IBM® Technical Support Appliance
Guía del asistente de configuración

Versión 2.7.0.0

Agosto de 2020

Tabla de contenido

Introducción

IBM Technical Support Appliance (TSA) es una herramienta de fácil uso que le permite obtener más valor de sus contratos con el servicio de soporte de IBM. TSA descubre elementos clave de las tecnologías de la información y sus relaciones dentro de su infraestructura de TI y transmite de forma segura los datos al servicio de soporte de IBM para su análisis. Estos datos proporcionan al servicio de soporte de IBM información sobre las complejas relaciones entre los servidores y los componentes de red de su centro de datos.

La intención de este documento es proporcionar información y orientación para ayudarle en la instalación, planificación y configuración de TSA.

Consideraciones de red previas al descubrimiento

Antes de configurar TSA para iniciar el descubrimiento y la transmisión, asegúrese de que se han abordado los siguientes elementos. Se presupone que TSA ya se ha instalado, la interfaz web es accesible y TSA se ha actualizado al nivel más actual; si no, consulte la Guía de configuración de Technical Support Appliance (denominada guía de configuración en adelante en este documento).

Consideraciones de red previas al descubrimiento para TSA	
Redes	
	Abra el acceso de cortafuegos desde TSA a IBM. Consulte la sección, **Requisitos de configuración para las conexiones al servicio de soporte de IBM** en la guía de configuración.
	Si se utiliza un proxy SSL para devolver la conexión a IBM, asegúrese de que está configurado en TSA. Consulte la sección, **Configuración de la conectividad con IBM** en la guía de configuración. • No se admite inspección SSL. Si se utiliza inspección SSL en el proxy, deshabilítelo para estos flujos.
	Si hay algún cortafuegos entre TSA y los dispositivos de destino, asegúrese de que los puertos necesarios estén abiertos. Para obtener más información, consulte la sección "Consideraciones sobre cortafuegos" en la página 41.

Documentación de utilidad

El enlace a continuación lo dirigirá directamente al sitio web de información de Technical Support Appliance. Allí se muestra todo lo necesario para empezar a trabajar con IBM Technical Support Appliance. Puede acceder a guías de configuración y documentación de

seguridad, ver informes de ejemplo y descargar el código de instalación de Technical Support Appliance de ibm.com.

Para obtener más información sobre Technical Support Appliance: https://ibm.biz/TSAdemo

Descripción general

TSA puede descubrir información sobre su infraestructura de TI, incluyendo los componentes de sistema operativo desplegados, componentes de firmware, servidores físicos, dispositivos de red, LAN virtual, etc. Para optimizar la amplitud y la profundidad de la información recopilada; se requieren tareas de configuración en TSA para identificar los dispositivos de descubrimiento.

TSA procura minimizar el impacto en el entorno de red del cliente. Así pues, el proceso de descubrimiento utiliza un método iterativo y mesurado que puede hacer que un descubrimiento completo tarde hasta 72 horas. Se puede supervisar el estado del trabajo de descubrimiento visualizando la sección **Resumen de trabajos** del panel **Resumen**.

Como parte del proceso de descubrimiento, TSA primero intenta detectar dispositivos dentro del alcance definido sin utilizar credenciales. Esto supone el uso de Nmap para descubrir y clasificar dispositivos mediante exploración de IP poco intrusiva, pila de huellas dactilares y correlación de puertos. Generalmente, esta actividad no debería ser lo suficientemente significativa como para activar un sistema de detección de intrusiones (IDS - intrusion detection system), pero puede ocurrir si los valores locales son muy estrictos.

Para que TSA pueda recopilar información sobre su infraestructura de TI, proporciónele lo siguiente:

- Alcances
- Credenciales de acceso

Definir conjuntos de alcances

Un conjunto de alcances es una agrupación lógica de alcances individuales. Los alcances utilizan direcciones IP para indicar a TSA dónde debe empezar a descubrir el entorno. Un conjunto de alcances se compone de uno o más alcances. Hay tres tipos de entradas de alcance:

- Subred - Definida por una dirección IP y una máscara de subred. Las subredes se limitan a subredes de clase C.
- Rango de IP - Incluye todas las direcciones IP entre el principio y el final.
- Dirección IP / Host - Una dirección IP o un nombre de host individual.

> El nombre de host se resuelve en el momento de la entrada y no en el momento del descubrimiento. Consulte la sección "Factores a considerar al crear alcances", en la página 6, para obtener información detallada.

Si se quiere, se pueden definir exclusiones de alcance para un alcance especificando una definición de host, de rango o de subred. Las direcciones IP resultantes no se considerarán parte del alcance y no se explorarán.

TSA admite tres tipos de conjuntos de alcances:

1. **Conjuntos de alcances generales**: permiten descubrir elementos de red de TI individuales. El conjunto de alcances contiene uno o varios alcances que identifican la ubicación de estos elementos de red utilizando una dirección IP, un rango de direcciones IP o una red o subred.
2. **Conjuntos de alcances dinámicos** de HMC: permiten especificar la dirección IP de una o más HMC de IBM POWER Systems junto con las credenciales asociadas. Además, también se puede recopilar información sobre todas las LPAR que gestionan las HMC sin necesidad de identificar las direcciones IP de las LPAR. El conjunto de alcances dinámico utiliza la información de credenciales que se le proporciona para acceder satisfactoriamente a estas LPAR.
3. **Conjuntos de alcances dinámicos de VMware**: permiten especificar la dirección IP de una o más instancias de VMware vCenter Server o ESXi junto con las credenciales asociadas. Además, también se puede recopilar información sobre todas las máquinas virtuales que VMware gestiona sin necesidad de identificar las direcciones IP de las máquinas virtuales. El conjunto de alcances dinámico utiliza la información de credenciales que se le proporciona para acceder satisfactoriamente a estas máquinas virtuales.

Para las HMC y los VMware vCenter Servers/ESXi, se recomienda el uso de conjuntos de alcances dinámicos. Los conjuntos de alcances dinámicos requieren mucha menos configuración en TSA que la creación y gestión de alcances de descubrimiento de LPAR/máquinas virtuales individuales. Asimismo, los conjuntos de alcances dinámicos permiten gestionar los entornos donde se añaden y suprimen LPAR o máquinas virtuales en el tiempo sin necesidad de modificar los conjuntos de alcances.

Para obtener instrucciones detalladas sobre cómo definir alcances de descubrimiento en TSA, consulte la sección **Configuración de alcances de descubrimiento** en la guía de configuración.

Factores a considerar al crear alcances

Aunque no hay estándares definidos para configurar alcances, a continuación se ofrecen algunas consideraciones prácticas que pueden ahorrar tiempo y esfuerzo:

- Cuando sea práctico, utilice conjuntos de alcances dinámicos para definir los descubrimientos de las HMC y las LPAR que gestionan, o de VMware vCenter Server / ESXi y las máquinas virtuales que gestionan. Si se utilizan conjuntos de

alcances dinámicos, no hay necesidad de definir los alcances de las LPAR ni de las máquinas virtuales.

- Utilice alcances de rango de IP o de subred para descubrir varios dispositivos en lugar de direcciones IP o nombres de host individuales. De esta forma se limitará el número de definiciones de alcance y se facilitará la administración.
- Si utiliza definiciones de alcance de subred, incluya sólo una por cada conjunto de alcances. Asegúrese de que la definición de alcance de subred se resuelve a una red de Clase C (256 direcciones IP) o inferior.
- Utilice la característica **Importar conjunto de alcances general** para crear un nuevo conjunto de alcances basado en el nombre especificado y la lista de direcciones IP de un archivo de texto de entrada. Para obtener más información, consulte la sección **Alcances de descubrimiento → Importar conjunto de alcances general** de la guía de configuración para obtener instrucciones.
- TSA solo almacena direcciones IP, actualmente. Esto significa que los nombres de host se resuelven en el momento de la entrada y no en el momento del descubrimiento. Como mejores prácticas, se recomienda utilizar Dirección IP o Rango de IP para la definición de alcance y no el nombre de host.
- Cuantas más direcciones IP haya en el conjunto de alcances, más durará el descubrimiento. Para minimizar el tiempo que dura un descubrimiento, configure los alcances de forma que apunten solo a los elementos que desea descubrir.

Si utiliza conjuntos de alcances generales, limite el número acumulativo de direcciones IP a las que resuelve un conjunto de alcances (después de ampliar las definiciones de alcances de rango o de subred) a 400 o menos. Pueden aparecer problemas de rendimiento, de servidor o de red durante el proceso de descubrimiento si se exploran más de 400 direcciones IP para un solo conjunto de alcances.

- TSA no impide definir direcciones IP en varios conjuntos de alcances. En general, esta práctica se debería evitar puesto que aumenta el tiempo de descubrimiento y no recopila ninguna información adicional.
- Agrupe los alcances en conjuntos de alcances que constituyan una agrupación lógica de dispositivos:
    - Agrupe el mismo tipo de dispositivo dentro de un conjunto de alcances. Por ejemplo, cree un conjunto de alcances para los subsistemas de almacenamiento IBM FlashSystem.

- Agrupe los dispositivos que se encuentren en la misma área geográfica.
- Agrupe los dispositivos de acuerdo con las aplicaciones o servicios empresariales.

Credenciales de descubrimiento

Con algunas excepciones, los descubrimientos requieren algún nivel de acceso para adquirir la información detallada que se necesita para conocer completamente el entorno.

Normalmente se deben crear cuentas de servicio en los dispositivos de descubrimiento para que las utilice el TSA. Consulte las secciones siguientes para conocer los derechos de acceso específicos que requiere cada tipo de plataforma. Para simplificar la administración de estas cuentas de servicio, utilice el mismo nombre de usuario para todos los dispositivos de una misma familia de productos.

La tarea de mantenimiento de las cuentas de servicio que TSA utiliza para conectarse a los dispositivos se puede simplificar utilizando una de las estrategias siguientes:

- Crear cuentas de servicio con contraseñas que no caduquen
- Utilizar claves SSH para dispositivos de familias de productos que admitan el uso de las mismas

Para obtener instrucciones detalladas sobre cómo definir credenciales de acceso en el dispositivo, consulte la sección **Configuración de credenciales de descubrimiento** en la guía de configuración.

Factores a considerar al configurar credenciales de descubrimiento

El dispositivo intenta utilizar las credenciales en el orden en que aparecen en la lista de acceso. Para acelerar el descubrimiento, asegúrese de que tiene las credenciales en el orden más adecuado para su entorno. Tenga en cuenta las siguientes consideraciones:

- Restrinja las credenciales a conjuntos de alcances específicos cuando corresponda. Esto limitará los intentos de inicio de sesión innecesarios y mejorará el rendimiento del descubrimiento.
- Se pueden utilizar claves SSH para los siguientes descubrimientos de dispositivos:
  - AIX
  - Cisco
  - Linux
  - HMC
  - IBM i
  - IVM

- Sun SPARC (Solaris)
- SVC / V7000
- VIOS
- Fortinet
- HP-UX
- IBM FlashSystem
- F5 Big IP
- Check Point

Solo se puede enlazar una credencial de clave SSH a un conjunto de alcances.

