` file on the Linux system.

```
# Cmnd alias specification
```

```
    Cmnd_Alias TSA_CMDS = /usr/sbin/dmidecode
```

```
# User privilege specification
```


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

 <User Name> is the non-root service account that TSA uses to collect Linux information. This <User Name> is a user on each Linux instance. The **/etc/sudoers** file on each Linux instance must be updated with the above specification.

Or

An alternative to the above modifications to **/etc/sudoers** is to use the following user privilege specification:

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

 <User Name> is the non-root service account that TSA uses to collect Linux information. This user specification allows the service account to use sudo authority on any Linux command.


HP-UX

To discover HP-UX devices, complete the following steps:

Credentials for access list:

- Computer System: Username / password or Username / SSH key authentication for the service account.
- To enable a non-root service account for sudo authority for HP-UX:
 - Modify **/usr/local/etc/sudoers** on each HP-UX device to allow TSA to run the specified commands using sudo authority.

```
# Cmnd alias specification  
  
Cmnd_Alias TSA_CMDS  
=/usr/sbin/diskinfo, /opt/hpvm/bin/hpvmstatus  
  
# User privilege specification  
  
<User Name> ALL=(ALL) NOPASSWD:TSA_CMDS
```

 <User Name> is the non-root service account that TSA uses to collect HP-UX information.

VMware vCenter Server and VMware ESXi

For VMware environments, use VMware Dynamic Scope Sets. With VMware Dynamic Scope Sets you create a scope definition for the VMware vCenter Server / ESXi and provide the associated VMware and virtual machine credentials, but do not need to create scopes for each managed virtual machine. When the VMware vCenter Server / ESXi is discovered, TSA

determines which virtual machines are in existence at that point in time and automatically scans each virtual machine.

For VMware environments where the configuration of virtual machines is generally static, an alternative method to VMware Dynamic Scope Sets is to iterate by adding scopes and credentials for entities in the following order:

1. **The vCenter Server instances:** This returns high level information about the ESXi hosts they manage, and the Virtual Machine guests contained therein.
2. **ESXi hosts:** Add ESXi hosts that are not managed by a vCenter Server.
3. **Individual Virtual Machine guests:** This allows collection of more detailed information regarding the operating system.

When configuring TSA for VMware environments, the following actions are recommended:

1. Configure TSA to discover VMware vCenter Servers where available. Discovering a VMware vCenter Server automatically causes TSA to collect information about all the VMware ESXi hosts that the vCenter Server manages. No configuration information about the ESXi hosts is required.
2. Configure TSA to discover VMware ESXi hosts only when the ESXi host is not managed by a VMware vCenter Server.
3. Install VMware Tools on each virtual machine that are hosted on the ESXi hosts. If VMware Tools is not installed, then some inventory data such as IP address or Operating System installed, will not be accessible.
4. Configure each VMware ESXi host to have the CIM interface active. The CIM interface allows TSA to collect detailed information about the adapters within the ESXi host. For more information about the CIM provider, see “[Appendix C](#)” on page 44.

To discover vCenter server instances as well as information about the ESXi servers they manage, complete the following steps:

Preparing the environment

- Install VMware Tools on each virtual machine that is hosted on the ESXi hosts.
- Configure each VMware ESXi host to have the CIM interface active.
- The CIM port (5989) must be reachable from the TSA (unblocked by firewalls, etc.) for full discovery.

Credentials for access list

- For VMware Dynamic Scope Sets - Username / password for the VMware vCenter Server service account.

- For General Discovery Scope Sets - Computer System: Username / password for the VMware vCenter Server service account.
- The service account must have **Administrator** role permissions or at least permissions to a custom Read-only role with following additional privileges:
 - Global → Licenses
 - Global → Settings
 - Host → CIM
 - Host → Configuration → Change settings
 - Host → CIM → CIM Interaction

To discover ESXi devices directly, complete the following steps:

Preparing the environment

- Install VMware Tools on each virtual machine that are hosted on the ESXi hosts.
- Configure each VMware ESXi host to have the CIM interface active.

Credentials for access list

- For VMware Dynamic Scope Sets - Username / password for the VMware ESXi service account.
- For General Discovery Scope Sets - Computer System: Username / password for the VMware ESXi service account.
- The service account must have **Administrator** role permissions.

Windows

TSA supports discovery of Windows instances with the following methods:

- WINRM
- SMB1

 Windows via WINRM is preferred as it is the more secure interface.

Windows via WINRM

To discover Windows devices via WINRM, complete the following steps:

Preparing the environment:

The most common way to prepare the environment is to use a server certificate generated by a certificate authority that is installed on the target Windows server. The certificate must meet the following conditions:

- The root and intermediate certificates from the certificate authority are in the Trusted Root Certification Authorities certificates.
- The server certificate is installed in the Personal certificates.
- The server certificate must show that it is issued to the fully qualified hostname of the server.
- The server certificate must include the private key for this server.