- Se recomienda crear cuentas de servicio separadas que TSA utilice exclusivamente con el nivel más bajo de autorización necesario.

Guía de inicio

En esta sección se describen algunas mejores prácticas y recomendaciones para configurar TSA.

Configuración inicial de TSA

Siga las instrucciones especificadas en las siguientes secciones de la guía de configuración:

- Instalación de Technical Support Appliance
- Inicio de sesión en Technical Support Appliance
- Aceptar el Acuerdo de licencia
- Configuración de Technical Support Appliance utilizando el asistente de instalación

Preparación para realizar descubrimientos

Se recomienda un proceso iterativo por el cual inicialmente se configure una pequeña porción de la red para su descubrimiento y se vayan añadiendo más secciones de la red con cada iteración hasta cubrir toda la red deseada.

> Se recomienda guardar una copia de seguridad de la configuración de TSA después de realizar adiciones/modificaciones significativas en los alcances o en las credenciales. Para obtener más información, consulte la sección "Copia de seguridad y restauración" en la Guía de configuración de IBM Technical Support Appliance.

Pasos de descubrimiento

Para cada iteración de descubrimiento, efectúe los pasos siguientes:

1. Prepare los dispositivos para el descubrimiento. Si tiene requisitos de configuración de dispositivos y credenciales especiales, consulte la sección "Configuración del descubrimiento de dispositivos" en la página 12.
2. Para los conjuntos de alcances dinámicos de HMC, efectúe los pasos siguientes:
   a. Añada las direcciones IP de las HMC en la página **Conjunto de alcances dinámicos de HMC**.
   b. Añada las credenciales de las HMC en la página **Conjunto de alcances dinámicos de HMC**.
   c. Seleccione los tipos de LPAR que desea descubrir. Proporcione credenciales para cada tipo.

   > Puede seleccionar los tipos de LPAR a descubrir al crear el conjunto de alcances dinámico, o puede añadir los tipos de LPAR en otra iteración más adelante editando el conjunto de alcances dinámico.

d. (Opcional) Utilice la función Probar de la página **Conjunto de alcances dinámicos de HMC** para verificar que las credenciales estén definidas correctamente y se puedan utilizar para establecer una conexión con las HMC o con sus LPAR.

3. Para los conjuntos de alcances dinámicos de VMWare, efectúe los pasos siguientes:
   a. Añada las direcciones IP de los VMware vCenter Servers.
   b. Añada las direcciones IP de los hosts VMware ESXi que no estén gestionados por un VMware vCenter Server.
   c. Añada las credenciales de las instancias de VMware vCenter Servers y ESXi en la página **Conjunto de alcances dinámicos de VMware**.
   d. Seleccione los tipos de máquina virtual que desea descubrir. Proporcione credenciales para cada tipo.

      Puede seleccionar los tipos de máquina virtual a descubrir al crear el conjunto de alcances dinámico, o puede añadir los tipos de máquina virtual en otra iteración más adelante editando el conjunto de alcances dinámico.

   e. (Opcional) Utilice la función Probar de la página **Conjunto de alcances dinámicos de VMware** para verificar que las credenciales están definidas correctamente y se pueden utilizar para establecer una conexión con las instancias de VMware vCenter Servers y ESXi, así como con sus máquinas virtuales.
4. Para los conjuntos de alcances generales, efectúe los pasos siguientes:
   a. Añada las direcciones IP deseadas en los conjuntos de alcances / alcances adecuados. Si existen cortafuegos entre la instancia de TSA y los dispositivos de descubrimiento, asegúrese que el cortafuegos tiene los puertos adecuados abiertos para permitir que el descubrimiento se realice satisfactoriamente. Para obtener información sobre los puertos que deben estar accesibles para cada tipo de plataforma, consulte la sección "Consideraciones sobre cortafuegos" en la página 41.
   b. Cree las credenciales necesarias. Utilice la función Probar del panel **Nuevo Descubrimiento Credenciales** para verificar que la credencial está definida correctamente y que se puede utilizar para establecer una conexión con un dispositivo de destino.
5. Ejecute un descubrimiento completo para explorar las direcciones IP añadidas para esta iteración.
6. Ejecute una transmisión para cargar los datos en IBM.

Configuración del descubrimiento de dispositivos

Además de proporcionar credenciales, pueden ser necesarios requisitos previos de configuración de dispositivos de descubrimiento específicos para que TSA pueda descubrir y recopilar eficazmente información útil de componentes. Esta sección le permite identificar los dispositivos de descubrimiento de su entorno que van a requerir configuraciones específicas. Se recomienda crear cuentas de servicio con las autorizaciones mínimas necesarias y consultar la sección "Consideraciones sobre cortafuegos" para obtener información sobre puertos y protocolos.

- Para los dispositivos para los que están abiertos tanto el puerto SSH como el puerto Telnet, TSA intentará primero una conexión utilizando SSH (por motivos de seguridad). Si esta conexión SSH falla, TSA probará la conexión utilizando Telnet.

Sistemas operativos y hosts

Plataforma
IBM Power Systems • Hardware Management Console (HMC) • Integrated Virtualization Manager (IVM) • Particiones VIOS (Virtual I/O Server) • AIX • Linux on Power
IBM i
UNIX Systems • Solaris • Solaris vía iLOM • Linux • HP-UX
VMware vCenter Server y VMware ESXi
Windows
Dispositivos de cajero automático

Módulo de gestión

- Flex System Manager (FSM)
- Chassis Management Module (CMM)
- Advanced Management Module (AMM)
- Servidor Blade HP ProLiant vía HP OnBoard Administrator
- Módulo de gestión integrado (IMM e IMM2)
- Servidores HP Integrity y HP9000 vía iLO

Pulse en cualquiera de los enlaces anteriores para obtener información detallada.

IBM Power Systems

Para IBM Power Systems, donde la configuración de LPAR la gestiona una HMC o un IVM, utilice conjuntos de alcances dinámicos de HMC. Con los conjuntos de alcances dinámicos de HMC puede crear una definición de alcance para las HMC y proporcionar las credenciales asociadas de HMC y LPAR, pero no es necesario crear alcances para cada LPAR gestionada. Cuando se descubre la HMC, el TSA determina las LPAR que existan en ese momento y automáticamente explora cada una de las LPAR.

Para IBM Power Systems, donde la configuración de LPAR es generalmente estática, hay un método alternativo a los conjuntos de alcances dinámicos de HMC que consiste en iterar añadiendo alcances y credenciales para las entidades en el siguiente orden:

1. **Las instancias de HMC o de IVM**: La HMC devuelve información general sobre todos los sistemas Power que gestiona y las particiones lógicas que contienen. El IVM (Integrated Virtualization Manager) devuelve información similar del sistema que gestiona.
2. **Las particiones VIOS**: Esto devuelve información sobre los adaptadores físicos y los recursos de los que estas particiones son propietarias.
3. **Particiones individuales**: En algunos casos, una partición no VIOS es propietaria de adaptadores físicos.

Hardware Management Console (HMC)

Para descubrir instancias de HMC, efectúe los pasos siguientes:

Preparación del entorno:

- Para que TSA pueda recopilar información sobre la gestión de LPAR a través de la HMC, ésta debe poder comunicarse con las LPAR que utilizan herramientas RMC.

Asegúrese de que la HMC y las LPAR estén configuradas para permitir esta comunicación. Para obtener más información herramientas RMC para Linux, consulte https://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/yum.html

- Para habilitar la recopilación de datos segura, se debe habilitar la ejecución remota de mandatos en la HMC. Para obtener información, consulte "Habilitación e inhabilitación de mandatos remotos de la consola HMC" en la siguiente dirección: https://www.ibm.com/support/knowledgecenter/es/POWER7/p7ha1/enablinganddisablinghmcremotecommands.htm

Credenciales para la lista de acceso:

- Para conjuntos de alcances dinámicos de HMC: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de HMC.
- Para conjuntos de alcances de descubrimiento generales: Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de HMC.
- El usuario de la HMC debe tener los siguientes roles:
  - Rol de recursos: AllSystemResources
  - Rol de tareas (basado en **hmcoperator** con tareas de línea de mandatos):
    - Sistema gestionado (lshwres, lssyscfg)
    - Partición lógica (lshwres, lssyscfg, viosvrcmd)
    - Configuración de HMC (lshmc)
- Si es necesario, se puede utilizar un usuario (cuenta de servicio) con autorización **hmcviewer**, sin embargo, el resultado será en una recopilación de datos parcial.

> Al ejecutar con autorización de **hmcviewer**, no se puede obtener información sobre los adaptadores que son propiedad de particiones VIOS. Para obtener esta información, asegúrese de que la cuenta de servicio tiene como mínimo la autorización de **hmcoperator**. Si no es posible, añada alcances y credenciales directamente a las particiones VIOS además de a la HMC.

Integrated Virtualization Manager (IVM)

Para descubrir instancias de IVM, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de IVM.
- La cuenta de servicio debe tener permiso sólo de visualización.

Particiones VIOS (Virtual I/O Server)

Para descubrir instancias de VIOS, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Para conjuntos de alcances dinámicos de HMC: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de partición VIOS.
- Para conjuntos de alcances de descubrimiento generales: Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de partición VIOS.
- La cuenta de servicio debe ser una cuenta de administrador (como por ejemplo **padmin**).
- La cuenta de servicio debe tener el atributo de usuario **rlogin=true**. Puede establecer este atributo utilizando SMIT o editando el archivo **/etc/security/user**.
- El parámetro **PermitUserEnvironment** del archivo **/etc/ssh/sshd_config** debe estar establecido en **yes**.

AIX

Para descubrir instancias de AIX, efectúe los pasos siguientes:

Preparación del entorno:

- Asegúrese de que los paquetes bos.perf.tools y openSSH/openSSL están instalados.
- Deshabilite el fallo por intento de inicio de sesión no válido de la cuenta de servicio.

Credenciales para la lista de acceso:

- Para conjuntos de alcances dinámicos de HMC: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de partición AIX.
- Para conjuntos de alcances de descubrimiento generales: Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de AIX.
- La cuenta de servicio puede ser root o bien una cuenta con autorización sudo.

- La cuenta de servicio debe tener el atributo de usuario **rlogin=true**. Puede establecer este atributo utilizando SMIT o editando el archivo **/etc/security/user**.
- Para habilitar una cuenta de servicio no root con autorización sudo para AIX:
  - Instale el RPM de sudo (sudo-1.6.9p15-2noldap) y los conjuntos de archivos ssh (openssh.base.server, openssh.base.client en la instancia de AIX).
  - Cree un ID de usuario no root en la instancia de AIX de destino que TSA pueda utilizar para acceder al sistema.
  - Modifique **/etc/sudoers** en cada una de las instancias de AIX para permitir que TSA ejecute los mandatos especificados utilizando autorización sudo.

    # Especificación de Cmnd alias

    ```
    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
    ```

    # Especificación de privilegios de usuario

    ```
    <Nombre de usuario> ALL = NOPASSWD: TSA_CMDS
    ```

    <Nombre de usuario> es la cuenta de servicio no root que TSA utiliza para recopilar información de AIX. Este <Nombre de usuario> es un usuario en cada instancia de AIX. Es necesario actualizar el archivo **/etc/sudoers** de cada instancia de AIX con la especificación anterior.

    O bien

    Una alternativa a las modificaciones mencionadas en **/etc/sudoers** es utilizar la especificación siguiente de privilegio de usuario:

    ```
    <Nombre de usuario> ALL = NOPASSWD: ALL
    ```

    <Nombre de usuario> es la cuenta de servicio no root que TSA utiliza para recopilar información de AIX. Esta especificación de usuario permite que la cuenta de servicio utilice autorización sudo en cualquier mandato de AIX.

Linux on Power

Para descubrir instancias de Linux on Power, efectúe los pasos siguientes:

Preparación del entorno:

- Deshabilite el fallo por intento de inicio de sesión no válido de la cuenta de servicio

Credenciales para la lista de acceso:

- Para conjuntos de alcances dinámicos de HMC: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de partición Linux.
- Para conjuntos de alcances de descubrimiento generales: Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de Linux.
- Para habilitar una cuenta de servicio no root con autorización sudo para Linux:
  - Cree un ID de usuario no root en la instancia de Linux de destino que TSA pueda utilizar para acceder al sistema.
  - Modifique **/etc/sudoers** en cada una de las instancias de Linux para permitir que TSA ejecute los mandatos especificados utilizando autorización sudo.

    # Especificación de Cmnd alias

    ```
    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
    ```

    # Especificación de privilegios de usuario

    ```
    <Nombre de usuario> ALL = NOPASSWD: TSA_CMDS
    ```

    - <Nombre de usuario> es la cuenta de servicio no root que TSA utiliza para recopilar información de Linux. Este <Nombre de usuario> es un usuario en cada instancia de Linux. Es necesario actualizar el archivo **/etc/sudoers** de cada instancia de Linux con la especificación anterior.

    O bien

    Una alternativa a las modificaciones mencionadas en **/etc/sudoers** es utilizar la especificación siguiente de privilegio de usuario:

    ```
    <Nombre de usuario> ALL = NOPASSWD: ALL
    ```

    - <Nombre de usuario> es la cuenta de servicio no root que TSA utiliza para recopilar información de Linux. Esta especificación de usuario

permite que la cuenta de servicio utilice autorización sudo en cualquier mandato de Linux.

- Si utiliza el portal IBM Proweb para AIX como parte de su oferta de soporte de IBM, se recomienda configurar TSA utilizando Conjuntos de alcances dinámicos de HMC. De forma alternativa, puede configurar TSA para descubrir las HMC y las particiones lógicas (incluyendo VIOS) en los Power Systems.
- Si realiza una exploración utilizando Conjuntos de alcances dinámicos de HMC, obtiene información de configuración del sistema operativo más detallada para cada LPAR que ProWeb pueda recuperar y analizar.

> Para obtener información sobre cómo añadir alcances y credenciales para entornos de HMC, consulte la sección **Alcances dinámicos de HMC** en la Guía de configuración de IBM Technical Support Appliance.

- Nivel de datos recopilados para el informe explorando varias entidades de Power Systems:
  - Si explora únicamente las HMC, obtendrá información esencial sobre la pestaña Identificado, la topología de HMC, Power Systems Firmware, recomendaciones de IBM i, recomendaciones de Linux, las pestañas HMC/VIOS/AIX y Contrato y alguna información sobre el adaptador.
  - Explorando directamente las particiones VIOS, obtendrá información adicional sobre el firmware de adaptador y el almacenamiento conectado.
  - Explorando directamente las LPAR, obtendrá más información sobre la LPAR, incluyendo información detallada sobre el sistema operativo e instancias de software específico, como por ejemplo PowerHA, GPFS y PowerSC.

IBM i

Las instancias de IBM i se descubren utilizando una conexión SSH. Si la instancia de IBM i no tiene SSH instalado y configurado, siga los pasos siguientes:

Preparación del entorno:

Asegúrese de que los siguientes productos/opciones están instalados y configurados para IBM i 7.2:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, opción 30
- Portable App Solutions Environment, 5770-SS1, opción 33

- IBM Developer Kit for Java, 5770-JV1

Asegúrese de que los siguientes productos/opciones están instalados y configurados para IBM i 7.3:

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

Asegúrese de que los siguientes productos/opciones están instalados y configurados para IBM i 7.4:

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

Para iniciar el daemon SSH, ejecute el mandato siguiente:

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

Para iniciar el servicio SSHD en IBM i, ejecute el mandato siguiente:

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

Para obtener información adicional sobre cómo configurar SSH en IBM i, consulte los capítulos 21-23 de este Redbook - http://www.redbooks.ibm.com/redpapers/pdfs/redp4163.pdf

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede tener cualquier clase de usuario, incluyendo ***USER**, aunque se necesitan requisitos de autorización sobre objetos adicionales para recopilar información de PTF (lo que se hace utilizando el mandato **DSPPTF**).
- **DSPPTF** se proporciona con las siguientes restricciones de autorización sobre objetos:
  - El mandato se proporciona con la autorización pública ***EXCLUDE**

- **Los perfiles de usuario QPGMR**, **QSYSOPR**, **QSRV** y **QSRVBAS** se proporcionan con autorizaciones privadas para utilizar este mandato
- Como siempre, el perfil de usuario **QSECOFR** o cualquier perfil de usuario que tenga la clase ***SECOFR** puede ejecutar este mandato

- En el objeto **QSYS/DSPPTF** del tipo de objeto ***CMD** se pueden editar las autorizaciones para permitir a cualquier otro usuario ejecutar este mandato.
- Si se crea una cuenta de servicio nueva para TSA, son válidas las siguientes recomendaciones:
  - Cree el perfil de usuario con la clase de usuario ***USER**
  - Utilice el mandato **GRTOBJAUT** para permitir a este perfil de usuario ejecutar el mandato **DSPPTF**; el objeto es **QSYS/DSPPTF**, del tipo de objeto ***CMD**.

UNIX Systems

Solaris

Para descubrir dispositivos Solaris, efectúe los pasos siguientes:

Preparación del entorno:

- En sistemas Solaris, asegúrese de que el paquete SUNWscpu (Source Compatibility) está instalado.
- En algunos sistemas Solaris, se debe instalar y configurar SNEEP para obtener números de serie.

Credenciales para la lista de acceso:

- Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio.
- La cuenta de servicio puede ser no root.

Solaris vía Oracle iLOM

Para descubrir dispositivos Solaris vía Oracle iLOM, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede tener privilegios de **Operador** o de **Administrador**.

Linux

Si la instancia de Linux se ejecuta en un IBM Power System, consulte la sección Linux on Power en la página 17, bajo IBM Power Systems, para obtener instrucciones.

Para descubrir dispositivos Linux on x86, efectúe los pasos siguientes:

Preparación del entorno:

- Asegúrese de que el paquete pciutils está instalado. El mandato `lspci` que contiene se utiliza para recopilar información sobre adaptadores y conexiones con dispositivos de almacenamiento externos.

Credenciales para la lista de acceso:

- Para conjuntos de alcances dinámicos de VMware: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de máquina virtual Linux.
- Para conjuntos de alcances de descubrimiento generales– Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio de Linux.
- Establezca `/bin/sh` como la shell de esta cuenta.
- Para Linux (x86), la cuenta de servicio puede ser root o bien una cuenta con autorización `sudo` .
- Para descubrir utilizando una cuenta de servicio no root, añada lo siguiente en el archivo **/etc/sudoers** en el sistema Linux.

  # Especificación de Cmnd alias

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

  # Especificación de privilegios de usuario

  ```
  <Nombre de usuario> ALL = NOPASSWD: TSA_CMDS
  ```

  > <Nombre de usuario> es la cuenta de servicio no root que TSA utiliza para recopilar información de Linux. Este <Nombre de usuario> es un usuario en cada instancia de Linux. Es necesario actualizar el archivo **/etc/sudoers** de cada instancia de Linux con la especificación anterior.

  O bien

  Una alternativa a las modificaciones mencionadas en **/etc/sudoers** es utilizar la especificación siguiente de privilegio de usuario:

  ```
  <Nombre de usuario> ALL = NOPASSWD: ALL
  ```

  > <Nombre de usuario> es la cuenta de servicio no root que TSA utiliza para recopilar información de Linux. Esta especificación de usuario permite que la cuenta de servicio utilice autorización sudo en cualquier mandato de Linux.

HP-UX

Para descubrir dispositivos HP-UX, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio.
- Para habilitar una cuenta de servicio no root con autorización sudo para HP-UX:
  - Modifique el archivo **/usr/local/etc/sudoers** en cada uno de los dispositivos HP-UX para permitir que TSA ejecute los mandatos especificados utilizando autorización sudo.

    # Especificación de Cmnd alias

    ```
    Cmnd_Alias TSA_CMDS
    =/usr/sbin/diskinfo,/opt/hpvm/bin/hpvmstatus
    ```

    # Especificación de privilegios de usuario

    ```
    <Nombre de usuario> ALL=(ALL) NOPASSWD:TSA_CMDS
    ```

    <Nombre de usuario> es la cuenta de servicio no root que TSA utiliza para recopilar información de HP-UX.

VMware vCenter Server y VMware ESXi

Para entornos VMware, utilice conjuntos de alcances dinámicos de VMware. Con los conjuntos de alcances dinámicos de VMware puede crear una definición de alcance para VMware vCenter Server / ESXi y proporcionar las credenciales asociadas de VMware y máquina virtual, pero no es necesario crear alcances para cada máquina virtual gestionada. Cuando se descubre el VMware vCenter Server / ESXi, TSA determina las máquinas virtuales que existan en ese momento y automáticamente explora cada una de ellas.

Para entornos VMware donde la configuración de las máquinas virtuales es generalmente estática, hay un método alternativo a los conjuntos de alcances dinámicos de VMware que consiste en iterar añadiendo alcances y credenciales para las entidades en el orden siguiente:

1. **Las instancias de vCenter Server**: Esto devuelve información general sobre los hosts ESXi que gestionan y los invitados de máquina virtual que contienen.
2. **Hosts ESXi**: Añada los hosts ESXi que no estén gestionados por un vCenter Server.
3. **Invitados de máquina virtual individuales**: Esto permite recopilar información más detallada sobre el sistema operativo.

Al configurar TSA para entornos VMware, se recomiendan las siguientes acciones:

1. Configure TSA para descubrir VMware vCenter Servers cuando los haya disponibles. Descubrir un VMware vCenter Server automáticamente, hace que TSA recopile

información sobre todos los hosts VMware ESXi que gestiona el vCenter Server. No se requiere ninguna información de configuración sobre los hosts ESXi.