The following command configures WINRM for remote HTTPS connections:

```
winrm quickconfig -transport:https
```

This command does the following:

- Enables WINRM if not currently active
- Modifies the WINRM service so that WINRM starts automatically on restarts
- Configures the WINRM HTTPS listener
- Modifies the Windows Firewall rules to allow remote HTTPS connections

The command produces the following output. Enter **y** to confirm the changes.

```
WinRM service is already running on this machine.
WinRM is not set up to allow remote access to this machine for
management.
The following changes must be made:

Create a WinRM listener on HTTPS://* to accept WS-Man requests to
any IP on this machine.
Configure CertificateThumbprint setting for the service, to be
used for CredSSP authentication.
Configure LocalAccountTokenFilterPolicy to grant administrative
rights remotely to local users.

Make these changes [y/n]? y

WinRM has been updated for remote management.

Created a WinRM listener on HTTPS://* to accept WS-Man requests
to any IP on this machine.
Configured required settings for the service.
Configured LocalAccountTokenFilterPolicy to grant administrative
rights remotely to local users.
```

Finally, to allow user id / password authentication over HTTPS, run the following command:

```
winrm set winrm/config/service/auth @{Basic="true"}
```

An alternative is to use a self-signed certificate. The instructions for this configuration are in [Appendix D: Windows using WINRM](#) on page 48.

Credentials for access list:

- For VMware Dynamic Scope Sets: Username / password for the service account.

- For General Discovery Scope Sets: Computer System (Windows): Username / password for the service account.
- The service account must be a member of one of the following groups:
 - Administrators
 - WinRMRemoteWMIUsers__

To add a user to the WinRMRemoteWMIUsers__ group, use the following command:

```
net localgroup WinRMRemoteWMIUsers__ [user_id] /add
```

Windows via SMB1

To discover Windows devices, complete the following steps:

Preparing the environment:

- Ensure that Windows Scripting Host (WSH) or the Windows Management Instrumentation (WMI) service and VBScript are enabled on the target device.
- Ensure that port 445 is not blocked by firewall or IP security policies as TSA requires Server Message Block (SMBv1) protocol over TCP/IP.
- To apply security policies, go to **Start** → **Control Panel** → **Administrative Tools**, then choose the following navigation based on whether your policies are stored locally or in an Active Directory:
 - Locally stored policy: Administrative Tools → Local Security Policy → IP Security Policies on Local Computer
 - Policies Stored in Active Directory: Administrative Tools → Default Domain Security Settings → IP Security Policies on Active Directory or Administrative Tools → Default Domain Controller Security Settings → IP Security Policies on Active Directory
- TSA requires access to the hidden remote administration disk share for access to the system %TEMP% and other directories. Access to the Interprocess Communications share (IPC\$) is also required for TSA to access remote registries. Ensure the Interprocess Communication share Server service is started. To start the Server service, go to → **Control Panel** → **Administrative Tools** → **Services** → **Server**.
- Ensure that the Remote Registry Service is active. This is required for TSA to establish a session with the Windows device.

Credentials for access list:

Windows release 2012 R2 and newer:

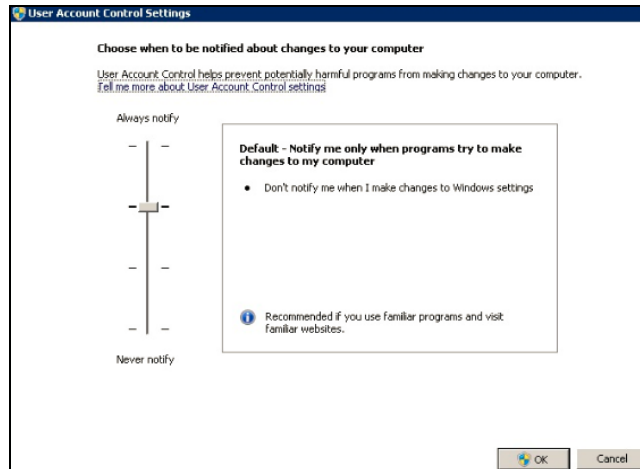
- For VMware Dynamic Scope Sets - Base Administrator account / password. This account will work regardless of the User Account Control (UAC) settings.
- For General Discovery Scope Sets - Computer system (Windows): Base Administrator account / password. This account will work regardless of the User Account Control (UAC) settings.

It is possible to use an account other than the base Administrator account if certain conditions are met. The account must be a local or domain administrator account and the User Account Control (UAC) settings must meet certain requirements. Reference the table below for the combinations of account type and UAC setting that are supported. Reference Microsoft Windows documentation for additional details regarding UAC.

	User Account Control Settings			
	Always Notify	Notify me only when programs try to make changes to my computer (default setting)	Notify me only when programs try to make changes to my computer (do not dim my desktop)	Never Notify
Base Administrator	Yes	Yes	Yes	Yes
User in Domain Administrators Group	No	Yes	Yes	Yes
User in Local Administrators Group	No	Yes	Yes	Yes
Non-Administrator Account (Domain or Local)	No	No	No	No

To access UAC Settings, click **Start**, then click **Control Panel**. Type **uac** in the search box and then click **Change User Account Control settings**.

The following is the default setting:



ATM Devices

Certain models of ATM devices can be discovered. To discover ATM devices, including basic information about their components, complete the following steps:

Preparing the environment:

- Wincor Nixdorf models - Follow instructions for [Windows via SMB](#).

Management Module

For IBM Flex Systems it is best to iterate by adding scopes and credentials for entities in the following order:

1. **The Flex System Manager (FSM):** This returns high level information about the Flex System Managers and the Chassis they manage along with their associated compute nodes.