2. Configure TSA para descubrir hosts VMware ESXi solo cuando el host ESXi no esté gestionado por un VMware vCenter Server.
3. Instale VMware Tools en cada una de las máquinas virtuales alojadas en los hosts ESXi. Si VMware Tools no está instalado, algunos datos de inventario, como por ejemplo la dirección IP o el sistema operativo instalado, no serán accesibles.
4. Configure cada uno de los hosts VMware ESXi de forma que tenga la interfaz CIM activa. La interfaz CIM permite a TSA recopilar información detallada sobre los adaptadores dentro del host ESXi. Para obtener más información sobre el proveedor CIM, consulte el "Apéndice C" en la página 44.

Para descubrir instancias de servidor de vCenter así como información sobre los servidores ESXi que gestionan, efectúe los pasos siguientes:

Preparación del entorno

- Instale VMware Tools en cada una de las máquinas virtuales alojada en los hosts ESXi.
- Configure cada uno de los hosts VMware ESXi de forma que tenga la interfaz CIM activa.
- El puerto CIM (5989) debe ser accesible desde el TSA (no bloqueado por cortafuegos o similares) para un descubrimiento completo.

Credenciales para la lista de acceso

- Para conjuntos de alcances dinámicos de VMware: Nombre de usuario / contraseña de la cuenta de servicio de VMware vCenter Server.
- Para conjuntos de alcances de descubrimiento generales: Sistema: Nombre de usuario / contraseña de la cuenta de servicio de VMware vCenter Server.
- La cuenta de servicio debe tener permisos de rol de **Administrador** o, por los menos, permisos para un rol de sólo lectura personalizado con los siguientes privilegios adicionales:
  - Global → Licencias
  - Global → Configuración
  - Host → CIM
  - Host → Configuración → Cambiar configuración
  - Host → CIM→ Interacción CIM

Para descubrir dispositivos ESXi directamente, efectúe los pasos siguientes:

Preparación del entorno

- Instale VMware Tools en cada una de las máquinas virtuales alojadas en los hosts ESXi.
- Configure cada uno de los hosts VMware ESXi de forma que tenga la interfaz CIM activa.

Credenciales para la lista de acceso

- Para conjuntos de alcances dinámicos de VMware: Nombre de usuario / contraseña de la cuenta de servicio de VMware ESXi.
- Para conjuntos de alcances de descubrimiento generales: Sistema: Nombre de usuario / contraseña de la cuenta de servicio de VMware ESXi.
- La cuenta de servicio debe tener permisos de rol de **Administrador**.

Windows

TSA admite el descubrimiento en instancias de Windows con los siguientes métodos:

- WINRM
- SMB1

> Se prefiere Windows vía WINRM ya que la interfaz es más segura.

Windows vía WINRM

Para descubrir dispositivos Windows vía WINRM, efectúe los pasos siguientes:

Preparación del entorno:

La forma más común de preparar el entorno es utilizar un certificado de servidor, generado por una entidad emisora de certificados, que se instala en el servidor Windows de destino. El certificado debe cumplir las siguientes condiciones:

- Los certificados raíz e intermedio de la entidad emisora de certificados se encuentran en Certificados de entidades de certificación raíz de confianza.
- El certificado de servidor está instalado en Certificados personales.
- El certificado de servidor debe mostrar que se ha emitido para el nombre de host completo del servidor.
- El certificado de servidor debe incluir la clave privada de este servidor.

El siguiente mandato configura WINRM para conexiones HTTPS remotas:

winrm quickconfig -transport:https

Este mandato hace lo siguiente:

- Habilita WINRM si no está activo
- Modifica el servicio WINRM de forma que WINRM se inicie automáticamente al reiniciar
- Configura el escucha HTTPS de WINRM
- Modifica las reglas del cortafuegos de Windows para permitir conexiones HTTPS remotas

Este mandato genera la salida siguiente. Introduzca **y** para confirmar los cambios.

```
El servicio WinRM ya se está ejecutando en esta máquina.
WinRM no está configurado para permitir el acceso remoto a esta
máquina para su gestión.
Se deben hacer los siguientes cambios:

Crear un escucha de WinRM en HTTPS://* para aceptar solicitudes
WS-Man a cualquier IP de esta máquina.
Configurar el valor CertificateThumbprint del servicio, para
utilizar en la autenticación CredSSP.
Configurar LocalAccountTokenFilterPolicy para otorgar derechos de
administración remota a los usuarios locales.

¿Realizar estos cambios [s/n]? s

Se ha actualizado WinRM para la gestión remota.

Se ha creado un escucha de WinRM en HTTPS://* para aceptar
solicitudes WS-Man a cualquier IP de esta máquina.
Se han configurado los valores necesarios para el servicio.
Se ha configurado LocalAccountTokenFilterPolicy para otorgar
derechos de administración remota a los usuarios locales.
```

Finalmente, para permitir la autenticación con ID de usuario / contraseña sobre HTTPS, ejecute el mandato siguiente:

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

Una alternativa es utilizar un certificado autofirmado. Las instrucciones para esta configuración se encuentran en Apéndice D: Windows con WINRM en la página 53.

Credenciales para la lista de acceso:

- Para conjuntos de alcances dinámicos de VMware: Nombre de usuario / contraseña de la cuenta de servicio.
- Para conjuntos de alcances de descubrimiento generales: Sistema (Windows): Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe ser miembro de uno de los siguientes grupos:
  - Administradores

- WinRMRemoteWMIUsers__

Para añadir un usuario al grupo WinRMRemoteWMIUsers__, utilice el mandato siguiente:

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

Windows vía SMB1

Para descubrir dispositivos Windows, efectúe los pasos siguientes:

Preparación del entorno:

- Asegúrese de que Windows Scripting Host (WSH) o el servicio Windows Management Instrumentation (WMI) y VBScript estén habilitados en el dispositivo de destino.
- Asegúrese de que el puerto 445 no está bloqueado por políticas de cortafuegos o de seguridad de IP ya que TSA requiere el protocolo Server Message Block (SMBv1) sobre TCP/IP.
- Para aplicar políticas de seguridad, vaya a **Inicio → Panel de control → Herramientas administrativas**, y elija la siguiente navegación según si sus políticas están almacenadas localmente o en un Active Directory:
  - Política almacenada localmente : **Herramientas administrativas → Política de seguridad local → Políticas de seguridad de IP** en el sistema local
  - Políticas almacenadas en Active Directory : **Herramientas administrativas → Configuración de seguridad de dominio predeterminada → Políticas de seguridad de IP** en Active Directory o **Herramientas administrativas → Configuración de seguridad de controlador de dominio predeterminada → Políticas de seguridad de IP** en Active Directory
- TSA requiere acceso al recurso compartido de disco de administración remota oculta para poder acceder al directorio de sistema %TEMP% y a otros directorios. También necesita acceso al recurso compartido IPC$ (Interprocess Communications) para poder acceder a los registros remotos. Asegúrese de que el servicio de servidor del recurso compartido Interprocess Communication esté iniciado. Para iniciar el servicio de servidor, vaya a → **Panel de control → Herramientas administrativas → Servicios → Servidor**.
- Asegúrese de que el servicio de registro remoto está activo. TSA lo necesita para establecer una sesión con el dispositivo Windows.

Credenciales para la lista de acceso:

Windows release 2012 R2 y posteriores:

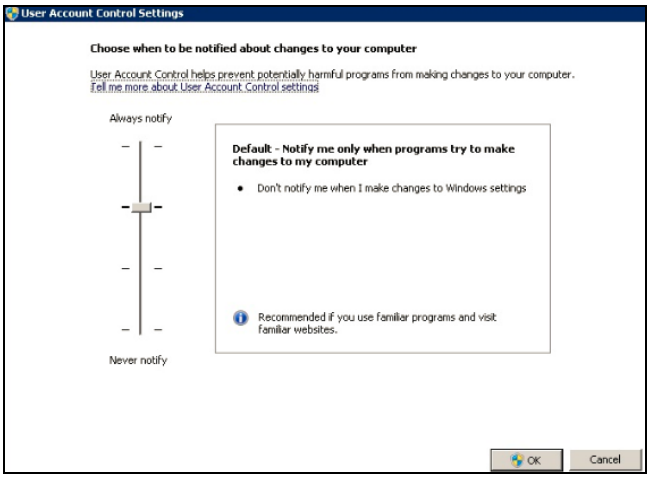
- Para conjuntos de alcances dinámicos de VMware: Cuenta de administrador base / contraseña. Esta cuenta funcionará independientemente de la configuración del control de cuentas de usuario (UAC User Account Control).
- Para conjuntos de alcances de descubrimiento generales: Sistema (Windows): Cuenta de administrador base / contraseña. Esta cuenta funcionará independientemente de la configuración del control de cuentas de usuario (UAC User Account Control).

Se puede utilizar una cuenta distinta de la cuenta de administrador base si se cumplen ciertas condiciones. La cuenta debe ser una cuenta de administrador local o del dominio y la configuración del control de cuentas de usuario (UAC) debe cumplir ciertos requisitos. Consulte la tabla siguiente para conocer las combinaciones de tipo de cuenta y parámetro de UAC soportadas. Consulte la documentación de Microsoft Windows para obtener detalles adicionales sobre UAC.

	Configuración del Control de cuentas de usuario (UAC)			
	Notificar siempre	**Notificarme solo cuando los programas intenten hacer cambios en mi sistema (valor predeterminado)**	**Notificarme solo cuando los programas intenten hacer cambios en mi sistema (no atenuar mi escritorio)**	**No notificar nunca**
Administrador base	**Sí**	**Sí**	**Sí**	**Sí**
Usuario en el grupo de Administradores del dominio	**No**	**Sí**	**Sí**	**Sí**
Usuario en el grupo de Administradores locales	**No**	**Sí**	**Sí**	**Sí**
Cuenta que no es de administrador (de dominio o local)	**No**	**No**	**No**	**No**

> Para acceder a la configuración de UAC, pulse **Inicio** y después pulse **Panel de Control**. Escriba **uac** en el recuadro de búsqueda y pulse **Cambiar configuración del Control de cuentas de usuario**.

El valor predeterminado es el siguiente:



Dispositivos de cajero automático

Ciertos modelos de dispositivos de cajero automático se pueden descubrir. Para descubrir dispositivos de cajero automático, incluyendo información básica sobre sus componentes, efectúe los pasos siguientes:

Preparación del entorno:

- Modelos Wincor Nixdorf - Siga las instrucciones para Windows vía SMB.

Módulo de gestión

Para IBM Flex Systems es mejor iterar añadiendo alcances y credenciales para las entidades en el siguiente orden:

1. **El Flex System Manager (FSM):** Esto devuelve información general sobre los gestores de sistemas Flex y los chasis que gestionan junto con sus nodos de cálculo asociados.

   > Si no hay FSM, se recomienda explorar los CMM y las HMC que gestionen nodos de cálculo POWER en sistemas Flex.

2. **El módulo de gestión de chasis (CMM - Chassis Management Module):** Para los chasis que no están gestionados por un FSM, apunte a cada CMM para recuperar información general sobre cada chasis y sus nodos asociados.
3. **Los nodos de cálculo:** Esto devuelve información detallada sobre el sistema operativo.