 If FSMs are not present, it is recommended to scan the CMMs and any HMCs managing POWER compute nodes on Flex systems.

2. **The Chassis Management Module (CMM):** For chassis that are not managed by an FSM, point to each CMM to retrieve high level information about each chassis and its associated nodes.
3. **The Compute nodes:** This returns detailed information about the Operating System.

Flex System Manager (FSM) Devices

To discover FSM devices, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account must have **SMAdmin** authority.

Chassis Management Module (CMM) Devices

To discover CMM devices, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account must have at least **operator** authority.

Advanced Management Module (AMM) Devices

To discover AMM devices, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account must have at least **operator** authority.

HP Proliant Blade Server via HP OnBoard Administrator

For Hewlett Packard (HP) ProLiant Servers, it is best to add scopes and credentials for entities of the HP OnBoard Administrator (HP OBA). The HP OBA will return high level information about the HP OnBoard Administrator, the enclosure it manages and the compute nodes contained within the enclosure.

To discover an HP Proliant Blade server via HP OnBoard Administrator (OBA), complete the following steps:

Preparing the environment:

- HP OBA must be in active mode.

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account must have either **OA administrator**, **OA operator**, or **OA user** authority on the HP Onboard Administrator. The **OA user** authority role is recommended.

 TSA collects information from HP OnBoard Administrators that are in active state only. No information is collected from HP OnBoard Administrators that are in standby state.
--

Integrated Management Module (IMM) & Integrated Management Module II (IMM2) Devices

To discover IMM & IMM2 devices, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account can have any valid authority.

HP Integrity & HP9000 Servers via iLO

The iLO is a separate processor card within an HP Integrity & HP9000 Server that provides basic hardware information about the server. The iLO is active as soon as the server is plugged in, even if the server itself is not powered on yet.

To discover the Summary-level inventory information via iLO for HP Integrity & HP9000 servers, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account can use any valid authority level. User authority is recommended.

Dell Server via Integrated Dell Remote Access Controller (iDRAC)

The iDRAC is a separate processor card within a Dell Server that provides basic hardware information about the server. The iDRAC is disabled by default and needs to be enabled and configured to be used.

The following prerequisites are required:

- The iDRAC needs to be enabled and configured for its use.
- An iDRAC service module needs to be installed in the operating system for the OS information to be discoverable.

To discover the Summary-level inventory information via iDRAC for Dell servers, complete the following steps:


Credentials for access list:

- Computer system: Username / password for the service account.
- The service account must have at least administrator authority level.
- The credential must have SSH access to run CLI commands.

Network Devices

This section provides detailed information on the following types of network devices:

Platform
<u>BNT Switches</u>
<u>Brocade Switches</u>
<u>Check Point</u>
<u>Cisco Switches</u>

F5 Big-IP (TMOS)
Fortinet (FortiOS)
IBM b-type Storage Area Network (SAN) switches
Juniper Switches
Palo Alto Networks (PAN-OS)
QLogic Switches
 Click each of the above links for detailed information.

BNT Switches

To discover BNT switches, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account must have **admin** authority.

Brocade

To discover Brocade devices, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- Virtual Fabric mode disabled: The service account can use any valid authority. **User** authority is recommended.
- Virtual Fabric mode enabled: The service account requires **Admin** authority on Fabric OS.

Check Point

To discover Check Point systems, complete the following steps:

Credentials for access list:


- Computer System: Username / password or Username / SSH key authentication for the service account.
- The service account must have administrator authority (**adminRole**).
- The service account must have SSH access to run CLI commands.

Cisco

To discover Cisco devices, you can use the following computer system credentials or the SNMP credentials.

Credentials for access list:

- Computer System: Username / password or Username / SSH key authentication for the service account.
- Other (Cisco Device): Username / password, and optional enable password authentication for the service account.
- Other (Cisco Works): Username / password authentication for the service account.
- The service account requires **network-admin** role privileges.
- SNMP: Enter community string (for SNMPv1 and SNMPv2).
- SNMP (SNMPv3):
 - Enter:
 - username
 - password
 - private password (optional)
 - Select authentication protocol: none, MD5, SHA

 It is important that a single community string is made available to TSA that has read-only access to ALL in scope network devices.

F5 Big-IP (TMOS)

To discover F5 Big-IP systems that are running TMOS, complete the following steps:

Credentials for access list:

- Computer System: Username / password or Username / SSH key authentication for the service account.
- The service account must have F5 administrator authority.
- The service account must have SSH access to run TMSH CLI commands.

Fortinet (FortiOS)

To discover Fortinet devices that are running FortiOS, complete the following steps:

Preparing the environment

- Ensure that the system console is configured to display the entire command output:

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

end

Credentials for access list:

- Computer System: Username / password or Username / SSH key authentication for the service account.
- The service account must have at least Read-Only permissions.

IBM b-type Storage Area Network (SAN) switches

To discover IBM b-type SAN devices, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- Virtual Fabric mode disabled: The service account can use any valid authority. **User** authority is recommended.
- Virtual Fabric mode enabled: The service account requires **Admin** authority on Fabric OS.

Juniper

To discover Juniper devices, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account
- The service account must have administrator authority.

 Note: Discovery of memory size information requires Junos® version 12.1 or later to be installed on the device.
--

Palo Alto Networks (PAN-OS)

To discover Palo Alto Network systems that are running PAN-OS, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account must have Superuser or Superuser (read-only)
- The service account must have REST API access (port 443).

QLogic Switches


To discover QLogic switches, complete the following steps:

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account must have administrator authority.

Storage Devices

This section provides detailed information on the following types of Storage and Tape devices:

Platform
<u>EMC Corporation Storage</u>
<u>HP StorageWorks P2000 Modular Smart Array</u>
<u>IBM DS3xxx, DS4xxx or DS5xxx</u>
<u>IBM DS6xxx or DS8xxx</u>
<u>IBM FlashSystem, v9000</u>
<u>IBM ProtecTier</u>
<u>IBM SVC or V7000/V3700</u>
<u>IBM TS3100 Tape Library</u>
<u>IBM TS3200 Tape Library</u>
<u>IBM TS3310 Tape Library</u>
<u>IBM TS3494, TS3953 Tape Libraries</u>
<u>IBM TS3500, TS3584 Tape Libraries</u>
<u>IBM TS4300 Tape Library</u>
<u>IBM TS4500 Tape Library</u>
<u>IBM TS7700 Tape Library</u>
<u>IBM V7000 Unified</u>
<u>IBM XIV</u>
<u>nSeries or NetApp</u>
 Click each of the above links for detailed information.

EMC Corporation Storage

EMC CLARiiON / VNX / VMAX


To discover EMC CLARiiON / VNX / VMAX devices, complete the following steps:

Preparing the environment:

- Ensure that an instance of the EMC SMI-S Provider product is installed on a Windows or Linux system. By default, TSA follows the EMC SMI-S recommendation to discover the location of the provider using SLP. If your network security policy blocks SLP network traffic, TSA can be configured to directly access the EMC SMI-S Provider without the use of SLP.
- If your network security does not allow SLP network traffic, use the **Discovery Settings** → **Connection Settings** page to provide information about which ports the EMC SMI-S Providers listen for query requests.
- Ensure that at least one of the IP addresses that the SMI-S Provider is utilizing is defined in a scope set. TSA will connect to the SMI-S Provider to retrieve information about the EMC devices that it manages. The IP addresses of the individual EMC devices do not need to be placed in a scope set. TSA attempts to connect to the SMI-S provider using HTTPS if available, otherwise HTTP is used.

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account can use any valid role. The **monitor** role is recommended.

 Only the credentials for the SMI-S provider need to be entered in TSA. No credentials for the EMC devices need to be entered.

EMC Data Domain

To discover EMC Data Domain devices, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account can have any level of authority. It is recommended to use the lowest level of authority.

HP StorageWorks P2000 Modular Smart Array

To discover HP Storage systems, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account can have any level of authority. It is recommended to use the lowest level of authority.

IBM DS3xxx, DS4xxx or DS5xxx Storage

To discover IBM DS3xxx, DS4xxx or DS5xxx devices, complete the following steps:

Preparing the environment:

- Ensure that the storage manager allows the use of remote **smcli** commands.

Credentials for access list:

- For non-secured storage devices, no credentials are required.
- For secured storage devices, complete the following steps:
 - Computer system: Username / password for the service account.
 - The service account can have either the **admin** or **monitor** role. The **monitor** role is recommended.

IBM DS6xxx / DS8xxx Storage

To discover IBM DS6xxx / DS8xxx devices, complete the following steps:

Preparing the environment:

- Ensure that the storage manager allows the use of remote **dscli** commands.

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account must have the **monitor** role.

IBM FlashSystem, v9000

To discover IBM FlashSystems, complete the following steps:

Preparing the environment:

- For older models, the MCP (Management Control Port) must be in active state to discover the system successfully.
 - To check if a system is in active state, run the command - `system status`.
 - Of the two IP addresses, if one IP goes down, the system goes into passive state. To make the other Ethernet port active, run the command - `sync activate`.
 - The discovered system must be the management IP address and/or configuration node.

Credentials for access list:

- Computer system: Username / password or Username / SSH key authentication for the service account.
- The service account can use any valid role. The **monitor** role is recommended.

IBM ProtecTIER

To discover ProtecTIER devices, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account must have administrator privileges.

IBM SVC, V7000/V3700 storage

To discover SVC and V7000/V3700 devices, complete the following steps:

Credentials for access list:

- Computer system: Username / password or Username / SSH key for authentication.
- The service account can use any valid role. The **monitor** role is recommended.

IBM TS3100 Tape Library

To discover TS3100 Tape Library devices, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account must have administrator authority.

IBM TS3200 Tape Library

To discover TS3200 Tape Library devices, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account must have administrator authority.

IBM TS3310 Tape Library

To discover TS3310 Tape Library devices, complete the following steps:

Preparing the environment:

- The web service is configured in secured mode always.

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account must have administrator authority.

IBM TS3494, TS3953 Tape Libraries

To discover TS3494, TS3953 Tape Library devices, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account can have the minimum authority required.

IBM TS3500, TS3584 Tape Libraries

The following prerequisites are required:

- The TS3500 Tape Library must be at firmware level 8xxx (or higher).
- The Advanced Library Management System (ALMS) must be installed and enabled.

 Both SSL and non-SSL connections are supported.