Dispositivos Flex System Manager (FSM)

Para descubrir dispositivos FSM, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como **SMAdmin**.

Dispositivos Chassis Management Module (CMM)

Para descubrir dispositivos CMM, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener por lo menos autorización como **operador**.

Dispositivos Advanced Management Module (AMM)

Para descubrir dispositivos AMM, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener por lo menos autorización como **operador**.

Servidor Blade HP Proliant vía HP OnBoard Administrator

Para Hewlett Packard (HP) ProLiant Servers es mejor añadir alcances y credenciales para las entidades de HP OnBoard Administrator (HP OBA). El HP OBA devolverá información general sobre el HP OnBoard Administrator, el alojamiento que gestiona y los nodos de cálculo que contiene el alojamiento.

Para descubrir un servidor Blade HP Proliant vía HP OnBoard Administrator (OBA), efectúe los pasos siguientes:

Preparación del entorno:

- HP OBA debe estar en modo activo.

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como **Administrador de OA**, **Operador de OA** o **Usuario de OA** en HP Onboard Administrator. Se recomienda el rol de **autorización de Usuario de OA**.

> TSA recopila información solo de los HP OnBoard Administrator que están en estado activo. No se recopila ninguna información de los HP OnBoard Administrator que están en estado en espera.

Dispositivos Módulo de gestión integrado (IMM) y Módulo de gestión integrado II (IMM2)

Para descubrir dispositivos IMM e IMM2, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede tener cualquier autorización válida.

Servidores HP Integrity y HP9000 vía iLO

El iLO es una tarjeta de procesador separada dentro de un servidor HP Integrity y HP9000 que proporciona información básica de hardware sobre el servidor. El iLO está activo tan pronto como se conecta el servidor, aunque el servidor en sí no se haya encendido todavía.

Para descubrir la información de inventario a nivel de resumen vía iLO para servidores HP Integrity y HP9000, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede utilizar cualquier nivel de autorización válido. Se recomienda la autorización de **Usuario**.

Dispositivos de red

En esta sección se proporciona información detallada sobre los siguientes tipos de dispositivos de red:

Plataforma
Conmutadores BNT
Conmutadores Brocade
Check Point
Conmutadores Cisco
F5 Big-IP (TMOS)
Fortinet (FortiOS)
Conmutadores IBM SAN (Storage Area Network) de tipo b
Conmutadores Juniper
Palo Alto Networks (PAN-OS)
Conmutadores QLogic

> Pulse en cualquiera de los enlaces anteriores para obtener información detallada.

Conmutadores BNT

Para descubrir conmutadores BNT, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como **admin**.

Brocade

Para descubrir dispositivos Brocade, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- Modo Virtual Fabric deshabilitado: La cuenta de servicio puede utilizar cualquier autorización válida. Se recomienda la autorización de **Usuario**.
- Modo Virtual Fabric habilitado: La cuenta de servicio requiere autorización de **Administrador** en Fabric OS.

Check Point

Para descubrir sistemas Check Point, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como administrador (**adminRole**).
- La cuenta de servicio debe tener acceso SSH para ejecutar mandatos de CLI.

Cisco

Para descubrir dispositivos Cisco, puede utilizar las siguientes credenciales de sistema o las credenciales SNMP:

Credenciales para la lista de acceso:

- Sistema informático, Otra (dispositivo Cisco) u Otra (CiscoWorks): Nombre de usuario / contraseña o Nombre de usuario / clave SSH de la cuenta de servicio.
- La cuenta de servicio requiere privilegios de rol de **administrador de red**.
- SNMP: Introduzca una cadena de comunidad (para SNMPv1 y SNMPv2).
- SNMP (SNMPv3):
  - Especifique:

- nombre de usuario
- contraseña
- contraseña privada (opcional)

- Seleccione el protocolo de autenticación: ninguno, MD5, SHA

> Es importante que se ponga a disponibilidad de TSA una cadena de comunidad que tenga acceso de sólo lectura a TODO en los dispositivos de red de alcance.

F5 Big-IP (TMOS)

Para descubrir sistemas F5 Big-IP que ejecutan TMOS, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como administrador de F5.
- La cuenta de servicio debe tener acceso SSH para ejecutar mandatos de CLI de TMSH.

Fortinet (FortiOS)

Para descubrir dispositivos Fortinet que ejecutan FortiOS, efectúe los pasos siguientes:

Preparación del entorno

- Asegúrese de que la consola del sistema está configurada para mostrar la salida de mandato completa:

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

Credenciales para la lista de acceso:

- Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio.
- La cuenta de servicio debe tener por lo menos permisos de sólo lectura.

Conmutadores IBM SAN (Storage Area Network) de tipo b

Para descubrir dispositivos IBM SAN de tipo b, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- Modo Virtual Fabric deshabilitado: La cuenta de servicio puede utilizar cualquier autorización válida. Se recomienda la autorización de **Usuario**.

- Modo Virtual Fabric habilitado: La cuenta de servicio requiere autorización de **Administrador** en Fabric OS.

Juniper

Para descubrir dispositivos Juniper, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio
- La cuenta de servicio debe tener autorización como administrador.

> **Nota**: El descubrimiento de información de tamaño de memoria requiere que en el dispositivo esté instalado Junos® versión 12.1 o posterior.

Palo Alto Networks (PAN-OS)

Para descubrir sistemas Palo Alto Network que ejecutan PAN-OS, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener Superusuario o Superusuario (sólo lectura)
- La cuenta de servicio debe tener acceso a la API REST (puerto 443).

Conmutadores QLogic

Para descubrir conmutadores QLogic, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como administrador.

Dispositivos de almacenamiento

En esta sección se proporciona información detallada sobre los siguientes tipos de dispositivos de almacenamiento y de cinta:

Plataforma
Almacenamiento EMC Corporation
HP StorageWorks P2000 Modular Smart Array
IBM DS3xxx, DS4xxx o DS5xxx
IBM DS6xxx o DS8xxx
IBM FlashSystem, v9000

Plataforma
IBM ProtecTier
IBM SVC o V7000/V3700
Biblioteca de cintas IBM TS3100
Biblioteca de cintas IBM TS3200
Biblioteca de cintas IBM TS3310
Bibliotecas de cintas IBM TS3494, TS3953
Bibliotecas de cintas IBM TS3500, TS3584
Biblioteca de cintas IBM TS4500
Biblioteca de cintas IBM TS7700
IBM V7000 Unified
IBM XIV
nSeries o NetApp
Pulse en cualquiera de los enlaces anteriores para obtener información detallada.

Almacenamiento EMC Corporation

EMC CLARiiON / VNX / VMAX

Para descubrir dispositivos EMC CLARiiON / VNX / VMAX, efectúe los pasos siguientes:

Preparación del entorno:

- Asegúrese de que hay una instancia del producto Proveedor SMI-S de EMC instalada en un sistema Windows o Linux. De forma predeterminada, TSA sigue la recomendación de SMI-S de EMC de descubrir la ubicación del proveedor utilizando SLP. Si su política de seguridad de red bloquea el tráfico de red de SLP, se puede configurar TSA para que acceda directamente al Proveedor SMI-S de EMC sin utilizar SLP.
- Si la seguridad de su red no admite el tráfico de red SLP, utilice la página **Configuración de descubrimiento→ Configuración de conexión** para

proporcionar información sobre los puertos en los que los Proveedores SMI-S de EMC están a la escucha de solicitudes de consulta.

- Asegúrese de que al menos una de las direcciones IP que utiliza el Proveedor SMI-S está definida en un conjunto de alcances. TSA se conectará al Proveedor SMI-S para recuperar información sobre los dispositivos EMC que gestiona. Las direcciones IP de los dispositivos EMC individuales no necesitan estar en un conjunto de alcances. TSA intenta conectarse al Proveedor SMI-S utilizando HTTPS si está disponible, si no, se utiliza HTTP.

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede utilizar cualquier rol válido. Se recomienda el rol de **supervisor**.

Solo es necesario introducir las credenciales del proveedor SMI-S en TSA. No es necesario introducir credenciales para los dispositivos EMC.

EMC Data Domain

Para descubrir dispositivos EMC Data Domain, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede tener la autorización mínima necesaria.

HP StorageWorks P2000 Modular Smart Array

Para descubrir sistemas de almacenamiento de HP, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede tener la autorización mínima necesaria.

Almacenamiento IBM DS3xxx, DS4xxx o DS5xxx

Para descubrir dispositivos IBM DS3xxx, DS4xxx o DS5xxx, efectúe los pasos siguientes:

Preparación del entorno:

- Asegúrese de que el gestor de almacenamiento permite el uso de mandatos **smcli** remotos.

Credenciales para la lista de acceso:

- Para dispositivos de almacenamiento no protegidos, no se requieren credenciales.
- Para dispositivos de almacenamiento protegidos, efectúe los pasos siguientes:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede tener rol de **administrador** o el rol de **supervisor**. Se recomienda el rol de **supervisor**.

Almacenamiento IBM DS6xxx / DS8xxx

Para descubrir dispositivos IBM DS6xxx / DS8xxx, efectúe los pasos siguientes:

Preparación del entorno:

- Asegúrese de que el gestor de almacenamiento permite el uso de mandatos **dscli** remotos.

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener el rol de **supervisor**.

IBM FlashSystem, v9000

Para descubrir sistemas IBM FlashSystem, efectúe los pasos siguientes:

Preparación del entorno:

- En los modelos antiguos, el MCP (Management Control Port, puerto de control de gestión) debe estar en estado activo para poder descubrir satisfactoriamente el sistema.
  - Para comprobar si un sistema está en estado activo, ejecute el mandato - `system status`.
  - De las dos direcciones IP, si cae una de las IP, el sistema pasa a estado pasivo. Para activar el otro puerto Ethernet, ejecute el mandato: `sync activate`.
  - El sistema descubierto debe ser la dirección IP de gestión y/o el nodo de configuración.

Credenciales para la lista de acceso:

- Sistema: Autenticación con Nombre de usuario / contraseña o con Nombre de usuario / clave SSH de la cuenta de servicio.
- La cuenta de servicio puede utilizar cualquier rol válido. Se recomienda el rol de **supervisor**.

IBM ProtecTIER

Para descubrir dispositivos ProtecTIER, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.

- La cuenta de servicio debe tener privilegios de administrador.

Almacenamiento IBM SVC, V7000/V3700

Para descubrir dispositivos SVC y V7000/V3700, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña o Nombre de usuario / clave SSH para la autenticación.
- La cuenta de servicio puede utilizar cualquier rol válido. Se recomienda el rol de **supervisor**.

Biblioteca de cintas IBM TS3100

Para descubrir dispositivos de Biblioteca de cintas TS3100, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como administrador.

Biblioteca de cintas IBM TS3200

Para descubrir dispositivos de Biblioteca de cintas TS3200, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como administrador.

Biblioteca de cintas IBM TS3310

Para descubrir dispositivos de Biblioteca de cintas TS3310, efectúe los pasos siguientes:

Preparación del entorno:

- El servicio web se configura siempre en modalidad segura.