To discover TS35xx Tape Library devices, complete the following steps:

Preparing the environment:

- The TS3500 web interface can be configured for **No password protection** or **Password protection**
 - If **Password Protection** is activated, create a credential as described in **Credentials for access list** below.
 - If **Password protection** is disabled, no credentials are required.

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account must have administrator authority.

IBM TS4300 Tape Library

The following prerequisites are required:

- The TS4300 Tape Library must have the Rest API enabled on port 3031 via HTTPS.

To discover TS4300 Tape Library devices, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account must at least have the **Service** authority level.
- The credential must have access to the Rest API on port 3031 via HTTPS.

IBM TS4500 Tape Library

The following prerequisites are required:

- The TS4500 Tape Library must be at firmware level 1.4.1.2 or higher.
- The Advanced Library Management System (ALMS) must be installed and enabled.

 Both SSL and non-SSL connections are supported.

To discover TS4500 Tape Library devices, complete the following steps:

Preparing the environment:

- The TS4500 web interface can be configured to require username / password or can be configured that username / password are not required.

Credentials for access list:

- Computer system: Username / password for the service account is only required if the TS4500 is configured to require login credentials.
- The service account must be mapped to the **Service** role.

IBM TS7700 Tape Library

To discover TS7700 Tape Library devices, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account needs only **Read-Only** authority.

IBM V7000 Unified Storage

To discover V7000 Unified devices, complete the following steps:

Credentials for access list:

- Computer system: Username / password for the service account.
- The service account can use any valid role. The **monitor** role is recommended.

IBM XIV Storage

To discover XIV devices, complete the following steps:

Preparing the environment:

- Ensure that the storage manager allows the use of remote **xcli** commands.

Credentials for access list:

- Computer System: Username / password for the service account.
- The service account must have the **read-only** user role.
- Be aware that XIV systems may have a low threshold for invalid sign-on attempts before generating alerts. If you are using a large credential set, you may exceed this limit and cause unnecessary problems to be reported. Try to group the XIV devices in a single scope set and restrict their service account credentials to that scope set.

nSeries or NetApp Storage

To discover nSeries or NetApp devices, complete the following steps:

Preparing the environment:

- Data collection is supported for systems configured with the Data ONTAP CLI, RLM CLI and SP CLI. However, the BMC CLI is not supported.
- The **telnet.distinct.enable** option must be turned on.

Credentials for access list:


- Computer system: Username / password for the service account.
- The service account can have any level of authority. It is recommended to use the lowest level of authority.


Firewall Considerations

Firewall(s) between the appliance and the discovery devices could prevent a complete and successful discovery from occurring.

In cases where it is necessary to traverse a firewall, ports may have to be opened in the firewall, depending on the type of device the user would like to discover. Typically ports 22 (SSH) and 161 (SNMP) should be opened, followed by the appropriate ones in the following table based on the supported devices.

Discovery Endpoint	Ports	Interface / Protocol
Numerous	161	SNMP
Storage Devices		
DS6000 / DS8000	1750 (HTTP) or 1751 (HTTPS)	DSCLI
DS3000 / DS4000 / DS5000	2463	SMCLI
XIV	7778	XCLI
nSeries or NetApp	22 / 23	SSH or Telnet
SVC or V7000/V3700	22	SSH
V7000 Unified	22	SSH
IBM TS3100 / TS3200	80	HTTP
IBM TS3310	80	HTTP
IBM TS3500	443 / 80	HTTPS or HTTP
IBM TS4300	3031	HTTPS (on port 3031)
IBM TS4500	443 / 80	HTTPS or HTTP
IBM TS7700	443 / 80	HTTPS or HTTP
IBM TS3494, TS3953	23	Telnet
IBM ProtecTier	22	SSH
HP Storage	22 / 23	SSH or Telnet
IBM Flash System, v9000	22	SSH

Discovery Endpoint	Ports	Interface / Protocol
EMC Corporation Storage - CLARiiion/VNX/VMAX	427 - (default) when SLP discovery is allowed, else if SLP discovery is disabled, this port is not used. HTTPS / HTTP ports configured by EMC SMI-S provider; default values are 5989 / 5988	SLP, HTTPS / HTTP
	 You can enable or disable the SLP discovery option to discover EMC storage devices through EMC SMI-S Providers.	
EMC Corporation Storage – EMC Data Domain	22	SSH*
Operating Systems and Hosts		
FSM	22 / 23	SSH or Telnet
CMM	22 / 23	SSH or Telnet
AMM	22 / 23	SSH or Telnet
HP Proliant Blade Server via HP OnBoard Administrator	22 / 23	SSH or Telnet
IMM & IMM2	22 / 23	SSH or Telnet
HP iLO for the HP Integrity / HP 9000 servers	22 / 23	SSH* or Telnet
Dell iDRAC	22 / 23	SSH or Telnet
Network Devices		
Brocade	161 / 22 / 23	SNMP, SSH, Telnet
IBM b-type Storage Area Network (SAN) switches	22 / 23	SSH, Telnet
Cisco	161 / 22 / 23	SNMP, SSH, Telnet
BNT	22 / 23	SSH or Telnet
Juniper	22 / 23	SSH or Telnet
QLogic	22 / 23	SSH* or Telnet

Discovery Endpoint	Ports	Interface / Protocol
Fortinet (FortiOS)	22 / 23	SSH or Telnet
Palo Alto Networks (PAN-OS)	443	HTTPS
F5 Big-IP (TMOS)	22 / 23	SSH or Telnet
Check Point	22 / 23	SSH or Telnet
Operating Systems / Server Platforms		
HMC	22	SSH
VIOS	22	SSH
AIX	22	SSH
Linux	22	SSH
Windows	445	SMBv1
VMware vCenter	443	HTTPS
VMware ESXi	443, 5989	HTTPS
IVM	22 / 23	SSH or Telnet
IBM i	22	SSH
SUN	22	SSH
 TSA supports only SSH v1 for the devices that are marked by SSH*.		

Discovery Issues

Most discovery problems are due to access or authorization issues.

The most common access issues are due to firewalls blocking access to the necessary ports on the device. The ports that need to be open and reachable vary by device type. See section “[Firewall Considerations](#)” on page 38 to determine which ports are applicable.

The most common authorization issues include the following:

- **No credentials defined.** Ensure that credentials for the devices are defined in TSA and the appropriate service accounts are created on the devices.
- **Credential username or password incorrect.** Use the **Test** function when creating or editing a credential to verify that the credential is valid.
- **Credential password expired.**
- **Credential lacking the necessary authorities on the device.** To determine the credential requirements for a target device, see section [Device Discovery Configuration](#) on page 10.
- **Use valid credential type.** For Windows devices, create a 'Computer System (Windows)' credential and not a 'Computer System' credential.

 Check the **Authentication Status** page (**Tools → Authentication Status**) to see if any service account credentials have expired passwords or have stopped working.

Ongoing Considerations

After the desired portions of the network have been defined in TSA and scanned successfully, TSA can be left to run periodic discoveries and transmissions on the desired schedules.

The following are some expected ongoing activities:

- Review the reports generated by TSA with your IBM representative on a periodic basis.
- Perform a backup via the TSA user interface periodically to save a copy of the TSA configuration.

 This operation does not save data collected by TSA. It only saves configuration information.

- Periodically check the **Authentication Status** page (**Tools → Authentication Status**) to see if any service account credentials have expired passwords or have stopped working.
- When the passwords are updated for the service accounts on the devices, be sure to update the passwords in TSA as well to keep the credential definition in TSA in sync with the credential on the target device.
- If your security policy allows for it, consider setting up service accounts with non-expiring passwords or use SSH keys. This eliminates the need to update the passwords in the TSA user interface and on the devices periodically.

Troubleshooting

Active Session for AMM Discovery

AMM devices have a setting that limits the number of simultaneous active sessions (maximum of 20). If this setting is not high enough to allow TSA to create a session, the AMM device cannot be discovered.

To change the limit of the active sessions of an AMM device, follow these steps:

1. Log in to the AMM web interface by typing the AMM device's IP address in a web browser.
2. Go to **MM Control** → **Login Profiles**.
3. Click login ID that TSA is using to discover the device.
4. Increase the **Maximum simultaneous active sessions** setting value.
5. Click **Save** at the lower right of the page.

Appendix A: Terms and Definitions

It is assumed that the reader has an in-depth understanding of Internet Protocol (IP) networks and protocols.

Term	Definition
Discovery device	Refers to deployed IT infrastructure components that can be discovered by TSA. Typical devices include: Servers, Computer Systems (e.g. IBM, Dell, and HP), Storage elements, and Network elements (e.g. switches, bridges, routers).

Appendix B: Miscellaneous Items

User Interface Download Functions

In some cases, when using a web browser, the Download All Logs (from the **Activity Log** page) or the file downloads (from the **Discovery History** page) does not complete successfully. To resolve this issue, try switching to another supported web browser as documented in the IBM Technical Support Appliance Setup Guide. If that is not an option, try resetting your browser's properties to their default settings.

Appendix C: CIM Provider for VMware ESXi

A CIM provider is a set of VMware ESXi plug-ins that can collect additional hardware and firmware information about the server that VMware ESXi is running on. Both TSA and the VMware vCenter can benefit from this additional information.

CIM provider plug-ins are developed by the server and component manufacturers. To ensure that CIM provider plug-ins are included in ESXi, use a customized installation image where the CIM provider plug-ins are included. For existing VMware ESXi instances that do not have the CIM provider installed, obtain the necessary plug-ins from the server and component manufacturers, and install into ESXi. VMware provides a list of the various plug-ins that are provided by manufacturers.