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como administrador.

Bibliotecas de cintas IBM TS3494, TS3953

Para descubrir dispositivos de Biblioteca de cintas TS3494, TS3953, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede tener la autorización mínima necesaria.

Bibliotecas de cintas IBM TS3500, TS3584

Son necesarios los siguientes requisitos previos:

- La biblioteca de cintas TS3500 debe tener el nivel de firmware 8xxx (o superior).
- ALMS (Advanced Library Management System) debe estar instalado y habilitado.

> Se admiten conexiones tanto SSL como no SSL.

Para descubrir dispositivos de Biblioteca de cintas TS35xx, efectúe los pasos siguientes:

Preparación del entorno:

- La interfaz web de TS3500 se puede configurar como **Sin protección por contraseña** o con **Protección por contraseña**
  - Si **Protección por contraseña** está activado, cree una credencial tal como se describe en **Credenciales para la lista de acceso** a continuación.
  - Si **Protección por contraseña** está deshabilitado, no se requieren credenciales.

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener autorización como administrador.

Biblioteca de cintas IBM TS4500

Son necesarios los siguientes requisitos previos:

- La biblioteca de cintas TS4500 debe tener el nivel de firmware 1.4.1.2 o superior (hasta el 1.7.0.0).
- ALMS (Advanced Library Management System) debe estar instalado y habilitado.

> Se admiten conexiones tanto SSL como no SSL.

Para descubrir dispositivos de Biblioteca de cintas TS4500, efectúe los pasos siguientes:

Preparación del entorno:

- La interfaz web de TS4500 solo se puede configurar con **Protección por contraseña**.

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe estar correlacionada al rol **Servicio**.

Biblioteca de cintas IBM TS7700

Para descubrir dispositivos de Biblioteca de cintas TS7700, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio solo necesita autorización de **Sólo lectura**.

Almacenamiento IBM V7000 Unified

Para descubrir dispositivos V7000 Unified, efectúe los pasos siguientes:

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede utilizar cualquier rol válido. Se recomienda el rol de **supervisor**.

Almacenamiento IBM XIV

Para descubrir dispositivos XIV, efectúe los pasos siguientes:

Preparación del entorno:

- Asegúrese de que el gestor de almacenamiento permite el uso de mandatos **xcli** remotos.

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio debe tener el rol de usuario de **Sólo lectura**.
- Tenga en cuenta que los sistemas XIV pueden tener un umbral bajo para intentos de inicio de sesión no válidos hasta generar alertas. Si utiliza un conjunto de credenciales grande, puede que supere este límite y provoque que se informe de problemas innecesariamente. Intente agrupar los dispositivos XIV en un solo conjunto de alcances y restrinja sus credenciales de cuenta de servicio a ese conjunto de alcances.

Almacenamiento nSeries o NetApp

Para descubrir dispositivos nSeries o NetApp, efectúe los pasos siguientes:

Preparación del entorno:

- Solo se admite recopilación de datos para sistemas configurados con la CLI de Data ONTAP, la CLI de RLM y la CLI de SP. En cambio, la CLI de BMC no está soportada.
- La opción **telnet.distinct.enable** debe estar activada.

Credenciales para la lista de acceso:

- Sistema: Nombre de usuario / contraseña de la cuenta de servicio.
- La cuenta de servicio puede tener la autorización mínima necesaria.

Consideraciones sobre cortafuegos

El/los cortafuegos entre TSA y los dispositivos de descubrimiento pueden impedir que se realice un descubrimiento completo y satisfactorio.

En los casos en que sea necesario atravesar un cortafuegos, puede que se tengan que abrir puertos en el cortafuegos, según el tipo de dispositivo que el usuario desee descubrir. Normalmente se deben abrir los puertos 22 (SSH) y 161 (SNMP), y también los puertos adecuados de la tabla siguiente según los dispositivos soportados.

Punto final de descubrimiento	**Puertos**	**Interfaz / Protocolo**
Diversos	161	SNMP
Dispositivos de almacenamiento		
DS6000 / DS8000	1750 (HTTP) o 1751 (HTTPS)	DSCLI
DS3000 / DS4000 / DS5000	2463	SMCLI
XIV	7778	XCLI
nSeries o NetApp	22 / 23	SSH o Telnet
SVC o V7000/V3700	22	SSH
V7000 Unified	22	SSH
IBM TS3500	443 / 80	HTTPS o HTTP
IBM TS4500	443 / 80	HTTPS o HTTP
IBM TS7700	443 / 80	HTTPS o HTTP
IBM TS3100 / TS3200 / TS3310	80	HTTP
IBM TS3494, TS3953	23	Telnet
IBM ProtecTier	22	SSH
Almacenamiento HP	22 / 23	SSH o Telnet
IBM Flash System, v9000	22	SSH

Punto final de descubrimiento	Puertos	Interfaz / Protocolo
EMC Corporation Storage - CLARiion/VNX/VMAX	427 - (predeterminado) cuando se permite descubrimiento SLP, si no, si el descubrimiento SLP está inhabilitado, este puerto no se utiliza. Puertos HTTPS / HTTP configurados por el proveedor SMI-S de EMC; los valores predeterminados son 5989 / 5988	SLP, HTTPS / HTTP
	Puede habilitar o deshabilitar la opción de descubrimiento SLP para descubrir dispositivos de almacenamiento EMC mediante proveedores SMI-S de EMC.	
EMC Corporation Storage – EMC Data Domain	22	SSH*
Sistemas operativos y hosts		
FSM	22 / 23	SSH o Telnet
CMM	22 / 23	SSH o Telnet
AMM	22 / 23	SSH o Telnet
Servidor Blade HP Proliant vía HP OnBoard Administrator	22 / 23	SSH o Telnet
IMM e IMM2	22 / 23	SSH o Telnet
HP iLO para servidores HP Integrity / HP 9000	22 / 23	SSH* o Telnet
Dispositivos de red		
Brocade	161 / 22 /23	SNMP, SSH, Telnet
Conmutadores IBM SAN (Storage Area Network) de tipo b	22 /23	SSH, Telnet
Cisco	161 / 22 / 23	SNMP, SSH, Telnet
BNT	22 / 23	SSH o Telnet

Punto final de descubrimiento	Puertos	Interfaz / Protocolo
Juniper	22 / 23	SSH o Telnet
QLogic	22 / 23	SSH* o Telnet
Fortinet (FortiOS)	22 / 23	SSH o Telnet
Palo Alto Networks (PAN-OS)	443	HTTPS
F5 Big-IP (TMOS)	22 / 23	SSH o Telnet
Check Point	22 / 23	SSH o Telnet
Sistemas operativos / Plataformas de servidor		
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 o Telnet
IBM i	22	SSH
SUN	22	SSH

- TSA solo admite SSH v1 para los dispositivos marcados como SSH*.

Problemas en el descubrimiento

La mayoría de los problemas relacionados con el descubrimiento se deben a problemas de acceso o de autorización.

Los problemas de acceso más comunes se deben a cortafuegos que bloquean el acceso a los puertos necesarios en el dispositivo. Los puertos que tienen que estar abiertos y accesibles varían según el tipo de dispositivo. Consulte la sección "Consideraciones sobre cortafuegos" en la página 41 para determinar los puertos aplicables.

Los problemas de autorización más comunes incluyen los siguientes:

- **No se han definido credenciales**. Asegúrese de que se han definido credenciales para los dispositivos en TSA y que se han creado las cuentas de servicio adecuadas en los dispositivos.
- **Nombre de usuario o contraseña de la credencial incorrectos**. Utilice la función **Prueba** al crear o editar una credencial para verificar que la credencial es válida.
- **Contraseña de credencial caducada**.
- **La credencial no tiene las autorizaciones necesarias en el dispositivo**. Para determinar los requisitos de credenciales de un dispositivo de destino, consulte la sección Configuración del descubrimiento de dispositivos en la página 12.
- **Utilizar el tipo de credencial válido**. Para dispositivos Windows, cree una credencial 'Sistema (Windows)' en lugar de una credencial 'Sistema'.

Consulte la página **Estado de autenticación (Herramientas→ Estado de autenticación)** para ver si ha caducado o ha dejado de funcionar la contraseña de alguna credencial de cuenta de servicio.

Consideraciones regulares

Una vez que se han definido las partes deseadas de la red en TSA y se han explorado satisfactoriamente, se puede dejar que TSA ejecute descubrimientos y transmisiones periódicos según las planificaciones deseadas.

A continuación, se indican algunas actividades regulares necesarias:

- Revise de forma regular los informes que genera TSA con su representante de IBM.
- Periódicamente, haga una copia de seguridad mediante la interfaz de usuario de TSA para guardar una copia de la configuración de TSA.

> Esta operación no guarda los datos recopilados por TSA. Solo guarda información de configuración.

- Compruebe periódicamente la página **Estado de autenticación (Herramientas → Estado de autenticación)** para ver si ha caducado o ha dejado de funcionar la contraseña de alguna credencial de cuenta de servicio.
- Al actualizar las contraseñas de las cuentas de servicio en los dispositivos, asegúrese de actualizar también las contraseñas en TSA para mantener la definición de credenciales en TSA sincronizadas con las credenciales en el dispositivo de destino.
- Si su política de seguridad lo permite, considere la posibilidad de configurar cuentas de servicio con contraseñas que no caduquen o de utilizar claves SSH. Esto elimina la necesidad de actualizar periódicamente las contraseñas en la interfaz de usuario de TSA y en los dispositivos.

Resolución de problemas

Sesiones activas para descubrimiento de AMM

Los dispositivos AMM tienen un parámetro que limita el número de sesiones activas simultáneas (20 como máximo). Si este valor no es lo suficientemente alto como para permitir a TSA crear una sesión, no se puede descubrir el dispositivo AMM.

Para cambiar el límite de sesiones activas de un dispositivo AMM, siga estos pasos:

1. Inicie sesión en la interfaz web de AMM escribiendo la dirección IP del dispositivo AMM en un navegador web.
2. Vaya a **Control de MM → Perfiles de inicio de sesión**.
3. Pulse en el ID de inicio de sesión que TSA utiliza para descubrir el dispositivo.
4. Aumente el valor del parámetro **Número máximo de sesiones activas simultáneas**.
5. Pulse **Guardar** en la parte inferior derecha de la página.

Apéndice A: Términos y definiciones

Se supone que el lector conoce a fondo las redes y protocolos de IP (Internet Protocol).

Término	**Definición**
Dispositivo de descubrimiento	Se refiere a los componentes de infraestructura de TI que TSA puede descubrir. Los dispositivos más frecuentes son: servidores, sistemas informáticos (p. ej. IBM, Dell y HP), elementos de almacenamiento y elementos de red (p. ej. conmutadores, puentes, direccionadores).

Apéndice B: Otros

Funciones de descarga de la interfaz de usuario

En algunos casos, al utilizar un navegador web, la función Descargar todos los registros (en la página **Registro de actividad** page), las descargas de archivos (en la página **Historial de descubrimiento**) o las descargas de documentación (en la página **Documentación**) no se completan correctamente. Para resolver este problema, pruebe a cambiar a otro navegador web soportado, como se documenta en la Guía de configuración de IBM Technical Support Appliance. Si no tiene esta opción, pruebe a restablecer las propiedades del navegador a los valores predeterminados.

Apéndice C: Proveedor CIM para VMware ESXi

Un proveedor CIM es un conjunto de plugins de VMware ESXi que pueden recopilar información adicional de hardware y firmware sobre el servidor en el se ejecuta VMware ESXi.Tanto TSA como el VMware vCenter pueden beneficiarse de esta información adicional.

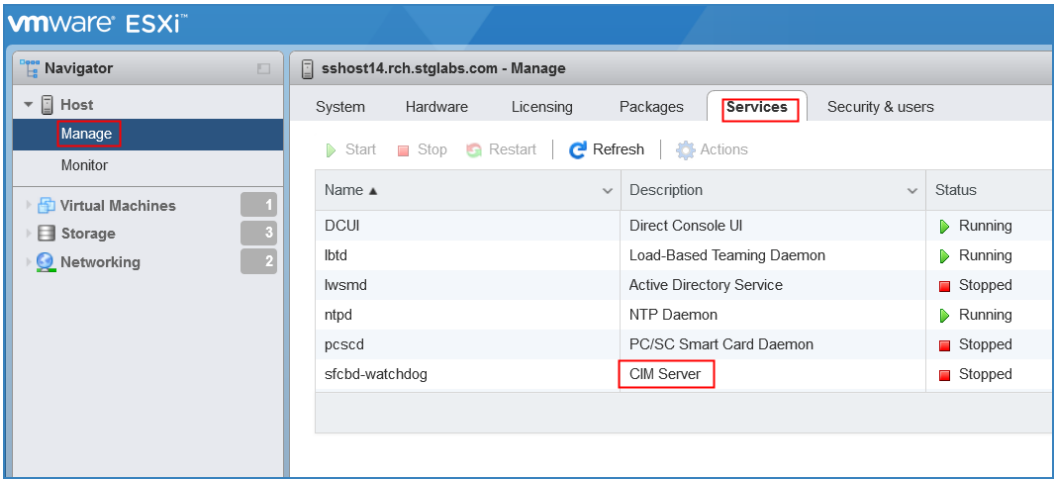
Los plugins de proveedor CIM los desarrollan los fabricantes de servidores y componentes. Para asegurarse de que se incluyen plugins de proveedor CIM en ESXi, utilice una imagen de instalación personalizada que incluya los plugins de proveedor CIM. Para las instancias existentes de VMware ESXi que no tienen el proveedor CIM instalado, puede obtener los plugins que necesite de los fabricantes de servidores y componentes e instalarlos en ESXi. VMware proporciona una lista de los plugins que ofrecen los fabricantes.

Para obtener más información, consulte https://www.vmware.com/resources/compatibility/pdf/vi_cim_guide.pdf.

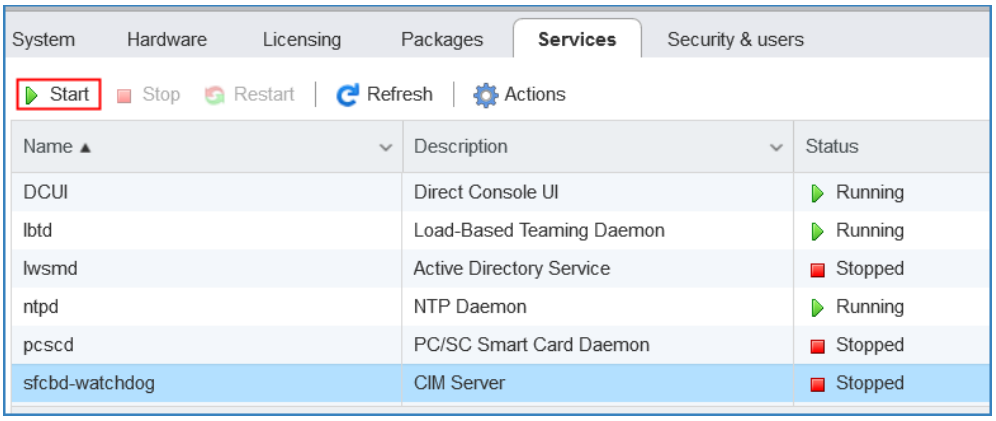
Para determinar si el proveedor CIM está activo, y para activarlo si no lo está, siga los pasos siguientes.

En el cliente web de VMware vSphere

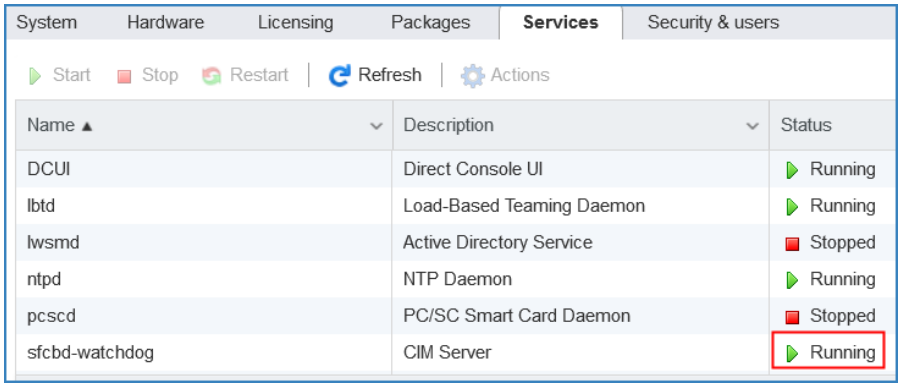
- Inicie sesión en el cliente web de VMware vSphere.
- Haga clic en **Host → Gestionar** en la ventana de navegación de la izquierda y seleccione la pestaña **Servicios** en el panel derecho.
- Se muestra un conjunto de servicios, incluyendo el **servidor CIM** .



- Si el **Servidor CIM** está en estado **Detenido**, selecciónelo y pulse **Iniciar**.

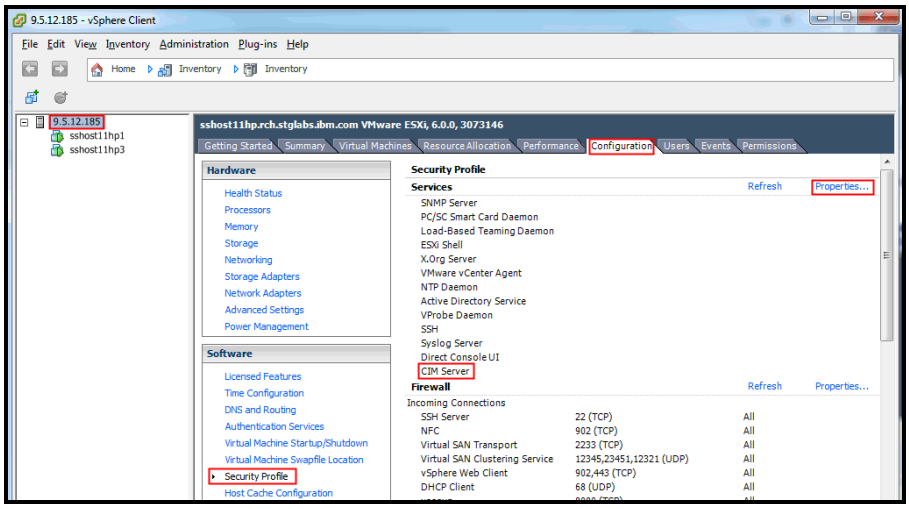


- El servicio de servidor CIM se inicia y el estado pasa a ser **En ejecución**.

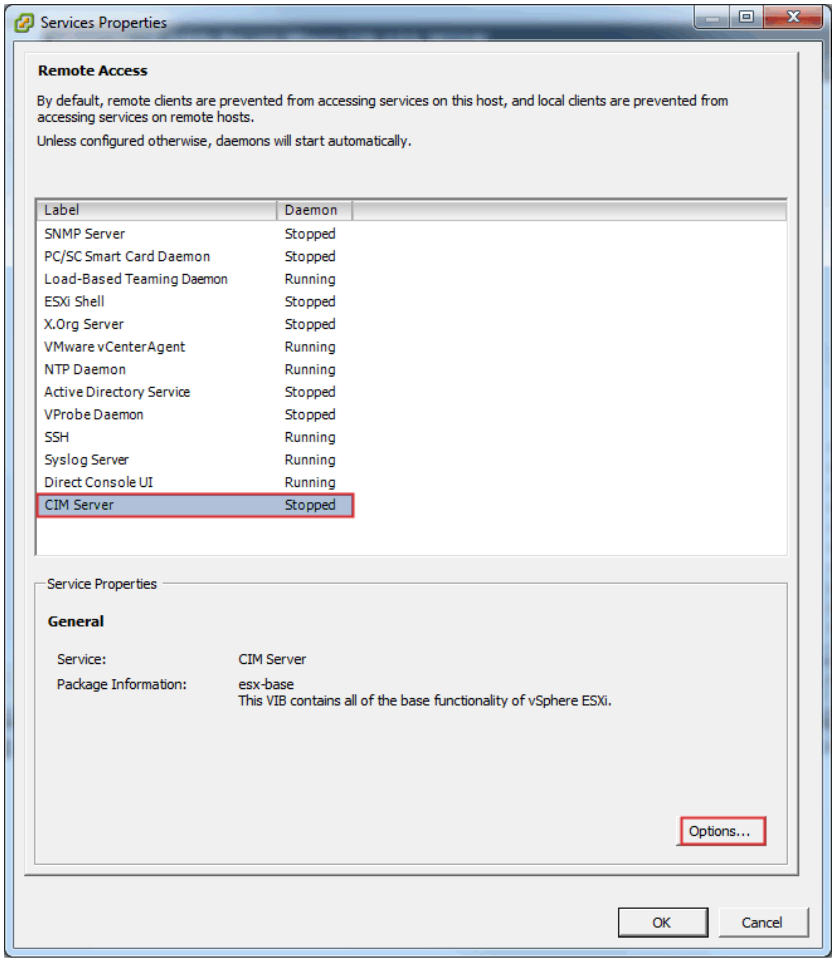


En el Cliente de VMware vSphere

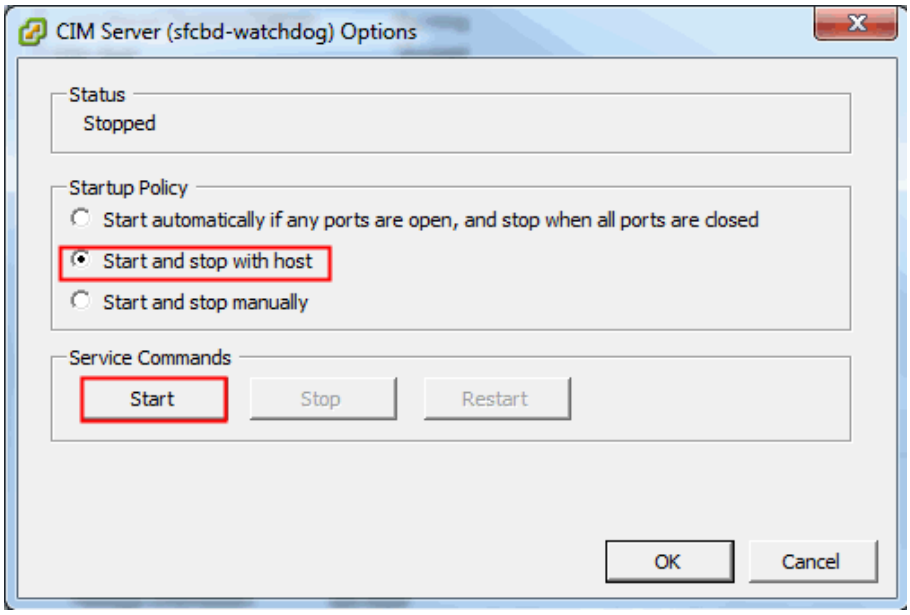
- Inicie el Cliente de VMware vSphere.
- Pulse en la IP de servidor ESXi en la ventana de navegación de la izquierda y seleccione la pestaña **Configuración** en el panel derecho.
- Seleccione **Perfil de seguridad** en el menú de selección **Software** en el panel derecho. Se mostrará un conjunto de servicios, incluyendo **Servidor CIM** en la sección **Servicios**.