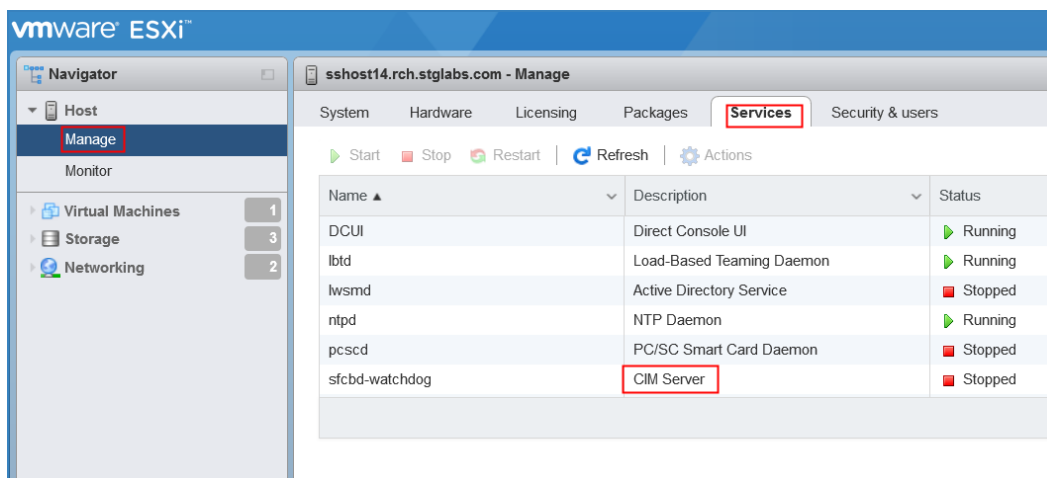
For more information, see

https://www.vmware.com/resources/compatibility/pdf/vi_cim_guide.pdf.

To determine if the CIM provider is active, and to turn on the CIM provider if it is not active, go through the following steps.

On VMware vSphere Web Client

- Login to the VMware vSphere Web Client.
- Click on **Host** → **Manage** in the left navigation window and select the **Services** tab in the right pane.
- A set of services including the **CIM Server** are displayed.



- If **CIM Server** is in **Stopped** state, then select it and click **Start**.

System Hardware Licensing Packages Services Security & users		
▶ Start ■ Stop ↻ Restart 🔄 Refresh ⚙️ Actions		
Name ▲	Description ▼	Status
DCUI	Direct Console UI	▶ Running
lbtd	Load-Based Teaming Daemon	▶ Running
lwsmd	Active Directory Service	■ Stopped
ntpd	NTP Daemon	▶ Running
pcscd	PC/SC Smart Card Daemon	■ Stopped
sfcdb-watchdog	CIM Server	■ Stopped

- The CIM Server service starts and the status will be in **Running** state.

System Hardware Licensing Packages Services Security & users		
▶ Start ■ Stop ↻ Restart 🔄 Refresh ⚙️ Actions		
Name ▲	Description ▼	Status
DCUI	Direct Console UI	▶ Running
lbtd	Load-Based Teaming Daemon	▶ Running
lwsmd	Active Directory Service	■ Stopped
ntpd	NTP Daemon	▶ Running
pcscd	PC/SC Smart Card Daemon	■ Stopped
sfcdb-watchdog	CIM Server	▶ Running

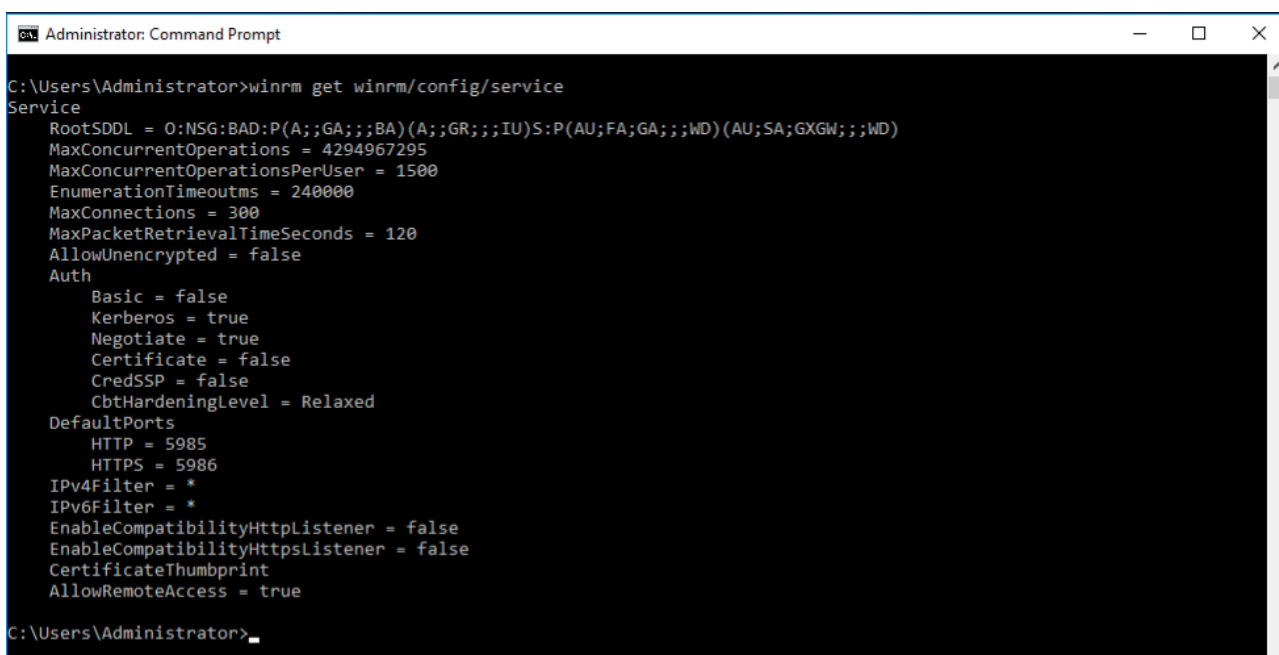
Appendix D: Windows using WINRM

For Windows 2012 Server, 2016 Server, and 2019 Server the WINRM service is started automatically. However, remote management is not enabled by default. Here is a brief outline on what is required to enable WINRM to allow remote connections using a self-signed certificate:

- Enable WINRM to accept HTTPS connections that authenticate with user ID / password
- Associate a self-signed certificate with the HTTPS listener for WINRM that was enabled
- Modify the Windows firewall to allow inbound connections via port 5986 (the default WINRM HTTPS port)

The following commands prepare WINRM to allow remote connections over HTTPS:

- Determine the current state of the WINRM service using this command:



```
Administrator: Command Prompt
C:\Users\Administrator>winrm get winrm/config/service
Service
RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
MaxConcurrentOperations = 4294967295
MaxConcurrentOperationsPerUser = 1500
EnumerationTimeoutms = 240000
MaxConnections = 300
MaxPacketRetrievalTimeSeconds = 120
AllowUnencrypted = false
Auth
  Basic = false
  Kerberos = true
  Negotiate = true
  Certificate = false
  CredSSP = false
  CbtHardeningLevel = Relaxed
DefaultPorts
  HTTP = 5985
  HTTPS = 5986
IPv4Filter = *
IPv6Filter = *
EnableCompatibilityHttpListener = false
EnableCompatibilityHttpsListener = false
CertificateThumbprint
AllowRemoteAccess = true
C:\Users\Administrator>
```

`winrm get winrm/config/service`

- The value for **AllowUnencrypted** must be *false*. If *true*, use the following command to change to *false*:

`winrm set winrm/config/service @{AllowUnencrypted="false"}`

- The value for **Basic** must be *true*. If *false*, use the following command to change to *true*:
`winrm set winrm/config/service/auth @{Basic="true"}`
- Determine if WINRM has an HTTPS listener using this command:
`winrm enumerate winrm/config/listener`

```

Administrator: Command Prompt
C:\Users\Administrator>winrm enumerate winrm/config/listener
Listener
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 9.5.80.125, 127.0.0.1, ::1, 2001:0:5ef5:79fb:34be:1cf4:f6fa:af82, 2002:905:150e:251:d7f:a049:285a:ae33, fd55:faaf:e1ab:2251:d7f:a049:285a:ae33, fe80::200:5efe:9.5.80.125%6, fe80::d7f:a049:285a:ae33%7, fe80::34be:1cf4:f6fa:af82%3
C:\Users\Administrator>

```

- In the command example above, only an HTTP listener exists, so an HTTPS listener needs to be configured. To enable the HTTPS listener if not configured:
 - Using PowerShell, create a self-signed certificate:
`New-SelfSignedCertificate -DnsName "myHost@example.com" -CertStoreLocation Cert:\LocalMachine\My`

Replace the DnsName (**myHost@example.com**) in the above example with the Windows fully-qualified domain name for the Windows server.

- Save the certificate thumbprint for the next step

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-SelfSignedCertificate -DnsName "testServer.testCo.com" -CertStoreLocation Cert:\LocalMachine\My

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint          Subject
-----
90973CF1FBC575A3E57011371BE158AD8A6AFF80  CN=testServer.testCo.com

PS C:\Users\Administrator>

```

- Create the HTTPS listener:
`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="myHost@example.com"; CertificateThumbprint="[COPIED_CERTIFICATE_THUMBPRINT]"}`
- Check to ensure HTTPS is now configured:
`winrm enumerate winrm/config/listener`

- Modify the Windows firewall to allow inbound remote connections to WINRM:
 - Go to Control Panel → System and Security → Windows Firewall
 - Click Advanced settings. The Windows Firewall with Advanced Security window displays.
 - Click Inbound Rules.
 - Select Actions menu and click on New Rule. The New Inbound Rule Wizard displays.
 - Select **Port** and click **Next**.
 - Select **TCP → Specific local ports** and specify 5986. Click **Next**.
 - Select **Allow the connection** option and click **Next**.
 - Select the **Domain**, **Private**, and **Public** checkboxes if not already checked and click **Next**.
 - Give the new rule a name (such as Windows Remote Management (HTTPS-In)) and click **Finish**.

Notices

© IBM Corporation 2022
IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
Produced in the United States of
America
June 2022.
All Rights Reserved

This document was developed for products and/or services offered in the United States. IBM may not offer the products, features, or services discussed in this document in other countries.

The information may be subject to change without notice. Consult your local IBM business contact for information on the products, features and services available in your area.

All statements regarding IBM future directions and intent are subject to change or withdrawal without notice and represent goals and objectives only.

IBM, the IBM logo, POWER, System I, System p, i5/OS, are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both. A full list of U.S. trademarks owned by IBM may be found at <http://www.ibm.com/legal/copytrade.shtml>.

Other company, product, and service names may be trademarks or service marks of others.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

This equipment is subject to FCC rules. It will comply with the appropriate FCC rules before final delivery to the buyer.

Information concerning non-IBM products was obtained from the suppliers of these products.

Questions on the capabilities of the non-IBM products should be addressed with the suppliers.

The IBM home page on the Internet can be found at <http://www.ibm.com>.

The IBM System p home page on the Internet can be found at <http://www.ibm.com/systems/p>.

The IBM System I home page on the Internet may be found at <http://www.ibm.com/systems/i>.

PSW03007-USEN-00