- Seleccione el elemento **Propiedades...** en la sección **Servicios** .



- Si el **servidor CIM** está en estado **Detenido**, selecciónelo y pulse **Opciones...**. Se visualizará la siguiente ventana de diálogo.



- Seleccione la **Política de inicio (Opción Iniciar y detener con host**) y pulse **Iniciar** para activar el servidor CIM.

Apéndice D: Windows con WINRM

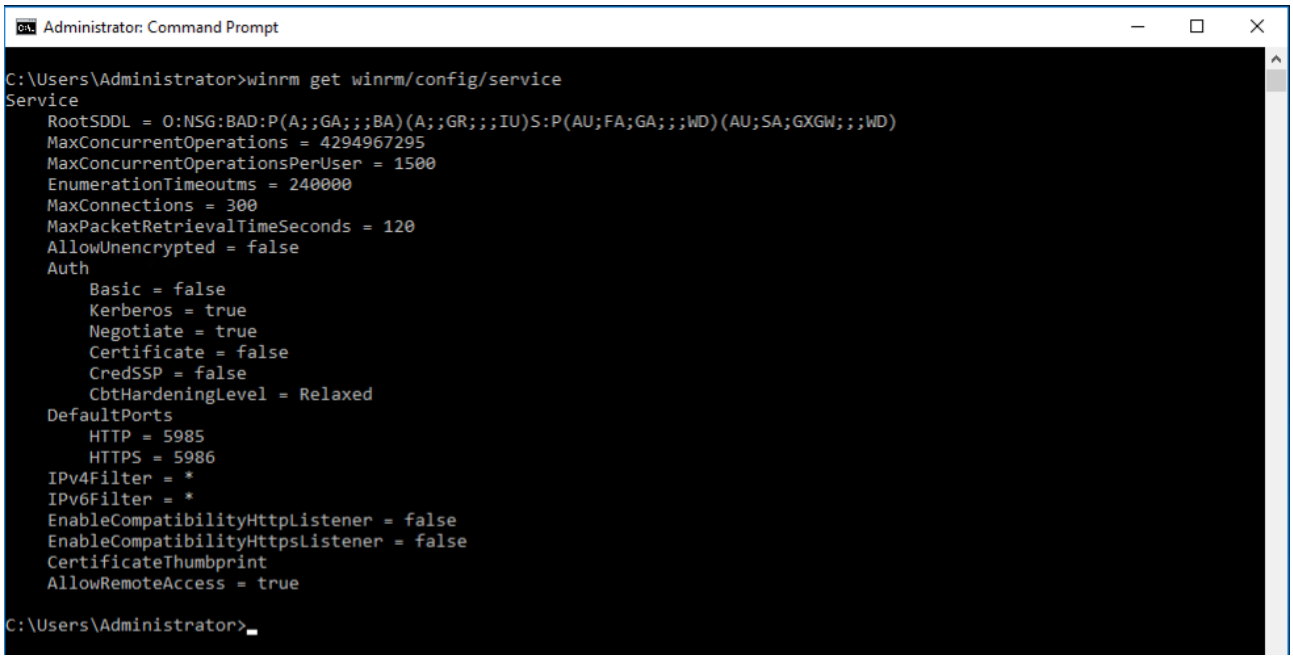
Para un servidor Windows 2012 y 2016, el servicio WINRM se inicia automáticamente. Sin embargo, la gestión remota no está habilitada de forma predeterminada. A continuación, se proporciona un breve resumen de lo que se necesita para habilitar WINRM para permitir una conexión remota utilizando un certificado autofirmado:

- Habilite WINRM para que acepte conexiones HTTPS que se autentiquen con ID de usuario / contraseña
- Asocie un certificado autofirmado al escucha HTTPS para el WINRM que se ha habilitado
- Modifique el cortafuegos de Windows para que permita conexiones entrantes a través del puerto 5986 (el puerto default HTTPS predeterminado para WINRM)

Los siguientes mandatos preparan WINRM para que permita conexiones remotas por HTTPS:

- Determine el estado actual del servicio WINRM con este mandato:

  winrm get winrm/config/service



- El valor de **AllowUnencrypted** debe ser *false*. Si es *true*, utilice el mandato siguiente para cambiarlo a *false*:

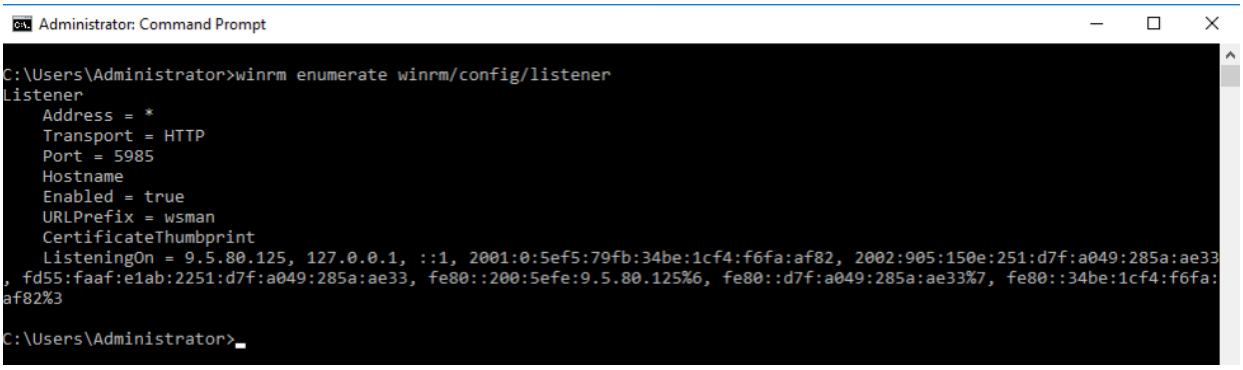
  winrm set winrm/config/service @{AllowUnencrypted="false"}

- El valor de **Basic** debe ser *true*. Si es *false*, utilice el mandato siguiente para cambiarlo a *true*:

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

- Determine si WINRM tiene un escucha HTTPS utilizando este mandato:

  winrm enumerate winrm/config/listener



- En el ejemplo de mandato anterior, solo hay un escucha HTTP, por lo que es necesario configurar un escucha de HTTPS. Para habilitar la escucha HTTPS si no está configurado:
  - Utilizando PowerShell, cree un certificado autofirmado:

    New-SelfSignedCertificate -DnsName "myHost@myBusiness.com" -CertStoreLocation Cert:\LocalMachine\My

    > Sustituya el DnsName **(myHost@myBusiness.com)** del ejemplo anterior por el nombre de dominio de Windows completo del servidor Windows.

  - Guarde el certificado de huella para el paso siguiente

- Cree el escucha de HTTPS:

  winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="myHost@myBusiness.com"; CertificateThumbprint="[COPIED_CERTIFICATE_THUMBPRINT]"}

- Asegúrese de que HTTPS está configurado con:
  winrm enumerate winrm/config/listener
- Modifique el cortafuegos de Windows para permitir conexiones remotas entrantes a WINRM:
  - Vaya a **Panel de control → Sistema y seguridad → Firewall de Windows**
  - Pulse **Configuración avanzada.** Se visualiza la ventana **Firewall de Windows con seguridad avanzada**.
  - Pulse **Reglas de entrada**.
  - Seleccione el menú **Acciones** y pulse en **Nueva regla**. Se visualiza el **Asistente para nueva regla de entrada.**
  - Seleccione **Puerto** y pulse **Siguiente.**
  - Seleccione **TCP → Puertos locales específico** y especifique 5986. Pulse **Siguiente.**
  - Seleccione la opción **Permitir la conexión** y pulse **Siguiente.**
  - Marque los recuadros de selección **Dominio**, **Privado** y **Público** si no están ya marcados y pulse **Siguiente.**
  - Asigne un nombre a la nueva regla (como por ejemplo Administración remota de Windows (HTTPS entrante) y pulse **Finalizar**

Avisos

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
Producido en los Estados Unidos de América
Agosto de 2020.

Este documento se ha desarrollado para productos y/o servicios ofrecidos en los Estados Unidos. Es posible que IBM no ofrezca los productos, características o servicios descritos en este documento en otros países.

La información puede verse sujeta a cambios sin previo aviso. Consulte a su contacto profesional local de IBM para obtener información sobre los productos, características y servicios disponibles en su zona.

Todas las afirmaciones respecto a direcciones e intenciones futuras de IBM están sujetas a cambios o a su retirada sin previo aviso y representan únicamente metas y objetivos.

IBM, el logotipo de IBM, POWER, System I, System p, i5/OS son marcas comerciales o marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países. Puede encontrar una lista completa de las marcas registradas en EE.UU. propiedad de IBM en http://www.ibm.com/legal/copytrade.shtml.

Otros nombres de compañías, productos y servicios pueden ser marcas registradas o marcas de servicio de terceros.

Los productos de hardware de IBM están fabricados a partir de componentes nuevos o bien a partir de componentes nuevos y reutilizados. En cualquier caso, se aplican nuestros términos de garantía.

Este equipamiento está sujeto a las reglas de la FCC. Cumplirá las reglas apropiadas de la FCC antes de su entrega final al comprador.

La información sobre productos que no son de IBM se ha obtenido de los proveedores de estos productos.

Las preguntas sobre las prestaciones de estos productos no IBM se deben dirigir a sus proveedores.

La página de inicio de IBM en Internet se encuentra en http://www.ibm.com.

La página de inicio de IBM System p en Internet se encuentra en http://www.ibm.com/systems/p.

La página de inicio de IBM System I en Internet se encuentra en http://www.ibm.com/systems/i.

PSW03007-USEN-00